



**ВОРОНЕЖСКИЙ ИНСТИТУТ
МВД РОССИИ**

**ОБЩЕСТВЕННАЯ БЕЗОПАСНОСТЬ,
ЗАКОННОСТЬ И ПРАВОПОРЯДОК
В III ТЫСЯЧЕЛЕТИИ**

Сборник статей

Выпуск 5

Часть 2

Воронеж

2019

Воронежский институт МВД России

**ОБЩЕСТВЕННАЯ БЕЗОПАСНОСТЬ, ЗАКОННОСТЬ
И ПРАВОПОРЯДОК В III ТЫСЯЧЕЛЕТИИ**

Сборник статей

Выпуск 5

Часть 2

Воронеж - 2019

ББК 67.99(2)
О-28

Редакционная коллегия:

Председатель: *О.И. Бокова, доктор технических наук, профессор*

Заместитель председателя: *Е.А. Пидусов, кандидат юридических наук, доцент*

Члены редакционной коллегии:

А.Н. Глушков, кандидат технических наук, доцент;

И.С. Завьялова, кандидат юридических наук,

С.А. Звягин, доктор экономических наук, доцент;

А.В. Кирнос, кандидат политических наук, доцент;

О.И. Копытина, кандидат педагогических наук;

И.А. Кравцов, кандидат юридических наук, доцент;

Т.В. Мецеракова, кандидат физико-математических наук;

О.И. Нестеровский, кандидат технических наук, доцент;

Н.В. Полякова, кандидат юридических наук, доцент;

А.Г. Прокопов, кандидат юридических наук;

Н.М. Савицкий, кандидат исторических наук

О-28 **Общественная безопасность, законность и правопорядок в III тысячелетии : сборник статей. Вып. 5. – Часть 2. – Воронеж : Воронежский институт МВД России, 2019. – 351 с.**

ISBN 978-5-88591-738-4

ISBN 978-5-88591-740-7

В ежегодном сборнике содержатся статьи, подготовленные по результатам Международной научно-практической конференции «Общественная безопасность, законность и правопорядок в III тысячелетии» (27 июня 2019 года). Издание предназначено для профессорско-преподавательского состава, курсантов, слушателей образовательных организаций МВД России, студентов, адъюнктов, аспирантов, сотрудников правоохранительных органов.

О $\frac{2404010000 - 31}{221 - 19}$ 58 (II) - 19

67.99(2)

ISBN 978-5-88591-738-4

ISBN 978-5-88591-740-7 Воронежский институт МВД России, 2019

СОДЕРЖАНИЕ

ГРАЖДАНСКО-ПРАВОВЫЕ И ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

Азарова И.В. Особенности гражданско-правовой ответственности за экологические правонарушения	7
Бузин Р.В., Ильченко Л.К. Формирование инвестиционного механизма в интересах обеспечения экономической безопасности государства	12
Воронцова Н.А. Безопасность потребителей в Евразийском экономическом союзе	18
Гаврилова Н.А. К вопросу о надлежащем способе защиты права по спорам, связанным с границами земельного участка.....	21
Жаглин А.В., Коробейникова Л.С. ТОС как форма самоорганизации граждан: отдельные проблемы функционирования.....	26
Жаглина М.Е. Страхование сотрудников органов внутренних дел: вопросы правоприменения	31
Звягин С.А. Подложная бухгалтерская документация в системе доказательств противоправных экономических действий.....	37
Климова И.А. Некоторые таможенные аспекты упрощения процедур торговли по соглашению USMCA и ТКЕАЭС	41
Коробов Г.А. Справедливость и право.....	45
Коробов Г.А., Азарова И.В. Теоретико-правовой аспект уголовной ответственности за экологические преступления	49
Мазина Г.П. Юридическая ответственность за нарушение экологического законодательства: понятие, виды, проблемы обоснования	53
Мальцев Е.П. Эксперт-бухгалтер как субъект бухгалтерской экспертизы: особенности определения организационно-правового статуса.....	58
Матвеев С.П. Правовой статус сотрудников органов внутренних дел	63
Мещерякова Е.И. Методологические подходы к экономико-правовому анализу преступлений в сфере бюджетной деятельности	68
Стрыгина И.Е. Неформатная бухгалтерская документация и ее экспертиза.....	72
Фоменко Т.Н. Бухгалтерская экспертиза в системе бюджетных отношений.....	76
Хауия Саулет. Понятие и виды поручительства	80

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ, ЖИВУЧЕСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ И СВЯЗИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Авсентьев О.С., Рубцова И.О. Описательные модели защиты информации в системах электронного документооборота специального назначения	87
Асанов А.С., Ивануткин А.Г. Интеграция систем военной связи в единое информационное пространство	93
Бондарь К.М., Дунин В.С. Направления развития потенциала кадрового обеспечения в сфере подготовки специалистов информационной безопасности для территориальных подразделений МВД России	97
Безрядин В.А., Хворов Р.А. Основные направления повышения оперативности радиоконтроля в Военно-воздушных силах	101
Бредихина Е.В., Дмитриев С.А. Анализ антенных систем для комплекса широкополосной радиосвязи	106
Василевский А.А., Стафеев М.А. Методика оценки качества системы радиотехнического обеспечения полетов авиационной базы.....	110

Галуза М.А., Климов А.И., Кузнецов А.В. Методика проектирования полосковой антенны вытекающей волны с низким уровнем бокового излучения	115
Гилев И.В., Канавин С.В. Типовая модель функционирования системы радиосвязи специального назначения в условиях информационного конфликта	120
Головченко Е.В., Афанасьев А.Д., Баев К.С. Модель системы управления авиационного формирования	123
Данилов Р.М., Рыбак А.В. Глобализация вычислительных сетей в России	129
Дмитриев С.А., Бредихина Е.В. Специальный комплекс широкополосной радиосвязи	133
Жайворонок Д.А. Программные продукты обеспечения безопасности виртуальных частных сетей	136
Жуков М.М., Удалов В.П. Построение матрицы чувствительности рисков для компонент распределенной технической системы, ущерба в которых имеют распределение Парето	138
Зарубин С.В., Перминов Г.В. Некоторые аспекты оптимизации настроек компонента планирования защищенной сети Vipnet administrator	141
Зверев Г.И. К вопросу об описании структурно-параметрической модели эргатических систем	145
Истомин С.А., Коратаев П.Д., Пакляченко М.Ю. Точностные характеристики аппаратуры глобальных навигационных спутниковых систем	147
Кобзистый С.Ю. Актуальные вопросы инженерно-технического обеспечения учреждений и органов уголовно-исполнительной системы	151
Колтаков Е.В., Стафеев М.А. Методика оценки управляемости системы связи и радиотехнического обеспечения авиационного объединения	156
Костин С.В., Мишин Д.С., Сотников А.А. Перспективы применения нейронной сети Хопфилда в биометрической идентификации	158
Меньших Т.В. Анализ особенностей процессов принятия решений в системах управления специального назначения при возникновении чрезвычайных обстоятельств	164
Мишин Д.С., Еременко В.Т., Паньков С.Л. Актуальные проблемы внедрения облачных технологий в деятельность правоохранительных органов	167
Оболонская А.В. Особенности построения демодуляторов сигналов с фазоразностной манипуляцией	172
Перминов Г.В., Зарубин С.В. Анализ актуальности проблемы пассивного перехвата трафика в современных компьютерных сетях	176
Печников С.С. Увеличение времени работы средств радиосвязи, стоящих на вооружении в органах внутренних дел	180
Рыбак А.В. Вопросы кадрового обеспечения территориальных органов МВД России	185
Рыбокитов А.Е. Риск-модели нарушения информационной безопасности в мобильных самоорганизующихся сетях связи	189
Спешилов Э.В. К вопросу о цифровых системах фазовой автоподстройки (PLL)	192
Терентьев А.А., Пьянков О.В. Визуализация результатов обработки экспертных оценок по степени предпочтения объектов	195
Удалов В.П., Жуков М.М. Особенности экспертного оценивания параметров надежности системы безопасности объекта информатизации	200
Хворов Р.А., Безрядин В.А. Формирование теоретической основы методики выявления временного резерва автоматизированной системы радиоконтроля	203
Шерстюков С.А., Печников С.С. Проблемы технического сопряжения стандартов систем радиосвязи в предмодуляционном и усилительном трактах	207
Шугай О.Е., Орлова Д.Е. Математическая модель оценки рисков при выборе направления развития предприятия уголовно-исполнительной системы	212

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Абросимова Е.М., Иванченко О.С. Показатели защищенности и эффективности реализации информационных процессов в системах безопасности ОВД.....	215
Бороненков А.И., Саваровский А.Б. Информационное противодействие современному терроризму как способ борьбы с его проявлениями.....	218
Герасименко Е.С. Разработка систем контроля доступа охраняемого объекта.....	222
Голиков А.А., Толстых О.В. Некоторые аспекты безопасности дорожного движения в России и мире	225
Данилова О.Ю., Попов А.В. К вопросу об использовании полиномиальных кодов при передаче сообщений в подразделениях органов внутренних дел.....	229
Дровникова И.Г., Арутюнова В.И., Алфёров В.П. Аналитическая модель оценки эффективности функционирования подсистемы защиты конфиденциальных сведений при реализации слабо уязвимого разграничения доступа к информационному ресурсу систем электронного документооборота	234
Дровникова И.Г., Алфёров В.П. Алгоритмизация оценки показателя эффективности функционирования подсистемы защиты конфиденциальных сведений системы электронного документооборота	240
Дровникова И.Г., Етепнев А.С. К вопросу оценки надёжности системы защиты информации автоматизированной системы	245
Жилин Р.А., Шпак А.В. Проблема квалификации преступлений против объектов критической информационной инфраструктуры.....	248
Жилин Р.А., Саркисов В.Г. Анализ результатов вычислительного эксперимента по формированию однородных групп нарушителей охраны объектов критической информационной инфраструктуры.....	253
Жилин Р.А. Категориальная иерархия нарушителей объектов критической информационной инфраструктуры	257
Зверева Д.Д. Обоснование необходимости оптимизации процессов модернизации инфокоммуникационных сетей.....	261
Калков Д.Ю., Гудков М.А. К вопросу проектирования систем охранных телевизионных с учетом обеспечения их собственной безопасности	264
Конобеевских В.В. Визуально-аналитическая деятельность при работе с данными из социальных сетей	267
Кузнецова Н.Н. К вопросу специфики начального этапа проектирования систем оповещения.....	270
Лунёв Ю.С., Амирханян В.Г. Программный комплекс сопряжения микроконтроллера с ЭВМ для контроля безопасности объекта информатизации.....	274
Мещерякова Т.В., Фирюлин М.Е., Родионов Е.А. Функциональная модель сервиса обеспечения деятельности дежурных частей в ИСОД МВД России.....	277
Мишин С.А., Солодуха Р.А. Разработка концептуальной модели системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел	282
Мишин А.В., Мишин С.А. Принципы проверки согласованности экспертных мнений	287
Мишин С.А., Солодуха Р.А. Организация и ведение базы данных системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел	292
Никулина Е.Ю. Проблемы и пути решения задачи перехода на использование отечественного программного обеспечения.....	297

Обухова Л.А. Тенденции развития киберпреступности в сфере информационных технологий на территории России.....	300
Попов А.Д. Использование программной среды имитационного моделирования с целью разработки модели системы защиты информации от несанкционированного доступа в автоматизированных системах ОВД.....	304
Рогозин Е.А., Каднова А.М. К вопросу о решении научной задачи количественной оценки эрготехнических характеристик систем защиты информации от несанкционированного доступа в автоматизированных системах ОВД	307
Рогозин Е.А., Каднова А.М., Фирюлин М.Е. Классификация и анализ существующих угроз несанкционированного доступа в автоматизированных системах ОВД.....	310
Самороковский А.Ф., Горлов В.В. Модель управления территориальными органами МВД России на начальном этапе массовых беспорядков.....	314
Самороковский А.Ф., Толстых А.А. Анализ применимости искусственных нейронных сетей к задаче выделения топографической информации с печатных носителей.....	319
Сафонова Н.Л. Анализ разработки моделей надежности программного обеспечения в авиации.....	323
Сидоров А.В., Гречаный С.А., Романов М.С. Перспективные инструменты для серверной части WEB-приложений при разработке автоматизированных информационных систем.....	327
Синегубова С.В., Синегубов С.В. Модель сегмента мобильной связи.....	333
Сошнева Д.А., Ахлюстин С.Б. Особенности организации взаимодействия войск национальной гвардии с Министерством внутренних дел Российской Федерации при выполнении задач по охране общественного порядка и обеспечения общественной безопасности	337
Спиридонова Н.Е. Анализ существующих подходов к количественной оценке интероперабельности систем	341
Таравков М.В. Вопросы правового регулирования применения систем видеонаблюдения	343
Толстых А.А., Ступников Д.С. Обучение с подкреплением в задачах управления робототехнических систем	347

ГРАЖДАНСКО-ПРАВОВЫЕ И ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

Азарова Ирина Владимировна

ОСОБЕННОСТИ ГРАЖДАНСКО-ПРАВОВОЙ ОТВЕТСТВЕННОСТИ ЗА ЭКОЛОГИЧЕСКИЕ ПРАВОНАРУШЕНИЯ

FEATURES OF CIVIL LIABILITY FOR ENVIRONMENTAL OFFENSES

Данная статья посвящена рассмотрению особенностей наступления гражданско-правовой ответственности за экологические правонарушения, разрешения вопросов возмещения экологического вреда.

This article is devoted to consideration of features of approach of civil liability for ecological offenses, the resolution of questions of compensation of ecological harm.

Право граждан на благоприятную окружающую среду, достоверную информацию о ее состоянии и на возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением, гарантировано Конституцией РФ и закреплено в статье 42 [1].

Юридическая ответственность за экологические правонарушения заключается в неблагоприятных последствиях, наступающих для нарушителя экологических требований и складывается из правоотношений между государством в лице специально уполномоченных органов в области охраны окружающей среды, правоохранительных органов, иных уполномоченных субъектов и должностными, физическими или юридическими органами, которые совершили правонарушение в области охраны окружающей среды по поводу применения к ним мер воздействия и принуждения.

В настоящий момент в рамках российского законодательства к юридической ответственности за экологические правонарушения могут быть привлечены лица, достигшие 16 лет. В свою очередь гражданское законодательство говорит об ограниченной ответственности, которая начинается с 14 и до 18 лет, а по наступлению совершеннолетия – полную.

Гражданско-правовая ответственность за экологические правонарушения является имущественной ответственностью физических и юридических лиц, устанавливаемой нормами экологического и гражданского законодательства. Основными нормативными правовыми актами, регулируемыми указанные отношения, являются:

1. Конституция РФ.
2. Закон «Об охране окружающей среды» от 10.01.2002 № 7-ФЗ [2].
3. Гражданский кодекс РФ[3] (далее- ГК РФ).
4. Гражданско-процессуальный кодекс РФ[4] (далее - ГПК РФ).
5. Земельный кодекс РФ[5].
6. Водный кодекс РФ[6].
7. Лесной кодекс РФ[7] (и другие отраслевые законы).

Отметим тот факт, что в настоящее время в российском законодательстве не существует единого кодифицированного законодательства в области охраны окружающей среды. Однако, основой, фундаментом, любого права должен стать в соответствии с иерархией источников права кодифицированный нормативный акт, подчиняющий себе федеральные законы относительно этого права. Так, в соответствии с действующим

законодательством, если закон противоречит кодексу, которому он подчиняется, то данный закон необходимо признать недействительным в части выявленных противоречий. Таким образом, в нашей стране создалась опасная ситуация, когда теоретически можно принять противоречащие друг другу законы, и они будут действительны, потому что основные принципы, заложенные в них, сравнить не с чем. На наш взгляд, это связано с тем, что природные объекты имеют особый правовой режим, который определяется нормами различной отраслевой принадлежности. Но несмотря на это в действующем российском законодательстве необходимо создание Экологического кодекса.

Гражданское законодательство регулирует наступление ответственности за совершение гражданско-правовых экологических деликтов, в том числе причиняемых источником повышенной опасности (без виновная или абсолютная ответственность). Другими словами ответственность за совершение правонарушения в данном случае будет наступать без вины в соответствии с статьей 1079 ГК РФ.

Суть гражданско-правовой ответственности состоит в отличие от уголовной и административной в том, чтобы восстановить потерпевшей стороне прежнее положение путем возмещения имущественного или морального вреда, который был причинен в результате нарушения установленных законом экологических предписаний. Еще одной ее отличительной чертой является то, что она может возлагаться на правонарушителя наряду с применением мер дисциплинарного, административного и уголовного воздействия, то есть в совокупности.

Таким образом, основанием применения гражданско-правовой ответственности является противоправное деяние, которым причиняется вред окружающей среде и здоровью человека. Такими гражданско-правовыми деликтами могут быть: загрязнение; истощение; порча; уничтожение; нерациональное использование природных ресурсов; деградация; разрушение естественных экологических систем, природных комплексов и природных ландшафтов.

Экологическое правонарушение причиняет вред, под которым понимается реальный ущерб и упущенная выгода. Реальным ущербом в экологической сфере может быть, например, уменьшение лесного массива, снижение плодородия почвы и увеличение расходов на восстановление, а упущенная выгода может заключаться, например, в неполученных доходах, от хозяйственного использования той почвы, плодородие которой снизилось[8]. Возмещение указанного вреда конкретизируется нормами гражданского законодательства (ст. 1064 ГК РФ).

Так, Калининский районный суд города Уфы Республики Башкортостан рассмотрев в открытом судебном заседании гражданское дело по иску Управления коммунального хозяйства и благоустройства Администрации городского округа город Уфа Республики Башкортостан к индивидуальному предпринимателю Теплову А. А., Филатову М. А. о взыскании ущерба, причиненного городским лесам решил удовлетворить[9].

Отметим, что различные категории гражданско-правовой ответственности даются в юридической литературе. Так, М.М. Бринчук считает, что «гражданско-правовая ответственность за экологические правонарушения состоит в возложении на правонарушителя обязанности возместить потерпевшей стороне (другому лицу или государству) имущественный, материальный или моральный вред, причиненный в результате несоблюдения правовых экологических предписаний, установленных законодательством российской федерации» [10].

Однако, на наш взгляд, М.М. Бринчук относится к тем авторам, которые являются сторонниками концепции самостоятельной эколого-правовой ответственности, которая, по его мнению, применяется во всех случаях причинения вреда природным

объектам, которые в большой степени принадлежат на праве собственности Российской Федерации или ее субъектам и являются ее достоянием.

Обратим внимание на мнение А. П. Анисимова, который достаточно справедливо рассуждает о том, что представленная нами выше изложенная позиция является не однозначной, так как «экологическая ответственность» представляет собой частный случай специальных деликтов, которые не указаны в ГК РФ [11].

Также отметим, что в практике судебных органов при рассмотрении вопросов природопользования и охраны окружающей среды эколого-правовой вид ответственности до настоящего времени не получил широкого распространения. В этих целях судами применяются общие положения гражданского права об обязательствах, возникающих из причинения вреда.

Несомненно, юридическая ответственность за экологические правонарушения имеет ряд определённых качеств. По мнению С.А. Боголюбова основными чертами гражданско-правовой ответственности за экологические правонарушения являются:

- причинение имущественного вреда охраняемым экологическим объектам выступает основанием;
- гражданское законодательство является формой выражения и закрепления данной ответственности;
- физические лица, должностные лица и юридические лица, а также суды выступают субъектами правовых отношений;
- ответственность налагается в процессуальном порядке (гражданско-процессуальном и арбитражно-процессуальном);
- последствиями экологического деликта является санкция, налагаемая на нарушителя;
- суды общей юрисдикции наделены действительными полномочиями по определению и назначению гражданско-правовой ответственности[12].

Следует подчеркнуть важную особенность гражданско-правовой ответственности за ущерб, причиненный окружающей природной среде, возмещение вреда включает компенсацию как реального ущерба, так и будущих расходов[13]. Поэтому важным является установление не только самого факта противоправного поведения, но и факта причинения вреда и его размера. Установление данных фактов являлся сложно доказуемой категорией, что приводит к малому количеству удовлетворенных исков[14].

На наш взгляд, современное состояние окружающей среды и другие важные экологические проблемы, обусловленные в первую очередь потребительским, безответственным отношением к природе, которые свидетельствуют о надвигающейся экологической катастрофе. В настоящий момент данная проблема приобретает мировые масштабы. Однако, государство уже предпринимает множество усилий, направленных на улучшение экологической обстановки в стране. Так, 2017 год в нашей стране был объявлен годом экологии.

Отметим, что экологические правонарушения и преступления не являются редкостью, однако статистика указывает на то, что предусмотренные меры уголовной и материальной ответственности не являются эффективными. Так по данным Судебного Департамента РФ в 2018 году за экологические преступления было осуждено 7702 лиц, что составляет менее 1% от общего количества осужденных лиц. А по гражданским делам рассмотрено в судах общей юрисдикции дел о возмещении ущерба за нарушение природоохранного законодательства в 2018 году 3524, что составляет 0,02% от общего количества гражданских дел, рассмотренных в судах[15].

По нашему мнению, это связано с многими причинами, к которым относятся и недостатки статистического учета, которые отражают не все многообразие экологической преступности и правонарушений, а также высокая степень латентности экологической преступности, по оценкам отдельных исследователей, достигающие 90-95 %

[16], а также недостатки законодательного характера и проблемы правоприменения.

Предполагается, что обобщение норм двух самостоятельных отраслей права, а именно гражданского и экологического, является необходимой задачей законодателя. Опираясь на мнение Е.С. Болтанова [17] «для построения общей концепции возмещения экологического вреда нельзя обойтись без изложенных в главе 59 ГК РФ устоявшихся, апробированных временем гражданско-правовых конструкций. Разрешение вопросов возмещения экологического вреда являются отправными как для законодателя, так и для правоприменителя, при этом учитывается правило общего характера – цивилистические положения.

Итак, комплексный характер сложных отношений, складывающихся в сфере взаимодействия общества и природы, требует и комплексного подхода в их регулировании нормами как экологического, так и гражданского права. Цивилистические подходы при решении вопросов возмещения экологического вреда являются приоритетными как для законодателя, так и для правоприменителя.

ЛИТЕРАТУРА

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собр. законодательства Рос. Федерации. - 2014. – № 31. – Ст. 4398.
2. Об охране окружающей среды: федер. закон от 10.01.2002 № 7-ФЗ (ред. от 29.07.2018) // Собр. законодательства Рос. Федерации. - 2002. – № 2. – Ст. 133.
3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 03.08.2018) (с изм. и доп., вступ. в силу с 01.06.2019) // Собр. законодательства Рос. Федерации. - 1994. – № 32. – Ст. 3301.
4. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 28.12.2018) // Собр. законодательства Рос. Федерации. - 2002. – № 46. – Ст. 4532.
5. Земельный кодекс Российской Федерации от 25.10.2001 № 136-ФЗ (ред. от 25.12.2018) (с изм. и доп., вступ. в силу с 01.06.2019) // Собр. законодательства Рос. Федерации. – 2001. – № 44. – Ст. 4147.
6. Водный кодекс Российской Федерации от 03.06.2006 № 74-ФЗ (ред. от 27.12.2018) // Собр. законодательства Рос. Федерации. – 2006. – № 23. – Ст. 2381.
7. Лесной кодекс Российской Федерации от 04.12.2006 № 200-ФЗ (ред. от 18.12.2018) // Собр. законодательства Рос. Федерации. – 2006. – № 50. – Ст. 5278.
8. Безопасность жизнедеятельности: учеб. пособие для вузов / Под ред. проф. Л.А. Муравья. – 2-е изд., перераб. и доп. – М. : ЮНИТИ-ДАНА, 2017. – С.210.
9. Решение № 2-6021/2017 2-6021/2017~М-5010/2017 М-5010/2017 от 27 декабря 2017 г. по делу № 2-6021/2017–[Электронный ресурс]. - URL : https://sudact.ru/regular/doc/6T7tveJBIU5N/?regular-txt=экологическое+правонарушение&regular-case_doc=&regular-lawchunkinfo=Статья+1079.+Ответственность+за+вред%2C+причиненный+деятельностью%2C+создающей+повышенную+опасность+для+окружающих%28ГК+РФ%29&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1569654822151&snippet_pos=3080#snippet(дата обращения: 15.05.2019).
10. Бринчук М. М. Экологическое право: учебник. – 2-е изд. – М.: Вентанаграф, 2014. – С. 376.

11. Анисимов А.П., Чаркин С.А. Эколого-правовая ответственность за экологические правонарушения: дискуссионные вопросы // Материалы Всероссийской научно-практической конференции, Международной научно-практической конференции преподавателей, практических сотрудников, студентов, магистрантов, аспирантов, соискателей. Сборник научных статей. – Саратов, Саратовский источник. – 2016. – С.13-16.
12. Боголюбов С.А. Экологическое право: учебник – 2-е изд. - М.: Юрайт, 2011. – С. 297.
13. Скобина Е.А., Слепченко К.А. Особенности гражданско-правовой ответственности за экологические правонарушения // Молодой ученый. – 2017. – №49. – С. 271-275. – URL <https://moluch.ru/archive/183/46934/> (дата обращения: 28.06.2019).
14. Ивановская Н. В. Особенности оснований гражданско-правовой ответственности за причинение экологического вреда // Вестник РУДН. Серия: Юридические науки. – 2008. – № 3. – URL: <http://cyberle.Nei.Neka.ru/article/№/osobe.Ne.Nosti-os.Nova.Nei-y-grazhdan.Nsko-pravovoy-otvetstve.Ne.Nosti-za-prichi.Ne.Nie-ekologicheskogo-vreda> (дата обращения: 28.06.2019).
15. Сайт Министерства внутренних дел Российской Федерации. Состояние преступности в России за 2018 год [Электронный ресурс]. – URL: <https://мвд.рф/Deljatel.Nost/statistics> (дата обращения: 29.06.19).
16. Дворецкий М.Ю., Краснослободцева Н.В. Уголовно-правовые проблемы эффективности применения норм об ответственности за экологические преступления // Вестник Тамбовского университета. – 2016. – №3. – С.58.
17. Болтанова Е.С. Возмещение экологического вреда: соотношение норм экологического и гражданского законодательства // Имущественные отношения в Российской Федерации. 2017. – № 8. – С. 11.

СВЕДЕНИЯ ОБ АВТОРЕ

Азарова Ирина Владимировна. Старший преподаватель кафедры гражданско-правовых и экономических дисциплин.

Воронежский институт МВД России.

E-mail: aziravlad@rambler.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-53-68.

Azarov Irina Vladimirovna – senior lecturer of the Department of civil law and economic disciplines.

Voronezh Institute of MIA of Russian.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-53-68.

Ключевые слова: экологическое правонарушение, гражданско-правовая ответственность, возмещение вреда, реальный ущерб, упущенная выгода.

Key words: environmental offense, civil liability, compensation for damage, real damage, lost profits.

УДК 349.6

Бужин Роман Владимирович,
кандидат экономических наук;
Ильченко Лариса Константиновна

**ФОРМИРОВАНИЕ ИНВЕСТИЦИОННОГО МЕХАНИЗМА
В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ
ГОСУДАРСТВА**

**FORMATION OF THE INVESTMENT MECHANISM
IN THE INTERESTS OF ENSURING THE ECONOMIC
SECURITY OF THE STATE**

Важнейшим национальным приоритетом государства является обеспечение его экономической безопасности, в том числе посредством формирования благоприятного инвестиционного климата. Неотъемлемой составляющей в реализации этого процесса выступает создание эффективного инвестиционного механизма, сущность которого с позиции экономической безопасности государства рассматривается в настоящей статье.

The most important national priority of the state is to ensure its economic security, including through the formation of a favorable investment climate. An integral component in the implementation of this process is the creation of an effective investment mechanism, the essence of which is considered in this article from the standpoint of the economic security of the state.

Механизмы в экономическом понимании представляют собой недостаточно исследованную проблему. Упрощенно, механизм – это совокупность явлений и процессов, протекание которых подчинено определенным логическим правилам. Полагаем, что механизм, в частности инвестиционный, следует понимать, как структурированную систему процессов, событий и явлений, подчиняющуюся определенным законам и направленную на достижение конкретных целей. Объективно экономические механизмы оказывают значительное влияние, а иногда и определяют безопасность экономических субъектов. Состояние, меры и возможности обеспечения, прежде всего экономической безопасности, напрямую зависят от развитости и направленности экономических механизмов. На макроуровне особое место занимает инвестиционный механизм, определяющий все фазы воспроизводственного процесса.

Наиболее часто инвестиционный механизм рассматривают как совокупность целей, принципов и методов аккумуляирования и вложения инвестиционных ресурсов, а также инструментов и способов воздействия на инвестиционный процесс для минимизации рисков и формирования положительного инвестиционного эффекта. При этом ученые, изучающие инвестиционный механизм, как правило, выделяют несколько подсистем (внутренних механизмов) входящих в него.

Правовая подсистема, т.е. совокупность законодательных и правоприменительных нормативных локальных документов, регулирующих и регламентирующих инвестиционные процессы в государстве.

Организационная подсистема – представляет собой структуры, снабжающие предпочтение субъектов и объектов инвестирования, контроль инвестиционных вкладов, аккомпанемент движения инвестиционных ресурсов, формирования финансовых потоков, разбора финансового состояния, оценку и реализацию границ по достаточности эффективности и устойчивости инвестиционной деятельности.

Ресурсная подсистема предполагает анализ возможных источников получения инвестиционных ресурсов. При всем многообразии источников финансирования различают три важнейшие группы инвестиционных ресурсов: собственные средства экономических субъектов (уставный капитал, нераспределенная прибыль, амортизационные отчисления и т.п.); заёмные средства (долгосрочные и краткосрочные кредиты банков и т.п.); привлеченные средства (средства бюджетов разных уровней, внебюджетные фонды и т.п.).

Иногда выделяют и психоэмоциональную подсистему, т.е. те аргументы для деятельности и экономические ожидания, которыми руководствуются вероятные инвесторы при определении объектов вложения ресурсов. Эта составляющая обеспечивает взаимодействие абстрактного инвестиционного механизма с наружной по отношению к нему экономической и общественной средой.

Кроме того, инвестиционный механизм обязан рассматриваться в отчетливой привязке к другим инвестиционным процессам, прежде всего, инвестициям как элементу. Это означает, что в инвестиционном механизме действуют те же взгляды на объект, субъект, содержание, специфики и безопасности тех или иных процессов.

Специфика механизма инвестиционных процессов определяется особенностями процесса воспроизводства и ведения инновационной и инвестиционной деятельности в определенных экономических условиях. Исследование сущности инвестиционных механизмов важно как в теоретической парадигме, так и умозрительной, спекулятивной ситуации.

В целях формирования границ безопасности инвестиционного механизма необходимо определить: как толковать «инвестиционную деятельность», как практическую дефиницию, каким образом взаимодействуют инвестиционный и иные экономические механизмы и как сопоставляются такие базовые категории, как «инвестирование» и «управление инвестициями». Проблема соотношения инвестиционных и других экономических механизмов определяется механизмами привлечения и размещения ресурсов, которые могут быть как инвестиционными, так и не инвестиционными по сути.

В рамках абстрактного механизма инвестирования с помощью классического инвестирования осуществляется привлечение ресурсов с целью их последующего размещения в воспроизводство основного капитала в той или иной форме. Государство на своем уровне и сами частные вкладчики на микроуровне осуществляют управление инвестиционными процессами. Управление охватывает весь процесс инвестирования и является необходимым условием эффективного осуществления этого процесса. Тем не менее инвестиционный механизм главным своим внешним компонентом представлен таким реально осознаваемым процессом, как инвестирование. А по мере необходимости адаптации инвестиционного механизма к изменяющимся условиям хозяйствования в его структуре и под воздействием субъективных правовых факторов в каждой макросистеме сформировались компоненты управления. Экономическая природа инвестиционного механизма – есть результат обобщения и критического переосмысления накопленного опыта в каждой макроэкономической системе.

Таким образом, содержание инвестиционного механизма определяется, как правило, условиями функционирования субъекта. В этой связи представляется целесообразным выделять классические (естественные) стабилизационные и антикризисные (чрезвычайные) инвестиционные механизмы.

Здесь принципиальное разделение идет по целям функционирования того или иного механизма. В частности, целями инвестиционного механизма могут являться достижение predetermined экономического или общественного эффекта, а в качестве технологической основы инвестирования и управления инвестициями могут быть использованы либо традиционные, либо передовые достижения прогресса на конкретную точку времени, в том числе IT-технологии. В то же время ряд российских экономистов, например, Н.Д. Барковский, Н.И. Валенцева, И.Д. Мамонова, С.В. Штейншлейгер, В.В.

Земсков отождествляют механизм с отдельными экономическими процессами, например, кредитными и пытаются назвать это механизмами. Однако в инвестиционной сфере отличие процессов от механизмов заключается в том, что содержание первого всегда определяется как последовательность действий, этапов, процедур, тогда как объективная, неизменная схема реализации этого процесса может признаваться механизмом.

Стартом инвестиционной деятельности в рыночной экономике неизменно будут: наличие свободного капитала у потенциального инвестора; непреодолимое желание инвестора разместить свободный капитал на имеющихся условиях; наличие доходных, постоянно развивающихся секторов экономики; административный режим, способствующий эффективному размещению и движению капитала в прямом (инвестирование) и обратном (вывоз, обналичивание, конвертация) направлениях.

С позиций экономической безопасности все указанные процессы должны быть подчинены трем целям: стабильности, устойчивости и воспроизводству в рамках макроэкономической системы. Здесь возникает ряд проблем, которые препятствуют синхронизации инвестиционного механизма и механизмов обеспечения экономической безопасности. Прежде всего, это отсутствие механизмов защиты субъектов, реальной ответственности за неисполнение правовых норм и механизма реализации нормативных правовых актов для всех экономических субъектов, прежде всего государства. Подобная ситуация порождает многочисленные «личные» толкования законов, как правило, в пользу надзорных и контролирующих инстанций, порождая многочисленные коррупционные и организационные нарушения, препятствуя обеспечению безопасности населения и государства, в том числе в инвестиционной сфере.

Значительным аспектом правового регулирования обеспечения экономической безопасности являются вопросы юридической ответственности как в совершенном, так и процессуальном виде их реализации. Проблемой остается контроль за объемами теневой экономики, уровнем вовлечения в теневые процессы предпринимателей и государственных чиновников. Правовой нигилизм в большинстве бытовых вопросов порождает не только рост коррупции, но и инвестиционную проблему – вовлечение в инвестиционные процессы доходов, полученных преступным путем. В данном случае теневые средства являются прямыми конкурентами легальным ресурсам, причем в силу подпольности более дешевыми и удобными для использования в «серой» инвестиционной деятельности. О проблемах подобного инвестирования было сказано еще 12 лет назад. Такая инвестиционная деятельность также остается за пределами правового поля, государство ограничено в возможностях влияния на инвестиционные процессы и регулирования инвестиционной безопасности национальной экономики [1].

Другим препятствием правовому обеспечению экономической безопасности в инвестиционной сфере национальной экономики являются запутанный и явно усложненный уголовный процесс, слабое «силовое» обеспечение гражданского и арбитражного процессов, позволяющие затягивать принятие решений по делам, отклонять претензии и обвинения из-за незначительных неточностей в документах, просто игнорировать судебные решения и т.п. Особенно остро этот аспект проявляется в корпоративных спорах, где субъекты обладают значительными материальными и организационными ресурсами и способны внеправовыми методами влиять на судебные и административные решения. Объем выявленных экономических преступлений не падает на протяжении последних 10 лет, несмотря на постоянную декриминализацию властями тех или иных действий злоумышленников в экономической сфере, а рост отдельных форм преступлений в финансовой и кредитной сфере (прежде всего регистрируемых мошенничеств) вырос в 15 раз за тот же период [3].

Роль государства в научно-техническом развитии экономики определяется как мировыми тенденциями, так и особенностями исторического развития страны. Струк-

тура экономики России ориентирована на экспорт продуктов с низкой добавленной стоимостью, но масштаб экспорта позволяет организовать значительные финансовые ресурсы, в том числе государственные, которые могут быть использованы для технического перевооружения производства и развития новых технологий. Главный вопрос – каким путем решить проблему технической отсталости.

Первый вариант – приобретение передовых технологических решений и оборудования у других государств. Такой путь можно назвать «ранее японским или китайским», он дешев с финансовой стороны и краток по времени. При этих позитивах он требует постоянного обновления, следовательно, зависимость от предметов потребления перерастет в зависимость от комплектующих, компьютерных программ, профессиональной наладки, диагностики и модернизации средств производства.

Второй вариант – самостоятельное создание нового оборудования, материалов, технологий и их внедрение в производство. России потребуется значительный объем материальных, трудовых, финансовых ресурсов и длительное время, причем результат не гарантирован, в отличие от первого пути.

Думается, что для России, провозгласившей инновационную направленность экономического развития, необходим третий путь, органично совмещающий два вышеперечисленных варианта. В некоторых сегментах, например, военно-промышленном, энергетическом, которые имеют достаточный инвестиционный потенциал, необходимо сконцентрировать усилия на самостоятельном развитии. В других, наиболее важных с позиций экономической безопасности страны, – строительстве и производстве строительных материалов, сельском хозяйстве, промышленном машиностроении и т.п., необходимо обновлять именно технологии, не стесняясь приобретать наиболее передовые, в том числе и за счет бюджетов всех уровней. Считаем, что для подобных целей должен быть создан специальный государственный фонд, формируемый из налоговых поступлений и, главное, пошлин от импорта готовых товаров подобного направления из-за рубежа.

С другой стороны, в сфере услуг необходимо срочно обновлять основные фонды, для чего необходимо приобретение нового оборудования. Здесь государство может максимально упростить процедуры не только приобретения, но и кредитования и амортизации, если приобретается новое, экологически безопасное и энергетически эффективное оборудование, независимо от страны происхождения, игнорируя политические и репутационные мотивы.

Выбор конкретного варианта участия в инвестиционной деятельности в каждой стране осуществляется государством самостоятельно, с оценкой двух основных факторов. Во-первых, важность проекта для национальной экономики в целом или для экономики региона. Во-вторых, если проект имеет достаточное значение, то насколько проблематичной (рискованной) будет его реализация без участия государства. Современная политическая система не рискует государственными ресурсами. Оценка эффективности проектов предпринимателем и государством разная. Для предпринимателя главное – доход (проценты, дивиденды), для государства – возможное увеличение совокупного продукта (ВВП) или других социально значимых позиций. Поэтому управленческие решения государственного служащего и предпринимателя существенно различны по сути. Упрощенно инвестиционное взаимодействие государства и бизнеса выглядит так: налоги с бизнеса – это субсидии (дотации, льготы по налогам и сборам) от государства. Здесь государство может эффективно регулировать процесс именно через налоговые рычаги двумя способами:

- единое, равное уменьшение налогов при осуществлении инвестиционной деятельности;

- дифференцированный подход, зависящий от выполнения каких-либо условий или соответствия стандартам.

Тем не менее государство является центральным субъектом обеспечения экономической безопасности национальной экономики. Возможности и методы государственного воздействия на экономику, в том числе и переходную, достаточно подробно рассмотрены в отечественной экономической литературе [2].

Для регулирования экономической безопасности страны могут быть использованы все доступные государству методы. Так, управление государственной собственностью, ориентированное на обеспечение экономической безопасности, побуждает инвестиционную активность в смежных отраслях и не дает снизиться в отраслях участия за счет обострения конкурентной борьбы и мультипликационного эффекта. Цель антимонопольного регулирования в формировании и развитии конкурентной среды, которая может достигаться как методом создания государственных предприятий, так и дробления, приватизации и разгосударствления, для достижения целей инвестиционных и безопасности. Более того, процессы слияния и поглощения компаний непосредственно определяются направлением и масштабами инвестиционной деятельности. Исполнение же государственного бюджета является базой для всех перечисленных методов прямого воздействия на экономику и регулятором инвестиционной деятельности в стране в целом.

Значительные ресурсы, аккумулируемые в различных резервных государственных фондах, позволяют российскому правительству проводить активную инвестиционную деятельность, обеспечивая высокий уровень национальной экономической безопасности, однако использование классической, либеральной концепции регулирования экономики значительно ограничивает данное направление. Как известно, главной целью такой политики является поддержание стабильности экономических параметров функционирования. На таких постулатах и строится политика российского правительства в экономике, то есть само государство ограничивает свою способность регулировать экономику только фискальными механизмами.

Считаем, что достичь одновременно инвестиционных целей и обеспечить безопасность национальной экономики России можно сочетанием стимулирования и контроля, что позволит максимально реализовать цели системы обеспечения экономической безопасности, но при этом центральным становится вопрос структуры механизма, способствующего ее обеспечению. Здесь у экономики России будут проблемы до тех пор, пока не будет сформирован эффективный инвестиционный механизм, где вопросы безопасности не будут противопоставляться вопросам экономической эффективности и способствовать не только экономическому росту, но и повышению уровня жизни населения.

ЛИТЕРАТУРА

1. Бузин Р.В. Теневая инвестиционная деятельность как угроза экономической безопасности России / Р.В. Бузин // Политэкономические проблемы современных социально-экономических систем : материалы Международной научно-практической конференции / Под ред. И.Т. Корогодина, В.В. Гаврилова : в 2 ч. – Воронеж : Воронежский государственный университет, 2007. – Ч.2. – С. 15-21.
2. Рисин И.Е. Теория и практика государственного регулирования современной экономики / И.Е. Рисин, Ю.И. Трещевский. – М., 2000.
3. Статистический сборник: преступность и правонарушения (2014-2018). – Москва: ГИАЦ МВД России, 2018. – С. 9, 32-36.

СВЕДЕНИЯ ОБ АВТОРАХ

Бузин Роман Владимирович. Начальник научно-исследовательского отдела. Кандидат экономических наук.

Воронежский институт МВД России.

E-mail: rbuzin@mvd.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-70.

Ильченко Лариса Константиновна. Старший научный сотрудник научно-исследовательского отдела.

Воронежский институт МВД России.

E-mail: lilchenko2@mvd.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-23.

Buzin Roman Vladimirovich. Head of the research department. PhD in Economics.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: rbuzin@mvd.ru

Russia, 394065, Voronezh, 53 Patriot Avenue. Tel. (473) 200-51-70.

Ilchenko Larisa Konstantinovna. Senior Researcher, Research Department.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: lilchenko2@mvd.ru

Russia, 394065, Voronezh, 53 Patriot Avenue. Tel. (473) 200-51-23.

Ключевые слова: экономика; инвестиции; экономическая безопасность; инвестиционный механизм.

Key words: economy; investments; economic security; investment mechanism.

УДК 330.332.

БЕЗОПАСНОСТЬ ПОТРЕБИТЕЛЕЙ В ЕВРАЗИЙСКОМ ЭКОНОМИЧЕСКОМ СОЮЗЕ

CONSUMER PROTECTION IN THE EURASIAN ECONOMIC UNION

Проводится анализ международно-правовой практики, применяемой в Евразийском экономическом союзе (далее – ЕАЭС) по вопросам безопасности потребителей.

The author carries out analysis of the international legal practice of the Eurasian Economic Union (further – EEU) on consumer safety issues.

Созданию Евразийского экономического союза предшествовал довольно долгий путь интеграционного развития, от Договора о Таможенном союзе 1995 года до предшественника ЕАЭС – Евразийского экономического сообщества. [1, 3, 6]

Как результат многолетних интеграционных процессов, 29 мая 2014 года был подписан Договор о Евразийском экономическом союзе, участниками которого в настоящее время являются Российская Федерация, Республика Беларусь, Республика Армения, Республика Казахстан, Кыргызская Республика. Данный Договор предусматривает отдельный раздел, касающийся взаимодействия в сфере защиты прав потребителей, в котором четко установлено, что права потребителей и их защита гарантируются законодательством государств-членов о защите прав потребителей, а также самим Договором [4].

При этом следует отметить, что граждане государства-члена проживающие на его территории, пользуются на территориях других государств-членов такой же защитой в области прав потребителей, что и граждане этих других государств-членов.¹

В случае нарушения вышеуказанных прав, граждане могут обращаться в государственные и общественные организации по защите прав потребителей, а также суды [4].

Обеспечение гарантий надлежащей защиты прав потребителей является одним из направлений развития интеграции, отмеченных в Декларации, подписанной президентами государств-членов ЕАЭС в 2018 году [5].

Одной из задач, которая стоит перед государствами – членами ЕАЭС, является принятие согласованных решений, направленных на защиту интересов потребителей. Направления сотрудничества закреплены в отдельном приложении 12 к Договору в виде Протокола. Это касается различных требований к потребительской продукции, начиная от санитарно-эпидемиологических и гигиенических, ветеринарных и карантинно-фитосанитарных требований безопасности, в том числе включая сведения, вносимые в маркировку пищевой продукции [2].

Решения по обеспечению безопасности потребительской продукции, принимаемые в ЕАЭС, основываются на оценке рисков и скоординированной деятельности государств. При этом, главенствующую роль занимает гармонизация национального законодательства в сфере защиты прав потребителей, которая осуществляется государствами в соответствии с рекомендациями Евразийской экономической комиссии (ЕЭК). Именно этой структуре – ЕЭК, предоставлено право разрабатывать и предлагать странам ЕАЭС механизмы, которые смогут обеспечить оптимальный уровень безопасности продукции и при этом предоставить изготовителям возможность использовать новые

¹ Статья 60 Договора о ЕАЭС

технологии и материалы. Требования, которые должны выполнять производители, установлены в технических регламентах. В настоящее время, около 70% продукции на рынке ЕАЭС охвачены требованиями технических регламентов.

Новое в техническом регулировании можно продемонстрировать следующим перечнем конкретных решений:

- технический регламент на изделия электротехники, запрещающий применение свинца, ртути и других вредных для здоровья человека и экологии металлов в бытовых приборах, например, в компьютерах, холодильниках, телевизорах, мобильных телефонах;
- изменения в техническом регламенте на колесные транспортные средства, включающие требования по оборудованию автомобилей скорой помощи современными системами помощи больным;
- технический регламент о безопасности оборудования для детских игровых площадок, устанавливающий единые требования к конструкции оборудования по обеспечению его прочности и устойчивости, в том числе, в оборудовании не должно застревать тело или одежда ребенка, не должно быть острых концов или кромок;
- изменения в части маркировки пищевой продукции, устанавливающие минимальную величину шрифта для маркировки и определяющие критерии, в соответствии с которыми текст маркировки признается легко читаемым и понятным;
- технический регламент на алкогольную продукцию, систематизирующий нормы межгосударственных и национальных стандартов на алкогольную продукцию;
- требования к молочной продукции, касающиеся необходимости указания на продуктах заменителя молочного жира, если он применялся, шрифтом не менее 2,5 мм на лицевой стороне упаковки;
- технический регламент на аттракционы, предусматривающий меры для снижения риска травматизма при их эксплуатации, распространяющийся на колеса обозрения, катапульты, батуты, горки, электромобили, водные аттракционы;
- требования обязательной маркировки продукции с содержанием ГМО, если в составе продукции содержание ГМО превышает 0,9 %, причем для адаптации бизнеса к этому нововведению установлен переходный период в полтора года.

Это лишь небольшая часть результатов работы ЕАЭС по принятию решений в сфере безопасности потребителей.

ЕЭК принимает меры по установлению обязательных для исполнения санитарных, ветеринарных, ветеринарно-санитарных и карантинных фитосанитарных требований и процедур, коротко обозначаемых как СФР-меры. На всей территории ЕАЭС в сфере СФР-мер действуют:

- единые перечни товаров, в отношении которых устанавливаются обязательные требования;
- единые фитосанитарные требования;
- единые формы документов, подтверждающих безопасность продукции;
- единый порядок проведения контрольно-надзорных мероприятий.

Несмотря на большую работу, проведенную в сфере совершенствования мер по безопасности потребителей, необходимо внести ряд изменений в Договор о ЕАЭС, например, в части использования электронных фитосанитарных сертификатов. Кроме того, принять новые решения в части прослеживания продукции животного происхождения для сведения к нулю появления на рынках небезопасных пищевых продуктов животного происхождения; внести изменения в Единые карантинные фитосанитарные требования с учетом современных достижений; внести предложения по подготовке единых правил по защите прав потребителей на всей территории ЕАЭС.

ЛИТЕРАТУРА

1. Балытников В.В., Боклан Д.С. Евразийский экономический союз: предпосылки создания, проблемы формирования, перспективы развития / В.В. Балытникова, Д.С. Боклан // Сравнительное конституционное обозрение. – 2015. – № 3. – С. 69–81.
2. Воронцова Н.А. Правовой анализ положений Договора о Евразийском экономическом союзе/Воронцова Н.А.// Московский журнал международного права. – 2014. – №4. – С. 78–87.
3. Воронцова Н.А. Евразийское экономическое сообщество как международная организация / Н.А. Воронцова // Внешнеэкономический бюллетень, 2004. – №6.
4. Договор о Евразийском экономическом союзе. – Москва: 2014. – 680 с.
5. Декларация о дальнейшем развитии интеграционных процессов в рамках Евразийского экономического союза от 06.12.2018 (электронный ресурс)... <http://www.eurasiancommission.org/ru/Pages/ses.aspx>. Дата доступа: 6.03.2019
6. Шумилов В.М., Боклан Д.С., Лифшиц И.М. Правовые новеллы Договора о Евразийском экономическом союзе / В.М. Шумилов, Д.С. Боклан, И.М. Лифшиц // Российский внешнеэкономический вестник. – 2015. – № 3(106).

СВЕДЕНИЯ ОБ АВТОРЕ

Воронцова Наталья Анатольевна. Профессор кафедры международного права. Доктор юридических наук.

Московский государственный институт международных отношений Министерства иностранных дел Российской Федерации.

E-mail. N.Vorontsova@mail.ru

Россия, 119454, Москва, пр.Вернадского,76.

Тел.+79037214259.

Vorontsova Natalia. Professor of the Chair of International Law. Dr. of Law.

Moscow state institute of international relations of the Ministry of foreign affairs Russian Federation.

E-mail. N.Vorontsova@mail.ru

Work address: Russia, 119454, Moscow, Vernadsky Prospect, 76.

Тел.+79037214259.

Ключевые слова: Евразийский экономический союз, безопасность потребителей, СФР-меры.

Key words: Eurasian Economic Union, consumer safety, SFR measures

УДК 339.543

**К ВОПРОСУ О НАДЛЕЖАЩЕМ СПОСОБЕ ЗАЩИТЫ ПРАВА ПО СПОРАМ,
СВЯЗАННЫМ С ГРАНИЦАМИ ЗЕМЕЛЬНОГО УЧАСТКА**

**TO THE QUESTION OF THE APPROPRIATE REMEDY
ON THE DISPUTES RELATED TO BORDERS
LAND PLOT**

Данная статья посвящена спорам, связанным с границами земельного участка. Описывает надлежащие способы защиты права, обстоятельства, подлежащие доказыванию, вопросы применения срока исковой давности и ошибки судебной практики.

This article is devoted to disputes related to the boundaries of the land. Describes the appropriate ways to protect the right, the circumstances to be proved, the application of the Statute of limitations and errors of judicial practice.

Утверждая можно отметить, что земельные споры являются наиболее сложной категорией гражданских дел, которые вызывают как у судей, так и у лиц, участвующих в деле, множество неясностей и вопросов, и зачастую требуют специальных познаний.

Такие дела довольно часто встречаются в судебной практике. При этом единообразного применения и толкования норм материального права при их рассмотрении не выработано. Данные споры, как правило, представляют собой длительный процесс судебного разбирательства, включающий в себя многочисленные и многочасовые судебные заседания, производство судебных экспертиз, допросы свидетелей, кадастровых инженеров, специалистов, экспертов, который зачастую приводит к нарушению судом срока рассмотрения дела, установленного гражданско-процессуальным законом.

При поступлении такого иска в большинстве случаев назначается предварительное судебное заседание либо стороны в рамках подготовки дела к судебному разбирательству вызываются судьей на беседу в целях установления значимых по делу обстоятельств, определения предмета доказывания, поскольку содержание иска такой категории и реальная проблема бывают диаметрально противоположными.

Количество именно земельных споров, находящихся на рассмотрении у каждого из судей дает некую внутреннюю оценку их загруженности и квалификации.

Несмотря на то, что практически всегда (более 90% споров) стороны участвуют в деле рассматриваемой категории с квалифицированными представителями, в том числе и лицами, имеющими статус адвоката, однако специалистов, понимающих предмет доказывания по спорам в области земельных правоотношений, очень мало. Довольно часто истцы обращаются в суд с неправильными требованиями либо не заявляют необходимой совокупности требований, что влечет за собой невозможность защиты права и отказ в исках (например, в некоторых случаях, без наличия требования о признании результатов межевания недействительными, требование об установлении границ не имеет перспектив). При этом разъяснение судом права на уточнение оснований и предмета иска сторона истца игнорирует.

Итак, статья 304 Гражданского Кодекса РФ [1] предоставляет собственнику возможность требовать устранения нарушений его прав, даже если эти нарушения и не связаны с лишением владения.

Судебная практика показывает, что при одних и тех же стечении случаев, когда истцы обращаются с иском, параллельно заявляя требование об истребовании части зе-

мельного участка из чужого незаконного владения и требование об устранении препятствий в пользовании земельным участком. Не понятно: «Какой же способ защиты прав подлежит применению?».

Гражданский Кодекс РФ в статье 12 предусматривает различные способы защиты гражданских прав.

Как известно, право собственности включает в себя права владения, пользования и распоряжения своим имуществом.

Для определения надлежащего способа защиты гражданского права по спорам, связанным с границами земельного участка, значимым обстоятельством является факт владения спорной частью земельного участка либо факт утраты владения этим земельным участком (его частью).

Владение не является самостоятельным вещным правом. Оно выступает звеном иных прав или выражается в фактическом действии (отношении), но это вовсе не значит, что право владения не подлежит гражданско-правовой защите.

ГК РФ не содержит определения понятия «владение».

Значение слова «владеть» в русском языке - это фактическое обладание вещью; территория, находящаяся под чьей-либо властью, в чьем либо управлении [2].

Негативный иск будет являться надлежащим способом защиты права, если местоположение границ земельного участка не изменено, т.е. земельный участок не выбыл из владения, но собственник или законный владелец лишены возможности нормально его использовать (например, если на смежном земельном участке незаконно возведен объект, препятствующий попаданию дневного света по установленным нормативам в помещения здания истца. Если владение земельным участком не утрачено виндикационный иск подан быть не может.

Таким образом, если часть земельного участка выбыла из владения, основания для удовлетворения негативного иска отсутствуют. Данная позиция изложена в определении Верховного Суда РФ [3].

А вот в случае захвата соседом части земельного участка подлежит предъявлению виндикационный иск.

В судебной практике являются распространёнными споры, предметом которых выступает захват части земельного участка истца собственником соседнего земельного участка путем установки забора. В большинстве случаев по таким спорам истцы заявляют требования об устранении препятствий в пользовании земельным участком путем переноса забора и суды удовлетворяют такие требования, формулируя резолютивную часть решения следующим образом: «Обязать Д. не чинить препятствий Б. в пользовании земельным участком «...» и перенести ограждение...» [4]. Такие действия суда противоречат вышеприведенной позиции Верховного суда РФ.

Так, требование об устранении препятствий в пользовании земельным участком может быть заявлено лишь при сохранении владения им, т.е. при наличии факта свободного доступа собственника к принадлежащему земельному участку.

Факт утраты собственником права владения в отношении части принадлежащего земельного участка (установка забора, возведение строения) не дает права на заявление таких требований.

При этом срок исковой давности также находится в зависимости от факта владения. К негативным искам срок исковой давности применению не подлежит. А вот к виндикационным искам подлежит применению трехлетний срок исковой давности, установленный ч. 1 ст. 196 ГК РФ.

По виндикационному иску подлежит установлению местоположение земельного участка, т.е. его границы. При этом исковые требования должны заявляться с учетом того каким способом определены границы участка. Если проведено межевание, то несоответ-

ствие фактических границ земельного участка границам, определенным в ходе выполнения кадастровых работ, выступает доказательством нарушения прав истца. Кроме того, в случае если границы установлены в ходе работ по межеванию, а требований о признании таких работ недействительными не заявлено, фактически сложившиеся границы участков не учитываются не зависимо от длительности их существования.

В случае несогласия истца с границами, установленными в ходе выполнения кадастровых работ, в совокупность требований должно входить требование и об оспаривании результатов межевания, исключении сведений о границах земельного участка из ЕГРН (ГКН).

Если кадастровые работы не проводились, то требование об установлении границ земельного участка может быть заявлено по усмотрению истца. Суды считают такое требование самостоятельным способом защиты права, в связи с чем это требование может быть заявлено как самостоятельно (при необходимости согласования границы), так и входить в совокупность требований (по спорам об устранении кадастровой ошибки или о признании межевания недействительным).

Есть случаи, в которых удовлетворение судом требования не влечет за собой восстановление права. Так, факт удовлетворения требований о признании результатов межевания недействительными не приведет к восстановлению границ земельного участка, поскольку права на недвижимость, зарегистрированные в установленном порядке (в ЕГРН), исправление ошибок в ЕГРН может быть произведено только в судебном порядке [5], то бишь только при наличии в резолютивной части судебного акта указания на необходимость исправления ошибки (исключения или изменения сведений в ЕГРН) Управление государственной регистрации, кадастра и картографии произведет соответствующие действия.

Без заявления требований о признании результатов межевания недействительными доказать координаты земельного участка и, соответственно, установить границы земельного участка не представляется возможным.

Таким образом, для восстановления нарушенного права на земельный участок необходимо заявлять совокупность требований:

- о признании результатов межевания недействительными;
- об устранении ошибок или внесении изменений в Единый государственный реестр недвижимости, об установлении границ земельного участка.

В отношении установления границ земельного участка существуют следующие правила:

- границы земельного участка в Российской Федерации устанавливаются путем определения координат характерных точек этих границ [6];
- в случае уточнения местоположения земельного участка его границы устанавливаются из правоустанавливающего документа, а в случае отсутствия такового - из документов, подтверждающих его границы при его образовании (из первичных землеотводных документов);
- если документального подтверждения местоположения земельного участка не имеется, то границы участка определяются с учетом утвержденного проекта межевания территории;
- в случае отсутствия в проекте межевания территории информации о спорном земельном участке, его границами признаются фактические границы землепользования, существующие не менее 15 лет с учетом привязок к местности (линий электропередач, газопроводов, многолетних деревьев, прудов, рек и иных объектов, если таковые отражены в планах БТИ, топографических съемках и т.д.), которые позволяют установить его границы.

Встречаются споры, при рассмотрении которых границы земельного участка не представляется возможным установить не по одному из выше указанных правил. Вместе с тем оставлять такие споры не разрешенным и отказывать в исках Верховный Суд РФ [7] запрещает, говоря о нарушении ст. 2 ГПК РФ [8]. В таких ситуациях суд вправе установить границы земельного участка по своему внутреннему убеждению, с учетом закона, подлежащего применению и интересов собственников смежных земельных участков.

Суды должны допускать отказ в защите права лишь в случае злоупотребления истцом своим правом.

При рассмотрении споров о границах участка судом сопоставляется фактическая площадь земельного участка и его документальная площадь (площадь, указанная в правоустанавливающих или первичных землеотводных документах) с учетом существующих привязок к местности.

Если установлена разница площадей, необходимо определение земель, за счет которых произошло расхождение площадей. В такой ситуации подлежат выяснению вопросы:

- производилось ли сторонами по делу расширение границ принадлежащих им земельным участком за счет прирезок (самовольно занятых государственных или муниципальных земель);

- имел ли место перенос сторонами или прежними собственниками спорной границы участка.

Вместе с тем даже в случае соответствия площадей земельных участков необходимо устанавливать, не имел ли место отказ ответчика (или истца) от части принадлежащего ему земельного участка и захват части участка соседа.

По искам об истребовании имущества из чужого незаконного владения значимыми по делу обстоятельствами являются:

- наличие у истца прав на земельный участок в установленных границах и определенной площадью;

- незаконность владения лицом этим участком (его частью);

- каким образом имущество выбыло из владения: по воли или помимо воли собственника (законного владельца).

Действующее законодательство предоставляет право собственнику земельного участка отчуждать, а также передавать его, оставаясь собственником.

Если истец передал ответчику в фактическое владение на основании добровольного соглашения (как устного, так и письменного) часть земельного участка и такой порядок пользования существует на протяжении длительно времени, требования истца удовлетворению не подлежат.

Кроме того, существуют методические рекомендации по проведению межевания объектов землеустройства от 17.02.2003, которые предусматривают погрешность для города – допустимое расхождение между фактической и документальной границей в размере 0,30 м.

Таким образом, для того, чтобы нарушенное право было восстановлено необходимо использовать надлежащий способ защиты права, а взаимосвязанные и взаимообусловленные требования заявлять в рамках одного дела, поскольку это сократит и время восстановления права, и размер судебных расходов.

ЛИТЕРАТУРА

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ.
2. Ожегов С.И. Толковый словарь русского языка : 80 000 слов и фразеологических выражений / С.И. Ожегов, Н.Ю. Шведова; Российская академия наук; Институт русского языка им. В.В. Виноградова. – 4-е изд., доп. – М.: Азбуковник, 1997. – С.67.
3. Определение Верховного Суда РФ от 08.12.2015 №4-КГ15-62.
4. Гражданское дело №2-830/2018. Архив Новоусманского районного суда Воронежской области.
5. Федеральный закон от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости» // Доступ из СПС «Консультант Плюс».
6. Федеральный закон от 13.07.2015 № 218-ФЗ «О государственной регистрации недвижимости» // Доступ из СПС «Консультант Плюс».
7. Определение Верховного Суда РФ от 20.06.2017 №38-КГ17-5.
8. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ.

СВЕДЕНИЯ ОБ АВТОРЕ

Гаврилова Наталья Александровна. Новоусманский районный суд Воронежской области, помощник судьи. Кандидат юридических наук.

E-mail: gavriloVA-5418@mail.ru.

Россия, 396310, Воронежская область, Новоусманский район, село Новая Усмань, улица Авдеева, дом 9. Телефон (47341) 5-46-69.

Gavrilova Natalia Alexandrovna. Novaya Usman district court, Voronezh Region. Assistant judge. Candidate of sciences (law).

E-mail: gavriloVA-5418@mail.ru.

Work address: Russia, 396310, Voronezh Region, Novaya Usman, Avdeyeva Street, 9. Tel. (47341) 5-46-69.

Ключевые слова к статье: земельный участок, границы, владение, негаторный иск, виндикационный иск, срок исковой давности.

Key words: land, boundaries, own, ownership, negatory claim replevin, the Statute of limitations.

УДК 347.9

Жаглин Андрей Вячеславович,
кандидат юридических наук, доцент;
Коробейникова Лариса Сергеевна,
кандидат экономических наук, доцент

ТОС КАК ФОРМА САМООРГАНИЗАЦИИ ГРАЖДАН: ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ФУНКЦИОНИРОВАНИЯ

TOS AS A FORM OF SELF-ORGANIZATION OF CITIZENS: SOME PROBLEMS OF FUNCTIONING

В статье рассматривается понятие территориального общественного самоуправления в Российской Федерации как формы народовластия. Исследуются отдельные правовые и организационные проблемы их деятельности.

The article deals with the concept of territorial public self-government in the Russian Federation as a form of democracy. Separate legal and organizational problems of their activity are investigated.

В 1998 г. Российская Федерация ратифицировала положения Европейской Хартии местного самоуправления, среди которых два основополагающих: «...органы местного самоуправления являются одной из главных основ любого демократического строя», а «...право граждан участвовать в управлении государственными делами относится к демократическим принципам, разделяемым всеми Государствами – членами Совета Европы» [1]. Данные идеи нашли свое отражение в статьях Закона Российской Федерации от 6 июля 1991 года № 1550-1 «О местном самоуправлении в Российской Федерации» [2], в гл.8 Конституции Российской Федерации, а в последующем были детализированы в нормах Федерального закона от 06 октября 2003 года № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» [3]. В соответствии со ст.1 указанного нормативного правового акта, «местное самоуправление составляет одну из основ конституционного строя Российской Федерации, признается, гарантируется и осуществляется на всей территории Российской Федерации», а ст.12 Конституции Российской Федерации закрепляет, что «местное самоуправление в пределах своих полномочий самостоятельно» [4]. Закрепленная на законодательном уровне самостоятельность местного самоуправления имеет определенную цель – оказать позитивное влияние на процесс становления и развития гражданского общества, которое занимает пограничное положение между органами государственной власти и общественной самодеятельностью [5].

Одним из значимых институтов местного самоуправления является территориальное общественное самоуправление (ТОС) [6]. Согласно ст. 27 Федерального закона № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», под территориальным общественным самоуправлением (ТОС) понимается самоорганизация граждан по месту их жительства на части территории поселения, внутригородской территории города федерального значения, муниципального округа, городского округа, внутригородского района, а также в расположенных на межселенной территории населенных пунктах (либо на части их территории) для самостоятельного и под свою ответственность осуществления собственных инициатив по вопросам местного значения.

По смыслу закона, рассматриваемый уровень народовластия не нуждается как в инструментах публично-властного воздействия, так и в полномочиях по изданию правовых актов. Здесь вполне достаточно сформировавшихся механизмов самоорганизации населения, содержание которых направлено на определение наиболее эффективных путей решения локальных проблем и добровольное исполнение жителями

принимаемых на себя обязательств[7]. ТОСы создаются в инициативном порядке гражданами как «снизу», так и по инициативе органов государственной или местной власти – «сверху». Как правило, территориальное общественное самоуправление возникает там, где жители начинают самостоятельно заботиться о комфорте на территории своего проживания, чистоте и красоте своего двора, улицы или даже целого поселения [8]. Простота порядка формирования ТОСов, приближенность к населению, тесная связь их деятельности с повседневными жизненными интересами граждан обеспечивают массовость этих организаций, обуславливают необходимость последовательного повышения их роли в системе местного самоуправления [9].

В этой связи, вице-спикер Совета Федерации Андрей Турчак отмечает, что «ТОС – это как раз тот механизм, с помощью которого жители могут полноценно участвовать в решении вопросов, которые напрямую затрагивают их повседневную жизнь» [10]. Посредством функционирования ТОСов реализуется важная и необходимая для населения работа, направленная на благоустройство территорий, создание комфортной среды проживания, помощь ветеранам и нуждающимся в социальной поддержке. Кроме того, деятельность рассматриваемых организаций содействует укреплению общественного порядка, позволяет организовывать и проводить различные социально значимые мероприятия.

По данным Министерства юстиции Российской Федерации в настоящее время на территориях более 5,6 тыс. муниципалитетов нашей страны насчитывается более 30,1 тыс. ТОСов, охватывающих как городские, так и сельские территории [11]. При этом, самоорганизация граждан по месту их жительства может принимать две основные формы: в качестве юридического лица и без него. Данные формы отличаются возможностями по привлечению финансовых средств. Очевидно, что деятельность ТОСа в форме юридического лица будет более эффективной, а такая форма выгоднее. Однако ее создание сопряжено с определенными трудностями. В частности, в законодательстве отсутствует отдельная организационно-правовая форма некоммерческой организации, в которой создается ТОС. Видимо, поэтому, статус юридического лица имеют менее десяти процентов российских ТОСов. Большинство регистрируется в форме общественной организации, которая не дает достаточных полномочий для активного функционирования и взаимодействия с органами местного самоуправления [12].

Более того, действующее законодательство, по существу, закрепляет лишь две формы взаимодействия ТОС с органами местного самоуправления: внесение органами ТОС проектов муниципальных правовых актов, а также заключение органами ТОС договоров с органами местного самоуправления. В связи с этим территориальное общественное самоуправление наиболее функционально и эффективно лишь при поддержке органами региональной и муниципальной власти. Эта поддержка выражается в организационной [13], финансовой помощи, в том числе посредством выделения субсидий (грантов) на реализацию конкретных проектов ТОС по результатам конкурса. Так, в рамках государственной программы Воронежской области «Содействие развитию муниципальных образований и местного самоуправления» Правительством Воронежской области предоставляются субсидии из областного бюджета некоммерческой организации – Ассоциация «Совет муниципальных образований Воронежской области» на поощрение проектов, реализуемых в рамках территориального общественного самоуправления в муниципальных образованиях Воронежской области [14]. К примеру, в 2019 году в рамках конкурса общественно полезных проектов ТОС было выделено 90 млн. руб. Однако, этого явно недостаточно для реализации всех заявленных ТОСами социально-значимых проектов: благоустройство территорий и мест отдыха, строительство детских и спортивных площадок, ремонт мостов и дорог, благоустройство родников и колодцев, обеспечение водой и ряд других работ. Поэтому, распределение выделенных средств было организовано на конкурсной основе. Ассоциация «Совет муниципальных образований Воронежской области» в 2019 году приняла заявки на конкурс общественно полезных проектов от 1003 ТОС. Победителями конкурса стало

всего 260 организаций. Однако, если внимательно ознакомиться с содержанием фактически всех заявленных проектов, то станет очевидным, что они, по существу, входят в перечень вопросов местного значения городского, сельского поселения, закрепленных ст. 14 Федерального закона № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации». Получается, что благодаря активности членов победивших ТОС, региональным правительством выборочно будут профинансированы проекты, реализация которых должна осуществляться органами местного самоуправления в соответствии с законом и исходя из интересов местного населения.

Следующей проблемой, связанной с существованием ТОС без образования юридического лица, является невозможность быть полноправным субъектом права собственности. И, несмотря на то, что учрежденным ТОСам для осуществления их деятельности в безвозмездное пользование органами местного самоуправления могут предоставляться помещения, оргтехника, оборудование, иные материальные ресурсы, эти объекты продолжают оставаться муниципальной собственностью. ТОСы лишь приобретают право владения и пользования данным имуществом [15]. Причем, источники формирования собственности могут быть различными: взносы граждан, материальная помощь различных организаций, средства грантов и т.п. Но, в конечном счете, при отсутствии юридического лица у ТОСа эта собственность становится муниципальной. Значит и содержание этой собственности, ответственность за ее состояние ложится на плечи муниципального образования. И может сложиться ситуация, когда инициативные проекты граждан, проживающих на территории конкретного ТОСа, будут «головной болью» для органов местного самоуправления, поскольку их финансовое сопровождение, в том числе после их реализации, не предусмотрено местным бюджетом. К примеру, на территории ТОС по инициативе граждан был разбит сквер, установлены элементы спортивного оборудования, детской площадки. Кто будет убирать эту территорию, поддерживать техническое состояние установленного оборудования, отвечать за его сохранность? Граждане или органы местного самоуправления? Даже если между органами местного самоуправления и ТОСом будет заключен договор о содержании указанной собственности, можно ли будет привлечь ТОС к ответственности за его ненадлежащее исполнение? По нашему мнению, это невозможно.

Полагаем, что возникновение подобных ситуаций обусловлено тем, что реальный статус ТОС в современном законодательстве не определен. Возможности граждан, организовавших ТОС, ограничены не только законом и финансовыми ресурсами, но и желанием органов местного самоуправления реализовывать их проекты. И хотя в отдельных источниках, посвященных деятельности ТОСов, отмечается, что органы ТОС могут осуществлять хозяйственную деятельность по благоустройству территории, иную хозяйственную деятельность, направленную на удовлетворение социально-бытовых потребностей граждан, проживающих на соответствующей территории, как за счет средств указанных граждан, так и на основании договора между органами ТОС и органами местного самоуправления с использованием средств местного бюджета [6], ключевым здесь все же является слово «могут». Причем на усмотрение органов местного самоуправления, поскольку указанный договор – добровольное соглашение двух сторон.

ЛИТЕРАТУРА

1. Европейская хартия местного самоуправления ETS № 122 (Страсбург, 15 октября 1985 г.). // Собрание законодательства Российской Федерации. - 1998 г. - № 36. - Ст. 4466.
2. О местном самоуправлении в Российской Федерации: фед. закон от 6 июля 1991 года № 1550-1 (с изм. и доп.) [Электронный ресурс].- URL : <https://base.garant.ru/10102703.htm> (дата обращения: 25.06.2019).

3. Об общих принципах организации местного самоуправления в фед. закон от 06.10.2003 № 131-ФЗ (с изм. и доп.) [Электронный ресурс]. - URL : <http://base.garant.ru/186367.htm>(дата обращения: 25.06.2019).

4. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ). [Электронный ресурс]. - URL : http://consultant.ru/document/cons_doc_LAW_28399.htm (дата обращения: 25.06.2019).

5. Яковлева М.А. Местное самоуправление как институт гражданского общества / М.А. Яковлева // Фундаментальная наука вузам [Электронный ресурс]. - URL : <https://cyberleninka.ru/article/n/mestnoe-samoupravlenie-kak-institut-grazhdanskogo-obschestva-1> (дата обращения: 25.06.2019).

6. Территориальное общественное самоуправление как основа развития территорий: Учебное пособие / Отв. ред. А.А. Ларичев, А.В. Баталин. -Петрозаводск: Карельский научный центр РАН, 2017. - 186 с. [Электронный ресурс]. - URL : <http://www.petrozavodsk-mo.ru/files/Posobie%20-TOS2017.pdf>(дата обращения: 25.06.2019).

7. Комментарий к Федеральному закону «Об общих принципах организации местного самоуправления в Российской Федерации» (постатейный) / И.В. Бабичев, В.В. Волков, А.В. Мадьярова и др.; под ред. И.В. Бабичева, Е.С. Шугриной. - 2-е изд., перераб. и доп. - М.: НОРМА, ИНФРА-М, 2015. - 672 с.

8. Что такое ТОС и зачем он нужен [Электронный ресурс]. - URL : <http://tos36.ru/что-такое-тос-и-зачем-он-нужен> (дата обращения: 25.06.2019).

9. Кутафин О.Е., Фадеев В.И. Муниципальное право Российской Федерации : учебник / О.Е. Кутафин, В.И. Фадеев. - 3-е изд., перераб. и доп. - Москва : Проспект, 2011. - 672 с.

10. А. Турчак. Территориальное общественное самоуправление позволяет гражданам полноценно участвовать в решении актуальных вопросов. [Электронный ресурс]. - URL : <http://council.gov.ru/events/news/94147> (дата обращения: 25.06.2019).

11. Шурыгина Е. Территориальное общественное самоуправление на карте России / Е. Шурыгина // Российская муниципальная практика. - № 02 (80). - 2019. - С. 20 - 27. [Электронный ресурс]. - URL : http://promweekly.ru/archive/rmp/RMP_2_2019.pdf (дата обращения: 25.06.2019).

12. Мисливская Г. Ближе к жизни / Г. Мисливская // Российская газета. - Федеральный выпуск. - № 148(7611). [Электронный ресурс]. - URL : <https://rg.ru/2018/07/10/miniust-utochnil-status-organizacij-tos.html>(дата обращения: 25.06.2019).

13. Распоряжение главы города Воронежа от 4 марта 2002 года № 215-р «Об утверждении методических рекомендаций по планированию работы органа территориального общественного самоуправления на год» [Электронный ресурс]. - URL : <http://docs.cntd.ru/document/440505447>(дата обращения: 25.06.2019).

14. Постановление Правительства Воронежской области от 2 июля 2015 г. № 545 «Об утверждении порядка предоставления субсидии из областного бюджета некоммерческой организации - Ассоциация "Совет муниципальных образований Воронежской области" на поощрение проектов, реализуемых в рамках территориального общественного самоуправления в муниципальных образованиях Воронежской области, в рамках подпрограммы "Реализация государственной политики в сфере социально-экономического развития муниципальных образований" государственной программы Воронежской области "Содействие развитию муниципальных образований и местного самоуправления". [Электронный ресурс]. - URL : <http://www.consultant.ru/regbase/cgi/online.cgi?req=doc&base=RLAW181&n=65836#09632522836538294> (дата обращения: 25.06.2019).

15. Раздьяконова Е.В. ТОС как субъект права муниципальной собственности в Российской Федерации / Раздьяконова Е.В. [Электронный ресурс]. - URL : <http://geum.ru/lav/index-32383.php>(дата обращения: 25.06.2019).

СВЕДЕНИЯ ОБ АВТОРАХ

Жаглин Андрей Вячеславович. Старший преподаватель кафедры гражданско-правовых и экономических дисциплин. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: gagdrej@mail.ru

Россия, 394056, Воронеж, проспект патриотов, 53. Тел. (473) 200-53-02.

Коробейникова Лариса Сергеевна, кандидат экономических наук, доцент. Заведующая кафедрой экономического анализа и аудита.

Воронежский государственный университет.

E-mail: korobeinikova@vsu.ru

Россия, 394018, Воронеж, Университетская площадь, 1.

Тел. (473) 222-60-92.

Zhaglin Andrey Vyacheslavovich. Senior Lecturer, Department of Civil Law and Economic Disciplines. Candidate of legal sciences, associate professor.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: gagdrej@mail.ru

Russia, 394056, Voronezh, Avenue of Patriots, 53. Tel. (473) 200-53-02.

Korobeynikova Larisa Sergeevna, Candidate of Economic Sciences, Associate Professor. Head of the Department of Economic Analysis and Audit.

Voronezh State University.

E-mail: korobeinikova@vsu.ru

Russia, 394018, Voronezh, University Square, 1. Tel. (473) 222-60-92.

Ключевые слова: местное самоуправление; муниципальное образование; территориальное общественное самоуправление; благоустройство территорий.

Key words: local self-government; municipal formation; territorial public self-government; improvement of territories.

УДК 342

СТРАХОВАНИЕ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ: ВОПРОСЫ ПРАВОПРИМЕНЕНИЯ

INSURANCE OF EMPLOYEES OF INTERNAL AFFAIRS BODIES: ISSUES OF ENFORCEMENT

Данная статья посвящена рассмотрению вопросов страхования жизни и здоровья сотрудников органов внутренних дел. На основе анализа законодательства и судебной практики делается ряд выводов о применении нормативных актов, регулирующих порядок осуществления страховых и иных выплат сотрудникам.

This article is devoted to the issues of life and health insurance of employees of the internal Affairs bodies. Based on the analysis of legislation and judicial practice, a number of conclusions are made on the application of regulations governing the procedure for the implementation of insurance and other payments to employees.

Служба в органах внутренних дел, в особенности в полиции, считается одной из самых опасных. В целях повышения безопасности службы и уровня социальной защищенности сотрудников государство оберегает данную категорию лиц, осуществляя их обязательное страхование.

Мировой опыт показывает, что социальное страхование представляет собой важный институт социальной политики, целью которого является обеспечение конституционного права граждан на материальное обеспечение в определенных случаях.

Ст. 43 ФЗ «О полиции» [1] и ФЗ «Об обязательном государственном страховании жизни и здоровья военнослужащих, граждан, призванных на военные сборы, лиц рядового и начальствующего состава органов внутренних дел Российской Федерации, Государственной противопожарной службы, сотрудников учреждений и органов уголовно-исполнительной системы, сотрудников войск национальной гвардии Российской Федерации» от 28 марта 1998 г. № 52-ФЗ (далее ФЗ № 52) [2] в качестве одной из гарантий, предоставляемых сотрудникам органов внутренних дел, рассматривают страхование их жизни, здоровья и имущества.

Согласно данным нормативно-правовым актам, страховыми интересами (объектами страхования) признаются жизнь и здоровье сотрудника органов внутренних дел, как во время прохождения службы, так и в течение года после увольнения со службы.

Отметим, что данный вид страхования является обязательным для страхователя – Министерства внутренних дел РФ, которое за счет средств, выделенных на эти цели из федерального бюджета, должно осуществлять страхование сотрудников органов внутренних дел. При этом, в соответствии со ст. 927 ГК РФ, для страховщиков заключение договоров страхования на предложенных страхователем условиях не обязательно. Это положение вполне оправдано, однако, влечет ряд проблем практической реализации данной социальной гарантии сотрудников.

В роли страховщика могут выступать лишь юридические лица, удовлетворяющие определенным требованиям. Во-первых, это должны быть страховые организации. Во-вторых, у них должна быть лицензия Банка России на осуществление именно обязательного государственного страхования. В-третьих, они должны соответствовать требованиям законодательства РФ о государственной тайне и иметь опыт работы в сфере личного страхования не менее двух лет.

Ст. 2 ФЗ № 52 предусматривает выбор страховщика на основании контрактной системы в силу положений ФЗ от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [3]. Размеры страховых тарифов (премий) и условия страхования устанавливаются в законодательном порядке и договором страхования корректироваться не могут. Сегодня заключение таких контрактов многие страховые компании рассматривают как убыточные, поскольку страховая премия не покрывает расходов по выплатам при наступлении страховых случаев, которых становится все больше. В этой связи в 2016 г. МВД РФ впервые столкнулось со сложностями при заключении контракта: он дважды объявлялся несостоявшимся по причине отсутствия заявок страховых компаний. Такая же ситуация возникла и в 2017 году. В результате несвоевременного заключения соответствующих контрактов и, как следствие, договора страхования МВД РФ столкнулось с необходимостью самому выплачивать страховые суммы сотрудникам или выгодоприобретателям за счет бюджетных средств в силу ст. 937 ГК РФ и ст. 7 ФЗ № 52.

На сегодняшний день МВД России заключен государственный контракт обязательного государственного страхования жизни и здоровья лиц рядового и начальствующего состава органов внутренних дел с ООО «Центральное страховое общество» на период с 1 января 2018 г. по 31 декабря 2019 г.

Страховые случаи, при наступлении которых производится страховая выплата сотрудникам органов внутренних дел, указаны в ст. 4 ФЗ № 52.

Необходимо отметить, что ФЗ № 52 не связывает наступление страхового случая с непосредственным исполнением служебных обязанностей сотрудником в момент гибели или получения увечья. Необходимо лишь, чтобы страховой случай наступил в период прохождения службы в органах внутренних дел или до истечения года с момента увольнения со службы.

Иная ситуация складывается при получении выплат в соответствии со ст. 43 ФЗ «О полиции», действие которой распространяется не только на сотрудников полиции, но и на иных сотрудников органов внутренних дел. Условием получения денежного возмещения является гибель или увечье сотрудника при выполнении служебных обязанностей, а также вследствие заболевания, полученного в период прохождения службы. При этом, в соответствии со ст. 68 ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменения в отдельные законодательные акты Российской Федерации» от 30 ноября 2011 г. № 342-ФЗ (далее ФЗ № 342) [4], сотрудник считается выполняющим служебные обязанности не только при нахождении на рабочем месте и в течение рабочего дня.

Данной статьей установлены и случаи гибели или увечья сотрудника, которые не влекут компенсационных выплат (состояние состояние алкогольного, наркотического или иного токсического опьянения, совершение умышленного преступления, самоубийство сотрудника).

Следует отметить, что в ст. 10 ФЗ № 52 названы фактически те же самые основания освобождения страховщика от выплаты страхового возмещения. Однако, самоубийство сотрудника здесь рассматривается как страховой случай. Таким образом, можно констатировать, что в случае самоубийства сотрудника страховое возмещение будет выплачиваться по ФЗ № 52 и не будет по ст. 43 ФЗ «О полиции», кроме случаев, когда оно вызвано доведением до самоубийства или болезненным состоянием.

Размер выплачиваемых сумм установлен ст. 5 ФЗ № 52 и ст. 43 ФЗ «О полиции».

Так в соответствии со ст. 5 ФЗ № 52, предусмотрены следующие страховые суммы:

– 2 млн. руб., которые выплачиваются в случае смерти сотрудника (бывшего сотрудника);

- 1,5 млн. руб., которые выплачиваются при установлении сотруднику (бывшему сотруднику) инвалидности I группы;
- 1 млн. руб., которые выплачиваются при установлении сотруднику (бывшему сотруднику) инвалидности II группы;
- 500 тыс. руб., которые выплачиваются при установлении сотруднику (бывшему сотруднику) инвалидности III группы;
- 200 тыс. руб., которые выплачиваются при получении сотрудником тяжелого увечья;
- 50 тыс. руб., которые выплачиваются при получении сотрудником легкого увечья.

Ст. 43 ФЗ «О полиции» устанавливает следующий размер выплат:

- 3 млн. руб. в случае смерти сотрудника (бывшего сотрудника);
- 2 млн. руб. в случае получения сотрудником увечья (травмы), исключающего дальнейшую службу в полиции. При установлении инвалидности сотруднику также будет выплачиваться ежемесячная денежная компенсация, исходя из размера оклада месячного содержания и надбавки за выслугу лет, с учетом следующих коэффициентов: для инвалидов I группы – 1, II группы – 0,5, III группы – 0,3.

При этом размеры единовременных выплат ежегодно индексируются, исходя из уровня инфляции, а ежемесячных выплат – соответственно увеличению размеров окладов денежного содержания сотрудников.

Вопросы выплаты единовременного пособия в размере 2 миллионов рублей, предусмотренного ч. 5 ст. 43 ФЗ «О полиции», неоднократно становились предметом судебного рассмотрения. При этом в судебных постановлениях указывалось, что основанием для выплаты такого пособия является невозможность дальнейшего прохождения службы в органах внутренних дел, которая устанавливается на основании заключения ВВК. В Постановлении Конституционного суда РФ от 1 марта 2017 г. № 3-П [5] определено, что при признании сотрудника негодным к службе (категория «Д»), контракт с ним расторгается, поскольку дальнейшее продолжение службы невозможно на любых должностях. Соответственно, такому сотруднику должно быть выплачено единовременное пособие в размере 2 млн. рублей. Если же сотрудник признан ограниченно годным к службе (категория «В») или годным к службе с незначительными ограничениями (категория «Б»), он подлежит увольнению только при отсутствии возможности перевода на другую должность в органах внутренних дел, подходящую по состоянию здоровья, или при отказе от такого перевода. Соответственно, право на получение единовременного пособия возникает только в случае, когда возможность перевода на подходящую должность отсутствует (сотрудник подлежит увольнению по п. 8 ч. 2 ст. 82 ФЗ № 342). В случае же отказа сотрудника от предложенного перевода, он утрачивает право на получение единовременного пособия, так как его выплата связана именно с невозможностью дальнейшего прохождения службы, и подлежит увольнению по п. 3 ч. 3 или п. 8 ч. 2 ст. 82 ФЗ № 342. Однако, и при увольнении по состоянию здоровья решающее значение имеет добровольный отказ сотрудника от продолжения службы.

Поэтому в соответствующих судебных постановлениях делается вывод, что если сотрудник органов внутренних дел «отказался от перевода на предложенную вакантную должность, подходящую ему по состоянию здоровья, то он не вправе претендовать на предусмотренное единовременное пособие, поскольку возможность дальнейшего прохождения службы для него сохранялась, но, реализуя конституционное право на свободное распоряжение своими способностями к труду, он добровольно отказался от ее прохождения» [6].

Таким образом, систематическое толкование правовых норм, регулирующих порядок выплаты единовременного пособия в случае невозможности дальнейшего про-

хождения службы, а также позиции Конституционного Суда РФ, выраженной в постановлении от 1 марта 2017 г. № 3-П, позволяет сделать вывод о том, что сотрудник вправе получить упомянутое пособие при наличии одновременно следующих условий:

- получение сотрудником увечья или иного повреждения здоровья, связанного с исполнением служебных обязанностей и исключающего дальнейшее прохождение службы;

- невозможность для такого сотрудника продолжить службу в органах внутренних дел на других должностях.

Выгодоприобретателями по договорам страхования являются сами застрахованные лица, а в случае их гибели – лица, имеющие право на получение страхового возмещения, которое выплачивается им в равных долях. В соответствии со ст. 2 ФЗ № 52 таковыми являются:

- супруг, состоявший с сотрудником в зарегистрированном браке на день гибели (смерти) последнего;

- родители (усыновители) сотрудника;

- дедушка и бабушка, при условии, что они воспитывали или содержали сотрудника не менее трех лет в связи с отсутствием родителей;

- отчим и мачеха сотрудника, при условии, что они воспитывали или содержали его не менее пяти лет;

- дети сотрудника: несовершеннолетние, инвалиды детства, обучающиеся в образовательных организациях до 23 лет;

- подопечные сотрудника.

В ч.3 ст. 43 ФЗ «О полиции» в числе выгодоприобретателей указаны члены семьи и иждивенцы сотрудника. К первым отнесены все те же супруг, родители и дети (несовершеннолетние, инвалиды детства, обучающиеся в образовательных организациях по очной форме обучения до 23 лет). К иждивенцам, помимо детей, закон относит лиц, находившихся на полном содержании погибшего сотрудника или получавших от него помощь, которая была для них постоянным и основным источником существования. Отметим, что если иждивенчество детей умершего в указанных выше случаях предполагается, то для признания находящимися на его иждивении других лиц требуется судебное решение. Таким образом, круг лиц, имеющих право на получение соответствующих выплат в случае гибели (смерти) сотрудника, несколько отличается в нормативно-правовых актах, регулирующих порядок производства компенсационных выплат.

Помимо страховых выплат сотрудник полиции (члены его семьи или иждивенцы) при наличии указанных в ст. 43 ФЗ «О полиции» оснований, может рассчитывать на выплату единовременных пособий и возмещение ущерба, причиненного имуществу сотрудника и его близких. Важно отметить, что сотрудник (выгодоприобретатели) могут получить одновременно и страховые суммы по ФЗ № 52 от страховщика, и выплаты по ст. 43 ФЗ «О полиции» от МВД РФ, поскольку это различные суммы, выплачиваемые по различным основаниям и из разных источников. В то же время, при одновременном возникновении нескольких оснований для получения соответствующих выплат, они производятся лишь по одному из них по выбору получателя (ч. 9 ст. 43 ФЗ «О полиции»). Например, по одному из дел судом было указано, что одновременное получение выплат в соответствии со ст. 43 ФЗ «О полиции» и ст. 21 ФЗ от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» [7] невозможно, поскольку данными законами предусмотрено право выбора сотрудником органов внутренних дел при повреждении здоровья одного из оснований выплат [8].

Таким образом, подводя итог, можно сделать следующие выводы:

- 1) ФЗ № 52 урегулированы вопросы страхования жизни и здоровья сотруд-

ников, в то время как ФЗ «О полиции» предусматривает порядок производства выплат в предусмотренных законом случаях за счет средств федерального бюджета;

2) основанием получения страховых выплат является получение травмы (увечья, заболевания) или смерти (гибели) в период прохождения службы, выплаты же, предусмотренные ст. 43 ФЗ «О полиции» производятся только в случае, если травма, заболевание, смерть наступят при исполнении служебных обязанностей, а не просто в период прохождения службы в полиции (органах внутренних дел), на что неоднократно обращалось внимание в судебной практике [9];

3) систематическое толкование правовых норм, регулирующих порядок выплаты единовременного пособия в случае невозможности дальнейшего прохождения службы, а также позиции Конституционного Суда РФ, выраженной в постановлении от 1 марта 2017 г. № 3-П, позволяет сделать вывод о том, что сотрудник вправе получить упомянутое пособие при наличии одновременно следующих условий:

- получение сотрудником увечья или иного повреждения здоровья, связанного с исполнением служебных обязанностей и исключающего дальнейшее прохождение службы;

- невозможность для такого сотрудника продолжить службу в органах внутренних дел на других должностях;

4) при наличии соответствующих оснований сотрудник (бывший сотрудник, выгодоприобретатели) могут рассчитывать на получение одновременно страховых выплат и выплат по ст. 43 ФЗ «О полиции». Так, в Постановлении Конституционного Суда РФ от 01 марта 2017 г. № 3-П «По делу о проверке конституционности части 5 статьи 43 Федерального закона «О полиции» в связи с жалобами граждан В.А. Семенова и Н.В. Шмакова» указывалось, что наряду с выплатой страховых сумм по обязательному государственному страхованию жизни и здоровья, сотрудникам органов внутренних дел, получившим в связи с выполнением служебных обязанностей увечье или иное повреждение здоровья, исключающее возможность дальнейшего прохождения службы, предоставляются и другие имеющие целью возмещение вреда здоровью денежные выплаты и иные виды компенсаций.

ЛИТЕРАТУРА

1. О полиции: федер. закон от 07 февраля 2011 г. № 3-ФЗ // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900.

2. Об обязательном государственном страховании жизни и здоровья военнослужащих, граждан, призванных на военные сборы, лиц рядового и начальствующего состава органов внутренних дел Российской Федерации, Государственной противопожарной службы, сотрудников учреждений и органов уголовно-исполнительной системы, сотрудников войск национальной гвардии Российской Федерации: фед. закон от 28 марта 1998 г. № 52-ФЗ // Собрание законодательства РФ. – 1998. – № 13 – Ст. 1474.

3. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: фед. закон от 5 апреля 2013 г. № 44-ФЗ // Собрание законодательства РФ. – 2013. – № 14. – Ст. 1652.

4. О службе в органах внутренних дел Российской Федерации и внесении изменения в отдельные законодательные акты Российской Федерации: фед. закон от 30 ноября 2011 г. № 342-ФЗ // Собрание законодательства РФ. – 2011. – № 49 (ч. 1). – Ст. 7020.

5. Постановление Конституционного суда РФ от 1 марта 2017 г. № 3-П «По делу о проверке конституционности части 5 статьи 43 Федерального закона «О полиции» в

связи с жалобами граждан В.А. Семенова и Н.В. Шмакова» [Электронный ресурс]. – URL : konstitutsionnogo-suda-rf-ot-01032017-n-3-p/#100025 (дата обращения 17.06.2019).

6. Определение Верховного Суда РФ от 07 мая 2018 г. № 21-КГ18-4 [Электронный ресурс]. – URL : <http://legalacts.ru/sud/opredelenie-verkhovnogo-suda-rf-ot-07052018-n-21-kg18-4/> (дата обращения 17.06.2019).

7. О противодействии терроризму: фед. закон от 6 марта 2006 г. № 35-ФЗ // Собрание законодательства РФ. – 2006. – № 11. – Ст. 1146.

8. Определение Липецкого областного суда от 30 января 2012 г. по делу № 33-224/2012 г. [Электронный ресурс]. – URL : <http://sudact.ru/regular/doc/> (дата обращения 17.06.2019).

9. Обзор практики рассмотрения судами дел о возмещении вреда, причиненного жизни или здоровью военнослужащих, граждан, призванных на военные сборы, лиц рядового и начальствующего состава органов внутренних дел Российской Федерации, Государственной противопожарной службы, органов по контролю за оборотом наркотических средств и психотропных веществ, сотрудников учреждений и органов уголовно-исполнительной системы : утв. Президиумом Верховного Суда РФ 23 декабря 2015 г. [Электронный ресурс]. – URL : <http://www.legalacts.ru/sud/obzor-praktiki-rassmotreniia-sudami-del-o-vozmeshchenii-vreda-prichinennogo-zhizni-ili-zdoroviu-voennosluzhashchikh-grazhdan-prizvannykh-na-voennye-sbory/> (дата обращения 17.06.2019)

СВЕДЕНИЯ ОБ АВТОРЕ

Жаглина Марина Евгеньевна. Доцент кафедры гражданско-правовых и экономических дисциплин. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: mzhaglina@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-53-02.

Zhaglina Marina Evgenievna. Associate Professor of the chair Civil law and Economic disciplines. Candidate of law, associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: mzhaglina@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-53-02.

Ключевые слова: страхование сотрудников органов внутренних дел; жизнь и здоровье сотрудников органов внутренних дел; страховая выплата; страховой случай.

Key words: insurance of employees of internal Affairs bodies; life and health of employees of internal Affairs bodies; insurance payment; insurance case.

УДК 347.1

ПОДЛОЖНАЯ БУХГАЛТЕРСКАЯ ДОКУМЕНТАЦИЯ В СИСТЕМЕ ДОКАЗАТЕЛЬСТВ ПРОТИВОПРАВНЫХ ЭКОНОМИЧЕСКИХ ДЕЙСТВИЙ

FALSE ACCOUNTING RECORDS IN THE SYSTEM EVIDENCE OF ILLEGAL ECONOMIC ACTIONS

В работе сформулировано авторское определение бухгалтерского подлога в современных условиях противодействия экономической преступности, рассмотрены существующие виды и способы подлога, в том числе - в условиях применения информационно-коммуникационных технологий.

The paper formulates the author's definition of accounting forgery in modern conditions of combating economic crime, considers the existing types and methods of forgery, including the use of information and communication technologies.

При возникновении проблем определения правдивости и достоверности бухгалтерских документов и отчетных данных экономических субъектов появляется необходимость изучения соответствующими лицами (следователями, дознавателями, экспертами-бухгалтерами и др.) такой категории судебной бухгалтерии, как «бухгалтерский подлог». Понятия подложного бухгалтерского документа и действий должностных лиц, связанных с осуществлением подлога при совершении и оформлении фактов хозяйственной жизни, регулярно рассматривались в работах ученых и практиков в различные периоды существования нашего государства.

Вместе с тем, по различным причинам некоторые авторы, исследующие способы совершения неправомерных экономических действий, затрагивающих систему бухгалтерского учета и отчетности экономических субъектов, не рассматривают подлог в бухгалтерской учетной и отчетной документации.

В данной работе мы попытаемся сформулировать определение бухгалтерского подлога в современных условиях противодействия экономической преступности, рассмотреть существующие способы подлога, в том числе в условиях применения информационно-коммуникационных технологий.

Категория «подложный бухгалтерский документ» довольно подробно рассматривалась в работах таких известных отечественных ученых в области судебной бухгалтерии и бухгалтерской экспертизы, как С.П. Голубятников [1], Ж.А. Кеворкова [5], Е.Р. Россинская [4] и др. Практикующие в сфере правовой бухгалтерии специалисты приводят следующее определение «бухгалтерского» подлога – «это всегда умышленные действия человека, преследующего цель ввести в заблуждение должностных лиц, сотрудников частной или государственной организации, чтобы получить какую-либо выгоду» [2]. В ряде публикаций авторы ассоциируют подлог в бухгалтерских документах с их подделкой (Д.А. Курбанова [3]). На наш взгляд, подобное мнение несколько ограничивает возможности оценки противоправных действий в системе бухгалтерского учета и не отвечает современному состоянию мер противодействия экономическим правонарушениям и преступлениям.

Вместе с тем, с учетом развития информационных технологий считаем важным сформулировать собственное определение «бухгалтерского» подлога, под которым предлагаем понимать корыстные умышленные действия, направленные на введение в заблуждение должностных лиц экономических субъектов, путем искажения реквизитов

бухгалтерских документов или содержания фактов хозяйственной жизни в бумажном виде или на электронных носителях.

В работах многих ученых и практиков чаще всего рассматривается два основных вида подлога в бухгалтерских документах – материальный и интеллектуальный. Материальный подлог, как правило, связан с искажением данных первичных бухгалтерских документов с целью получения противоправной выгоды (наживы). В основном такие действия совершаются для сокрытия недостатков материальных ценностей и денежных средств, искусственного создания излишков, манипуляций с дебиторской и кредиторской задолженностями и т.п.

Второй вид бухгалтерского подлога – интеллектуальный – заключается в правильном оформлении бухгалтерской документации, которая в тоже время содержит неправомерные сведения о совершенных фактах хозяйственной жизни.

В целях детализации представленных видов на основании проведенного анализа практических материалов проведения судебно-бухгалтерских экспертиз по противоправным экономическим действиям предлагаем структурировать способы бухгалтерского подлога в зависимости от субъекта совершения по четырем группам, а именно:

1 группа – на уровне материально-ответственных лиц экономических субъектов. Такие подлоги являются материальными и совершаются для хищения имущества или денежных средств путем сокрытия недостатков или создания излишков. При таких подлогах искажаются данные первичных документов в бумажном виде или в электронном варианте, отражающих движение активов экономических субъектов как внутри него, так при купле-продаже имущества. При этом, в отдельных практических ситуациях могут иметь место расхождения между бумажной и электронной версией одного и того же документа.

2 группа – подлоги на уровне руководства структурных подразделений экономических субъектов, которые, как правило, носят организованный характер с вовлечением должностных лиц такого подразделения (цех, участок, отдел и др.). В основном рассматриваемые подлоги совершаются с целью сокрытия противоправной хозяйственной деятельности в рамках какого-либо подразделения экономического субъекта, связанной с выпуском неучтенной продукции и ее нелегальной продажей, мошенническими действиями и т.п. Такие подлоги могут как материальными, так и интеллектуальными.

3 группа – подлоги, санкционированные руководством экономического субъекта или его владельцами. В данном случае подлог совершается работниками бухгалтерии по указанию руководства или владельцев для осуществления определенной категории экономических преступлений или правонарушений. Он является интеллектуальным по сути, сопряжен с искажением бухгалтерских отчетных данных и связан с такими противоправными действиями, как:

- незаконное получение кредита;
- уклонение от уплаты налогов;
- незаконное обналичивание денежных средств;
- неправомерные действия при банкротстве экономического субъекта, связанные с выводами активов из-под контроля правомочных собственников;
- мошеннические действия с целью привлечения инвестиций и их последующего присвоения;
- легализация доходов, полученных преступным путем;
- хищение, присвоение и нецелевое расходование бюджетных средств и др.

4 группа подлогов связана с неправомерными действиями работников бухгалтерского аппарата экономического субъекта, выполняемыми индивидуально или в сговоре с другими должностными лицами с целью наживы. Примером таких действий могут служить манипуляции с дебиторской и кредиторской задолженностью, неоприхо-

дование наличных денежных средств, хищение заработной платы работников экономического субъекта и т.п. Подобные подлоги могут относиться и к материальному, и к интеллектуальному виду в зависимости от применяемого способа сокрытия следов.

Таким образом, среди выделенных нами способов бухгалтерского подлога, которые могут совершаться различными категориями должностных лиц, включая и бухгалтерских работников, в одном случае присутствует только материальный подлог (1 способ), в другом случае - только интеллектуальный подлог (3 способ), в двух случаях – оба вида подлога (2 и 4 способ).

Также следует отметить, что рассматриваемые подлоги, затрагивающие систему бухгалтерского учета и отчетности, предлагается считать «бухгалтерскими» вне зависимости от того, какие должностные лица участвуют в противоправной схеме совершения экономического правонарушения или преступления.

С учетом рассмотренных видов бухгалтерского подлога предлагается выделить следующие основные способы подлога в бухгалтерских документах:

- внесение искаженных данных о наличии товарно-материальных ценностей в инвентаризационные описи с целью сокрытия их недостач или излишков;
- отражение неправильного количества поступивших материальных ценностей с составлением подложного документа, содержащего заниженное количество полученного имущества;
- манипуляции с дебиторской и кредиторской задолженностью;
- подлоги в авансовых отчетах должностных лиц с целью присвоения умышленных перерасходов;
- подлоги в кассовых первичных документах, кассовой книге и кассовых отчетах в бумажном и электронном варианте;
- манипуляции при начислении и перечислении (выдаче) заработанных сумм работников экономического субъекта;
- составление бестоварных документов движения материальных ценностей с целью сокрытия выпуска неучтенной продукции;
- искажение данных бухгалтерской (финансовой) отчетности и их подтасовка для совершения определенной категории противоправной деятельности;
- создание фирм-«однодневок» с целью наживы и проведения неправомερных финансовых операций.

Рассмотренный перечень способов совершения подлогов в бухгалтерских документах не может быть исчерпывающим, является базовым для его последующего дополнения и трансформации.

ЛИТЕРАТУРА

1. Голубятников С.П. Основы бухгалтерского учета и судебно-бухгалтерской экспертизы : учебник / С.П. Голубятников ; под ред. С.С. Остроумова. – Волгоград : ВСШ МВД СССР, 1980. – 452 с.
2. Куприянова В.Н. Ответственность за использование подложного документа. ЮрСовет. Доступно о праве и его применении. [Электронный ресурс] - URL: <http://juresovet.ru/otvetstvennost-za-ispolzovanie-podlozhnogo-dokumenta/> (дата обращения - 10.03.2019).
3. Курбанова Д.А. Использование поддельных документов. БУКВА ПРАВА. [Электронный ресурс] - URL: <https://bukvaprava.ru/2018/03/23/otvetstvennost-za-ispolzovanie-podlozhnyh-dokumentov/> (дата обращения - 10.03.2019).

4. Судебно-бухгалтерская экспертиза : учеб. пособие для студентов вузов / Е.Р. Россинская [и др.] ; под ред. Е.Р. Россинской, Н.Д. Эриашвили. – 2-е изд., перераб. и доп. – М. : ЮНИТИ-ДАНА, 2009. – 383 с.

5. Судебно-экономическая экспертиза. Практикум: учеб. пособие для студентов вузов, обучающихся по специальностям «Бухгалтерский учет, анализ и аудит», «Экономическая безопасность», направлению «Экономика» / Ж.А. Кеворкова, И.В. Бахолдина. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2015. – 191 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Звягин Сергей Анатольевич. Начальник кафедры гражданско-правовых и экономических дисциплин. Доктор экономических наук, доцент.

Воронежский институт МВД России.

E-mail: patzv@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-53-73.

Zvyagin Sergei Anatolyevich. Head of the Department of civil law and economic disciplines. Doctor of economic Sciences, associate Professor/

Voronezh Institute of MIA of Russia.

E-mail: patzv@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. 200-53-73.

Ключевые слова: подлог в бухгалтерских документах, противоправные экономические действия, экономический субъект, должностные лица, искажение бухгалтерского документа.

Key words: forgery in accounting documents, illegal economic actions, economic entity, officials, distortion of the accounting document.

УДК 657.6.012.16

**НЕКОТОРЫЕ ТАМОЖЕННЫЕ АСПЕКТЫ УПРОЩЕНИЯ ПРОЦЕДУР
ТОРГОВЛИ ПО СОГЛАШЕНИЮ USMCA И ТКЕАЭС**

**SOME CUSTOMS ASPECTS OF TRADE FACILITATION UNDER THE USMCA
AGREEMENT AND THE EEU CUSTOMS CODE**

Проведен сравнительный анализ двух нормативно-правовых актов, выявлены их сходства, различия и предложены пути их дальнейшего совершенствования.

Comparative analysis of two legal acts, defining their similarities and differences, as well as ways of their further improvement.

В 2013 г., на 9-й Министерской конференции Всемирной торговой организации, прошедшей на о. Бали в Индонезии, было принято Соглашение об упрощении процедур торговли (Trade Facilitation Agreement – TFA) [1]. Договор вступил в силу в феврале 2017 г., после его ратификации более чем двумя третями членов ВТО. Целью документа является ускорение перемещения, выпуска и очистки товаров в условиях увеличения прозрачности и предсказуемости таможенных операций, повышения эффективности взаимодействия и координации таможенных органов [2].

Нормы Соглашения об упрощении процедур торговли в той или иной степени вошли в Таможенный кодекс ЕАЭС (вступивший в силу в 2018 г.) и в новое соглашение между США, Мексикой и Канадой (United States-Mexico-Canada Agreement (USMCA)). Несмотря на то, что изначально США вели отдельные переговоры с Канадой и Мексикой по возможному заключению двусторонних договоров, в результате страны пришли к решению заключить данное трехстороннее Соглашение [3].

USMCA призвано заменить действующее с 1994 года Североамериканское соглашение о свободной торговле (NAFTA) [4]. Подписание документа состоялось на полях саммита G20 в Аргентине 30 ноября 2018 г. Для вступления Соглашения в силу необходима его ратификация в парламентах трех стран-участниц (что, по предварительным оценкам, может произойти во второй половине 2019 г.), а до этих пор продолжает действовать Соглашение НАФТА.

Глава 7 USMCA «Таможенное администрирование и упрощение процедур торговли» построена на основе положений главы 5 Соглашения НАФТА «Таможенные процедуры» и дополняется рядом уточняющих норм, заимствованных из Соглашения ВТО по упрощению процедур торговли (TFA) 2013 г. [5, 6] и Транстихоокеанского партнерства (TPP) 2016 г.

Стоит отметить, что само понятие «упрощение процедур торговли» из названия главы 7 USMCA является нововведением: в Соглашении НАФТА такой термин не содержится. Есть различия и в структуре двух договоров: положения относительно правил происхождения в новом Соглашении, в отличие от текста НАФТА, вынесены в отдельную – четвертую – главу.

Одной из новелл Соглашения USMCA, по сравнению с Североамериканским соглашением о свободной торговле, является статья 7.8 «Ускорение процедуры перевозки». В соответствии с ее положениями, каждая сторона должна обеспечить проведение ускоренных таможенных процедур при сохранении надлежащего уровня таможенного контроля. К таким процедурам относятся: использование механизма «единого окна» при подаче одного общего документа (к примеру, декларации), отражающего данные всех товаров в «экспресс-грузе»; обеспечение немедленного выпуска грузов сразу по их прибытии

при условии предоставления всей требуемой документации; отказ от обложения налогами или пошлинами и от формальностей при ввозе грузов определенной стоимости. Понятия «минимальный объем документации» и «меньшее количество формальностей», применяемые к экспресс-грузам, в рассматриваемой статье не раскрываются – предположительно, они будут определены в подзаконных актах и практике государств¹.

В свою очередь, Таможенный кодекс ЕАЭС (далее – ТК ЕАЭС) не содержит подобных развернутых положений по скоростным перевозкам. В документе лишь дается понятие «экспресс-груза»², а также указывается на «первоочередной порядок совершения таможенных операций в отношении отдельных категорий товаров»³, к которым относятся в том числе и «экспресс-грузы». В настоящее время в Евразийской экономической комиссии идет работа по формированию двух блоков предложений, направленных на дальнейшее совершенствование правового регулирования операций с экспресс-грузами. К первому из них относится идея создания института экспресс-оператора, тогда как второй блок посвящен вопросам оптимизации формы реестра экспресс-грузов [7]. В научной среде высказываются также предложения по созданию конкуренции на рынке доставки экспресс-грузов, полному переходу на их электронное декларирование, что будет способствовать прозрачности проведения таможенных операций [8].

Представляется, что при дальнейшем развитии законодательства ЕАЭС в данной сфере можно учесть и положения Соглашения USMCA по введению системы «единого окна» в отношении экспресс-грузов, а также снижению порога стоимости для их беспошлинного ввоза.

Следующим нововведением USMCA, по сравнению с Соглашением НАФТА, является статья 7.7 «Выпуск товаров», содержащая как элементы Соглашения об упрощении процедур торговли ВТО (ТФА), так и Транстихоокеанского партнерства (ТРП). В соответствии с ней государства обязуются обеспечить незамедлительный выпуск товаров по получении таможенной декларации и выполнению всех применимых требований и процедур. Стоит отметить, что в Соглашении ТРП срок выпуска товаров установлен в 48 часов. В Соглашении USMCA также содержится обязанность обеспечения предварительного таможенного оформления и отказа от требования помещения товаров под процедуру временного хранения по их прибытии. Государства-участницы Соглашения обязуются осуществлять выпуск товаров до принятия окончательного решения и уплаты любых таможенных пошлин или сборов при соблюдении определенных условий.

Что касается ЕАЭС, то схожая процедура выпуска товаров установлена в главе 18 «Выпуск товаров и таможенные операции, связанные с выпуском товаров» ТК ЕАЭС. Так, в соответствии со статьей 119 ТК «Сроки выпуска товаров», их выпуск должен быть завершен таможенным органом в течение 4 часов с момента регистрации таможенной декларации либо, при предварительном таможенном декларировании товаров, с момента наступления одного из обстоятельств (изменение (дополнение) сведений, заявленных в таможенной декларации; получение таможенным органом, зарегистрировавшим таможенную декларацию, уведомления о размещении товаров в зоне таможенного контроля, указанной в таможенной декларации, или выдача таможенным органом разрешения на выгрузку товаров, перевозимых водными судами, в месте прибытия, указанном в таможенной декларации). Помимо этого, при условии предоставления обеспечения уплаты таможенных платежей, выпуск товаров, по аналогии с Соглашением USMCA, может быть произведен до получения результатов таможенной экс-

¹ Overview of Chapter 7 of the US-Mexico-Canada Agreement. Whiteand Case. Электронный доступ: <https://www.whitecase.com/publications/alert/overview-chapter-7-customs-administration-and-trade-facilitation-us-mexico-canada>

² Ст. 2, п. 1, 52) ТКЕАЭС

³ Ст. 81 ТК ЕАЭС

пертизы. [9] Для уполномоченных экономических операторов (УЭО) действует система специальных упрощений при выпуске товаров [10] (таких, как совершение таможенных операций, связанных с таможенным декларированием и выпуском товаров, в таможенном органе, отличном от таможенного органа, в регионе деятельности которого находятся товары, если такие таможенные органы расположены на территории одного государства-члена; выпуск товаров до подачи декларации на товары)¹.

Таким образом, на данный момент максимально сжатые сроки выпуска товаров установлены новым Соглашением США-Канада-Мексика, тогда как ТК ЕАЭС предоставляет таможенным органам на данную процедуру 4 часа.

Подводя итоги, хотелось бы отметить тенденцию развития правового регулирования процедур упрощения торговли: на особое значение данного института указывает выделение комплекса его норм в отдельную главу Соглашения USMCA, а также его более детальное регулирование, как в рамках указанного Соглашения, так и нового Таможенного кодекса ЕАЭС. Тем не менее, очевидна необходимость дальнейшего дополнения данной правовой базы подзаконными актами и практикой государств, что позволит создать целостный механизм регулирования упрощения процедур торговли.

Представляется, что некоторые положения Соглашения USMCA могут послужить положительным примером для дальнейшего развития законодательства ЕАЭС в таможенной сфере. Среди таких норм: формирование комплексного правового регулирования в области ускоренных процедур перевозки, включая предоставление экспресс-операторам возможности их немедленного выпуска и подачи единого документа на все товары в экспресс-грузе через систему «единого окна»; обеспечение незамедлительного выпуска товаров по получении таможенной декларации и выполнению всех применимых требований и процедур. Все данные меры будут способствовать снижению временных и финансовых издержек участников внешнеэкономической деятельности и, как следствие, способствовать ускорению и удешевлению международной торговли в целом.

ЛИТЕРАТУРА

1. Antonia Eliason. The Trade Facilitation Agreement: A New Hope for the World Trade Organization // *World Trade Review*, 2015. – V. 14 – No. 4. – P. 643–670.
2. Neufeld N. Breaking New Ground: The WTO Agreement on Trade Facilitation // *Pharmaceuticals Policy & Law*, 2016. – V. 18(1–4). – P. 67–78.
3. Patten, D. CritCrim (2018). <https://doi.org/10.1007/s10612-018-9425-8> - Springer Netherlands.
4. NAFTA Is Renegotiated and Signed by the United States // *International Economic Law*. doi:10.1017/ajil.2018.113.
5. Воронцова Н.А. Всемирная торговая организация: к вопросу об упрощении таможенных процедур торговли. Часть 1 / Н.А. Воронцова // *Московский журнал международного права*, 2018. – № 1. – С. 44–59.
6. Воронцова Н.А. Всемирная торговая организация: к вопросу об упрощении таможенных процедур торговли. Часть 2 / Н.А. Воронцова // *Московский журнал международного права*, 2018. – № 3. – С. 53–64.
7. Сивенкова А.И., Шуклина З.Н. Особенности таможенного оформления в условиях функционирования Евразийского Экономического Союза / А.И. Сивенкова, З.Н. Шуклина // *Молодой ученый*, 2017. – № 6. – С. 297–300.
8. Гокинаева И.А. Особенности таможенных операций с товарами категории экспресс-грузов / И.А. Гокинаева // *Вестник Российской академии естественных наук*, 2015. № 19(3). – С. 34–36.

¹Пп. 5), 9), п. 3, ст. 437 ТК ЕАЭС

9. Лысак Е.Д. Новеллы Таможенного кодекса Евразийского экономического Союза / Е.Д. Лысак // Таможенная политика России на Дальнем Востоке, 2017. – № 3(80). – С. 45–52.

10. Гревцева Л.Г., Аносов А.В. Таможенный кодекс ЕАЭС: возможности и перспективы / Л.Г. Гревцова, А.В. Аносов // Вестник Нижегородского университета им. Н.И. Лобачевского, 2015. – № 5. – С. 198–203.

СВЕДЕНИЯ ОБ АВТОРЕ

Климова Ирина Александровна. Аспирант кафедры международного права МГИМО МИД РФ, г. Москва.

E-mail: irinaklimova333@gmail.com

Россия, 119454, г. Москва, проспект Вернадского, 76.

Тел. +7-903-552-30-39.

Klimova Irina Alexandrovna. International law Ph.D student at MGIMO, Moscow.

E-mail: irinaklimova333@gmail.com

Work address: Russia, 119454, Moscow, Vernadsky Prospect, 76.

Tel. +7-903-552-30-39.

Ключевые слова: экономика, торговля, таможенные процедуры

Key words: economy, trade, customs procedures

УДК 339.543

СПРАВЕДЛИВОСТЬ И ПРАВО

JUSTICE AND LAW

Справедливость и право - две важнейшие категории, без которых невозможно представить существование любого человека. Их исследованию и анализу посвящены сотни тысяч разнообразных трудов на протяжении всей истории развития современной цивилизации. Как заметил классик политической философии Джон Ролз: «Справедливость — это первая добродетель общественных институтов, точно так же как истина — первая добродетель систем мысли. Теория, как бы она ни была элегантна и экономна, должна быть отвергнута или подвергнута ревизии, если она не истинна. Подобным же образом законы и институты, как бы они ни были эффективны и успешно устроены, должны быть реформированы или ликвидированы, если они несправедливы» [1].

Justice and law as two major categories of the theory of law. Discussion of their correlation in schools of legal positivism, natural law and integrative. Principles of justice according to John Rawls. General, private, substantive and procedural fairness. Egalitarian and hierarchical justice. The split of society in Russia due to the lack of fundamental agreement on the fundamental values of common justice. The path to unity is the real embodiment of the constitutional norm on the implementation of the principle of the social state.

Всегда и везде (у всех народов) считалось, что право должно быть справедливым. При этом важнейший цивилизационный институт рассматривался либо как воплощение справедливости, либо выдвигалась цель привести его в соответствие со справедливостью. Из этого следовало, что справедливость является одной из вечных ценностей или основных принципов права. Больше того, представители практически всех концепций правопонимания едины во мнении, что справедливость — не только вечная, но и высшая ценность в праве. Все остальные ценности соизмеряются с ней и действительны лишь при условии, что они не противоречат справедливости.

Для классического позитивизма как одного из трех главных течений теории права (Г. Кельзен и его отечественные последователи М.И. Байтин, Ф.М. Раянов др.) категория справедливости хотя и субъективна, а значит изменчива, но, несомненно, самоценна. Однако, что немаловажно, отнюдь не в рамках самого правопонимания, а как отдельный социальный регулятор.

Противоположная позиция представлена в рамках естественно-правового подхода, а именно в его современной российской интерпретации академика В.С. Нерсесянца и его школы. В «Философии права» он писал, что «справедливость — категория и характеристика правовая, а не внеправовая (не моральная, нравственная, религиозная и т.д.). Более того, только право и справедливо» [2]. Таким образом, справедливость либо тождественна праву и выступает в качестве его синонима, либо представляет собой одну из основополагающих характеристик права. Справедливость, таким образом, не только имманентна праву, но прямо названа правовой категорией. А поскольку право декларируется естественно-правовой школой высшей ценностью, то справедливость выступает всего лишь в качестве его, пусть и важнейшего, но всего только свойства, некой принадлежности. Вывод напрашивается сам собой: справедливость сама по себе перестает существовать, став элементом права.

Джон Ролз совершенно правильно отмечал по этому поводу, что «принципы справедливости... принадлежат к идеальной теории» [3]. Но право-то вполне реально и

весьма действенно в нашей жизни. Значит, для школы В.С. Нерсисянца право стало идеальной категорией.

Третья точка зрения, как часто бывает, представляет собой определенный синтез двух первых. Ее выразителем до своей кончины в 2003 г. был профессор МГУ О.Э. Лейст. Стержнем ее является тезис о том, что право отнюдь не всепоглощающая всё и вся субстанция, как предполагают, например, С.С. Алексеев или тот же В.С. Нерсисянец, а лишь часть, пусть и важная, жизни общества. Иначе говоря, право не всеобъемлюще. Следовательно, и теория права не самодавлеющая, и не может быть «чистой» (концепция Г. Кельзена). «Сущность права, – писал О.Э. Лейст, – не может быть постигнута ни практическим правоведением, ни даже общей теорией права, если последняя не выйдет за пределы юридических категорий» [4]. Потому однозначно справедливость продолжает оставаться неюридической категорией, без которой, однако, теория права не может обойтись.

Дж. Ролз сформулировал два принципа справедливости (характерных для сегоднешнего, индустриального, а для ряда стран уже по существу постиндустриального общества), которые никто сегодня не в силах опровергнуть. Звучат они следующим образом: 1) все лица обладают равными основными свободами, аналогичными со свободой иных лиц; 2) социальное и экономическое неравенство должны быть организованы таким образом, чтобы они служили благу всех (и особенно наименее благополучных людей) и были связаны с положением и должностями, доступными всем» [5].

Из этих постулатов выходит, что справедливость в данном контексте представляет собой относительно равное распределение выгод и тягот среди членов общества при гарантировании равенства прав и обязанностей. Иначе говоря, справедливость рассматривается не как юридическая категория, а как реальная, формализованная.

Как хорошо известно юристам, существуют категории общей, частной, субстанциональной и процедурной справедливости. Общая справедливость представляет собой справедливость основных социальных институтов, т.е. это справедливость в целом. Частная (личная) справедливость есть нравственно санкционированная соразмерность в распределении выгод и тягот совместной жизни людей и возможна только в относительно развитом обществе с наличием права как главного регулятора общественных отношений.

Что касается субстанциональной справедливости, то это уже тот принцип, на котором, собственно, зиждется человеческое общество. На основе субстанциональной справедливости осуществляется сотрудничество его членов.

Пошаговое соблюдение вышеуказанных принципов представляет собой процедурную справедливость.

Надо отметить, что принципы справедливости в целом, и каждый в отдельности могут не реализовываться по тем или иным причинам, в том числе и от неспособности (нежелания) политической элиты, правоохранительных органов реализовать их в действительности» [6].

Согласно европейской традиции общая теория справедливости представляет собой совокупность двух типов субстанциональной справедливости, коррелирующих с двумя полярными типами общественных связей. Первый подход представляет эгалитарная справедливость, приоритетно провозглашенная в развитых высокоиндустриальных странах. Данный тип предполагает равенство всех без исключения граждан (подданных) в гражданских, политических, социально-экономических правах и свободах и, соответственно, в обязанностях. Формально-юридически современный западный социум – это общество эгалитарной справедливости.

Второй подход выражен традиционной иерархической общей справедливостью. Здесь отправным принципом выступает неравенство статусов отдельных индивидов и социальных групп. Причем неравенство морально оправдывается тем генеральным доводом, что в нем выражается (будто бы) различная степень совершенства индивидов и групп, которую они демонстрируют (или должны демонстрировать) в повседневной жизни общества. Де-юре, в мире практически не осталось стран с таким понимани-

ем справедливости. Но де-факто в странах посттоталитарных, авторитарных мы видим именно такое состояние.

Что касается России, то сегодняшнее состояние дел таково, что на лицо две фундаментальные проблемы справедливости. Первую представляет собой ни много ни мало как нормативный раскол общества, т.е. отсутствие консенсуса различных групп населения в отношении субстанциональных принципов общей справедливости. Вторая проблема заключается в явной нехватке процедурной справедливости, заключающейся в недореализованности властными структурами всех ступеней принципов, провозглашенных и закрепленных в Конституции. Для большинства неангажированных исследователей российское общество не просто неоднородно, а это общество, в котором отсутствует принципиальное согласие по отношению фундаментальных ценностей общей справедливости. Как нам представляется, именно в этом зерно всех наших проблем как социально-экономического, так и морально-нравственного характера. Идеи эгалитарной и иерархической (статусной) справедливости сталкиваются в нашем обществе сплошь и рядом. И если с позиций буквы закона победа первого подхода не вызывает сомнений, то в реальной жизни довольно часто победу одерживает второй.

Высокоразвитые государства недаром провозглашают себя не только правовыми, но и социальными. Это налагает на власть придерживающих гораздо больше ответственности за свою деятельность. Сегодня уже не достаточно провозглашения формально-юридического равенства (то, к чему призывают глашатаи рыночной экономики в гуманитарной науке, в том числе и в юриспруденции), что характерно лишь для крайних форм экономического либерализма. Государства, на которых фактически равняется наша сегодняшняя правящая элита отказались от такого социального дарвинизма уже несколько десятилетий назад. Категория «социальное государство», провозглашенная и в Российской Конституции (ст. 7) – это по существу выход за рамки юридического равноправия, признание его недостаточным сегодня. Это признание несправедливым неравенства стартовых условий различных социальных слоев, вышедших из советского периода развития страны, это стремление смягчить фактическое неравенство и расширить сферу равенства посредством перераспределения общественного богатства. XXI век совсем не похож на XVIII, когда манифестировалась великая триада свободы, равенства, братства. Идеологи Просвещения искренне думали, что установление юридического равноправия приведет к всеобщему братству и свободе. Но реалии жизни достаточно быстро показали, что социальное неравенство гораздо шире правового. И цель человечества, как понимается она сегодня по крайней мере прогрессивной, демократической наукой и практикой – это создание максимально комфортных условий для всех без исключения групп населения (пусть и в разной степени).

Справедливость остается (да и никогда не перестанет быть) наипервейшей проблемой, имеющей чрезвычайно важное значение и для теории права. А в эпохи радикальной смены одних порядков другими значимость этой проблемы вырастает многократно. В отличие от последователей академика В.С. Нерсисянца мы считаем, что справедливость как идеал жизни общества, не синонимично праву, а шире, объемнее его. А потому консенсус по вопросу справедливости в обществе – одно из неперемennых условий жизнеспособности всякого современного государства. Пока такого консенсуса в России нет. Отсюда острая насущность научной разработки проблемы справедливости, в том числе ее юридических аспектов.

ЛИТЕРАТУРА

1. Ролз Дж. Теория справедливости. Новосибирск: изд-во НГУ, 1995. С. 3.
2. Нерсисянц В.С. Философия права. М., 1998. С.28.
3. Ролз Дж. Теория справедливости. Новосибирск: изд-во НГУ, 1995. С. 349.
4. Общая теория государства и права. Академический курс в 2-х т. Под ред. Н.М. Марченко. Т. 2. М., 1998. С.30.
5. Ролз Дж. Там же. С.62.
6. См. Кашников Б. Н. Теория справедливости и возможность ее применения к политическому бытию России./ Вопросы философии. 1994, №2, С.29-42.

СВЕДЕНИЯ ОБ АВТОРЕ

Коробов Геннадий Алексеевич. Доцент кафедры гражданско-правовых и экономических дисциплин. Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: genkorobov@yandex. ru

Россия, 394006, г. Воронеж, пр. Патриотов, 53. Тел. (473) 2208—916.

Korobov, Gennady Alekseevich. Associate Professor of civil and economic disciplines. Candidate of legal Sciences, associate Professor.

Voronezh Institute of MIA Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

E-mail: genkorobov@yandex. ru

Ключевые слова: справедливость, право, позитивистский, естественно-правовой, интегративный подходы к правопониманию, общая, частная, субстанциональная, процедурная виды справедливости, эгалитарная и иерархическая справедливость, социальное государство, Россия, проблемы понимания справедливости.

Key words: ustice, law, positivist, natural law, integrative approaches to legal understanding, General, private, substantive, procedural types of justice, egalitarian and hierarchical justice, social state, Russia, problems of understanding justice.

УДК 340.12

Коробов Геннадий Алексеевич,
кандидат юридических наук;
Азарова Ирина Владимировна

ТЕОРЕТИКО-ПРАВОВОЙ АСПЕКТ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ЭКОЛОГИЧЕСКИЕ ПРЕСТУПЛЕНИЯ

THEORETICAL AND LEGAL ASPECT OF CRIMINAL LIABILITY FOR ENVIRONMENTAL CRIMES

Данная статья посвящена рассмотрению особенностей применения категориального аппарата в уголовном законодательстве, а также рассмотрен факт отсутствия среди субъектов уголовной ответственности за экологические преступления юридических лиц.

This article is devoted to consideration of features of application of the categorical device in the criminal legislation, and also the fact of absence among subjects of criminal responsibility for ecological crimes of legal entities is considered.

В соответствие с общей теорией права уголовно-правовая ответственность за экологические преступления как правовой институт – это система юридических мер, признанных обеспечивать эффективное применение и реализацию принудительных мер уголовно-правового воздействия на нарушителей в целях соблюдения установленного законом порядка использования природных ресурсов и сохранения благоприятных для человека условий окружающей среды.

За последние десятилетия было внесено множество изменений в уголовное законодательства относительно противодействия экологическим преступлениям. Так, изменилась концепция правовой и общественной оценки экологических правонарушений. На сегодняшний момент приоритет имеет защита экологических интересов, условий, благоприятных для состояния здоровья человека, но не защита экономических интересов как ранее.

Обратим внимание на тот факт, что Уголовный кодекс Российской Федерации [1] (далее – УК РФ) не содержит понятия «экологическое преступление», однако такое понятие выработано в теории уголовного права.

Так, по мнению Б.В. Яценко, под экологическими преступлениями понимаются «предусмотренные главой 26 Уголовного кодекса Российской Федерации общественно опасные деяния, посягающие на общественные отношения по сохранению благоприятной окружающей среды, рациональному использованию ее ресурсов и обеспечению экологической безопасности населения» [2].

А.И. Чучаев определяет экологическое преступление как «предусмотренное уголовным законом Российской Федерации общественно опасное виновное деяние, посягающее на общественные отношения, связанные с обеспечением сохранения для нормальной жизнедеятельности человека благоприятной окружающей природной среды, рациональным использованием ее ресурсов и экологической безопасности населения» [3].

В свою очередь Чураков Д.Б. считает, что «экологическое преступление представляет собой запрещенное уголовным законом общественно опасное виновное деяние, объектом посягательства которого являются общественные отношения, связанные с обеспечением сохранения благоприятной окружающей среды, разумным использованием ее ресурсов и экологической безопасности населения, для нормальной жизнедеятельности человека» [4].

С точки зрения Э.Н. Жевлакова, под определением «экологические преступления» следует понимать «предусмотренные уголовным законодательством общественно-опасные, виновные, наказуемые деяния, нарушающие общественные отношения, связанные с сохранением качественно благоприятной окружающей среды, рациональным использованием ее ресурсов и обеспечением экологической безопасности населения» [5].

В арсенале отечественной теории уголовного права имеются и иные определения экологического преступления. Однако, как нам представляется, наиболее приемлемой следует считать такую формулировку: экологическое преступление – это общественно опасное деяние (действие или бездействие), предусмотренное уголовным законом, посягающее на установленный экологический правопорядок путем причинения вреда общественным отношениям по сохранению, восстановлению, рациональному использованию окружающей среды, а также ее компонентов и экологическую безопасность населения.

По нашему мнению, данная дефиниция охватывает всю совокупность компонентов объекта посягательства, в частности, «общественные отношения в сфере обеспечения экологической безопасности населения», «сохранности благоприятной для нормальной жизнедеятельности человека окружающей среды», «рациональное использование ее ресурсов». А потому, предлагаем внести дополнение в главу 26 УК РФ «Экологические преступления», путем включения легального определения экологического преступления. Подобного рода дополнение позволит оптимизировать систему и правоприменительную практику, которая имеет основополагающее значение для определения круга деяний, признаваемых экологическим преступлением.

Отметим, что за совершение многих экологических правонарушений установлена одновременно и административная и уголовная ответственность (незаконная охота, порча земли, незаконная порубка деревьев и кустарников и др.). При квалификации таких смежных правонарушений возникает необходимость их разграничения. На основе анализа статей УК РФ и КоАП РФ[6], в которых предусматривается ответственность за однородные экологические правонарушения, можно сделать однозначный вывод о том, что, как правило, граница между экологическим правонарушением и преступлением лежит не в диспозиции, а гипотезе соответствующей статьи УК РФ, в той части нормы, которая указывает на условия ее применения.

Вообще в теории уголовного права одной из главных проблем является проблема определения и разграничения правоохранительными органами и судом степени общественной опасности схожих общественно опасных деяний. Нередко на практике встречаются ситуации, где они могут выступать как в качестве преступления, так и административного правонарушения. Поэтому частенько в деятельности компетентных органов возникают ошибки по разграничению экологических преступлений и административных правонарушений. Вот для того чтобы избежать некорректных (неправосудных) приговоров и постановлений суда, мы настаиваем на необходимости устранения данного пробела законодательства.

Кроме того, на наш взгляд, в законодательной регламентации существует и такая проблема как некорректное использование биологических терминов и ошибочное представление об обязательных признаках объективной стороны при определении некоторых составов экологических преступлений, например, описываемого ст.259 УК РФ, является одной из важных проблем, влияющих на качество применения норм уголовного права [7]. Так, законодателем используется странный термин «критическое местообитание» (в биологии используется термин «критическая масса популяции», что имеет отношение к данному составу), так еще и анализируемый состав сконструирован как материальный. Особенностью конструкции его является акцент на действии «уничтожение» как на процессе, а не на результате. Поскольку гибель целой популяции

очень длительный процесс, то возникает сложность применения данной статьи на практике, так как появляется реально неразрешимая проблема доказывания причинно-следственной связи между уничтожением места обитания и гибелью популяции.

Серьезной проблемой для квалификации является наличие оценочных признаков, в частности такого, как «значительный ущерб» (ст. ст. 255, 262 УК РФ), который в официальных источниках не раскрывается. Постановление Пленума Верховного Суда РФ «О применении судами законодательства об ответственности за нарушения в области окружающей среды и природопользования» предлагает некоторые ориентиры при определении значительного ущерба для преступления, описываемого ст. 262 УК РФ, но в результате изучения решений данной проблемы на практике, следует констатировать трудности применения единообразного подхода.

Также существенным моментом, затрудняющим применение уголовного закона в сфере охраны природной среды, является постулат о субъекте преступления — физическом лице, который исключает уголовную ответственность юридических лиц. Как совершенно верно считает А.В. Щербаков: данный вопрос представляет серьезную проблему [8]. Традиционно в теории права многие исследователи придерживаются позиции относительно субъекта преступления, что им может быть только физическое лицо. С высокой степенью достоверности предполагаем, что ученые основываются на принципах личной и виновной ответственности, а также цели наказания. Однако в практической деятельности существует ряд проблем, связанных с привлечением к эколого-правовой ответственности только физических лиц. В настоящий момент исследование проблемы ответственности юридических лиц в уголовном праве остается актуальным. Считается, что эта мера будет способствовать повышению эффективности борьбы с данными преступлениями применяя ее в практической деятельности.

Согласимся с мнением Э. Жевлакова и Л. Иванова в том, что необходимость установления уголовной ответственности юридических лиц диктуется не только тяжелой экологической ситуацией, но и перспективами дальнейшего негативного влияния на природную среду различных отраслей хозяйствования. Имеет место точка зрения о том, что материальные возможности физических лиц по возмещению ущерба весьма ограничены, в то время как юридическое лицо может быть подвергнуто штрафу в большем размере [9].

Основываясь на вышесказанном, можно сделать следующие выводы: неэффективность уголовной ответственности за экологические преступления во многом связана с недостатками законодательного регулирования, к которым можно отнести: бланкетность большинства норм уголовного законодательства главы 26 УК РФ об экологических преступлениях; недостаточность санкций, не учитывающих степень общественной опасности многих преступлений в данной области; некорректное использование экологических терминов и отсутствие их разъяснения в уголовном законодательстве; отсутствие среди субъектов уголовной ответственности за экологические преступления юридических лиц.

ЛИТЕРАТУРА

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 17.06.2019) // Собр. законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.

2. Уголовное право Российской Федерации. Общая часть: Учеб. / МГЮА; Под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. – 2-е изд. перераб. и доп. – М.: ИНФРА-М: КОНТРАКТ, 2011. – С. 704.

3. Боровиков В.Б. Уголовное право. Особенная часть: учебник для среднего профессионального образования. – 4-е изд., перераб. и доп. – М.: Издательство Юрайт, 2018. – С. 81.

4. Чураков Д.Б. Особенности квалификации преступлений в сфере лесопользования // Законность. – 2015. – № 2. – С. 46.

5. Бриллиантова А. В. Уголовное право России: Части Общая и Особенная: учебники // М.: Проспект. - 2018. – С. 798.

6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 17.06.2019) (с изм. и доп., вступ. в силу с 01.07.2019) // Собр. законодательства Рос. Федерации. – 2002. – № 1 (ч. 1). – Ст. 1.

7. Щербакова О.А. Проблемные вопросы законодательной регламентации уголовной ответственности за преступления против безопасности животного мира // Юридические науки: проблемы и перспективы: материалы VI Междунар. науч. конф. (г. Казань, октябрь 2017 г.). – Казань: Бук, 2017. – С. 81-85. – URL <https://moluch.ru/co№f/law/archive/281/12937/> (дата обращения: 28.06.2019).

8. Щербаков А.В. Проблемы определения субъекта преступления в современном уголовном праве // Пробелы в юридическом законодательстве. – 2013. – №2. – С.100.

9. Тарайко В.И. Некоторые направления совершенствования специально-криминологических мер предупреждения экологических преступлений [Электронный ресурс] - URL : <https://cyberleninka.ru/article/v/nekotorye-napravleniya-sovershenstvovaniya-spetsialno-kriminologicheskikh-mer-preduprezhdeniya-ekologicheskikh-prestupleniy> (дата обращения: 12.05.2019).

СВЕДЕНИЯ ОБ АВТОРЕ

Коробов Геннадий Алексеевич. Доцент кафедры гражданско-правовых и экономических дисциплин. Кандидат юридических наук, доцент.

Воронежский институт МВД России

E-mail: genkorobov@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-53-68.

Азарова Ирина Владимировна. Старший преподаватель кафедры гражданско-правовых и экономических дисциплин.

Воронежский институт МВД России.

E-mail: aziravlad@rambler.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-53-68.

Korobov, Gennady Alekseevich. Associate Professor of the Department of civil law and economic disciplines. Candidate of law, associate Professor.

Voronezh Institute of MIA of Russian.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-53-68.

Azarov Irina Vladimirovna – senior lecturer of the Department of civil law and economic disciplines.

Voronezh Institute of MIA of Russian.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-53-68.

Домашний почтовый адрес (полностью): 394064, г. Воронеж, ул. Героев Сибириков, д. 65, кв. 126.

Ключевые слова: экологическое преступление, уголовная ответственность, критическое местообитание, значительный ущерб, субъект преступления.

Key words: environmental crime, criminal liability, critical habitat, significant damage, subject of crime.

УДК 349.6

Мазина Галина Павловна

ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЭКОЛОГИЧЕСКОГО ЗАКОНОДАТЕЛЬСТВА: ПОНЯТИЕ, ВИДЫ, ПРОБЛЕМЫ ОБОСНОВАНИЯ

LEGAL RESPONSIBILITY FOR VIOLATION OF THE ECOLOGICAL LEGISLATION: CONCEPT, TYPES, JUSTIFICATION PROBLEMS

Рассматриваются вопросы юридической ответственности за нарушение законодательства об охране окружающей среды, анализируются действующее законодательство и проблемы применения и обоснования видов.

Questions of legal responsibility for violation of the legislation on environmental protection are considered, the current legislation and problems of application and justification of types are analyzed.

Современные ученые считают, что человечество уже живет в разрушающемся мире в условиях нарастающего жестокого экологического кризиса, который превращается в кризис цивилизации. На грани веков резко возросло негативное антропогенное воздействие на природу (интенсивное развитие научно-технического прогресса и рыночной экономики, появление большого количества собственников-природопользователей, объективное усложнение различных сторон социальной жизни), в результате которого происходит истощение природных ресурсов, изменение качественных характеристик природных объектов (атмосфера, воды, земли), сокращение видового разнообразия животного и растительного мира.

В ряду основных принципов, на которых должно строиться взаимодействие общества, государства и природы, следует отметить: приоритет охраны жизни и здоровья человека; обеспечение благоприятных экологических условий для жизни, труда и отдыха населения; рациональное использование природных ресурсов и недопущение необратимых последствий для природы и здоровья человека; соблюдение требований природоохранительного законодательства и неотвратимость наступления ответственности за их нарушение.

Юридическая ответственность, являясь важнейшим межотраслевым институтом, направлена на восстановление нарушенного правопорядка и стимулирование граждан на общественно полезные действия. Однако в силу сложности экологических правоотношений и большого массива нормативных актов на федеральном и региональном уровнях ответственность в экологическом праве приобретает свою специфику.

В правовой науке вопросам юридической ответственности за экологические правонарушения уделялось большое внимание, начиная с 80-годов прошлого века, когда были изданы труды советских ученых – Колбасова, О.С., Краснова Н.И., Петрова В.В. и ряда других авторов, послужившие базой для совершенствования правового регулирования и развития научных исследований видов такой ответственности.

Традиционным является выделение административной, дисциплинарной, гражданско-правовой, уголовной ответственности. В Законе об охране окружающей природной среды 1991 года [7] за экологические правонарушения предусматривалась также и материальная ответственность (ст. 81), кроме того было дано понятие экологического правонарушения и экологического преступления. Ст. 75 действующего Закона об охране окружающей среды 2002 года [6] отмечает, что за нарушение законодательства в области охраны окружающей среды устанавливается имущественная, а не гражданско-правовая ответственность.

Субъектами экологических правонарушений в зависимости от степени их вредоносных деяний выступают физические лица (граждане РФ, иностранцы, апатриды, беженцы и переселенцы) и юридические лица, должностные лица госорганов исполнительной власти, органов местного самоуправления, а также юридических лиц.

Объектом правонарушений в экологической сфере является экологический правопорядок, цель которого – сохранить природные богатства и естественную среду обитания для человека и животного мира, предотвратить вредное воздействие хозяйственной деятельности человека на природу, улучшить качество окружающей среды.

Уголовный кодекс РФ [5] содержит составы экологических преступлений (гл.26), выявляя черты экологичности, противоправности и общественной опасности деяний. Подавляющее большинство диспозиций норм уголовного закона является бланкетными, требующими обращения к обширному, сложному по структуре и используемой специальной терминологии интенсивно развивающемуся экологическому законодательству – о лесах, землях, водах, недрах, растительном и животном мире, континентальном шельфе, особо охраняемых природных объектах и пр. Криминализация ряда статей была вызвана ростом производственных аварий, нарушением правил хранения опасных веществ на полигонах, мусорниках, складах, свалках и других объектах.

Меры административной ответственности (преимущественно в виде штрафа) предусмотрены за нарушения законодательства об охране природы действующим КоАП РФ (ст.ст. 8.1 – 8.39) [3], в том числе за нарушение или несоблюдение требований и правил:

- в градостроительной деятельности и эксплуатации предприятий, сооружений;
- в обращении с агрохимикатами и пестицидами;
- в использовании земель, недр, вод, лесов, растительного мира;
- охраны и использования ресурсов на особо охраняемых природных территориях.

Дисциплинарная ответственность (замечание, выговор, увольнение) предусмотрена на совершение дисциплинарного проступка работником при исполнении им своих трудовых обязанностей (Ст. 192 ТК РФ) [4]. Кроме того, одним грубых нарушений, приводящих к увольнению, является установление комиссией или уполномоченным по охране труда, нарушений работником правил, приводящих к тяжким последствиям ли-

бо создающим угрозу таких последствий – авария, катастрофа (пп. «д» п. 6 части 1 статьи 81 ТК РФ).

Основанием привлечения к гражданско-правовой ответственности за экологические правонарушения является ст. 15 ГК РФ [2], устанавливающая правило: лицо, право которого нарушено, может требовать полного возмещения причиненных ему убытков (т.е. расходов, которые лицо произвело или произведет впоследствии для восстановления нарушенного права, включая реальный ущерб и упущенную выгоду).

Противовиблистическую концепцию поддерживают современные теоретики и практики (С.А. Боголюбов, И.Ю. Ребиков, А.П. Анисимов, С.А. Чаркин и др.), рассматривающие причиненный экологическим правонарушением вред, как разновидность гражданско-правового вреда, который подлежит возмещению в рамках гражданско-правового института возмещения вреда (гл. 59 ГК РФ) [8].

Идея выделения самостоятельной эколого-правовой ответственности в науке экологического права, принадлежит советскому ученому В.В. Петрову. По его мнению, такому виду ответственности присущи следующие особенности: регулирование специальными нормативными актами; наличие объекта охраны (природные элементы, а не материальные продукты человеческого труда); взыскание ущерба по специальным таксам [11].

Этой же концепции придерживались А.И. Бобылев [12], считавший, что экологическая ответственность наступает за совершение экологического правонарушения, и Б.В. Ерофеев [10], рассматривавший юридическую и эколого-правовую ответственность в трех аспектах: как государственное принуждение к исполнению требований, предписанных законодательством; как правоотношение; как правовой институт.

М.М. Бринчук [9], пересмотревший свои противовиблистические взгляды, стал наиболее последовательным сторонником концепции самостоятельной эколого-правовой ответственности, строя свою теорию на том, что охраняемые законом экологические интересы имеют преимущественно публично-правовой характер. Он считает, что в случае причинения вреда природным объектам, которые находятся в публичной собственности, применяется не гражданско-правовая (имущественная), а эколого-правовая ответственность, содержащая два вида экологических правонарушений, предметом которых являются: 1) возмещение экологического вреда; 2) неисполнение или ненадлежащее исполнение обязанностей, предусмотренных договором на природопользование и охрану окружающей среды.

Тенденцией развития природоресурсного законодательства является совершенствование правового регулирования в сфере специального природопользования на основе договоров, нарушение условий которых является одним из видов экологического правонарушения. Пленум Верховного Суда РФ поставил знак равенства между гражданско-правовой и имущественной ответственностью, отметив, что такая ответственность за вред, причиненный окружающей среде, может возникать в результате нарушения договора в сфере природопользования, а также в результате внедоговорного (деликтного) причинения вреда [14].

Следует отметить, что, объектом деликтного обязательства может выступать имущество, жизнь и здоровье граждан, но не природная среда и ее компоненты, поскольку эти объекты не предусмотрены гражданским законодательством. При оценке ущерба, нанесенного отдельным природным объектам, например, лесу, водным объектам и их обитателям, следует руководствоваться позицией Конституционного Суда РФ [13] относительно содержания термина «ущерб, причиненный экологическим правонарушением». В контексте ст. 42 Конституции РФ [1] он включает: экологический вред окружающей среде; вред, причиняемый здоровью человека (социальный вред); вред

имуществу, находящемуся в частной или публичной собственности (экономический вред).

Отметим дополнения, внесенные в Закон 2002 года (ст.ст. 80.1 – 80.2), затрагивающие объекты вреда, причиненного прошлой хозяйственной деятельностью, выявление и оценку которых вправе проводить государственные органы федерального или регионального уровня или органы местного самоуправления. Объекты накопленного вреда подлежат учету и включению в госреестр, разделение на категории для выделения приоритетных объектов с целью ликвидации накопленного вреда в первоочередном порядке. Полагаем, что возмещение экологического вреда, причиненного в прошлом, должно производиться в рамках эколого-правовой ответственности.

Таким образом, сделаем ряд выводов.

На современном этапе институт юридической ответственности, в том числе применительно к сфере взаимодействия человека и природы, носит комплексный характер, исследованы уголовная, административная, гражданско-правовая, дисциплинарная, материальная, имущественная, конституционная, таксовая ответственность.

Природа в соответствии с природоресурсным законодательством, как правило, находится в публичной, государственной собственности, а экологические интересы, интересы поддержания благоприятного состояния окружающей среды, экологического благополучия носят преимущественно публично-правовой характер, и нарушение этого публичного интереса не может быть предметом и основанием гражданской ответственности. А потому предлагаем дополнить указанные в Законе 2002 года виды ответственности самостоятельным видом – эколого-правовая ответственность.

ЛИТЕРАТУРА

1. Конституция Российской Федерации от 12 декабря 1993 г. (в ред. Федерального конституционного закона от 21.07.2014 № 11-ФКЗ) // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.
2. Гражданский кодекс Российской Федерации. Части первая, вторая, третья и четвертая. – Издательство: Норматика. – 2018. – 608 с.
3. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собр. законодательства Рос. Федерации. – 2002. – № 1 (ч. I). – Ст. 1.
4. Трудовой кодекс Российской Федерации. – М. : Издательство «Омега-Л», 2019. – 230 с.
5. Уголовный кодекс РФ. – Издательство: Норматика. – 2019. – 240 с.
6. Об охране окружающей среды : федер. закон от 10 янв. 2002 г. № 7-ФЗ // Собр. законодательства Рос. Федерации. – 2002. – № 2. – Ст. 133.
7. Об охране окружающей природной среды : закон РСФСР от 19.12.91 № 2060-I // Вестник ВСНД РФ и ВС РФ. – 1992. – № 10. – Ст. 457.
8. Боголюбов С.А. Актуальные проблемы экологического права: Учебник. М., 2011. С. 18.
9. Бринчук М.М. Эколого-правовая ответственность — самостоятельный вид ответственности // Lex Russica. 2016. № 6. С. 26—47.
10. Ерофеев Б.В. Экологическое право: учеб. М., 2004.
11. Петров В. В. Правовая охрана природы в СССР. — М., 1984.
12. Юридическая ответственность за экологические правонарушения / под ред. А.И. Бобылева, Н.А. Духно. М., 2001. С. 12.
13. Постановление Конституционного Суда РФ от 2 июня 2015 г. № 12-П по делу о проверке конституционности части 2 статьи 99, части 2 статьи 100 Лесного ко-

декса Российской Федерации и положений Постановления Правительства Российской Федерации «Об исчислении размера вреда, причиненного лесам вследствие нарушения лесного законодательства» в связи с жалобой общества с ограниченной ответственностью «Заполярнефть» // СЗ РФ. 2015. № 24. Ст. 3547.

14. Постановление Пленума Верховного Суда РФ от 18 нояб. 2012 г. № 21 «О применении судами законодательства об ответственности за нарушения в области охраны окружающей среды и природопользования» // Бюллетень Верховного Суда РФ. – 2012. - № 12.

СВЕДЕНИЯ ОБ АВТОРЕ

Мазина Галина Павловна. Старший преподаватель кафедры гражданско-правовых и экономических дисциплин.

Воронежский институт МВД России.

E-mail: galina_mazina@mail.ru.

Россия, 394065, г. Воронеж, пр-т Патриотов, 53. Тел. (473) 2005372.

Mazina Galina Pavlovna. Senior teacher of department of civil and economic disciplines.

Voronezh Institute of MIA Russia.

E-mail: galina_mazina@mail.ru.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005372.

Ключевые слова: юридическая ответственность за экологические правонарушения, уголовная ответственность, административная ответственность, гражданско-правовая ответственность, дисциплинарная ответственность, эколого-правовая ответственность, ущерб, причиненный экологическим правонарушением.

Key words: legal responsibility for ecological offenses, criminal liability, administrative responsibility, civil responsibility, disciplinary responsibility, ekologo-legal responsibility, the damage caused by ecological offense.

УДК 349.6

ЭКСПЕРТ-БУХГАЛТЕР КАК СУБЪЕКТ БУХГАЛТЕРСКОЙ ЭКСПЕРТИЗЫ: ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ ОРГАНИЗАЦИОННО-ПРАВОВОГО СТАТУСА

EXPERT ACCOUNTANT AS THE SUBJECT OF ACCOUNTING EXPERTISE: DETERMINATION OF THE ORGANIZATIONAL-LEGAL STATUS

Усложнение процесса производства экспертных действий требует более тщательного и взвешенного подхода к организационно-плановым аспектам бухгалтерской экспертизы, что обуславливает важность определения и научного осмысления содержания организационно-правового статуса эксперта-бухгалтера как субъекта бухгалтерской экспертизы на современном этапе развития теории, практики и законодательства.

The complexity of the process of expert actions requires a more thorough and balanced approach to the organizational and planning aspects of accounting expertise, which determines the importance of determining and scientific understanding of the content of the organizational and legal status of the expert accountant as the subject of accounting expertise at the present stage of development of theory, practice and legislation.

Исторически складывающийся процесс усложнения производства бухгалтерской экспертизы требует всё более тщательного и взвешенного подхода к её организационным аспектам. Организационная стадия экспертной бухгалтерской работы рассматривается в современных условиях в основном с позиций взаимодействия эксперта-бухгалтера с уполномоченным органом (лицом), назначившим экспертизу, в рамках правового поля (административно-процессуального, уголовно-процессуального и др.). При этом недостаточно исследуются имеющиеся проблемы рациональной организации экспертной бухгалтерской деятельности, направленной на получение конечного результата [1, с. 24].

На практике перед уполномоченными органами и их должностными лицами (следователями, дознавателями, судьями и др.) остро встает проблема отбора эксперта-бухгалтера, которому будет поручено проведение судебно-бухгалтерской экспертизы, а также установление его компетентности и профессиональной подготовки.

Федеральным законом № 73-ФЗ определено: «должность эксперта в государственных судебно-экспертных учреждениях может занимать гражданин Российской Федерации, имеющий высшее профессиональное образование и прошедший последующую подготовку по конкретной экспертной специальности в порядке, установленном нормативными правовыми актами соответствующих федеральных органов исполнительной власти. Должность эксперта в экспертных подразделениях федерального органа исполнительной власти внутренних дел может также занимать гражданин Российской Федерации, имеющий среднее специальное образование. Определение уровня профессиональной подготовки экспертов при аттестациях на право самостоятельного производства судебной экспертизы осуществляется экспертно-квалификационными комиссиями в порядке, установленном нормативными правовыми актами соответствующих федеральных органов исполнительной власти. Уровень профессиональной подготовки экспертов подлежит пересмотру указанными комиссиями каждые пять лет» [2].

С учетом требований указанной нормы права силовые ведомства для потребностей своих экспертных подразделений готовят инструкции и требования по аттестации подчиненных экспертов всех необходимых специальностей. В органах внутренних дел в настоящее время разработаны и действуют два Положения, а именно:

- об условиях аттестации экспертов, осуществляющих самостоятельно производство судебных экспертиз, а также об определении компетенций и профессиональной подготовки экспертов;

- о Центральной экспертно-квалификационной комиссии МВД России [3]. Аналогичные нормативные акты, регламентирующие порядок аттестации и определения уровня квалификации экспертов-бухгалтеров, применяются и в Министерстве юстиции РФ.

Проведенный анализ различных источников научного и учебно-методического характера позволил выделить наиболее общие критерии компетентности эксперта-бухгалтера:

- наличие специальной экспертной подготовки;
- высшее профессиональное или среднее специальное экономическое образование;
- знание нормативно-правовых актов, регламентирующих производство экспертиз в соответствующей структуре;
- знание частных методик и техники экспертных исследований;
- периодическое повышение квалификации;
- опыт практической работы в области учетной, контрольно-ревизионной работы, аудиторской деятельности, преподавания экономических дисциплин.

Предложенный перечень профессиональных компетенций может стать основой формулировки требований к умениям, знаниям, уровню квалификации эксперта-бухгалтера при разработке соответствующего профессионального стандарта.

В ряде научных публикаций авторы приводят отдельные требования к эксперту, отраженные в различных нормативных правовых актах. Впервые сравнение такого статуса, упомянутого в нормативных актах, было осуществлено в работах Л.В. Каширской, которая проводит сопоставление статуса эксперта, основываясь на нормах пяти источников права: ФЗ № 73-ФЗ, АПК РФ, ГПК РФ, КоАП РФ и УПК РФ. По нашему мнению, подвергнутый сравнительному анализу перечень нормативных правовых актов требует дополнения еще двумя источниками, а именно – в сфере административного судопроизводства и в области налогового законодательства [1,4,5].

Результаты проведенного сравнительного анализа представлены в таблице 1.

Таблица 1

Результаты сравнительного анализа статуса эксперта и требований, предъявляемых к нему, в соответствии с нормативными документами

Нормативный документ	Положение нормативного документа, отражающее статус эксперта и требования, предъявляемые к нему
1	2
О государственной судебно-экспертной деятельности в Российской Федерации : федеральный закон от 31.05.2001 № 73-ФЗ (статьи 12, 13)	«...аттестованный работник государственного судебно-экспертного учреждения, производящий судебную экспертизу в порядке исполнения своих должностных обязанностей». «...имеющий высшее профессиональное образование и прошедший последующую подготовку по конкретной экспертной специальности в порядке, установленном нормативными правовыми актами соответствующих федеральных органов исполнительной власти. Должность эксперта в экспертных подразделениях федерального органа исполнительной власти внутренних дел может также занимать гражданин Российской Федерации, имеющий среднее специальное образование» [2].
Уголовный кодекс Российской Федерации от 13 июня 1996 г. 63-ФЗ (статья 57)	«...лицо, обладающее специальными знаниями и назначенное в порядке, установленном настоящим Кодексом, для производства судебной экспертизы и дачи заключения».
Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (статья 79)	«...специальные знания в различных областях науки, техники, искусства, ремесла».

1	2
Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ (статья 55)	«...лицо, обладающее специальными знаниями по касающимся рассматриваемого дела вопросам и назначенное судом для дачи заключения в случаях и в порядке, которые предусмотрены настоящим Кодексом».
Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (статья 25.9)	«...любое не заинтересованное в исходе дела совершеннолетнее лицо, обладающее специальными познаниями в науке, технике, искусстве или ремесле, достаточными для проведения экспертизы и дачи экспертного заключения».
Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ (статья 95)	«...специальные познания в науке, искусстве, технике или ремесле. Вопросы, поставленные перед экспертом, и его заключение не могут выходить за пределы специальных познаний эксперта».
Кодекс административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ (статья 49)	«...лицо, которое обладает специальными знаниями и которому в случаях и порядке, предусмотренных настоящим Кодексом, поручено провести экспертизу и дать заключение по вопросам, поставленным перед ним и требующим специальных знаний, в целях выяснения обстоятельств по конкретному административному делу».

Анализируя положения рассмотренных нормативно-правовых актов, тем или иным образом регламентирующих положение эксперта или требования, предъявляемые к нему, считаем необходимым констатировать следующее:

1. По нашему мнению, ссылка в нормативных документах при отражении статуса эксперта на порядок, закрепленный в действующем законодательстве, является также неуместной. Считаем, что понятие эксперта и его правовой статус должны быть разработаны на основе единого системного подхода и сформулированы в наиболее универсальном виде, отвечающем потребностям практики.

2. В представленных источниках отмечаются разные характеристики статуса эксперта. Так, дача заключения экспертом упоминается в четырех источниках из семи. Специальные знания (познания) – в шести из семи. Постановка вопросов перед экспертом отражена в трех актах из семи и т.д. Результаты проведенного категориального анализа определений эксперта отражены в таблице 2 [5].

Как видно из материалов таблицы 2, у законодателя нет единого мнения о статусе и определении эксперта. Такая же ситуация преобладает в учебно-методической и научной литературе. В связи с этим, по нашему мнению, назрела необходимость в выработке и уточнении единого общего подхода к формулированию понятия «эксперт».

С этой целью на основании проведенного анализа статуса эксперта и требований, предъявляемых к нему в соответствии с нормативными документами, нами сформулировано универсальное определение эксперта, отвечающее потребностям практики и требованиям законодательства, а именно: это назначенное в установленном порядке незаинтересованное лицо, имеющее знания в определенной сфере деятельности, а также компетенции для ответов на поставленные вопросы и дачи экспертного заключения.

С учетом результатов проведенного исследования, касающегося статуса и понятия эксперта, следует разработать определение категории «эксперт-бухгалтер», ориентированное на имеющиеся подходы в нормативных правовых актах, источниках учебно-методического и научного характера.

Таблица 2

Результаты категориального анализа определений эксперта,
приведенных в нормативных правовых актах

Нормативный документ	Элементы характеристики статуса эксперта					
	дача заключения	специальные знания	поставка вопросов в пределах компетенции	не заинтересованное в исходе дела лицо	совершеннолетнее лицо	назначение в установленном порядке
1	2	3	4	5	6	7
Федеральный закон № 73-ФЗ (статьи 12, 13)	-	+	-	-	-	+
УПК РФ (статья 57)	+	+	-	-	-	+
ГПК РФ (статья 79)	-	+	-	-	-	-
АПК РФ (статья 55)	+	+	+	-	-	+
КоАП РФ (статья 25.9)	+	+	-	+	+	-
НК РФ (статья 95)	+	+	+	-	-	-
КАС РФ (статья 49)	+	+	+	-	-	+

Исходя из этого, считаем возможным предложить следующее определение эксперта-бухгалтера на основе разработанного определения эксперта: это назначенное в установленном порядке незаинтересованное лицо, имеющее знания в правовой сфере, бухгалтерском учете, финансовом контроле и анализе финансово-хозяйственной деятельности, достаточные для проведения экспертизы по поставленным уполномоченным органом (лицом) вопросам и дачи экспертного заключения [6].

Данное определение содержит все значимые составляющие организационно-правового статуса эксперта-бухгалтера (его независимость, уровень полномочий, спектр специальных знаний, которыми он должен обладать).

В связи с разработкой данного определения предлагается внести изменения в приказ МВД России от 09.01.2013 № 2 в части разграничений полномочий и специальных знаний экспертов экономической специальности, а именно – в приложение № 1 к приказу (Перечень экспертных специальностей, по которым в МВД России осуществляется аттестация экспертов, дающая право самостоятельно проводить судебные экспертизы, а также пересматривается уровень квалификации экспертов) [3].

Расширение перечня нормативных документов, определяющих организационно-правовой статус эксперта, позволило не только расширить диапазон сравнения статусных требований, но и осуществить анализ различных критериев содержания правового статуса эксперта, закрепленных в действующем законодательстве. Результаты проведенного анализа дают возможность разработать единый подход к статусу эксперта вообще и эксперта-бухгалтера в частности, и стать основой формулировки требований к умениям, знаниям, уровню квалификации эксперта-бухгалтера при разработке соответствующего профессионального стандарта.

Таким образом, на основании сравнительного анализа статуса эксперта и требований, предъявляемых к нему, в соответствии с нормативными правовыми актами, а также в результате категориального анализа определений эксперта, приведенных в нормативных правовых актах, можно утверждать о разработке авторских определений эксперта и эксперта-бухгалтера, максимально отвечающих потребностям практики и требованиям законодательства, содержащим все необходимые статусные элементы экспертной деятельности.

ЛИТЕРАТУРА

1. Белов А.А. Судебно-бухгалтерская экспертиза / А.А. Белов, А.Н. Белов. – Москва : Книжный мир, 2003. – 608 с.
2. О государственной судебно-экспертной деятельности в Российской Федерации : федеральный закон от 31.05.2001 № 73-ФЗ (ред. от 08.03.2015) // Собрание законодательства РФ. – 2001. – № 23. – Ст. 2291.
3. Вопросы определения уровня профессиональной подготовки экспертов в системе МВД России : приказ МВД России от 09.01.2013 № 2 (ред. от 11.10.2018) (вместе с Положением об аттестации экспертов на право самостоятельного производства судебных экспертиз и о порядке пересмотра уровня их профессиональной подготовки в системе Министерства внутренних дел Российской Федерации, Положением о Центральной экспертно-квалификационной комиссии Министерства внутренних дел Российской Федерации) // Российская газета. – 2013. – 8 мая.
4. Каширская Л.В. Методология и организация бухгалтерской экспертизы в бюджетных учреждениях : дис. ... д-ра экон. наук : 08.00.12 / Каширская Любовь Васильевна. – Москва, 2013. – 286 с.
5. Мальцев Е.П. Организационно-плановая документация бухгалтерской экспертизы / С.А. Звягин, Е.П. Мальцев // Международный бухгалтерский учет. – 2018. – Т. 21. – №5. – С. 543-558. – (авторских 1 п.л.).
6. Звягин С.А. Управление процессом бухгалтерской экспертизы в современных условиях / С.А. Звягин, Е.П. Мальцев // Вестник Воронежского государственного университета. Серия: Экономика и управление. – 2017. – №4. – С. 24-28. – (авторских 0,31 п.л.).

СВЕДЕНИЯ ОБ АВТОРЕ

Мальцев Евгений Павлович. Преподаватель кафедры административного права.
Воронежский институт МВД России.
E-mail: madm86@mail.ru
Россия, 394065, Воронеж, просп. Патриотов, 53. (473) 200-52-73.

Maltsev Evgeny Pavlovich. Teacher of the Department of administrative law.
E-mail: madm86@mail.ru
Voronezh Institute of MIA Russia.
Work address: Russia, 394065, Voronezh, Prospekt Patriotov, 53.
Tel. (473) 200-52-73.

Ключевые слова: бухгалтерская экспертиза, эксперт-бухгалтер, заключение эксперта-бухгалтера, управление бухгалтерской экспертизой.

Key words: examination, forensic accounting, expert accountant, expert accountant, process accounting expertise.

УДК: 330

ПРАВОВОЙ СТАТУС СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

LEGAL STATUS OF EMPLOYEES OF BODIES INTERNAL AFFAIRS

В статье рассматривается правовая природа статуса сотрудников органов внутренних дел, соотношение понятий «правовой статус» и «правовое положение». Нормативное регулирование правового статуса сотрудников органов внутренних дел.

The article discusses the legal nature of the status of employees of internal affairs bodies, the relationship between the concepts of "legal status" and "legal status". Regulatory regulation of the legal status of employees of internal affairs bodies.

Термин «status» имеет латинское происхождение и в переводе на русский язык означает «стояние, поза, положение». В современном русском языке термин «статус» используется для характеристики положения субъекта в различных сферах, например, «социальный статус», «культурный статус», «правовой статус».

С позиции оценки человека, как субъекта правоотношений именно правовой статус имеет первостепенное значение, поскольку конституирует совокупность полномочий и обязанностей данного субъекта. Например, в юридической литературе советского периода отмечалось, что «правовой статус граждан СССР включает основные права и обязанности, которые определены Конституцией СССР [1].

В современных научных источниках понимание правового статуса субъекта не имеет принципиальных отличий от его традиционного исторического значения, но дополняется отдельными уточняющими деталями. Так, Рассказов Л.П. трактует правовой статус, как «юридически закрепленное положение личности в обществе» [2]. Аналогичной точки зрения придерживается Ю.Н. Стариков, квалифицируя правовой статус личности, как юридическое (т.е. правовое) закрепление положения личности в обществе [3]. Правовой статус, как правовая категория неоднократно рассматривался в рамках диссертационных исследований. В кандидатской диссертации Бабенко С.В. в качестве правового статуса личности понимает важнейшую политико-правовую категорию, которая объединяет права, свободы, обязанности и ответственность, признаваемые государством за гражданами, формально закрепленные в нормативно-правовых актах и гарантируемые законом, в соответствии с которым, личность как субъект права соотносит свое поведение в обществе [4].

Таким образом, правовой статус личности неразрывно связан с формально-юридическим закреплением прав и обязанностей личности, то есть, фиксированием их в нормативных правовых актах. В связи с этим в научной литературе, нормативных актах применяется, наряду с термином «правовой статус» словосочетание «правовое положение». В частности, в Федеральном законе «О полиции» глава 6 имеет название «Правовое положение сотрудника полиции», в то же время в пункте 29, части 3, статьи 17 рассматриваемого закона термин «статус» применяется в отношении вынужденных переселенцев [5]. Таким образом, к сотрудникам полиции применен термин «правовое положение», а в отношении вынужденных переселенцев использован термин «статус». Иной подход в отношении терминологии можно отметить в тексте Федерального закона «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» [6], так как глава 3 в данном законе называется «Правовое положение (статус) сотрудника органов внутренних дел». Как видно, в данном случае законодатель применяет словосочетания «правовое

положение» и «статус» как равнозначные. Аналогичная редакция использована в Федеральном законе «О государственной гражданской службе Российской Федерации», где глава 3 озаглавлена «Правовое положение (статус) гражданского служащего». В Федеральном законе «О службе в таможенных органах Российской Федерации» применен термин «правовое положение». Как зафиксировано в тексте указанного закона, он «определяет порядок прохождения службы в таможенных органах и организациях Федеральной таможенной службы (далее - таможенные органы) и основы правового положения должностных лиц таможенных органов» [7].

Приведенные примеры свидетельствуют об отсутствии единых подходов в законодательной технике в отношении юридических конструкций, применяемых в текстах нормативных актов. Однако, несмотря на применение разных терминов («правовое положение» и «правовой статус») их смысловое содержание в нормативных актах совпадает. Это позволяет сделать вывод о том, что «правовое положение» и «правовой статус» термины аналогичные по смыслу и содержанию.

Исходя из высокой значимости деятельности органов внутренних дел в любом государстве, определяемой вопросами обеспечения национальной безопасности, наличием права применять от имени государства меры принуждения, правом владения и применения оружия правовой статус сотрудников этих органов регламентируется значительным количеством нормативных актов, как на международном уровне, так и на уровне национального законодательства.

В качестве примера международных актов можно привести Устав Международной организации уголовной полиции Интерпола [8], Решение ЕС от 06 апреля 2009 года № 2009/371/ПВД «О создании Европейского полицейского ведомства (Европол)» (Конвенция о Европоле) [9], Постановление Генеральной ассамблеи ООН от 17 декабря 1979 г. N 34/169 «О морально-нравственном поведении служащих, претворяющих законы» [10] и другие.

Поскольку служба в органах внутренних имеет неразрывную связь с гражданством общих правовой статус сотрудников, как граждан Российской Федерации определен в Конституции РФ. Сотрудники органов внутренних дел обладают правами и свободами, зафиксированными в главе 2 Конституции РФ. Вместе с тем правовой статус сотрудников органов внутренних дел имеет особенности, обусловленные в том числе конституционными нормами. Так, статья 55 Конституции РФ допускает ограничение прав и свобод человека и гражданина на основе федерального закона в интересах защиты государства и общества. Как известно, специальный правовой статус сотрудников органов внутренних дел предусматривает ограничения и запреты, установленные специальными законами «О полиции», «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации».

Правовой статус субъекта определяется, прежде всего, его связью с государством. Для сотрудников органов внутренних дел такая связь обусловлена назначением, характером, задачами, функциями органов внутренних дел. Служба в органах внутренних дел является федеральной государственной службой, что прямо закреплено в тексте статьи 1 Федерального закона «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». Служба в органах внутренних дел представляет собой профессиональную деятельность на должностях в рассматриваемых органах, а также в других органах, не являющихся органами внутренних дел, в случаях, предусмотренных законом. В связи с этим логично сделать вывод о том, что сотрудники органов внутренних дел являются государственными служащими.

Вместе с тем, признание сотрудников органов внутренних дел в качестве государственных служащих является новацией последних лет развития Российской Федерации. В советский период служба внутренних дел регламентировалась на подзаконном уровне Положением о советской милиции, утвержденным Постановлением Совета Министров СССР 17 августа 1962 года. В Положении о советской милиции прежде всего был зафиксирован правовой статус милиции, как административно-исполнительного органа

Советского государства, в главе 4 регламентировались в общих чертах условия службы в милиции, а в главе 5 материальное обеспечение советской милиции. Как таковой, правовой статус сотрудников милиции в тексте Положения о советской милиции определен не был.

Принятый в 1991 году Федеральный закон «О милиции» [11] также, как и Положение о советской милиции четко не определил правовой статус сотрудников милиции. Продолжая традицию Положения о советской милиции в статье 1 названного закона разъяснялся статус милиции, как системы государственных органов исполнительной власти, обязанных выполнять перечисленные в законе функции. В статье 17 Федерального закона «О милиции» было зафиксировано определение сотрудника милиции, как гражданина Российской Федерации, имеющего специальное звание, предусмотренное для сотрудников милиции, служащего в должности рядового или начальствующего состава органов внутренних дел. Таким образом, обобщая информацию из приведенных выше норм можно сделать вывод о том, что органы милиции отнесены к системе государственных органов исполнительной власти, а сотрудники милиции проходят службу в этих органах.

Вместе с тем текст Федерального закона «О милиции» не давал однозначного ответа на вопрос о правовом статусе сотрудников милиции, то есть, являются ли они государственными служащими или нет.

Ясную определенность по вопросу о правовом статусе сотрудников органов внутренних дел внес Федеральный закон «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации». В статье 1 закона установлено, что служба в органах внутренних дел является федеральной государственной службой. Следовательно, лица, проходящие службу в органах внутренних дел на соответствующих должностях, являются государственными служащими.

Рассматривая вопрос о правовом статусе сотрудников органов внутренних дел нельзя обойти вниманием факт внесения изменений в 2015 году в Федеральный закон «О системе государственной службы Российской Федерации» [12]. Как известно, с 1 января 2016 года Федеральным законом «О системе государственной службы Российской Федерации» предусматриваются, определенно, два вида федеральной государственной службы, это государственная гражданская служба, военная служба, и неопределенно, государственная служба иных видов. Напомним, что в действовавшей ранее редакции рассматриваемого закона упоминалась правоохранительная служба. Таким образом, представлялось правомерным сделать вывод о том, что сотрудники органов внутренних дел являясь федеральными государственными служащими проходят службу в органах, относящихся к правоохранительным, то есть, государственную правоохранительную службу.

По всей видимости, изменения в Федеральный закон «О системе государственной службы Российской Федерации», в части видов федеральной государственной, том числе, были внесены в связи с неопределенностью на теоретическом и практическом уровне в вопросе о понятии правоохранительной службы и правоохранительных органах. Однако исключение из текста закона термина «правоохранительная служба» послужило основанием для возобновления дискуссии о статусе сотрудников органов внутренних дел и в первую очередь это связывается с тем, что вид федеральной государственной службы для них в настоящее время не определен, так как обозначен в тексте федерального закона, как «государственная служба иных видов».

Представляется, что отказ на законодательном уровне от термина «правоохранительная служба», конечно же не должен восприниматься, как ограничение сектора правоохранительной деятельности как одной из государственных функций, и не приведет к сокращению видов правоохранительных органов. Служба, связанная с правоохранительной деятельностью, продолжает оставаться одним из узаконенных видов федеральной государственной службы. Примером этому может послужить ч. 3 ст. 5 Федерального закона от 5 декабря 2005 г. № 154-ФЗ «О государственной службе российского казачества» [13], в которой установлено, что «российское казачество проходит федеральную государственную службу, связанную с правоохранительной деятельностью, в соответствии с федеральным законодательством». Необходимо отметить, что служба, связанная с правоохранительной деятельностью, харак-

теризуется, как общими признаками, отличающими все виды государственной службы от других видов деятельности, так и специфическими признаками.

Принимая во внимание институциональное значение Федерального закона «О системе государственной службы Российской Федерации» необходимо совершенствовать его нормы на основе потребностей общества и государства, учитывая исторические, национальные правовые традиции, зарубежный опыт законоотворчества в области построения и организации государственной службы. Системный подход в построении отдельных видов федеральной государственной службы видится в том, что Федеральный закон «О системе государственной службы Российской Федерации» устанавливает отдельные виды государственной службы, правовое регулирование которых детализируется в специальных законах о соответствующем виде государственной службы. В настоящее время такое соответствие имеется в отношении государственной гражданской службы, военной службы. Применительно к службе в органах внутренних дел такое соответствие отсутствует, поскольку приняты специальные законы о полиции и органах внутренних дел, но в общем законе служба в этих органах не обозначена, так как предполагается, что она относится к «государственной службе иных видов».

Таким образом, нормы Федерального закона «О системе государственной службы Российской Федерации» целесообразно совершенствовать, в частности, по пути дальнейшей конкретизации таких понятий, как «государственная служба иных видов».

Учитывая тот факт, что под определение «правоохранительные органы» подходит значительное количество государственных органов, относящихся к различным министерствам и ведомствам, моно регулирование их деятельности маловероятно. В связи с этим, реальным представляется предложение о принятии по аналогии с Федеральным законом «О статусе военнослужащих» Федерального закона «О статусе сотрудников органов внутренних дел».

Важным элементом правового статуса сотрудников органов внутренних дел являются сформулированные в соответствующих законах дефиниции, должностных лиц, например, «сотрудник полиции», «военнослужащий», «гражданский служащий». Дефиниция сотрудника полиции, сформулированная в статье 25 Федерального закона «О полиции» устанавливает, что это гражданин Российской Федерации, осуществляющий служебную деятельность в должностях федеральной государственной службы в органах внутренних дел, имеющий специальное звание, которые присваиваются сотрудникам полиции.

В последнее время в специальной литературе отдельные авторы применяют к сотрудникам полиции словосочетание «служащий полиции». Такая терминология представляется не соответствующей действующему законодательству. Во-первых, статья 25 Федерального закона «О полиции» имеет название «Сотрудник полиции», а не «служащий полиции». Во-вторых, в текстах специальных законов («О полиции», «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации») термин «служащий» применяется только к государственным гражданским служащим.

Примером иной практики может послужить зарубежное законодательство. Так, на сайте Police-Nationale.net правовой статус сотрудника полиции в популярной форме определяется следующим образом: сотрудники национальной полиции являются служащими государственной гражданской службы при Министерстве внутренних дел. В то же время: жандармы - это военнослужащие, которые имеют двойное подчинение Министерству внутренних дел и Министерству обороны Франции. Муниципальные полицейские - это территориальные чиновники, нанятые мэром коммуны. В государствах, в которых законодательство формировалось под влиянием колониальных традиций Великобритании смысл определения сотрудника полиции можно изложить следующим образом: это лицо, которое состоит в должности в полицейских органах, либо назначено на службу в Полицейские силы [15]. При этом сотрудник полиции обозначается, как «police officer», что нередко переводят на русский язык, как «офицер полиции», что не соответствует смыслу ан-

гбийского термина, так как более правильный перевод на русский язык идентичен термину «служащий полиции» или «полицейский служащий».

Обобщая сказанное выше следует отметить, что статус сотрудников органов внутренних дел нуждается в дальнейшем совершенствовании как на уровне правового регулирования, так и в его содержательной части.

ЛИТЕРАТУРА

1. Богуславский М.М., Козырь М.И., Миньковский Г.М. и др. — М.: Сов. Энциклопедия, 1984 — С. 358.
2. Рассказов Л.П. Теория государства и права: Учебник для вузов. — 6-е изд. — М.: РИОР: ИНФА-М, 2014. — С.167.
3. Общее административное право: учебник: в 2 ч. /под ред. Ю.Н. Старилова; Воронежский государственный университет. — 2-е изд., пересмотр. и доп. — Воронеж: Издательский дом ВГУ, 2016. — С. 169.
4. См.: Бабенко С.В. Правовой статус личности в правовом государстве: вопросы теории: автореф. дисс. ... канд. юрид. наук. Краснодар, 2008.
5. Собрание законодательства РФ. — 2011. — № 7. — Ст. 900.
6. Собрание законодательства РФ. — 2011. — № 49 (ч.1). — Ст. 7020.
7. Собрание законодательства РФ. — 1997. — № 30. — Ст. 3586.
8. "Международное публичное право": Сборник документов, том 2, М.: БЕК, 1996.
9. Решение ЕС от 06 апреля 2009 года № 2009/371/ПВД «О создании Европейского полицейского ведомства (Европол)». — [Электронный ресурс]. — Режим доступа: <http://docs.pravo.ru/document/view/24869591>.
10. Информационно справочная система Консультант Плюс (Дата обращения: 14.06.2019 г.).
11. Ведомости СНД и ВС РСФСР. — 1991. — № 16. — Ст. 503.
12. Собрание законодательства РФ. — 2003. — № 22. — Ст. 2063.
13. Собрание законодательства РФ. — 2005. — № 50. — Ст. 5245.
14. La Police Nationale Française. — [Электронный ресурс]. — Режим доступа: <https://www.police-nationale.net/police-nationale/#differences-police-nationale-municipale-gendarmerie>.
15. POLICE ACT. Act 19 of 1974 – 1 August 1974. — [Электронный ресурс]. — Режим доступа: <http://www.icla.up.ac.za/images/un/use-of-force/Africa/Mauritius/Police%20Act%20Mauritius%201974>.

СВЕДЕНИЯ ОБ АВТОРАХ

Матвеев Сергей Прокофьевич. Профессор кафедры гражданско-правовых и экономических дисциплин. Доктор юридических наук, доцент.

Воронежский институт МВД России.

E-mail: ser35031333@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел.(473)200-53-05.

Matveev Sergey Prokofievich. Professor of the chair of Civil and Economic. Disciplines. Doctor of Law, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: ser35031333@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel.:(473)200-53-05.

Ключевые слова: полиция; сотрудники органов внутренних дел, правовой статус, правовое положение.

Key words: police; police officers, legal status, legal status

УДК 342

Мещерякова Елена Ивановна,
доктор педагогических наук, профессор

МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ЭКОНОМИКО-ПРАВОВОМУ АНАЛИЗУ ПРЕСТУПЛЕНИЙ В СФЕРЕ БЮДЖЕТНОЙ ДЕЯТЕЛЬНОСТИ

METHODOLOGICAL APPROACHES TO ECONOMIC AND LEGAL ANALYSIS OF CRIMES IN THE SULFUR BUDGET ACTIVITIES

В статье рассматриваются перспективы использования синергетического методологического подхода в качестве ведущего в процессе проведения исследований преступности в сфере бюджетной деятельности.

The article discusses the prospects for the use of a synergistic methodological approach as the lead in the process of conducting studies on crime in the SULFUR budget activities.

Исследование проблем, связанных с предупреждением и пресечением преступности в сфере бюджетной деятельности, продолжает оставаться актуальным на протяжении последних десятилетий. В соответствии с информацией, приведенной в ежегодном отчете Счетной палаты РФ, размещенном на официальном сайте, в 2018 году общая сумма нарушений и выявленных недостатков при поступлении и использовании бюджетных средств в денежном выражении составила 772 млрд.руб., однако при этом в бюджет удалось вернуть в 102,3 раза меньше – 7, 56 млрд.руб. [1, с.18-19]. По мнению председателя Счетной палаты РФ А.Л. Кудрина, «неправильно проводятся процедуры закупок, завышены цены, очень много омертвлено средств на недостроенные объекты или на объекты, которые просто простаивают, не использованы средства на счетах месяцами. Кроме того, несколько миллиардов утрачено – то есть, по сути, своровано» [2]. В то же время, к административной ответственности были привлечены всего лишь 130 лиц, уплативших штрафы на сумму 15,2 млн рублей. А в прокуратуру и следственные органы были переданы только 105 материалов, по которым возбуждено 35 уголовных дел. Очевидно, даже должным образом расследованные и доведенные до суда 35 уголовных дел вряд ли позволят возместить причиненный бюджетной сфере ущерб.

Все это красноречиво свидетельствует о том, что необходимо изучать, искать и находить эффективные способы защиты бюджетных интересов государства от преступных посягательств, уметь предупреждать преступления в сфере бюджетной деятельности, привлекать виновных к уголовной ответственности, возмещать причиненный бюджетной сфере ущерб. Важную роль в этой сложной правоохранительной деятельности могут сыграть исследования преступности в бюджетной сфере, проводимые на стыке двух направлений – экономического и правового.

Вряд ли вызывает сомнение утверждение о том, что экономический и правовой анализ в процессе проведения исследований преступности в сфере бюджетной деятельности неразрывно связаны. Ведь именно право не только формирует нормативный эквивалент развивающихся экономических отношений в бюджетной сфере, но и является тем универсальным инструментом управления, который способен обеспечить решение многих судьбоносных для государства проблем. При этом методологические аспекты экономико-правового анализа преступлений в сфере бюджетной деятельности важно рассматривать как основополагающее направление исследований, осуществляемых в сфере борьбы с экономической преступностью и обеспечения экономической безопасности государства. Однако именно методологические аспекты не получают должного

обоснования в проводимых экономико-правовых исследованиях, в том числе и связанных с анализом преступлений в сфере бюджетной деятельности, чем объясняется, на наш взгляд, недостаточная эффективность таких исследований. Как справедливо замечает д.ю.н., профессор Т. Я. Хабриева, «экономико-правовой анализ пока еще не имеет разработанной методологической базы, а отраслевая дифференциация знаний не позволяет достичь эффективности управления общественными процессами» [3, с.8].

В то же время, по нашему убеждению, обоснованный выбор и грамотное использование методологических подходов, соответствующих целям исследования проблем преступности в сфере бюджетной деятельности позволяет:

- 1) определить методологию исследования, построить его концепцию, выработать категориальный аппарат, содержательно наполнить исследование;
- 2) выстроить исследование в строгом соответствии с избранными методологическими подходами и тем самым сформировать его теоретические основы, вместе с тем обогатив область экономико-правового познания;
- 3) провести анализ правоприменительной практики, выявить те ключевые направления, в которых необходимо действовать для предупреждения и пресечения преступлений в сфере бюджетной деятельности.

Изучение диссертационных исследований, проведенных в последнее десятилетие, позволило установить, что в экономических исследованиях (специальность 08.00.01 – Экономическая теория, диссертации на соискание ученой степени доктора экономических наук Л.А. Карасевой, А.Н. Неверова, П.Н. Клюкина, В.Н. Немцева, А.Б. Кцоева, С.И. Кретьева, Г.М. Колпаковой, А.В. Никитова, Г.А. Щербакова) преобладают следующие методологические подходы: функционально-описательный; системно-воспроизводственный; диалектико-материалистический; субъективно-идеалистический и др. Что касается правовых исследований, то в них доминируют аксиологический; герменевтический; прагматический; феноменологический; культурно-исторический; синергетический и др. подходы (специальность 12.00.01 – Теория и история права и государства; история учений о праве и государстве, диссертации на соискание ученой степени доктора юридических наук И.Ю. Ташбековой, Л.А. Петручака, Е.Ю. Догадайло, Г.С. Беляевой, Н.В. Исаевой, А.В. Серегина, Г.М. Азнагуловой, Е.В. Резникова, Г.М. Лановой). При этом все исследователи уверены в том, что в использовании методологических подходов объединяющим выступает системный подход, в соответствии с которым методологию исследования формируют несколько подходов, в ряду которых выделяется основной, системообразующий.

Обоснованный выбор и грамотное использование методологических подходов, соответствующих целям исследования проблем преступности в сфере бюджетной деятельности позволяет, во-первых, определить методологию исследования, построить его концепцию, выработать категориальный аппарат, содержательно наполнить исследование; во-вторых, выстроить исследование в строгом соответствии с избранными методологическими подходами и их принципами, сформировав тем самым его теоретические основы, а вместе с тем обогатить область экономико-правового познания; в-третьих, провести анализ правоприменительной практики, выявить те ключевые направления, в которых необходимо действовать для предупреждения и пресечения преступлений в сфере бюджетной деятельности.

Однако система методологических подходов к исследованию проблем, связанных с экономико-правовым анализом преступлений в сфере бюджетной деятельности, – это одна из составляющих методологии, которую исследователь разрабатывает для изучения выявленных и определенных им проблем (аспектов проблемы), связанных с преступлениями в бюджетной сфере. Мы определяем методологию экономико-правового исследования преступлений в бюджетной деятельности как его логическую

организацию, предполагающую целостное осознание цели, выявление существующих в установленном предмете исследования и связанных с достижением его цели проблем, выбор методов, способов и приемов исследования, установление принципов проведения исследования и рациональной последовательности действий при его проведении.

Очень важно подчеркнуть, что методология экономико-правового исследования преступлений в бюджетной деятельности должна формироваться исследователем с учетом определенных уровней. Высший уровень – философская методология, которой определяются общие принципы познания, категориальный строй, проблематика как целостное явление. Общенаучный уровень, представляющий содержательные общенаучные концепции, которые выполняют методологические функции и воздействуют на фундаментальные характеристики экономики и права одновременно, но, возможно, в разной степени. Конкретно-научный уровень – методология экономико-правового исследования, определяемая методологией каждой конкретной науки и их взаимодействием, интеграция методов, приемов, способов, процедур исследования, присущих этим наукам. И завершающей, приближенной к объекту и предмету исследования, становится построенная на избранных методологических подходах и определенных принципах методика и техника научного исследования преступности в сфере бюджетной деятельности, представляющая набор процедур, обеспечивающих достижение установленной цели и получение запланированного результата.

Соглашаясь с тем, что в системе методологических подходов важно выделить основной (системообразующий), для проведения экономико-правового анализа преступлений в сфере бюджетной деятельности мы предлагаем использовать синергетический подход. Наша позиция согласуется с позициями многих исследователей, которые рассматривают синергетику не как новомодное увлечение, а как науку о законах самоорганизации сложных развивающихся систем, одна из важнейших задач которой состоит в организации упорядоченности их элементов. Нельзя не согласиться с одним из таких исследователей К.В.Шундиковым, который уверен, что «попытка применения синергетической методологии к познанию сущности системных объектов в правовой сфере представляется в этой связи (в связи с тем, что, по мнению автора, современная правовая система России характеризуется сочетанием процессов «организации и дезорганизации, состояний порядка и неустойчивости» – Е.М.) не только закономерным, но и просто необходимым этапом их исследований» [4, с.78].

Основания для предложения об использовании синергетического подхода в качестве ведущего, системообразующего для проведения экономико-правового анализа преступлений в бюджетной сфере связаны с тем, что:

1) и экономика, и право – сложные открытые системы, элементы которых находятся в сложной и неразрывной взаимосвязи, причем взаимосвязь наблюдается и между отдельными элементами этих относительно обособленных систем (в частности, в бюджетной деятельности переплетаются и экономические, и правовые аспекты, в преступлениях, связанных с бюджетной деятельностью, – тоже);

2) каждая из систем выполняет собственные социальные функции, они «вплетены» в социальную реальность и являются подсистемами системы еще более высокой степени сложности – социальной системы Российской Федерации;

3) отдельные элементы и экономической, и правовой систем связаны отношениями когерентности, т.е. взаимосвязи (принцип, согласно которому все элементы систем находятся во взаимосвязи). Преступность в бюджетной сфере – признак рассогласования в каждой из систем, порождающего флуктуации, т.е. колебания, связанные с отклонениями от равномерного распределения и ведущие к существенной перестройке системы;

4) преступность в бюджетной сфере приближает экономико-правовую систему к точкам бифуркации, причем как в каждой из систем, так и в их интеграции, что может привести либо к плавному их изменению, либо к радикальному изменению качественных характеристик систем. При этом точки бифуркации характеризуются как такой период или момент в развитии экономико-правовой системы, в котором она становится неустойчивой и возникает неопределенность, требующая существенных изменений в самой системе.

Изучение результатов исследований, проведенных в экономико-правовой сфере на основе системы методологических подходов, в которой ведущую роль играет синергетический подход, позволяет с уверенностью утверждать, что применительно к анализу преступности в сфере бюджетной деятельности это поможет:

1) обеспечить достаточную глубину исследований посредством использования тех преимуществ, которые создает интеграция методологических подходов экономического и правового содержания применительно и с учетом особенностей бюджетной деятельности, выявить те проблемы, которыми порождается и «подпитывается» преступность в этой специфической сфере, также выступающей в качестве сложной, открытой, саморазвивающейся системы;

2) выявить и описать механизмы самоорганизации экономико-правовой системы государства и ее подсистем, в том числе и бюджетной сферы, и преступности в сфере бюджетной деятельности, показать влияние на них как стабилизирующих, так и дестабилизирующих факторов, в особенности – факторов криминального характера, обосновать способности исследуемых систем и подсистем к восстановлению, воспроизводству, восприятию внешнего управляющего воздействия;

3) посредством разработки методологии исследования на философском, общенаучном, конкретно научном уровнях грамотно и обоснованно представить методологию исследования конкретного предмета, связанного с изучением отдельных проблем (аспектов проблем), возникающих в процессе проведения экономико-правового анализа преступлений в сфере бюджетной деятельности, на определенных в ходе исследования принципах целенаправленно выстроить его концепцию, эффективно применить авторские методики и инструменты, включающие набор процедур, обеспечивающих достижение установленной цели и получение запланированного результата.

ЛИТЕРАТУРА

1. [Электронный ресурс].URL: <http://portalus.ru>(дата обращения: 29.05. 2018).
2. Отчет о работе Счетной палаты РФ в 2018 году. [Электронный ресурс].URL: <http://www.ach.gov.ru>(дата обращения: 29.05. 2019).
3. Интервью председателя Счетной палаты РФ А.Л. Кудрина телеканалу Россия1 26.11.2018.[Электронный ресурс]. URL:https://www.gazeta.ru/science/2018/11/26_a_12072211.shtml
4. Хабриева Т. Я. Экономико-правовой анализ: методологический подход // Журнал российского права. 2010. №12. - С. 5-26.
5. Шундилов К.В. Синергетическая методология как познавательный ресурс правоведения / Наука теории и истории государства и права в поиске новых методологических решений: Коллективная монография / Отв. ред. А.А. Дорская. – СПб.:Астерион, 2012. – С 77-84.

СВЕДЕНИЯ ОБ АВТОРЕ

Мещерякова Елена Ивановна. Профессор кафедры гражданско-правовых и экономических дисциплин. Доктор педагогических наук, профессор.
Воронежский институт МВД России.
E-mail: elenamsol@yandex.ru
Россия, 394065, г. Воронеж, пр-т Патриотов, 53. Тел. (473) 2005-301.

Meshcheryakova Elena Ivanovna. Professor of the department of civil law and economic disciplines. Doctor of Pedagogy, Professor,
E-mail: elenamsol@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Voronezh Institute of the Ministry of the Interior of Russia

Ключевые слова: методология экономико-правового исследования, синергетический подход.

Keywords: methodology of economic and legal research, synergetic approach.

УДК 33.011, 34.01

Стрыгина Инна Евгеньевна,
кандидат экономических наук

НЕФОРМАТНАЯ БУХГАЛТЕРСКАЯ ДОКУМЕНТАЦИЯ И ЕЕ ЭКСПЕРТИЗА

NEFORMATNAJA ACCOUNTING DOCUMENTATION AND ITS EXAMINATION

В статье проведена группировка экономической информации на учетную и внеучетную, выделены обстоятельства, способствующие этому делению; составлен перечень типичных нарушений в отношении неформатной бухгалтерской документации, исследуемой в процессе бухгалтерской экспертизы.

The article grouped economic information into accounting and off-account, highlighted the circumstances contributing to this division; a list of typical irregularities in non-format accounting documents identified during the accounting process has been compiled.

С помощью документов бухгалтерского учета можно получить информацию о способах совершения экономических правонарушений и преступлений, суммах нанесенного материального ущерба, хозяйственном периоде и пр.

Чтобы получить достоверную информацию о выявленных противоправных действиях в ходе проведения судебно-бухгалтерской экспертизы экспертом-бухгалтером исследуются не только первичные документы, учетные регистры и бухгалтерская (финансовая) отчетность, но и неофициальные документы, а также неформатная документация, которая оказывает существенное влияние на отражение фактов хозяйственной жизни.

В некоторых ситуациях, возникающих при проведении судебно-бухгалтерской экспертизы, эксперт-бухгалтер в своем заключении выделяет в отдельные группы документов, которые содержат учетную и внеучетную информацию. Несмотря на то, что

влияние учетных и неформатных документов на формирование выводов экспертов-бухгалтеров неоднозначно, часто на практике такое деление не производится. При сборе экспертом-бухгалтером доказательств совершения противоправных экономических правонарушений и преступлений значение данных документов также неоднозначно. В качестве доказательства по фактам растрат или присвоения денежных средств принимаются первичные документы (приходные и расходные кассовые ордера, учетные регистры и др.), а по преступлениям, которые связаны с превышением должностных полномочий в качестве доказательств используются должностные инструкции, приказы, распоряжения и т.д.

К учетной информации относится учетная политика экономического субъекта, которая регламентирует методические и организационные аспекты учета и влияет на отражение результатов хозяйственной деятельности, а к внеучетной информации, которая также влияет на учетный процесс, относят заключенные предприятием договоры и другие документы.

Нами были выделены следующие обстоятельства, влияющие на процесс стандартизации информации и доказательств, ее содержащих на учетные и внеучетные группы:

- компетенция эксперта-бухгалтера в вопросах бухгалтерского учета;
- объекты, предоставленные эксперту-бухгалтеру для исследования;
- программное обеспечение учетного процесса;
- количество работников, которые были вовлечены в противоправную деятельность;
- приемы и способы совершения корыстных деяний.

Анализ и изучение теоретических и практических материалов позволили нам провести классификацию документов, влияющих на формирование доказательственной базы по противоправным действиям и используемых экспертами для обоснования выводов. Результаты данного исследования представлены в таблице 1

Таблица 1

Классификация учетной и неформатной документации,
используемой в экспертной работе

Учетная документация	Неформатная документация
1. Первичные учетные документы на бумажных и электронных носителях	1. Документы неофициального учета
2. Бухгалтерские регистры	2. Деловая переписка
3. Материалы инвентаризации	3. Акты ревизий и проверок
4. Бухгалтерская (финансовая) отчетность	4. Аудиторские заключения
	5. Заключения других экспертиз
	6. Технологическая и техническая документация
	7. Гражданско-правовые договоры

Важное значение при доказывании противоправных экономических действий в экспертной деятельности имеет выделение в экспертной работе таких документов, которые непосредственно не участвуют в учетном процессе, но которые могут служить прямым доказательством совершения экономических правонарушений и преступлений (неформатные документы с элементами интеллектуального или материального подлога, незаконные распоряжения, приказы и др.), а также являться источником информации противоправной деятельности (неофициальные документы, протоколы допросов долж-

ностных лиц и др.).

Необходимо отметить, что в научной и учебно-методической литературе на сегодняшний момент имеется немного разработок, которые затрагивают проблемы использования в системе финансового контроля документов, не включенных в учетный процесс. Также нет единого подхода к тому, как называть такие документы и какую документацию включать в ее состав, а также как применять содержащуюся в ней информацию в контрольно-ревизионной и экспертной работе.

В научной и учебно-методической литературе среди авторов нет единства мнений относительно понятия «внеучетный документ».

Каширская Л.В. [2, с. 176] считает, что часть внеучетных данных составляют основу системных документов, под которыми в данном контексте следует понимать документы, составляющие системную основу финансово-хозяйственной деятельности, содержащие учетную и внеучетную информацию, на основе которых определяется влияние на содержание фактов хозяйственной жизни или на базе которых они осуществляются».

Горшкова Л. [1] под внеучетным документом понимает «вспомогательные объекты судебной налоговой экспертизы».

Опираясь на источники научно-методического характера и учитывая практический опыт производства бухгалтерских экспертиз мы посчитали возможным сформулировать следующее определение внеучетных документов с точки зрения бухгалтерской экспертизы: это небухгалтерская документация экономического субъекта, оказывающая влияние на учетный процесс, а также на порядок и достоверность отражения фактов хозяйственной жизни в системе взаимосвязанных учетных и отчетных данных.

Основой неформатных документов являются: лицензионно-разрешительные документы, внутренние положения, нормативно-правовые документы, гражданско-правовые договоры, протоколы и др.

Нами предлагается выделить данную категорию документов в отдельный сегмент бухгалтерской экспертизы – «бухгалтерская экспертиза неформатных документов».

Для проведения судебно-бухгалтерской экспертизы неформатных документов на качественном уровне необходимо разработать методические особенности работы с данными документами в согласовании с порядком осуществления экспертных процедур на определенных стадиях экспертной работы.

Важным аспектом экспертного исследования неформатных документов является обобщение практического опыта с целью выделения характерных правонарушений, совершенных в отношении подобных документов.

На основании проведенного анализа практического материала нами был составлен перечень типичных нарушений в отношении неформатных документов:

- 1) полное или частичное отсутствие необходимой неформатной документации;
- 2) несвоевременное составление и внесение изменений в неформатную документацию;
- 3) непреднамеренные ошибки и умышленные искажения при составлении документов;
- 4) материальный и интеллектуальный подлог неформатной документации;
- 5) несоответствие данных неформатных документов другим материалам в системе взаимосвязанной экспертной документации;
- 6) отсутствие необходимых реквизитов неформатных документов;
- 7) нарушение типового порядка составления документов.

Можно сделать вывод, что неформатная документация имеет важное значение в деятельности экономических субъектов и оказывает большое влияние на полноту, ка-

чество и достоверность отражения фактов хозяйственной жизни в данных бухгалтерского учета и отчетности.

Кроме того, выделение рассматриваемой категории документов в отдельный сегмент бухгалтерской экспертизы – «бухгалтерскую экспертизу неформатных документов» позволит включать данный сегмент в базовую основу любой формы финансового контроля для последующего мониторинга, анализа и экспертного исследования противоправных действий в финансово-хозяйственной деятельности экономических субъектов.

ЛИТЕРАТУРА

1. Горшкова Л. Процедура налоговых проверок: причины признания проверки недействительной / Л. Горшкова // Финансовая газета. – 2010. – № 16 [Электронный ресурс]. – Режим доступа: <http://www.lawmix.ru/bux/111> (дата обращения: 05.06.2019 г).

2. Каширская Л.В. Методология и организация бухгалтерской экспертизы в бюджетных учреждениях : дис. д-ра экон. наук / Каширская Людмила Васильевна. – М., 2013. – 286 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Стрыгина Инна Евгеньевна, доцент кафедры гражданско-правовых и экономических дисциплин. Кандидат экономических наук.

Воронежский институт Министерства внутренних дел России.

E-mail: strigina.in@yandex.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-53-71.

Strygina Inna Evgenyevna. associate professor of civil and economic disciplines. Candidate of Economic Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: strigina.in@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-53-71.

Ключевые слова: судебно-бухгалтерская экспертиза, учетная и внеучетная информация, неформатная документация, противоправные экономические действия.

Key words: forensic examination, registration and extra registration information, not format documentation, illegal economic acts.

УДК 657.6.012.16

БУХГАЛТЕРСКАЯ ЭКСПЕРТИЗА В СИСТЕМЕ БЮДЖЕТНЫХ ОТНОШЕНИЙ

ACCOUNTING EXPERTISE IN THE SYSTEM OF BUDGET RELATIONS

В данной работе рассмотрены причины целесообразности глубокого исследования проблем проведения бухгалтерской экспертизы в системе бюджетных отношений с точки зрения необходимости использования в целях профилактики и предупреждения нецелевого, неэффективного и нерационального использования бюджетных ресурсов, повышения эффективности института ответственности за нарушения в бюджетной сфере, а также на усиление борьбы с коррупцией.

This paper discusses the reasons for the feasibility of in-depth study of the problems of accounting expertise in the system of budgetary relations in terms of the need to use for the prevention and prevention of misuse, inefficient and irrational use of budgetary resources, improving the efficiency of the institution of responsibility for violations in the budgetary sphere, as well as to strengthen the fight against corruption.

Использование бухгалтерской экспертизы в системе бюджетных отношений как инструмента раскрытия противоправных экономических правонарушений носит, по нашему мнению, достаточно локализованный характер. Вполне очевиден факт целесообразности глубокого исследования проблем проведения бухгалтерской экспертизы в системе бюджетных отношений с точки зрения необходимости использования в целях профилактики и предупреждения нецелевого, неэффективного и нерационального использования бюджетных ресурсов.

В Бюджетном кодексе РФ (статья 306.4) под нецелевым использованием бюджетных средств определяются случаи направления средств бюджета и оплаты денежных обязательств, не соответствующих полностью или частично целям, определенных законом о бюджете, бюджетной сметой, договором (соглашением) либо другим документом, являющимся правовым основанием предоставления указанных средств [3].

Борьба с неэффективным, нерациональным, а также нецелевым использованием бюджетных средств направлена на повышение эффективности института ответственности за нарушения в бюджетной сфере, а также на усиление борьбы с коррупцией. Исследование вопроса понимания сущности эффективного и рационального использования (расходования) бюджетных средств показало, что мнения ученых разделились. Одна группа ученых (Д. Юм, Д. Милль, А. Смит) считает, что эффективность использования (расходования) бюджетных средств связана с соотношением достигнутого (достижаемого) результата с произведенными затратами (теория экономики общественного сектора). Приверженцы неоклассической теории предполагают необходимость предоставления бюджетных ресурсов в распоряжение того пользователя, для которого они имеют наибольшую необходимость или ценность, а другая группа ученых (Е.В. Бушмин, О.Г. Горшков, В.Л. Никифоров) связывают понятие эффективности использования бюджетных средств с понятием максимально возможного получения результата.

Стремление к эффективному и рациональному использованию бюджетных средств на практике осуществляется в соответствии с такими законными принципами как: высокоэффективное, целевое использование бюджетных средств, соблюдение бюджетной дисциплины и режима экономии [2, С. 937-939]. На наш взгляд, принцип соблюдения бюджетной дисциплины и режима экономии особенно актуален в современных условиях санкций и ограничений в отношении отечественной экономики.

Оценивая работу контрольных и правоохранительных органов по предупреждению противоправных действий в сфере эффективного и рационального использования бюджетных средств, следует указать на тот факт, что работа в данном направлении осуществляется на постоянной основе. Однако, по причине разрушения устоявшейся системы социальной профилактики в 90-х гг. прошлого столетия наблюдалось снижение уровня результативности данной работы и, соответственно, имел место рост экономических правонарушений и преступлений. В связи с этим 11 августа 1998 г. подписывается Приказ МВД РФ № 490 «Об утверждении нормативных актов о деятельности органов внутренних дел по предупреждению преступлений». В наставлении по деятельности органов внутренних дел в сфере предупреждения преступлений определяются основные задачи, в перечень которых входит:

выявление и анализ причин и условий, способствующих совершению преступлений, принятие мер по их устранению или нейтрализации;

установление лиц, противоправные действия которых не содержат признаков преступления, но дают основания для принятия к ним мер профилактического воздействия;

установление и пресечение фактов приготовления к преступлению и покушению на преступление;

принятие к лицам, их совершившим, мер в соответствии с законодательством Российской Федерации [4].

Также был определен объект воздействия органов внутренних дел в сфере предупреждения преступлений (выявление и устранение причин и условий, способствующих формированию личности правонарушителя). В соответствии с данным приказом профилактические мероприятия заключаются в следующем:

контроле и оказании практической помощи;

подготовке и проведении комплексных и целевых оперативно-профилактических мероприятий по предупреждению преступлений;

участии и разработке совместно с другими федеральными органами исполнительной власти, организациями, общественными объединениями нормативных правовых актов и программно-целевых мероприятий;

разработке и обеспечении проведения комплексных оперативно-профилактических мероприятий [11].

Начало XXI века характеризуется ориентацией преимущественно на уголовно-репрессивные средства и методы, совершенствованием уголовного законодательства, разработкой программ мер усиления борьбы с экономической преступностью.

В современном обществе имеет место постепенное усиление роли государственного контроля в социально-экономической жизни российского общества, что позволяет укрепить финансово-контрольные звенья и организовать усилия по противодействию экономическим правонарушениям, о чем наглядно свидетельствуют данные официальной статистики.

Так, например, в 2016 году общий ущерб от преступлений в сфере освоения бюджета превысил 19 миллиардов рублей. В этой сфере было выявлено 7300 квалифицированных преступлений, которые связаны с хищением и нецелевым использованием бюджетных средств. [5]. В 2017 году в России правоохранительными органами выявлено свыше 105 тысяч преступлений экономической направленности [6]. По разным оценкам при расследовании около 60% таких преступлений требуется назначение бухгалтерских экспертиз.

В феврале 2018 года на расширенном заседании коллегии Министерства внутренних дел Российской Федерации Президент Российской Федерации В.В. Путин обратил внимание на то, что одним из важных направлений работы МВД является борьба с преступлениями в сфере экономики. Сотрудники правоохранительных органов вносят огромный вклад в укрепление экономической безопасности страны. Преступления в

сфере экономики из всех выявленных правоохранительными органами составляют 85 процентов. Глава МВД Российской Федерации В.А. Колокольцев сообщил об актуальности повышения защищенности российской экономики в условиях неблагоприятной внешней конъюнктуры [7]. Следовательно, в сложившейся ситуации на первый план выходит пресечение хищений бюджетных средств.

Статистика противоправных экономических действий по Воронежской области также свидетельствует об имеющих место экономических правонарушениях в бюджетной сфере. Например, в январе 2018 года пресс-служба ГУ МВД по Воронежскому региону сообщила о том, что бывшая сотрудница (бухгалтер) образовательного учреждения Новоусманского района Воронежской области в течение 4 лет переводила себе деньги под видом зарплаты (с 2013 по 2017 год). Сотрудники полиции возбудили уголовное дело по ч. 4 ст. 160 УК РФ (присвоение денежных средств в особо крупном размере). Ущерб составил 1,58 млн. рублей. [8]. В феврале 2018 года в пресс-службе региональной прокуратуры сообщили о том, что Грибановским райсудом рассмотрено дело директора школы, которого осудили за мошенничество с использованием служебного положения. Ущерб составил 100 тысяч рублей [9].

Проведение бухгалтерских экспертиз в данных случаях позволило определить сумму ущерба и круг лиц, причастных к совершению противоправного экономического действия, провести исследования записей бухгалтерского учета при осуществлении экспертной деятельности, которые будут направлены на установление:

- соответствий (несоответствий) фактов хозяйственной жизни требованиям бухгалтерского учета, действующим нормативным актам;

- соответствий (несоответствий) сведений, получаемых из материалов дела (протоколы допросов обвиняемых и свидетелей, актов документальной ревизии и др.);

- правильности использованных методов;

- данных непосредственно связанных с недостаточей или излишком материально-производственных запасов, денежных средств, а также на возможность определения периода их образования [1, с. 13].

Однако, материалы бухгалтерской экспертизы призваны определить не только сумму ущерба и выявить круг лиц, причастных к совершению противоправного действия, но и осуществить практическую работу по предупреждению правонарушений и злоупотреблений. В соответствии с Федеральным законом № 73-ФЗ от 31 мая 2001 г. «О государственной судебно-экспертной деятельности в Российской Федерации» эксперт-бухгалтер наделен рядом процессуальных прав и обязанностей [10]. В данные процессуальные права входит право разработать предложения и рекомендации, направленные на профилактику и предупреждение злоупотреблений в деятельности экономического субъекта. При назначении бухгалтерской экспертизы правоохранительные органы имеют право предложить эксперту-бухгалтеру проанализировать выявленные ошибки, причины и условия, при которых стало возможным совершение данного правонарушения и разработать рекомендации. Следовательно, эксперт-бухгалтер такие рекомендации может оформить инициативной запиской либо изложить предложения в отдельном разделе заключения (исследовательской части) и предоставить в правоохранительные органы вместе с основным заключением по результатам проведенной бухгалтерской экспертизы.

ЛИТЕРАТУРА

1. Судебно-экономическая экспертиза. Практикум: учеб. пособие для студентов вузов, обучающихся по специальностям «Бухгалтерский учет, анализ и аудит», «Экономическая безопасность», направлению «Экономика» / Ж.А. Кеворкова, И.В. Бахолдина. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2015. – 191 с.

2. Шарапова М. А. Рациональное использование бюджетных средств и условие повышения их эффективности // Молодой ученый. — 2016. — №10. — С. 937-939. — URL <https://moluch.ru/archive/114/30203/>. Дата обращения: 08.06.2018.

3. Бюджетный кодекс РФ статья 306.4. Нецелевое использование бюджетных средств. [Электронный ресурс]. Режим доступа: www.consultant.ru. Дата обращения 08.06.2018.

4. Приказ МВД РФ «Об утверждении нормативных актов о деятельности органов внутренних дел по предупреждению преступлений» от 11 августа 1998 г. № 490 [Электронный ресурс]. Режим доступа: www.consultant.ru. Дата обращения 08.06.2018.

5. Российская газета - Федеральный выпуск №7219 (53) «Разбираться детально». [Электронный ресурс]. Режим доступа: <https://rg.ru/>. Дата обращения 10.06.2018.

6. Состояние преступности в Российской Федерации за январь - декабрь 2017 года. Официальный сайт Министерства внутренних дел Российской Федерации. [Электронный ресурс]. Режим доступа: <https://мвд.рф/reports/item/12167987>. Дата обращения 10.06.2018.

7. Выступление В. Колокольцева на расширенном заседании коллегии. [Электронный ресурс]. Режим доступа: <http://www.kremlin.ru/events/president/news/56949>. Дата обращения 10.06.2018.

8. Новости@mail.ru. [Электронный ресурс]. Режим доступа: <https://news.mail.ru/incident/32202998/?frommail=1>. Дата обращения 15.06.2018.

9. Новости@mail.ru. [Электронный ресурс]. Режим доступа: <https://news.mail.ru/incident/32540202/?frommail=1>. Дата обращения 10.06.2018.

10. Федеральный Закон «О государственной судебно-экспертной деятельности в Российской Федерации» от 31 мая 2001 г. № 73-ФЗ. [Электронный ресурс]. Режим доступа: www.consultant.ru. Дата обращения 10.06.2018.

11. Приказ МВД России «О деятельности органов внутренних дел по предупреждению преступлений» от 17.01.2006 № 19 (ред. от 28.11.2017). [Электронный ресурс]. Режим доступа: www.consultant.ru. Дата обращения 10.06.2018.

СВЕДЕНИЯ ОБ АВТОРЕ

Фоменко Татьяна Николаевна. Соискатель по направлению «Финансы и кредит». Воронежский государственный аграрный университет им. Петра I.
E-mail: fom.tan87@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.
Тел. (473) 200-53-71.

Fomenko Tatyana Nikolaevna. Applicant in the direction of "Finance and credit". Voronezh state agrarian University Peter I.
E-mail: fom.tan87@mail.ru
Work address: Russia, 394065, Voronezh, prospect Patriotov, 53.
Tel. (473) 200-53-71.

Ключевые слова: бухгалтерская экспертиза, бюджетные отношения, экономические правонарушения, предупреждение правонарушений экономической направленности.

Key words: forensic accounting, budgetary relations, economic offences, prevention of offences of an economic nature.

УДК 336.126.008.6

ПОНЯТИЕ И ВИДЫ ПОРУЧИТЕЛЬСТВА

CONCEPT AND TYPES OF SURETY

В данной статье рассматриваются всестороннее изучение правовой природы договора поручительства и гарантии как способа обеспечения обязательств, а также проведение сравнительно-правового анализа и выявление различий между договором поручительства и гарантией. Кроме того, рассмотрены различные способы исполнения обязательств по договорам, вопросы прочности отношений между кредитором и должником.

This article deals with a comprehensive study of the legal nature of the contract of guarantee and guarantee as a way to ensure obligations, as well as comparative legal analysis and identification of differences between the contract of guarantee and guarantee. Besides, various ways of fulfillment of obligations under contracts, questions of durability of the relations between the creditor and the debtor are considered.

Поручительство (adpromissio) является одним из древнейших и наиболее распространенных в настоящее время способов обеспечения исполнения обязательств, поэтому в практике имеется множество видов поручительства.

Поручительство становится интересным, только тогда, когда кредитор не может получить вещного обеспечения. Кредитор может обратиться к поручителю только тогда, когда он не смог получить исполнение обязательства в отношении основного должника. Отсюда следует, что поручитель отвечает после основного должника, а не вместо него.

Одним из главных признаков поручительства является то, что обязательства поручителя являются акцессорными, дополнительными к обязательству главного должника, поэтому существует, пока существует главное обязательство, обеспеченное поручительством, и в размере не превышающим размер главного обязательства.

Так, Шершеневич Г.Ф. указывал, что под поручительством понимается присоединение к главному обязательству дополнительное условие об исполнении его третьим лицом, поручителем, в случае неисправности должника [1, С.325].

Существенным условием договора поручительства является наличие в договоре условий, позволяющие определить обязательство, обеспечиваемого поручительством и его объем. Если в договоре поручительства отсутствуют условия, позволяющие определить за исполнение какого обязательства дано поручительство (в частности, сведений о кредиторе, конкретном договоре), то такой договор поручительства может быть признан не заключенным.

Договор поручительства также следует считать незаключенным при отсутствии в нем условий, позволяющих определить, за кого дано поручительство, в обеспечении каких именно обязательств, их содержание и сумму. Отсутствие даты и номера обеспеченного договора существенного значения не имеет. Вместе с тем, указание номера и даты договора, устанавливающего обеспечение обязательства, не всегда может быть признано достаточным для их индивидуализации и может повлечь признание договора поручительства незаключенным.

Правовые механизмы поручительства подлежат классификации по следующим критериям:

1. В зависимости от содержания обязательств, возникающих у поручителя на:

- компенсационное (или отвлеченное) поручительство;
- замещающее поручительство.

Разница между данными видами поручительства состоит в том, что при компенсационном поручительстве поручитель обязуется компенсировать в денежном эквиваленте величину обязательств должника либо выполнить за должника денежные обязательства, если иное не предусмотрено договором поручительства.

При замещающем же поручительстве поручитель берет на себя обязанность исполнить само обязательство должника (передать не индивидуально-определенное имущество, выполнить работы, оказать услуги и т.п.) в полном объеме, если иное не предусмотрено договором поручительства.

Такое разделение имеет значение, когда обеспечивается какое-либо не денежное обязательство (по передаче имущества, выполнению работ, оказанию услуг). В качестве примера можно привести случай, когда обеспеченным обязательством является обязанность по поставке какого-либо товара (не индивидуально-определенного) и должник не выполняет надлежащим образом данное обязательство, то при компенсационном поручительстве обеспечивающая сторона, по общему правилу компенсирует обеспеченной стороне в денежном выражении стоимость нарушенного обязательства.

При замещающем же поручительстве обеспеченная сторона вправе требовать от поручителя поставки надлежащих товаров либо иных обязательств, предусмотренных в отношении должника в законодательстве либо иных обязательств, предусмотренных в отношении должника в законодательстве либо договоре, также выполнения способов обеспечения, если иное не определено соглашением сторон.

Ответственность поручителя зависит от вида поручительства. При компенсационном поручительстве поручитель несет ответственность за неисполнение денежного обязательства. При замещающем же поручительстве объемы и виды ответственности поручителя будут совпадать с соответствующими показателями ответственности должника, и будут зависеть от категории обеспеченного обязательства.

Указанное выше деление было известно еще древнеримскому праву. Так, Д.В. Дождев, рассматривая формы поручительства в праве Древнего Рима, указывает, что при совершении поручительства (*adpromissio*) в форме *sponsio* предметом последней является то же самое предоставление, которое обещалось по основной сделке. Так, если должник по основной сделке обязывался уплатить денежную сумму, то должник по *sponsio* (так называемый спонсор) обязывался уплатить такую же сумму; в обязательствах по передаче вещи или по производству работ *sponsio* обещал передать такую же вещь или выполнить такие же работы, что и главный должник. Отсюда следовал очень важный вывод – *sponsio* не могла иметь места по обязательствам строго личным и обязательствам, предметом которых являлись незаменимые вещи [2, С. 427].

В качестве другой важной черты *sponsio* И.А.Покровский выделял долевую ответственность в случае наличия нескольких спонсоров [3, С. 375].

Действующее законодательство не предусматривает механизм замещающего поручительства, хотя возможно может иметь место. По мнению Б.А. Белова особую остроту данный вопрос приобретает в современной банковской деятельности в случаях обеспечения обязательства по возврату валютных кредитов. Исходя из концепции «поручительства – ответственность» необходимо признать, что поручитель по такому договору обязан при неисправности заемщика возместить банку, причиненные этим убытки и уплатить санкции, причем сделать все это в национальной валюте. [4, С. 207].

2. В зависимости от объема обязательства поручителя различают:

- полное поручительство;
- частичное поручительство.

При полном поручительстве поручитель отвечает перед обеспеченной стороной в том же объеме, как и должник, включая уплату процентов, возмещение судебных издержек по взысканию долга и других убытков обеспеченной стороны, вызванных неисполнением или ненадлежащим исполнением обязательств должником.

Поскольку договор поручительства носит акцессорный характер, обязательство поручителя перед кредитором не может быть большим по объему, чем обязательство должника, за которого ручался поручитель. Частичное поручительство может быть установлено по соглашению сторон.

Частичное поручительство, в свою очередь, может быть разделено на:

- ограниченное частичное поручительство;
- раздельное частное поручительство;
- смешанное (ограниченно-раздельное) частичное поручительство.

При ограниченном частичном поручительстве ответственность поручителя определяется конкретной суммой в договоре, но без ограничения видов обязательств, за неисполнение или ненадлежащее исполнение которых со стороны должника отвечает поручитель.

При раздельном частичном поручительстве кредитор вправе требовать от поручителя исполнения либо компенсации за неисполнение со стороны должника определенных в договоре обязательств, но без ограничения суммы ответственности, которая может быть рассчитана исходя из положений действующего законодательства и договора. Отсюда следует, что поручитель может отвечать, например, только за возврат основной суммы долга либо данной суммы и уплаты неустойки и т.п.

Следует отметить, что в судебной практике простое указание в договоре поручительства на ответственность за возврат, например, долга и уплату процентов расценивается как условие об ограничении ответственности поручителя только этими суммами. Следовательно, при ограниченно-раздельном поручительстве ответственность поручителя может быть ограничена как определенной величиной денежных средств, так и видом обязательств, за неисполнение которых со стороны должника отвечает поручитель.

3. В зависимости от срока действия договора поручительства можно выделить:

- бессрочное поручительство;
- обычное (законное) срочное поручительство;
- договорное срочное поручительство.

При бессрочном поручительстве истечение сроков, указанных в законе либо в договоре не является основанием для его прекращения [4. ст.336. п.4]. Иными словами бессрочное поручительство может прекратиться только при наступлении иных оснований для его прекращения, например, с прекращением обеспеченного обязательства и т.п. Данный вид поручительства является обременительным для поручителя, и поэтому практически не используется в деловом обороте и не регламентирован действующим законодательством. Такое поручительство не может иметь место, поскольку в договоре должен быть установлен срок, в обратном случае применяются правила обычного (законного) срочного поручительства.

При этом необходимо отметить, что по умолчанию в договоре, действительно устанавливается обычное (законное) срочное поручительство, т.е. поручительство, которое действует в течение срока, указанного в законе. Например, согласно п.4 ст.336 ГК РК, когда срок поручительства не установлен в договоре, то оно прекращается, если кредитор в течение одного года со дня наступления срока исполнения обеспеченного обязательства не предъявит иск к поручителю. Когда срок исполнения основного обязательства не указан и не может быть определен или определен моментом востребования, то поручительство прекращается, если кредитор не предъявит иска к поручителю в течение двух лет со дня заключения договора поручительства [5].

Правовой режим договорного срочного поручительства устанавливается, если в договоре поручительства установлены сроки действия поручительства, отличные от сроков, приведенных в законодательстве.

4. Различают солидарное и субсидиарное поручительство.

Так, И.Б.Новицкий указывал, что классическое римское право, подчеркивая акцессорный характер поручительства, не признавало, однако, за ним субсидиарного характера, кредитор, не получившему в срок исполнения, предоставлялось по его усмотрению право обратиться взыскание или на должника, или на поручителя, то есть фактически имело место солидарное поручительство [6, С. 223].

При солидарном поручительстве в случае неисполнения либо ненадлежащего исполнения должником обеспеченного обязательства кредитор имеет право требовать неисполненного от должника и поручителя совместно, так и в отдельности, как в полном объеме, так и части обеспеченного обязательства. Не получив полного удовлетворения от должника либо от поручителя, обеспеченная сторона вправе требовать недополученного от другого. В случае солидарности требований ни должник, ни поручитель не вправе выдвигать против требований кредитора возражения, основанные на таких отношениях других участников сделки, в которых он не участвует.

Но позднее, это положение было изменено законом Юстиниана 535г., согласно которому поручителю была предоставлена льгота, состоящая в очередности ответственности. На основании данной льготы поручитель, против которого кредитор предъявлял иск, мог выставить возражение против иска с требованием, чтобы кредитор в первую очередь обратил взыскание на главного должника. Таким образом, было введено субсидиарное поручительство [7, С. 354].

В настоящее время, в гражданском праве по общему правилу, по умолчанию, устанавливается субсидиарное поручительство. Согласно ст. 330 ГК РК, в силу поручительства поручитель обязуется перед кредитором другого лица (должника) отвечать за исполнение обязательства этого лица полностью или частично субсидиарно.

Как регламентировано в п. 3 ст. 332 ГК РК, поручитель несет перед кредитором ответственность в пределах суммы, указанной в поручительстве, если иное не предусмотрено условиями поручительства. До предъявления требований к поручителю, несущему субсидиарную ответственность, кредитор должен принять разумные меры к удовлетворению этого требования должником, в частности, путем зачета встречного требования и обращения взыскания в установленном порядке на имущество должника [5].

При субсидиарной ответственности кредитор приобретает дополнительного должника, т.е. к нему можно обращаться только при недостаточности средств у основного должника.

В соответствии с п. 1 ст. 357 ГК РК, до предъявления требований к лицу, которое в соответствии с законом, иными правовыми актами или условиями обязательства несет ответственность дополнительно к ответственности другого лица, являющегося основным должником (субсидиарную ответственность), кредитор должен предъявить требование к основному должнику. Если основной должник отказался удовлетворить требование кредитора или кредитор не получил от него в разумный срок ответ на предъявленное требование, то это требование может быть предъявлено лицу, несущему субсидиарную ответственность.

В силу нормы п. 2 ст. 357 ГК РК, кредитор не вправе требовать удовлетворения своего требования к основному должнику от лица, несущего субсидиарную ответственность, если это требование может быть удовлетворено путем зачета встречного требования к основному должнику, либо бесспорного взыскания средств с основного должника.

Субсидиарное поручительство может возникнуть при наступлении следующих обстоятельств:

- после завершения процедур банкротства должника, в результате которых обнаружится, что обеспеченная сторона не получила удовлетворения.
- в случае объявления должника банкротом (в действующих гражданских законодательствах Швейцарии (Обязательственное право, ст.495), Финляндии и др.)
- при недостаточности средств у должника. В настоящее время данный правовой режим допускается (в качестве одной из разновидностей поручительства, в частности, в гражданском законодательстве Германии).
- при отказе должника в удовлетворении требования обеспеченной стороны или неполучении обеспеченной стороной от него в разумный срок ответа на предъявленное требование [8, С.70].

Поручительство - это обязательство придаточное (вспомогательное). Поэтому поручитель хотя и отвечает субсидиарно с должником, но не, безусловно, а лишь при наступлении факта неисполнения основного обязательства должником.

При введении в договор поручительства условия о том, что поручитель обязуется перед должником исполнить не исполненное им обеспечиваемое обязательство, возникает проблема отграничения поручительства от возложения исполнения обязательства на третье лицо.

По общему правилу поручитель и должник несут перед кредитором субсидиарную ответственность. Механизм возникновения субсидиарного обязательства поручителя и должника своеобразен.

Субсидиарная ответственность поручителя перед кредитором при неисполнении или ненадлежащем исполнении должником обеспеченного поручительством обязательства может быть предусмотрена законом или договором поручительства.

Основным назначением договора поручительства является возмещение убытков кредитора вследствие неисполнения или ненадлежащего исполнения обязательства должником с целью максимально снизить убытки и потери кредитора.

Таким образом, поручительство – это правовой способ обеспечения обязательств, связанный с привлечением дополнительного должника, поэтому договор поручительства все чаще используется в настоящее время для обеспечения исполнения обязательств по основным гражданско-правовым договорам.

Но вместе с тем, есть еще неразрешенные в законе и в науке вопросы, а также положения, которые требуют научного анализа и обоснования рекомендации в целях стабильности правоприменения, в частности, такие вопросы о правовой природе поручительства, содержании договора поручительства и о его субъектах, положения о характере возражений, выдвигаемых поручителем против требования кредитора, об отношениях между поручителем, исполнившим свое обязательство, и должником по главному обязательству, о порядке исполнения и прекращения обязательства поручительства.

Еще одним видом обязательства, имеющие большое значение и получившие в последнее время широкое распространение в юридической жизни - гарантийные обязательства,

Развитие данного института обусловлено, как потребностями, так и интересами субъектов предпринимательской и иной хозяйственной деятельности, заключающимися в максимальном снижении рисков причинения убытков вследствие неправомерных действий или же бездействия контрагентов, а также невозможности восстановления нарушенных прав за счет ответственного лица и созданием новых правовых конструкций, направленных на обеспечение указанных интересов, каковыми являются гарантия и поручительство.

Таким образом, подводя итоги настоящего исследования, необходимо отметить, что, несмотря на то, что текущий уровень платежной дисциплины и частое нарушение обычаев делового оборота требуют широкого применения различных способов обеспечения обязательств, на практике многие обеспечительные меры остаются невостребованными.

Это объясняется несколькими причинами:

1. Слабо развитую систему специализированных организаций по обеспечению гражданско-правовых договоров, разрозненность отдельных ее компонентов, несовершенство законодательной базы, а зачастую и отсутствие судебной практики по некоторым видам дел.

2. Непопулярность некоторых способов обеспечения обязательств объясняется и их спецификой.

3. Банковская гарантия, наряду с поручительством и иногда залогом, требуют привлечения третьих лиц в качестве гарантов надлежащего исполнения обязательства, что влечет определенный материальный риск для этих лиц. Чтобы максимально обезопасить поручителя и гаранта от убытков ГК РК провозглашает возмездный характер этих способов обеспечения обязательств.

Сейчас актуальное значение имеют положения гражданского законодательства об обязательствах, возникающих вследствие неосновательного обогащения. Должником, в таком обязательстве, является лицо, которое приобрело имущество за счет другого лица (кредитора) без установленных законодательством или сделкой оснований, и поэтому обязано возвратить последнему полученное имущество незаконным путем.

Кроме того, лицо, неосновательно получившее имущество, обязано возвратить или возместить все доходы, которые оно извлекло или должно было извлечь из этого имущества. На сумму неосновательного денежного обогащения начисляются проценты за пользование чужими средствами в размере средней ставки банковского процента, существующей в месте нахождения кредитора.

В ряде случаев, источником возникновения обязательств может служить судебное решение, например в такой ситуации, когда на рассмотрение суда сторонами переданы разногласия, возникшие при заключении договора. При таких обстоятельствах условия договора (а значит, и соответствующие обязательства сторон) определяются на основании решения суда. Обязательства могут возникнуть также из сделок, из актов государственных органов и органов местного самоуправления в случаях, предусмотренных законом, а также вследствие иных действий и событий, с которыми закон или иной правовой акт связывает наступление гражданско-правовых последствий.

Необходимо также отметить, что общая часть обязательственного права представляет собой наиболее традиционный институт гражданского права, поэтому его возобновление в гражданском законодательстве шло в основном по пути совершенствования и уточнения ранее действовавших норм.

ЛИТЕРАТУРА

1. Шершеневич Г.Ф. Учебник русского гражданского права.- Москва-1995г.-760с. (дата обращения: 05. 06. 2019).
2. Дождев Д.В. Римское частное право /под ред. В.С. Нерсисянца. - Москва-1996г.-330с. (дата обращения: 05. 06. 2019).
3. Покровский И.А. Римское право. - Москва-1993г.-608с. (дата обращения: 05. 06. 2019).

4. Белов В.А. Поручительство. Опыт теоретической конструкции и обобщения арбитражной практики. -Москва, «ЮрИнфо».-1998г.-410с. (дата обращения: 05. 06. 2019).
5. Гражданский кодекс Республики Казахстан (Общая часть), принят Верховным Советом Республики Казахстан 27 декабря 1994 года (с изменениями и дополнениями по состоянию на 02.04.2019 г.)www.zakon.kz(дата обращения: 05. 06. 2019).
6. Новицкий И.Б., Лунц Л.А. Общее учение об обязательствах. - Москва-1996г. (дата обращения: 05. 06. 2019).
7. Брагинский М.И., Витрянский В.В. Договорное право: общие положения. – Москва, Издательство «Сатурн».-1998г.-с.487-489. (дата обращения: 05. 06. 2019).
8. Звягинцева М.А. Субъекты договора поручительства. // Журнал российского права, 2000 № 7. // Консультант Плюс. (дата обращения: 05. 06. 2019).

СВЕДЕНИЯ ОБ АВТОРЕ

Хауия Саулет. Старший преподаватель, магистр права кафедры правового регулирования экономических отношений.

Карагандинский экономический университет Казпотребсоюза.

E-mail: saulet.kkk@mail.ru

Республика Казахстан, 100000, г. Караганда, ул. Академическая, 9.

Тел. 7212 441592, сот. 8702 366 11 63.

Khauiya Saulet. Senior lecturer, master of law of the chair of legal regulation of economic relations.

Karaganda Economic University of Kazpotrebsoyuz.

E-mail: saulet.kkk@mail.ru

The Republic of Kazakhstan, 100000, Karaganda, Academical Str., 9.

Tel.: 7212 441592, mob. 8702 366 11 63.

Ключевые слова: Обязательства, задаток, поручительство, залог, неустойка.

Key words: Obligations, deposit, guarantee, pledge, penalty.

УДК 341

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ, ЖИВУЧЕСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ И СВЯЗИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Авсентьев Олег Сергеевич,
доктор технических наук, профессор;
Рубцова Ирина Олеговна

ОПИСАТЕЛЬНЫЕ МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

DESCRIPTION MODES OF INFORMATION PROTECTION IN SYSTEMS OF ELECTRONIC DOCUMENT TURNOVER OF SPECIAL PURPOSE

Рассматриваются решаемые задачи и выполняемые функции систем электронного документооборота специального назначения в составе государственных информационных систем. Определяются особенности и условия обработки различных видов электронных документов, влияющие на эффективность защиты электронного документооборота. Приводятся описательные модели, учитывающие динамику обработки электронных документов.

The tasks to be solved and the functions performed by electronic document management systems for special purposes as part of state information systems are considered. The features and processing conditions of various types of electronic documents are determined that affect the effectiveness of the protection of electronic document management. Descriptive models are given that take into account the dynamics of processing electronic documents.

1. Введение. Система электронного документооборота (СЭД) – организационно-техническая система, обеспечивающая процесс создания, управления доступом и распространения электронных документов (ЭД) в компьютерных сетях, а также контроль над потоками документов в организации [1]. В настоящее время СЭД широко применяются в органах государственной власти, в государственных организациях и предприятиях, в различных коммерческих структурах и т.д. Циркулирующие в них электронные документы (ЭД) представляют интерес для многих заинтересованных сторон, начиная от спецслужб иностранных государств и заканчивая организациями-конкурентами и отдельными физическими лицами, имеющими корыстные или иные цели. В этих условиях все более востребованным на практике становится обеспечение безопасности электронного документооборота как с точки зрения сохранения конфиденциальности, целостности и доступности ЭД, так и защиты от нарушения функционирования самих СЭД.

Вместе с тем в документах государственных регуляторов сегодня отсутствуют требования к СЭД в части защиты от угроз электронному документообороту. Действующие нормативные документы, например, ФСТЭК России регламентируют требования к информационным системам в целом или к средствам вычислительной техники, при этом в этих требованиях не учитываются особенности электронного документооборота. В частности, в них не учитывается динамика обработки (создания, исполнения, согласования и т.д.) различных видов ЭД. Учет указанной динамики может не только существенно повлиять на эффективность защиты как «степень достижения поставленной цели защиты» [2] электронного документооборота, но и изменить требования по защите. Для такого учета нужно иметь математические модели динамики обработки ЭД и динамики реализации угроз безопасности ин-

формации в СЭД. До настоящего времени такие модели для СЭД не разрабатывались, а существующие математические модели для ИС не учитывают особенностей функционирования СЭД и динамику обработки в них ЭД. С учетом изложенного тема данной работы, посвященной разработке описательных и функциональных моделей электронного документооборота, является актуальной.

2. Структура и содержание процессов обработки электронных документов в системах электронного документооборота специального назначения. Электронный документооборот – это движение документов, созданных в электронном виде, в организации с момента их создания или момента их получения до завершения исполнения или отправления [3].

По решаемым задачам и выполняемым функциям СЭД в составе государственных информационных систем (ГИС) имеют ряд особенностей, обусловленных составом обрабатываемых документов и отдельными процедурами обработки, характерными для СЭД, обеспечивающих офисную деятельность учреждений, организаций и предприятий в государственном секторе. СЭД, используемые в ГИС, часто относят к информационно-организационным системам специального назначения (СЭД СН) [3].

К СЭД ГИС предъявляются более высокие требования, чем к СЭД, которые применяются в коммерческом секторе, так как большую часть документооборота в этом случае представляет информация государственного значения. Вместе с тем сегодня отсутствуют нормативные документы государственных регуляторов, в которых излагались бы требования к СЭД, несмотря на то, что в настоящее время в федеральных ведомствах используются разнообразные СЭД мирового уровня, крупных российских разработчиков, множество решений мелких компаний и даже индивидуально разработанные системы [1, 4, 5]. Указанные СЭД, как правило, имеют архитектуру «клиент-сервер».

С использованием СЭД решаются специфичные для такого рода систем задачи, связанные с подготовкой документов в электронной форме, их учетом, хранением, поиском в базе документов, рассылкой (в случае необходимости обеспечения коллективной работы с одним и тем же документом), модификацией, уничтожением, обеспечением защиты от несанкционированного доступа к документам и др.

В электронном документообороте для каждого вида документа создаётся отдельный автоматизированный документационный процесс, представляющий собой набор логически взаимосвязанных этапов обработки документов, на каждом из которых происходит трансформация определённых свойств документа [6]. При этом выполняется целый ряд специфичных действий, обуславливающих отличия СЭД СН от обычных систем офисного типа [7].

В ходе такого документационного процесса реализуются различные виды обработки документов, в том числе: общие виды обработки – создание, редактирование, переименование, сохранение, перемещение по маршруту, помещение в папку, индексирование, удаление; специализированные виды обработки – экспертиза, согласование, визирование, подписание, регистрация, классификация, исполнение, контроль, связывание документов по ссылкам, поиск и другие, определяемые спецификой документооборота в конкретном органе или организации.

Особенности СЭД СН обусловлены содержанием решаемых задач и составом реализуемых функций и процедур в ходе документооборота, которые могут существенно различаться для таких документов различного вида (входящие, исходящие, внутренние и организационно-распорядительные). При этом, угрозы безопасности информации в СЭД СН имеют определенную направленность на несанкционированные действия относительно циркулирующих в СЭД документов. а меры защиты ЭД применяются как для защиты операционной среды от проникновения с целью последующей

реализации указанных действий, так и для защиты определенных документов с соответствующим разграничением доступа к ним даже внутри операционной среды СЭД СН.

До настоящего времени описательные и формализованные функциональные модели функционирования СЭД СН как объектов защиты от угроз безопасности информации практически не разрабатывались, что привело к игнорированию специфики защиты электронного документооборота в СЭД СН. Такой подход привел к тому, что отсутствие привязки мер защиты к реализуемым функциям документооборота существенно искажает результаты оценки эффективности мер защиты и такая оценка часто оказывается некорректной. Кроме того, практически невозможной становится оценка эффективности защиты конкретных видов документов от копирования, модификации, уничтожения или реализации иных несанкционированных действий относительно каждого из таких документов.

В обобщенном виде информационный процесс в СЭД СН может быть представлен в виде совокупности типовых процедур, касающихся документооборота входящего, исходящего, внутреннего и организационно-распорядительного документов [8].

Информационные процессы реализуются определенными компонентами прикладного программного обеспечения (ПО), каждый из которых обеспечивает решение конкретного круга задач обработки документированной информации. Наиболее характерными действиями при этом являются действия по несанкционированному копированию ЭД, модификации их содержания, а также блокированию доступа к программному и информационному обеспечению СЭД. В результате противоправных действий возникает множество угроз безопасности информации.

В обобщенном виде информационный процесс в СЭД СН с учетом взаимосвязи частных информационных процессов, составляющих их процедур, используемых для реализации этих процедур компонентов ПО и возникающих в процессе реализации такого рода информационных процессов угроз безопасности информации, может быть представлен следующим образом [8].

Обозначим:

$IP = \{ip_i\}$ – множество информационных процессов ($i = \overline{1, I}$) различного назначения, реализуемых в СЭД СН;

$Pr = \{pr_{ij}\}$ – множество типовых процедур ($j = \overline{1, J}$) обработки документированной информации в СЭД СН, составляющих i -й информационный процесс;

$PO = \{po_{jk}\}$ – множество компонентов ($k = \overline{1, K}$) прикладного программного обеспечения (ПО), используемых для решения конкретных задач обработки документированной информации при реализации j -й информационной процедуры в СЭД СН;

$УБИ_k = \{уби_{km}\}$ – множество угроз ($m = \overline{1, M}$) безопасности информации, воздействующих на k -й компонент ПО в СЭД СН.

Каждый ip_i информационный процесс рассматривается как определенная последовательность информационных процедур. При этом одна и та же информационная процедура из их множества Pr_i может быть включена в последовательность различных информационных процессов.

Одинаковые компоненты ПО из их множества PO_j могут использоваться для реализации различных информационных процедур в составе информационных процессов различного назначения, а с одной и той же угрозой безопасности информации из их множества $УБИ_k$ может быть связано воздействие на различные компоненты ПО в зависимости от реализуемых этими компонентами ПО функций.

Применительно к СЭД СН указанные множества могут быть представлены в виде:

$$Pr = \bigcup_{i=1}^I Pr_i; Po = \bigcup_{j=1}^J Po_j; УБИ = \bigcup_{k=1}^K УБИ_k.$$

Соответствие процедур обработки документированной информации в СЭД компонентам ее ПО и угрозам безопасности информации может быть формально записано в виде

$$ip_i \hat{=} Pr_i \hat{=} Po_j \hat{=} УБИ_k,$$

где $\hat{=}$ – знак соответствия.

В обобщенном виде информационные процессы в СЭД СН представлены на рисунке.

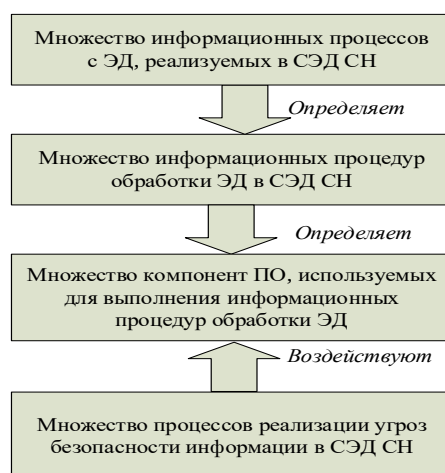


Рис. Обобщенное представление информационных процессов в СЭД СН в условиях угроз безопасности информации

В качестве примера в таблице приведен фрагмент функциональной модели и описание перечня, содержания и взаимосвязей всех существенных для решения вопросов оценки защищенности электронного документооборота процедур информационного процесса документооборота и функций, выполняемых в ходе реализации этих процедур, а также оценены времена выполнения этих функций для входящего документа.

Для всех этих процессов рассматриваемые процедуры во времени выполняются как последовательно, так и параллельно, что существенно затрудняет оценку суммарного времени обработки ЭД.

Следует отметить, что на время обработки различных документов существенно влияют несанкционированные действия, которые могут выполняться в ходе реализации угроз безопасности информации в СЭД СН, а также предпринимаемые меры защиты от противоправных действий.

Таблица

Процедуры и функции обработки входящего ЭД в СЭД СН

Наименование процедуры	Обозначение процедуры	Наименование функции	Обозначение функции	Время выполнения функции, мин
1	2	3	4	5
Графическое представление процесса обработки входящего электронного документа <pre>graph LR; ПВД --> РВД; РВД --> СВД; СВД --> СУА; СУА --> ПКР; ПКР --> ФКИ; ФКИ --> КИД; СУА --> ИсхРКК; ИсхРКК --> ВхРКК; ВхРКК --> ВДД; КИД --> ВДД; subgraph "Должностные лица взаимодействующих подразделений"; ИсхРКК; ВхРКК; ВДД; end</pre>				
Процедура приема входящего документа (ПВД)	$pr_{1.1}$	Прием входящей корреспонденции, пришедшей по электронной почте	$f_{1.1.1}$	0,2 – 5
		Размещение всех видов поступающих документов в буферном пространстве рабочей станции делопроизводителя (РСД),	$f_{1.1.2}$	0,5 – 3
Процедура регистрации входящих документов (РВД)	$pr_{1.2}$	Формирование регистрационно-контрольной карточки	$f_{1.2.1}$	1 – 5
		...		
		Внесение в базу данных электронного содержания документа в виде текста письма электронной почты	$f_{1.2.4}$	1 – 3
...				
Процедура вывода документа из действия (ВДД)	$pr_{1.10}$	Уничтожение электронного документа;	$f_{1.10.1}$	0,5 – 2
		Передача электронного документа на архивное хранение	$f_{1.10.2}$	0,5 – 2

3. Заключение. Разработанные таким образом описательные модели процессов обработки основных видов ЭД в СЭД СН могут быть использованы при разработке соответствующих функциональных моделей.

ЛИТЕРАТУРА

1. Система электронного документооборота – что это и зачем нужно? [Электронный ресурс] – Режим доступа <https://ip-on-line.ru/servisy/sistema-elektronnogo-dokumentooborot.html>. Дата обращения 4.06.2019.

2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения [Электронный ресурс] / утвержден приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст. – Режим доступа: <http://docs.cntd.ru/document/1200058320>. Дата обращения 4.06.2019.

3. ГОСТ Р 7.0.8-2013 Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения [Электронный ресурс] / утвержден приказом Федерального агентства по техническому регулированию и метрологии от 17.10.2013 № 1185-ст. – Режим доступа : <https://base.garant.ru/70650732/>. Дата обращения 4.06.2019.

4. Кленина, В. И. Внедрение информационной системы электронного документооборота и делопроизводства в органах государственной власти [Текст] / В. И. Кленина, Е. Н. Софинская // Человеческий капитал. – 2012. – № 7.

5. Левашина, Е.О. Анализ использования систем электронного документооборота органами исполнительной власти Российской Федерации [Электронный ресурс] / Е.О. Левашина. – Режим доступа: <https://cyberleninka.ru/article/n/analiz-ispolzovaniya-sistem-elektronnogo-dokumentoooborota-organami-ispolnitelnoy-vlasti-rossiyskoy-federatsii>. Дата обращения 4.06.2019.

6. Системы электронного документооборота. Актуальные проблемы авиации и космонавтики – 2014. Информационные технологии [Электронный ресурс] / А.З. Юзаева, Л.М. Савченко – Режим доступа: <https://cyberleninka.ru/article/n/sistemy-elektronnogo-dokumentoooborota>. Дата обращения 4.06.2019.

7. Система электронного документооборота (СЭД): что такое, особенности и рекомендации [Электронный ресурс]. – Режим доступа: <https://fb.ru/article/279568/sistema-elektronnogo-dokumentoooborota-sed-cto-takoe-osobennosti-i-rekomendatsii>. Дата обращения 4.06.2019.

8. Рубцова, И.О. Обобщенное представление информационных процессов в системах электронного документооборота специального назначения в условиях угроз безопасности информации [Текст] / И.О. Рубцова, О.С. Авсентьев // Вестник Воронежского института МВД России. – 2017. – № 4. – С. 108–115.

СВЕДЕНИЯ ОБ АВТОРАХ

Авсентьев Олег Сергеевич. Профессор кафедры информационной безопасности. Доктор технических наук, профессор.

Воронежский институт МВД России.

E-mail: osaos@mail.ru

Россия, 394065, г. Воронеж, пр-т. Патриотов, 53. Тел. (473) 2005 — 242.

Рубцова Ирина Олеговна. Аспирант кафедры организации и технологии защиты информации.

Белгородский университет кооперации, экономики и права.

E-mail: kaf-otzi@bukep.ru.

Россия, Белгород, ул. Садовая, 116а, 308023.

Avsentev Oleg Sergeevich. Professor of the chair of Information Security. Doctor of Technical Sciences. Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: ib@vimvd.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-5236.

Rubcova Irina Olegovna. Postgraduate student of the Department of organization and technology of information protection. Belgorod University of Cooperation, Economics and Law.

E-mail: kaf-otzi-zav@bukep.ru

116a ul. Sadovaya, Belgorod, Russian Federation, 308023, Phone. (472) 226-38-31.

Ключевые слова: система электронного документооборота, информационный процесс, защита от угроз безопасности информации, безопасность электронного документооборота.

Key words: electronic document management system, information process, protection against information security threats, electronic workflow security.

УДК 004.056:519.1.

Асанов Александр Сергеевич;
Ивануткин Александр Григорьевич,
доцент, кандидат военных наук

ИНТЕГРАЦИЯ СИСТЕМ ВОЕННОЙ СВЯЗИ В ЕДИНОЕ ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО

INTEGRATION OF COMMUNICATION, ELECTRONIC SUPPORT AND AUTOMATE THE MANAGEMENT OF AVIATION

В статье раскрыты понятия управления и информации, представлены основные свойства информации, дано определение интеграции систем военной связи. Кроме того раскрыта структура организации как процесса деятельности, так и результата деятельности. Определены фазы завершенности цикла деятельности. В ходе обоснования подхода к интеграции систем военной связи раскрыта и обоснована общая ее структура, объект и предмет.

Revealed the notions of control and information, presents the basic properties of information, the definition of the integration of communications, electronic security and automation controller. In addition the structure of an organization as a process of activities and performance. Defined phase of completion of the work cycle. Justifying approach to the integration of communications, electronic security and automation control disclosed and justified its overall structure, object and subject.

Для решения задач устойчивого, непрерывного и оперативного управления войсками (силами) и оружием создается система военной связи.

Во многих литературных источниках система военной связи определена как организационно-техническое объединение сил и средств связи, создаваемое для обеспечения обмена всеми видами сообщений (информации) в системе управления войсками (силами) и оружием.

Интеграция – процесс соединения, слияния, связывающий разрозненное в единое целое [1]; объединение в целое каких-либо частей или элементов [2].

Интеграция – понятие, означающее состояние связанности отдельных дифференцированных частей и функций системы, организма в целое, а также процесс, ведущий к такому состоянию [3].

Механизм интеграции содержит в себе все соединительные аспекты, составляющие основу соединения в пределах определенной действительности. Интеграция может быть временной (для выполнения частных задач) и постоянной.

Для исследования процессов интеграции сложных информационных систем, таких как системы военной связи может быть применен интеграционный подход, при котором в целях исследования построения данных систем, идеологии и технологии интеграции информационных процессов, помимо большого набора типов данных и технологий имеется соответствующая методология или хотя бы концепция, оптимально объединяющая это разнообразие данных и технологий [4].

Сам процесс интеграции информационных процессов можно представить как организацию определенного вида деятельности, включающий в себя 3 уровня деятельности: организационную деятельность, организационно-технологическую деятельность и техническую деятельность.

Если интеграцию рассматривать как процесс организации деятельности на всех трех уровнях, то естественно необходимо рассмотреть содержание понятия «организация». Под организацией в статье понимается: 1) внутренняя упорядоченность, согласо-

ванность взаимодействия более или менее дифференцированных и автономных частей целого, обусловленная его строением; 2) совокупность процессов или действий, ведущих к образованию и совершенствованию взаимосвязей между частями целого; 3) объединение людей, совместно реализующих некоторую программу или цель и действующих на основе определённых процедур и правил [3].

В данном случае будет использоваться понятие «организация», в основном, в первом и во втором значении, то есть и как процесс (второе значение), и как результат этого процесса (первое значение). Третье значение также используется – при описании коллективной научной и практической деятельности, управления проектами интеграции информационных процессов в объединениях, соединениях и частях.

Организовать деятельность означает упорядочить ее в целостную систему с чётко определёнными характеристиками и логической структурой и процессом ее осуществления – временной структурой. Логическая структура включает в себя следующие компоненты: субъект, объект, предмет, формы, средства, методы деятельности, ее результат. Внешними по отношению к этой структуре являются следующие характеристики деятельности: особенности, принципы, условия, нормы.

Процесс осуществления деятельности мы будем рассматривать в рамках проекта, реализуемого в определённой временной последовательности по фазам, стадиям и этапам, причём последовательность эта является общей для всех видов деятельности. Завершённость цикла деятельности (проекта) определяется тремя фазами: фаза проектирования, результатом которой является построенная модель создаваемой системы и план ее реализации; технологическая фаза, результатом которой является реализация системы; рефлексивная фаза, результатом которой является оценка реализованной системы и определение необходимости либо ее дальнейшей коррекции, либо «запуска» нового проекта.

Таким образом, можно предложить следующую «схему методологии интеграции»:

1. Характеристики интеграции: особенности, принципы, условия, нормы процесса интеграции (нормативно-правовая база).
2. Логическая структура интеграции: субъект, объект, предмет, формы, средства, методы, результат деятельности.
3. Временная структура интеграции: фазы; стадии; этапы интеграции.

Таким образом методология интеграции систем военной связи – учение о теории и практике их интеграции, включающее целостную, логически взаимосвязанную совокупность терминологии, теоретических, концептуальных и научно-практических основ, принципов и методов, используемых при решении проблем интеграции сложных технических систем в военной науке.

Методология интеграции содержит в себе совокупность методов интегрирования, принципов построения систем военной связи, как сложных систем, теорий их анализа и синтеза, а также теорий системного и комплексного описания процесса интеграции данных систем.

Естественно на первой фазе исследования процесса интеграции необходимо всецело рассмотреть особенности и принципы функционирования данных систем в едином информационном пространстве в современных условиях, а также провести анализ существующей нормативно-правовой базы. Наиболее сложным процессом на данном этапе является процесс организации взаимодействия должностных лиц, участвующих в организации связи.

Взаимодействие – это управляемый процесс обмена информационными, радиоэлектронными и другими воздействиями между взаимодействующими системами в ходе выполнения поставленной задачи.

Взаимодействие представляет собой объективно существующий, управляемый процесс. В результате целенаправленной деятельности координирующих органов и органов управления взаимодействие обретает организованный характер и выступает как согласован-

ные по оказанию содействия друг другу при выполнении этих задач [5]. В результате целенаправленной деятельности командующих, командиров (начальников) и штабов взаимодействие обретает организованный характер и выступает как согласованные действия войск (сил) по оказанию содействия друг другу при выполнении оперативных и боевых задач.

Взаимодействие, в зависимости от уровня его организации может быть стратегическим, оперативным и тактическим. Разумеется, возможны сочетания этих видов. В современных условиях сочетание, а именно комбинированные методы взаимодействия будут встречаться наиболее часто.

Для управления взаимодействием обычно создается система управления, для которой зачастую используются неосновные каналы связи и формируются временные органы управления. Такие свойства системы управления взаимодействием, как качество, устойчивость и оперативность в значительной, даже в решающей степени определяют эффективность взаимодействия [6].

Свойство устойчивости является фундаментальным свойством любой информационной системы. Данное свойство интуитивно может быть определено как некоторое постоянство, неизменность определенной структуры (статическая устойчивость) и поведения системы (динамическая устойчивость). Применительно к информационным системам определение устойчивости было дано выдающимся русским математиком Ляпуновым А.М.: «Устойчивость – это способность системы функционировать в состояниях близких к равновесному, в условиях постоянных внешних и внутренних возмущающих воздействий».

Взаимодействие неизбежно приводит к внешним и внутренним воздействиям для информационных систем, которые обязательно как следствие потребуют усиление такого свойства системы как устойчивость. По Б.С. Флейшману [7], различают активную и пассивную форму устойчивости. Активная форма устойчивости (надежность, отказоустойчивость, живучесть и пр.) присуща сложным системам, поведение которых основано на акте решения. Здесь акт решения определяется как выбор альтернатив, стремление системы достигнуть предпочтительное для нее состояние – целенаправленное поведение, а это состояние – ее целью. Пассивная форма (прочность, сбалансированность, гомеостазис) присуща простым системам, не способным к акту решения.

Так как штатный режим функционирования информационных систем, как правило, далек от равновесного, центральным элементом в данном случае является понятие структурно-функциональной устойчивости. При этом внешние и внутренние информационно-технические воздействия постоянно изменяют само равновесное состояние информационной системы. Соответственно мерой близости позволяющей решать изменяется ли поведение системы и как существенно под действием возмущения, здесь является множество выполняемых функций при взаимодействии [8].

В целях получения объективных результатов организации интеграции возникает необходимость разработки модели данного процесса.

Объектом интеграции является система управления войсками (силами). Предметом – система военной связи. Субъектом – должностное лицо, организующее функционирование данной системы в любых условиях обстановки. Для осуществления процесса интеграции необходимы формы, средства и методы интеграции вышеуказанных систем.

Система – совокупность элементов, находящихся в отношениях и связях между собой и образующих определенную целостность, единство [9].

Элементами системы военной связи являются узлы связи, опорная сеть связи, линии прямой связи, линии связи привязки, сеть связи с подвижными объектами, сеть фельдъегерско-почтовой связи, система управления связью, система технического обеспечения связи и АСУ, резервы.

Таким образом, в данной статье предложена общая структура методологии интеграции систем военной связи в единое информационное пространство, которая включа-

ет в себя 3 уровня: организационный, организационно-технологический и технический, которые характеризуются организационным и техническим взаимодействием между собой и обладающие достаточной устойчивостью в ходе организации деятельности субъектов интеграции всех звеньев управления на этапах проектирования, технологическом и этапе оценки реализованной интеграционной системы военной связи. Предложенная структура может быть применима для исследования проблем интеграции различных систем военного назначения.

ЛИТЕРАТУРА

1. Секлитова Л.А., Стрельникова Л.Л. Словарь космической философии. М.: Армита-Русь, 2004. С. 64-65.
2. Современный словарь иностранных слов. М.: Русский язык, 1993. С. 240.
3. Советский энциклопедический словарь. 2-е издание. М.: Советская Энциклопедия, 1982. С. 494, 197.
4. Ермишян А.Г. Теоретические основы построения систем военной связи в объединениях и соединениях: Учебник. Часть 1. Методологические основы построения организационно-технических систем военной связи. СПб.: ВАС, 2005. С. 57.
5. Афанасьев Ю.И. Теория взаимодействия. Анализ в условиях синхронизации процесса //Образовательные ресурсы и технологии. – 2014. - №3(6). [Электронный ресурс]. URL:http://www.muiv.ru/vestnik/pdf/pp/ot_2014_3_47_52.pdf.
6. Афанасьев Ю.И. Обоснование системы показателей эффективности взаимодействия войск (сил) противовоздушной обороны// Военная мысль. 2011. №6. С 47-51.
7. Калинин В.Н., Резников Б.А., Варакин Е.И. Теория систем и оптимального управления. Л.: Изд-во ВКА, 1979. Ч. 1. С. 456.
8. Афанасьев Ю.И. Устойчивости автоматизированных систем. Концепция устойчивого взаимодействия //Образовательные ресурсы и технологии. – 2014. - № 5(8). [Электронный ресурс]. URL:http://www.muiv.ru/vestnik/pdf/pp/ot_2014_5_86-94.pdf.
9. Фролов И.Т. Философский словарь. 5-е изд. М.: Политиздат, 1987. С. 427.

СВЕДЕНИЯ ОБ АВТОРАХ

Асанов Александр Сергеевич, слушатель кафедры (управления воинскими частями связи и РТО авиации).

ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: asan007@yandex.ru

Россия, 394064, Воронеж, ул. Старых Большевиков, 54а.

Тел. 8-919-1821484.

Ивануткин Александр Григорьевич, доцент кафедры (управления воинскими частями связи и РТО авиации).

Кандидат военных наук.

ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

Россия, 394064, Воронеж, ул. Старых Большевиков, 54а.

Тел. 8-951-872-83-02

Asanov Alexander Sergeevich. Learner department management of military units of communication and RTS aviation).

«Air force academy named by prof. N.E. Zhukovski and U.A. Gagarin» (c. Voronezh).

Work address: Russia,394064, Voronezh, St. Bolshevikov st., 54a.

Tel. 8-919-1821484.

Ivanutkin Alexander Grigoryevich, associate Professor of department (management of military units of communication and RTS aviation).

Candidate of military Sciences.

«Air force academy named by prof. N.E. Zhukovski and U.A. Gagarin» (с. Voronezh).

Work address: Russia, 394064, Voronezh, St. Bolshevikov st., 54a.

Tel. 8-951-872-83-02.

Ключевые слова: интеграция, система военной связи, организация деятельности, информационный процесс.

Keywords: integration, communications, electronic security and automation management, organization of activities, information process.

УДК 621.39

Бондарь Константин Михайлович,
кандидат технических наук, доцент;

Дунин Вадим Сергеевич,
кандидат технических наук

НАПРАВЛЕНИЯ РАЗВИТИЯ ПОТЕНЦИАЛА КАДРОВОГО ОБЕСПЕЧЕНИЯ В СФЕРЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ТЕРРИТОРИАЛЬНЫХ ПОДРАЗДЕЛЕНИЙ МВД РОССИИ

DIRECTIONS OF DEVELOPMENT OF POTENTIAL OF PERSONNEL FACILITIES IN THE FIELD OF PREPARING INFORMATION SAFETY SPECIALISTS FOR THE TERRITORIAL DIVISIONS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

В статье обозначены насущные проблемы становления кадрового потенциала в сфере подготовки специалистов информационной безопасности для МВД России, определены приоритетные направления развития и предложены практические рекомендации по совершенствованию подготовки специалистов новой формации в области информационного обеспечения и информационной безопасности профессиональной и служебной деятельности ОВД.

The article identifies the pressing problems of the formation of personnel potential in the field of training information security specialists for the Ministry of Internal Affairs of Russia, identified priority areas of development and proposed practical recommendations for improving the training of specialists of the new formation in the field of information support and information security professional and performance activities of the MIA of Russia.

Существующие ныне тенденции положительного и негативного влияния информационных технологий на развитие общества формируют актуальную необходимость учета и реагирования на информационные угрозы, способные нанести разнообразный по уровню вред и ущерб государству, обществу, личности. В этом плане законодатель России отражает значительный перечень таких угроз информационной безопасности, среди которых имеются в определенном смысле уже «классические», но и новые направления, определяемые технологическими и социальными факторами.

При этом основа эффективного обеспечения противодействия им определяется в комплексном, целенаправленном, взаимоувязанном использовании разнообразных ресурсов. В частности, в рамках данной работы речь пойдет о кадровом потенциале, специализированно подготавливаемом для прогнозирования, обнаружения, сдерживания, предотвращения, отражения информационных угроз и ликвидации последствий их проявления [1].

Проблема развития кадрового потенциала стала наиболее острой и обсуждаемой после того, когда информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства [5]. Это в свою очередь спровоцировало появление новых видов угроз в виде воздействий на социальную, культурную, технологическую, политическую и правоохранительную сферы. Доктрина информационной безопасности Российской Федерации напрямую указывает на опасности проявления угроз, происходящих в технической сфере – информационно-технические (ИТВ) и в гуманитарной – информационно-психологические воздействия (ИПВ) [1]. Как известно, МВД России является федеральным органом исполнительной власти в ведении которого находятся ключевые массивы данных о гражданах, событиях, об обстоятельствах осуществления противоправных деяний, предоставления государственных услуг и статистической информации. Органы внутренних дел сегодня испытывают серьезные противодействия со стороны злоумышленников, сталкиваются с современными технологически и кибернетически сложными видами преступлений, объекты информатизации которых (автоматизированные информационные системы, инфокоммуникационные ресурсы технических средств и систем) подвергаются опасным атакам.

В этих условиях активного воздействия на объекты МВД России со стороны потенциальных злоумышленников (киберпреступники, мошенники) требуются оперативные реакции на пресечение, предупреждение, выявление и расследование инцидентов информационной безопасности. Необходимы специалисты достаточного уровня квалификации, способные к противостоянию от противоправных воздействий на новом современном этапе развития информационного общества, цифровой экономики и интеллектуальных технологий [4].

В настоящее время существуют проблемные вопросы, требующие подготовки специалистов новой формации в области информационного обеспечения и информационной безопасности профессиональной и служебной деятельности:

- развитие информационного противодействия терроризму и экстремизму на основе имитационного моделирования информационных операций;
- повышение качества подготовки специалистов в области раскрытия и расследования преступлений, связанных с инфокоммуникационными технологиями (кибермошенничество, кибербуллинг, кибератаки);
- совершенствование технологических способов и методов применения прикладных сервисов обеспечения оперативно-служебной деятельности ИСОД МВД России, за счет наделения их интеллектуальным потенциалом и глубокой интеграции;
- обновление современных подходов к обеспечению условий создания надежной, адаптивной системы информационной безопасности ОВД.

Реалии подготовки специалистов в сфере информационной безопасности для МВД России охватывают обеспечение части указанных вопросов и проблем. В частности, такая подготовка ведется в Воронежском институте МВД России по специальностям и направлениям подготовки: «Компьютерная безопасность», «Инфокоммуникационные технологии и системы специальной связи», «Информационная безопасность телекоммуникационных систем», «Правоохранительная деятельность», «Информационная безопасность, направленность «Методы и системы защиты информации, информационная безопасность».

Вместе с тем, в рамках нормального функционирования и обеспечения имеющихся обозначенных информационных задач на уровне страны в МВД России следует отметить следующие недостатки:

- специалисты, выпускающиеся из Воронежского института МВД России, практически, не распределяются по территориям Сибирского и Дальневосточного федеральных округов [3];
- научно-практический потенциал данных территорий в рассматриваемой предметной области выглядит довольно скромно (например, на территории УМВД России по Хабаровскому краю в образовательных и научно-практических организациях

МВД России нет ни одного доктора наук, практические работники подготавливались по смежным специальностям и в лучшем случае проходили дополнительное обучение по требуемым направлениям);

- попытки открытия одной из требуемых специальностей в ДВЮИ МВД России, как единственной образовательной организации системы МВД России на Дальнем Востоке, многократно обсуждаемые в ДГСК МВД России с предоставлением необходимой документации о такой потенциальной возможности, начиная с 80-90 гг. XX века, так и не увенчались успехом.

Обозначенные выше проблемы и недостатки можно разрешить, если предпринять конкретные действия и предложить следующие направления решений отмеченных противоречий:

- открытие профильной специальности по применению безопасных информационных технологий в правоохранительной деятельности в ДВЮИ МВД России (например, «Безопасность информационных технологий в правоохранительной сфере»)
- потребуется существенное обновление материально-технической базы института;
- активизация подготовки гражданских специалистов с ориентацией на МВД России (например, в региональных образовательных организациях: «ДВГУПС», «ТОГУ», «ДВФУ», «КнАГУ») – потребуется активная пропаганда среди гражданской молодежи;
- обеспечение более широкого формирования направлений на обучение и распределение из Воронежского института МВД России (текущая практика говорит о подготовке для региональных УМВД России по 1-2 специалиста, что явно недостаточно для обеспечения требуемого кадрового потенциала) – потребуется более активное взаимодействие с руководителями территориальных органов внутренних дел;
- развитие научного потенциала по направлению подготовки «Информационная безопасность» – создание специализированных советов по федеральным округам к 2022 году [2] (потребуется докторов наук в требуемом количестве) или объединенных региональных советов с преференциями по созданию в отличие от общероссийских требований (например, в Новосибирске, но с обязательным льготным доступом аспирантов (адъюнктов) от Дальнего Востока).

ЛИТЕРАТУРА

1. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2016 № 646. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Белов Е.Б. Приоритеты профессионального образования по реализации мероприятий федерального проекта «Информационная безопасность» // Большой национальный форум информационной безопасности «Инфофорум-2019». URL: <https://infoforum.ru/conference/conference/program/cid/51> (дата обращения: 01.06.2019).
3. Белов Е.Б. Технологии по определению потребности в специалистах по защите информации и оценке степени подготовленности государственных гражданских служащих в сфере информационной безопасности // Восьмой ежегодный форум «Актуальные вопросы информационной безопасности», 19-20 июня 2019. URL: <https://icdv.ru/wp-content/uploads/2019/06/7.Belov-E.-Tehnologii-po-opredeleniyu-potrebnosti-v-spetsialistah-po-zashhite-informatsii-i-otsenke-stepeni-podgotovlennostigosudarstvennyh-grazhdanskih-sluzhashhih-v-sfere-informatsionnojbezopasnosti.pptx> (дата обращения: 22.06.2019).
4. Марченко А.В. Некоторые вопросы кадрового обеспечения в области информационной безопасности и методического обеспечения дополнительного профессионального образования в указанной области // Восьмой ежегодный форум «Актуальные вопросы информационной безопасности», 19-20 июня 2019. URL: <https://icdv.ru/wp-content/uploads/2019/06/6.Marchenko-A.-Metodicheskoe-obespechenie-DPO-v-oblasti-informatsionnoj-bezopasnosti.ppt> (дата обращения: 22.06.2019).

5. Разработка ведомственной (Минобрнауки России) целевой программы «Подготовка кадров в области информационной безопасности на 2022 - 2028 г.»
URL:http://dep-economy44.ru/uploads/files/deyatelnost/projectmanagement/NP__FP__RP/2019/2/FP_IB.pdf (дата обращения: 10.06.2019).

СВЕДЕНИЯ ОБ АВТОРАХ

Бондарь Константин Михайлович. Профессор кафедры информационного и технического обеспечения органов внутренних дел.

Дальневосточный юридический институт МВД России.

Кандидат технических наук, доцент.

E-mail: bondar_km@mail.ru.

Россия, 680020, Хабаровск, пер. Казарменный, д.15.

Тел. 8(4212)46-52-31.

Дунин Вадим Сергеевич. Заместитель начальника кафедры информационного и технического обеспечения органов внутренних дел.

Дальневосточный юридический институт МВД России.

Кандидат технических наук.

E-mail: vdunin2@mvd.ru.

Россия, 680020, Хабаровск, пер. Казарменный, д.15.

Тел. 8(4212)46-52-31.

Bondar Konstantin Mikhailovich. Professor of the Department of information and technical support of internal Affairs.

Far Eastern law Institute of the Russian interior Ministry.

Candidate of technical Sciences, associate Professor.

E-mail: bondar_km@mail.ru.

Russia, 680020, Khabarovsk, Ss. Kazarmennyj, d.15.

Phone 8(4212) 46-52-31.

Dunin Vadim Sergeevich. Deputy Head of the Department of information and technical support of internal Affairs.

Far Eastern law Institute of the Russian interior Ministry.

Candidate of technical Sciences.

E-mail: vdunin2@mvd.ru.

Russia, 680020, Khabarovsk, Ss. Kazarmennyj, d.15.

Phone 8(4212) 46-52-31.

Ключевые слова: кадровый потенциал, информационная безопасность, информационное противодействие, киберпреступность.

Keywords: human resources, information security, information counter, cybercrime.

УДК 004.056, 378.1

Безрядин Владислав Анатольевич,
кандидат технических наук;
Хворов Руслан Александрович,
кандидат технических наук

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ РАДИОКОНТРОЛЯ В ВОЕННО-ВОЗДУШНЫХ СИЛАХ

MAIN DIRECTIONS OF IMPROVEMENT RADIO CONTROL IN THE MILITARY-AIR FORCES

Рассматриваются направления повышения оперативности радиоконтроля. Обоснованы основные направления повышения оперативности радиоконтроля за счет автоматизации отдельных подэтапов подготовки и проведения радиоконтроля.

We consider the direction of increasing the efficiency of radio control. The main directions of improving the efficiency of radio monitoring through the automation of individual sub-stages of preparation and monitoring of radio monitoring have been substantiated.

В соответствии с Военной доктриной Российской Федерации (утверждена Президентом Российской Федерации 25 декабря 2014 г. № Пр-2976) к одной из основных военных угроз является воспрепятствование работе систем военного управления Российской Федерации, поэтому к основным задачам развития военной организации относятся и задача повышения эффективности и безопасности функционирования системы военного управления.

Обеспечение безопасности связи является одной из важных составных частей в общей системе мер по обеспечению информационной безопасности, сохранению государственной тайны и осуществляется взаимосвязано с мероприятиями оперативной маскировки, противодействия техническим средствам разведки, скрытого управления войсками (силами) и режима секретности.

Утечка информации, передаваемой по средствам и системам военной связи Военно-воздушных сил (ВВС) для обеспечения боевых возможностей авиационных соединений (частей), решаемых ими задач в достижении целей высоко динамичных боевых действий, позволит противнику своевременно создавать комплекс контрмер для снижения как боевой эффективности образцов вооружения и военной техники, так и авиационных соединений (частей) ВВС в целом.

Соответственно возрастает роль радиоконтроля (далее – РК) за соблюдением установленного порядка передачи служебной информации при использовании открытых каналов радиосвязи, который является формой организационно-технического контроля, позволяющего оценить степень утечки информации, составляющей государственную и служебную тайну, по доступным для радиоразведки каналам радиосвязи.

Основным противоречием, которое определяет направление исследований по повышению оперативности РК, является, с одной стороны – расширение возможностей радиоразведки по добыванию информации, увеличение объемов передаваемой по радиосвязи информации в интересах управления авиационными частями и подразделениями ВВС, а с другой – необходимость повышения возможностей органов безопасности связи в части оперативности РК, с целью своевременного принятия мер по безопасности связи в условиях существующей ограниченности сил и средств РК.

В результате анализа факторов, влияющих на оперативность РК в ВВС, задач, осуществляемых при проведении РК, определены следующие направления повышения оперативности РК:

внедрение автоматизированных комплексов обработки информации по ключевым словам (с целью выявления информативных файлов из общего количества файлов, полученных в ходе проведения РК) и автоматизация процесса формирования документов отчетности по результатам РК;

формирование типового перечня ключевых слов для обработки информации, полученной в ходе проведения РК;

автоматизация процесса планирования РК (оценка потенциальной разведдоступности объектов защиты, оценка потенциальной информативности каналов радиосвязи (КРС) объектов защиты, обоснования сил и средств на проведение РК, формирование задания на проведение РК);

автоматизация процесса выявления признаков нарушений при передаче сообщений по линиям связи.

В целом реализация указанных направлений повышения оперативности РК приведет к:

своевременной разработке и внедрению рекомендаций по безопасному применению средств связи и закрытию каналов возможной утечки сведений, подлежащих засекречиванию при использовании технических средств связи;

выявления и оперативного пресечения нарушений правил пользования техническими средствами связи, требований скрытого управления войсками (силами), установленных режимов работы технических средств связи и мер радиомаскировки.

Применительно к РК показателем оперативности РК целесообразно определить показатель $O_{РК}$, который позволяет оценить время выполнения всех операций (мероприятий) РК, начиная от его планирования и заканчивая принятием мер по результатам выявленных в ходе проведения РК нарушений установленного порядка ведения обмена информацией (радиопереговоров):

$$O_{РК} = \frac{1}{T_{подг} + T_{пров}}, \quad (1)$$

где $T_{подг}$ – время подготовительного этапа РК, рассчитываемое как:

$$T_{подг} = \sum_{i=1}^I t_i, \quad (2)$$

где i – операции подготовительного этапа РК;

I – общее количество подготовительного этапа;

$T_{пров}$ – время этапа проведения РК и обработки информации

$$T_{пров} = \sum_{j=1}^J t_j, \quad (3)$$

где i – операции этапа проведения РК и обработки информации РК;

I – общее количество операций этапа проведения РК и обработки информации РК;

Соответственно, приоритетность направлений повышения оперативности РК будет определяться исходя из максимизации значения оперативности РК (что соответствует минимизации времени подготовительного этапа и этапа проведения РК).

Одним из наиболее критических факторов, влияющим на оперативность РК, является среднее время обработки информации $T_{обр}$.

$$T_{обр} = \frac{t_{ср} \cdot K_{ф общ}}{K_{опер}} \cdot S_{внедр}, \quad (4)$$

где $t_{ср}$ – среднее время обработки одного информативного файла одним оператором;

$K_{ф общ}$ – общее количество информативных файлов, выявленных в процессе предварительной обработки информации по ключевым словам;

$K_{опер}$ – количество операторов по обработке информации;

$S_{внедр}$ – степень внедрения автоматизированных комплексов обработки информации, принимающая значения от некоторого значения S , определяемого эмпирическим (экспертным) путем (степень внедрения максимальна), и принимающего значение, близкое к нулевому значению (но отличное от нуля, так как среднее время обработки информации всегда больше нулевого значения), и до единицы (степень внедрения минимальна).

В данном подходе предполагается, что часть операций операторов по обработке информации будет автоматизирована (например, при выявлении признаков нарушений при обработке информативных файлов).

В результате оценки возможностей путей повышения оперативности РК направления были определены следующие направления, представленные в таблице 1.

Особенностью первого направления, включающего оценку потенциальной разведдоступности объектов защиты, оценка потенциальной информативности КРС объектов защиты, обоснования сил и средств на проведение РК, формирование задания на проведение РК, является то, что в едином информационном пространстве реализуются в автоматизированном виде различные этапы планирования РК от оценки потенциальной разведдоступности объектов защиты до формирования задания на проведение РК, и тем самым снижаются временные затраты на решение данных задач по сравнению с существующими возможностями планирования [1,2].

Особенностью второго направления является реализация автоматизации обработки информации по ключевым словам с целью выявления информативных файлов (файлов, содержащих ключевые слова) из общего количества файлов, полученных в ходе проведения РК. Современные комплексы регистрации информации записывают результаты РК в виде файлов (текстовых, аудио, графических и др.) и должны быть сопряжены с комплексами обработки информации, которые позволяют провести выявление информативных файлов по ключевым словам из общего количества файлов, полученных в ходе проведения РК, для их дальнейшей обработки специалистами (операторами) РК. Такой подход позволяет существенно повысить оперативность РК за счет уменьшения времени выявления информативных файлов из общего количества файлов.

Особенностью третьего направления является реализация в автоматизированном виде процесса выявления признаков нарушений при передаче сообщений по линиям связи. Как показывает анализ процесса обработки информации, одним из критичных этапов с точки зрения обработки информации является этап выявленных потенциально информативных материалов (файлов) специалистами контроля безопасности связи (операторами обработки информации). Несмотря на то, что данный этап является слабо формализуемым и требует работы специалистов «вручную», есть предпосылки для автоматизированной обработки таких файлов (с возможным использованием уже не отдельных ключевых слов, а их сочетаний). Такой подход позволит частично автоматизировать процесс обработки информации соответствующими специалистами.

Особенностью четвертого направления является возможность реализации формализованного представления результатов как предварительной обработки материалов РК (бланки РК), так и окончательной обработки результатов РК, предусматривающей формирование отчетных документов по результатам РК в соответствии с руководящими и нормативными документами по РК.

Таблица 1

Направления автоматизации подэтапов РК в интересах
повышения оперативности РК

	Подэтапы РК, на которых возможна автоматизация	Направления автоматизации подэтапов РК
1	Оценка потенциальной разведдоступности объектов защиты; оценка потенциальной информативности КРС объектов защиты; обоснование сил и средств на проведение РК; формирование задания на проведение РК	Автоматизация процесса планирования РК (оценки потенциальной разведдоступности объектов защиты, оценки потенциальной информативности КРС объектов защиты, обоснования сил и средств на проведение РК, формирования задания на проведение РК)
2	Формирование ключевых слов для выявления информативных файлов, полученных в ходе проведения РК объекта защиты; выявление информативных файлов по ключевым словам; обработки информации из информативных файлов	Автоматизация процесса обработки информации по ключевым словам (с целью выявления информативных файлов из общего количества файлов, полученных в ходе проведения РК). Формирование типового перечня ключевых слов для обработки информации, полученной в ходе проведения РК в интересах автоматизации процесса обработки информации по ключевым словам
3	Обработка информации из информативных файлов с целью выявления признаков нарушений при передаче сообщений по линиям (каналам) радиосвязи	Автоматизация процесса выявления признаков нарушений при передаче сообщений по линиям (каналам) радиосвязи
4	Формирование документов отчетности по информативным материалам РК	Автоматизация процесса формирования документов отчетности по информативным материалам РК

Предварительные расчеты среднего времени обработки материалов РК, проведенные при условии отсутствия комплексов автоматизированной обработки результатов контроля и при условии их использования (в качестве исходных данных анализировалось среднее количество контролируемых каналов, средний объем регистрируемой в них информации, среднее время обработки определенного объема информации в текстовом, графическом и речевом виде) показали, что внедрение автоматизированных комплексов позволит повысить оперативность РК на 25-35 %.

Таким образом, на основе определения возможности автоматизации соответствующих подэтапов РК и предварительной оценки влияния сформированных направлений на повышение оперативности РК, выявлены подэтапы РК, на которых возможно проведение автоматизации. Реализация указанных направлений повышения оперативности РК приведет к повышению оперативности РК на 25-35 %.

ЛИТЕРАТУРА

1. Андриенко А.А. Основы РЭБ, радиоэлектронная защита и безопасность связи. – Л.: ВАС, 1988. – 368 с.
2. Андриенко А.А. Основы радиоэлектронной борьбы, радиоэлектронная защита и безопасность связи и АСУ. Под.ред. М.В. Симонова. – Л.: ВАС, 1989. – 346 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Безрядин Владислав Анатольевич. Старший преподаватель кафедры управления воинскими частями связи и радиотехнического обеспечения авиации. Кандидат технических наук.

ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: bezryadin_vlad@mail.ru.

г. Воронеж, 364064, ул. Старых Большевиков, д.54 а.

Тел. 8-960-111-39-31.

Хворов Руслан Александрович, слушатель кафедры (управления воинскими частями связи и РТО авиации), Кандидат технических наук.

ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: khvoroff@rambler.ru

Россия, 394064, Воронеж, ул. Старых Большевиков, 54а.

Тел.8919 180 60 30.

Vladislav Bezryadin. Senior Lecturer, Chair of Signal Corps Management and Radio-technical support of Air Force. Candidate of Technical Sciences.

Military educational and scientific center of the Air Force Military «Air Force Academy name of professor N. E. Zhukovsky and Y. A. Gagarin»

E-mail: bezryadin_vlad@mail.ru.

Work address: Voronezh, 364064, st. Starykh Bolshevikov, 54 a.

Tel. 8-960-111-39-31.

Khvorov Ruslan Aleksandrovic. Learner department management of military units of communication and RTS aviation), Candidate of technical Sciences.

Military educational and scientific center of the Air Force Military «Air Force Academy name of professor N. E. Zhukovsky and Y. A. Gagarin»

Work address: Russia,394064, Voronezh, St. Bolshevikov st., 54a.

Tel. 8-919-180-60-30.

Ключевые слова: радиоконтроль; оперативность; автоматизация; обработка результатов; этап, подэтап.

Key words: radicontrol; efficiency; automation; processing of results; stage, substage.

УДК 621.391

**Бредихина Елена Владимировна;
Дмитриев Сергей Александрович,**
кандидат технических наук, доцент

АНАЛИЗ АНТЕННЫХ СИСТЕМ ДЛЯ КОМПЛЕКСА ШИРОКОПОЛОСНОЙ РАДИОСВЯЗИ

ANALYSIS OF ANTENNA SYSTEMS FOR THE COMPLEX BROADBAND RADIOCOMMUNICATION

Работа посвящена анализу антенных систем для комплекса широкополосной радиосвязи, который позволяет повысить эффективность использования широкополосного канала связи при его использовании для связи между объектами аэродрома и обеспечения безопасности полетов.

The work is devoted to the analysis of antenna systems for a broadband radio communication complex, which allows increasing the efficiency of using a broadband communication channel when using it for communication between aerodrome facilities and ensuring flight safety.

Эффективное применение ВВСТ для нужд обороны страны требует постоянного совершенствования пунктов управления, оснащенных современными средствами управления, связи и РТО.

Актуальность данной темы в том, что в современных условиях, все чаще возникает необходимость в передаче больших объемов информации с большими скоростями, особенно актуально это становится при использовании видеоконференцсвязи.

Для решения этих задач был разработан комплекс широкополосной радиосвязи, а также специальная антенная система СВЧ диапазона, которая позволяет с успехом решать поставленные задачи.

Комплекс широкополосной радиосвязи построен на базе отечественного одноплатного компьютера Module MB 77.07, который обеспечивает необходимый уровень производительности, поддерживает все современные интерфейсы, обладает высокопроизводительным графическим процессором.

В качестве приемо-передающего устройства используется FPV приемо-передатчик, работающий в диапазоне 5.8 ГГц и 2.4 ГГц, что позволяет обеспечить как пространственное, так и частотное разнесение сигнала, что обеспечит необходимый уровень электромагнитной совместимости. Также данный тип передатчиков при использовании направленной антенны, позволяет создать радиомост дальностью более 5 км.

Внутри помещений для облегчения задачи по интеграции комплекса в систему связи, предлагается использовать диапазон в 2.4 ГГц, поддержку которого имеют все современные ЭВМ и другие мультимедийные устройства.

Так как в комплексе используется криптомаршрутизатор, через который создается защищенное соединение с помощью специальных протоколов передачи данных, а также учитывая то, что волны в данном диапазоне затухают довольно быстро, то создать контролируемую зону для обеспечения безопасного использования беспроводного сегмента локальной вычислительной сети не составит никакого труда [1].

Антенно-фидерная система представляет собой набор из трех антенн, предназначенных для различных вариантов использования. Все разработанные антенны были смоделированы в программной среде «mmana-gal».

Микрополосковая антенна, представленная на рисунке 1, состоит из тонкой металлической пластины, расположенной на малом расстоянии параллельно плоскому металлическому экрану.

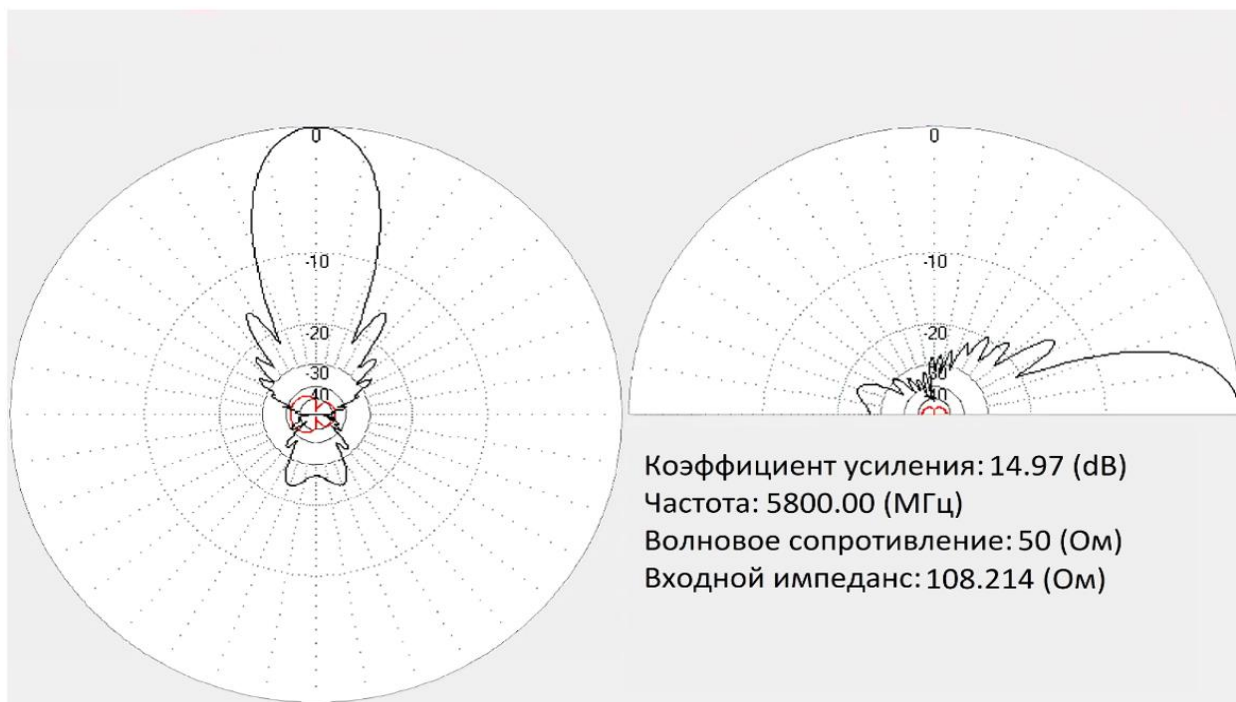


Рис.1. Диаграмма направленности микрополосковой антенны

Микрополосковая антенна изготавливается по технологии печатных плат. Питание осуществляется штырем, проходящим через экран. Используется для создания радиомоста между объектами аэродрома. Антенна разработана для использования в диапазоне 5.8 ГГц, имеет узкую диаграмму направленности и коэффициент усиления равный 17.12 dB. Обладает наилучшими направленными свойствами в горизонтальной плоскости, что показано на рисунке 2. Благодаря этому ее наиболее эффективно использовать для связи между объектами аэродрома для обеспечения электромагнитной совместимости с уже имеющимися средствами.[2]

Благодаря узкой диаграмме направленности и малому уровню боковых лепестков рассчитать размер контролируемой зоны при использовании данной антенны довольно легко.

Антенна двойной квадрат и штыревая антенна работают в диапазоне 2.4 ГГц. Антенна двойной квадрат, представленная на рисунке 2, обладает коэффициентом усиления 15.78 dB, что является очень хорошим показателем и позволит добиться уверенного уровня сигнала в практически любых условиях. Данная антенна имеет наибольший коэффициент усиления из моделируемых антенн и позволяет обеспечить высокий уровень сигнала внутри больших помещений.

Штыревая антенна, представленная на рисунке 3, используется в экранированных помещениях, для использования беспроводного сегмента локальной вычислительной сети. В диапазоне 2.4 ГГц волна достаточно быстро затухает и большинство помещений не потребует использования специальных экранов. Данный тип антенны, также как и антенна двойной квадрат предназначена для создания сети, внутри которой пользователи комплекса широкополосной радиосвязи смогут получать информацию с любых устройств поддерживающих протокол 802.11, что значительно упрощает интеграцию комплекса, так как поддержка данного стандарта имеется во всех современных мультимедийных устройствах. А следовательно не потребуются дорогостоящая разработка нового оборудования. Антенна имеет круговую диаграмму направленности и имеет коэффициент усиления 7.97 dB, этого хватит, для охвата помещения до 100 квадратных метров.

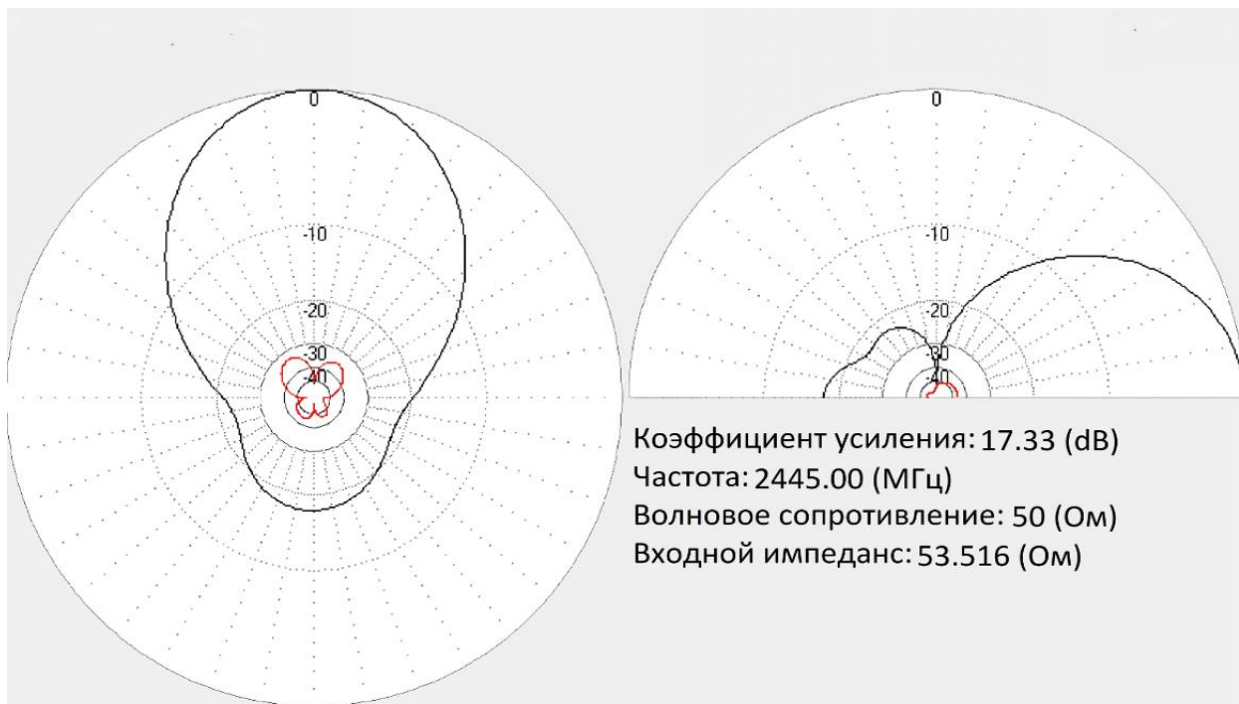


Рис. 2. Диаграмма направленности антенны двойной квадрат

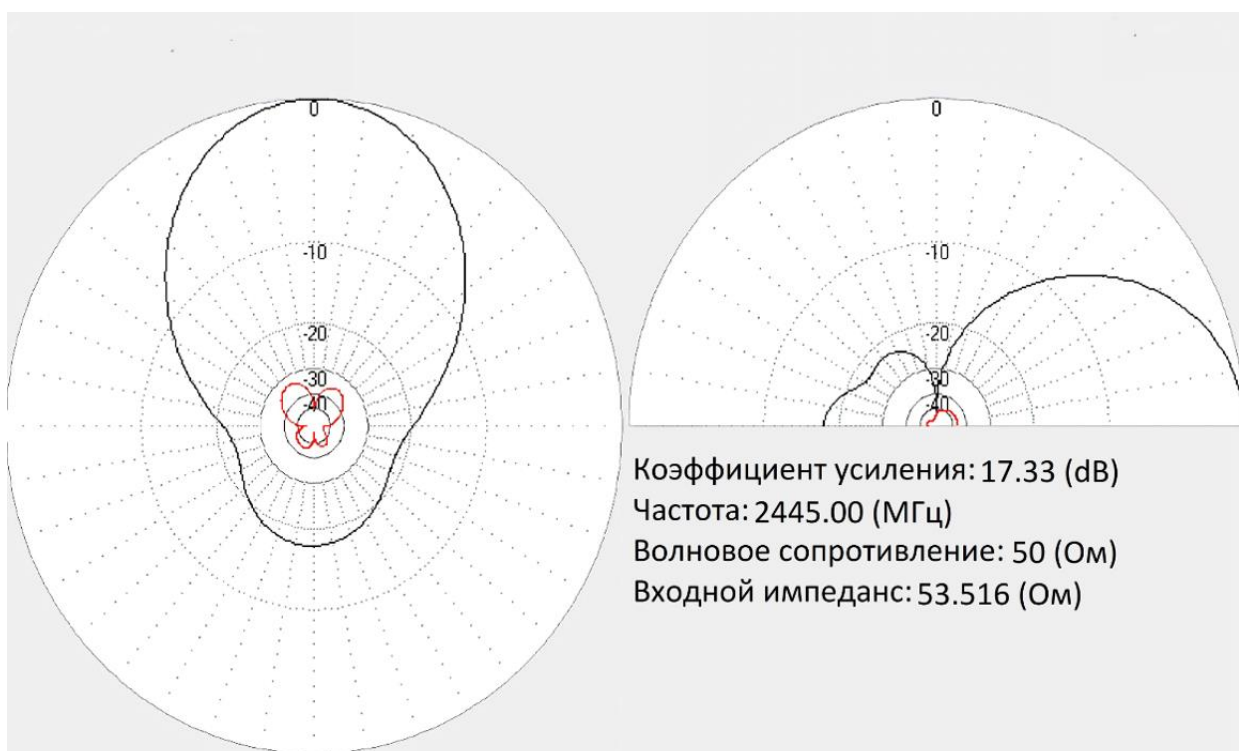


Рис. 3. Диаграмма направленности штыревой антенны

Исходя из данных полученных в ходе моделирования, можно сделать вывод о том, что микрополосковая антенна имеет наиболее узкую диаграмму направленности, работает в диапазоне частот в котором практически исключена возможность создания взаимных помех, а значит и решен вопрос электромагнитной совместимости с дей-

ствующими на аэродроме объектами связи и РТО и имеет наибольший коэффициент усиления, не только среди моделируемых антенн, но также и среди многих других антенн, предназначенных для работы в диапазоне 5.8 ГГц, что делает ее использование наиболее рациональным, для создания радиомоста в беспроводном сегменте ЛВС между объектами аэродрома в комплексе широкополосной радиосвязи связи.[3]

Использование штыревой и антенны двойной квадрат, как уже говорилось выше, наиболее рационально внутри помещений, так как они изначально моделировались для использования в диапазоне 2.4 ГГц, а также имеют значительно худшие характеристики по сравнению с микрополосковой антенной.

Таким образом, использование данного комплекса широкополосной радиосвязи совместно с разработанными антеннами, позволяет обеспечить взаимодействие между объектами аэродрома и действиями дежурных сил на качественно новом уровне. А также повысит эффективность управления войсками и выполнение мероприятий по обеспечению безопасности полетов.

ЛИТЕРАТУРА

1. Андруевич Л.К., Ищук А.А., Лайко К.А. Антенны и распространение радиоволн. Новосибирск.: НГТУ, 2006. 364 с.
2. Пуртов А.М. Системы и сети передачи данных. Омск: СибАДИ, 2010. 72 с.
3. Рошан П., Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11. М.: Издательский дом «Вильямс», 2003. 304 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Бредихина Елена Владимировна, Преподаватель 123 кафедры передающих и приемных радиоустройств (средств связи и РТО).

ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: strikecolder@gmail.com

Россия, 394064, Воронеж, ул. Старых Большевиков, 54а.

Тел. (999) 720-67-65.

Дмитриев Сергей Александрович. Доцент 123 кафедры передающих и приемных радиоустройств (средств связи и РТО). Кандидат технических наук, доцент.

ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: dsa_tambov@mail.ru

Россия, 394074, Воронеж, ул. Старых Большевиков, 54а.

Тел. (951) 549-35-25.

Bredikhina Yelena Vladimirovna. Tutor.

Military Air Academy named after prof. N.E. Zhukovsky and Yu.A. Gagarin, Voronezh.

Work address: Russia, 394064, Voronezh, st. Old Bolsheviks, 54a.

Tel. (999) 720-67-65.

Dmitriev Sergey Alexandrovich. Candidate of Technical Sciences, Associate Professor.

Military Air Academy named after prof. N.E. Zhukovsky and Yu.A. Gagarin, Voronezh.

Work address: Russia, 394064, Voronezh, ul. Old Bolsheviks, 54a.

Tel. (951) 549-35-25.

Ключевые слова: аэродром, безопасность полетов, широкополосная радиосвязь, Module MB 77.07, микрополосковая антенна.

Key words: airfield, flight safety, broadband radio communication, Module MB 77.07, microstrip antenna.

УДК 621.396

Василевский Александр Анатольевич;
Стафеев Михаил Александрович,
кандидат технических наук

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА СИСТЕМЫ РАДИОТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПОЛЕТОВ АВИАЦИОННОЙ БАЗЫ

METHODS OF EVALUATING THE QUALITY OF RADIOTECHNICAL FLIGHT AIR BASE

В статье предлагается методика оценки качества системы радиотехнического обеспечения полетов авиационной базы на основе показателей, характеризующих радиотехнические средства.

The article offers a methodology for the assessment of the quality of radio ensure aviation bases on the basis of indicators characterizing radio means.

Эффективность применения государственной авиации зависит от различных видов обеспечения, в том числе от радиотехнического обеспечения полетов (РТО). Решение задач РТО полетов возможно только при качественном комплексном применении средств РТО. В соответствии с решаемыми задачами средства РТО включают: наземные средства обеспечения радионавигации; наземные средства обеспечения взлета-посадки; средства обеспечения управления воздушным движением в районе аэродрома и др. [1].

Совокупность средств РТО, развернутых на аэродромах, вертодромах, посадочных площадках, авиационных полигонах, радионавигационных пунктах, составляет систему РТО полетов.

Для обоснованной разработки рекомендаций по построению и совершенствованию системы РТО полетов необходима методика ее оценки. В работе для оценки систем РТО полетов предлагается методика на основе технических показателей и показателей, характеризующих функциональные возможности радиотехнических средств с применением теории выбора и принятия решений, экспертных оценок и линейного программирования. Предлагаемая методика оценки системы РТО основывается на показателях полезности с привлечением методов экспертных систем [2].

Система РТО полетов авиационной базы имеет иерархическую структуру, представленную совокупностью средств РТО связанных между собой выполняемыми ими задачами. В итоге задача оценки качества системы РТО авиационной базы в целом складывается из ряда самостоятельных задач оценки качества элементов системы РТО полетов (рис. 1).

В методике частными показателями являются показатели качества конкретных средств РТО ($W_1, W_2, W_3, \dots, W_k, \dots, W_K$), общими показателями коэффициенты, характеризующие способность средств РТО выполнить конкретные функции системы РТО полетов ($W_{F1}, W_{F2}, W_{F3}, \dots, W_{Fl}, \dots, W_{FL}$). Обобщенным показателем является коэффициент качества системы РТО полетов в целом (W_{PTO}).

На первом этапе осуществляется оценка качества каждого отдельного средства РТО входящего в систему.

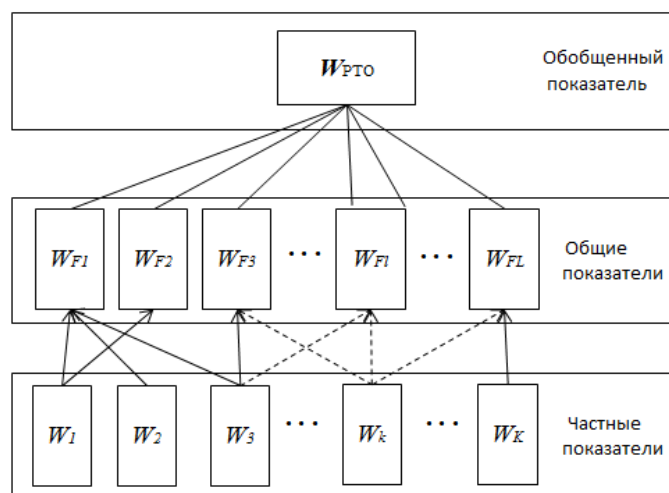


Рис. 1. Система показателей оценки качества системы радиотехнического обеспечения полетов

Расчет показателей качества средств РТО производится на основе технических показателей и показателей, характеризующих функциональные возможности выбранного средства РТО методами теории выбора и принятия решений с привлечением экспертных оценок с помощью формулы:

$$W_K = \alpha \sum_{i=1}^n g_i K_i^{(p)} + \beta K^{(f)}, \quad (1)$$

где W_K – относительный комплексный показатель качества k -го средства РТО;

α и β – групповые коэффициенты весомости по тактико-техническим характеристикам (ТТХ) и по функциональным возможностям средства РТО, они нормируются, исходя из условий $\alpha + \beta = 1$; $\alpha, \beta \in [0; 1]$;

$K_i^{(p)}$ и $K^{(f)}$ – коэффициенты весомости по перечню ТТХ и по перечню функциональных возможностей средства РТО, не охваченных тактико-техническими характеристиками; g_i – относительные численные значения ТТХ средства РТО.

Относительные численные значения ТТХ средств РТО (g_i) рассчитываются следующим образом, если возрастание численного значения параметра увеличивает степень выполнения конкретной задачи средства РТО:

$$g_i^{(1)} = \left\{ \frac{P_i}{P_{\delta}} \right\}; \quad (2)$$

если убывание численного значения параметра увеличивает степень выполнения конкретной задачи средства РТО:

$$g_i^{(2)} = \left\{ \frac{P_{\delta}}{P_i} \right\}, \quad (3)$$

где P_i – абсолютные численные значения i -ой ТТХ средства РТО ($i=1, 2, \dots, n$); P_{δ} – абсолютные численные значения ТТХ «эталонного» средства РТО, принятых за базу сравнения; n – количество ТТХ в перечне.

Коэффициенты весомости по перечню ТТХ устанавливаются в произвольной линейной шкале с последующим их нормированием по формуле:

$$K_i^{(p)} = \frac{\tilde{K}_i^{(p)}}{\sum_{i=1}^n \tilde{K}_i^{(p)}}, \quad (4)$$

где $\tilde{K}_i^{(p)}$ – коэффициенты весомости ТТХ, установленные в произвольной линейной шкале.

Коэффициенты весомости по перечню функциональных возможностей также устанавливаются в произвольной линейной шкале с последующим их пересчетом в коэффициент функциональной полноты средства РТО по формуле:

$$K^{(f)} = \frac{\sum_{j=1}^m K_j^{(f)} \xi_j}{\sum_{j=1}^m K_{\delta j}^{(f)} \xi_{\delta j}}, \quad (5)$$

где $K^{(f)}$ – коэффициент функциональной полноты средства РТО; $K_j^{(f)}$ – коэффициент весомости j -й функциональной возможности средства РТО ($j=1,2,\dots,m$); ξ_j – индекс наличия j -й функциональной возможности в средстве РТО (при наличии функциональной возможности $\xi_j=1$, при отсутствии $\xi_j=0$); $\xi_{\delta j}$ – индекс наличия j -й функциональной возможности в средстве РТО, принятой за базу сравнения (при наличии функциональной возможности $\xi_{\delta j}=1$, при отсутствии $\xi_{\delta j}=0$); $K_{\delta j}^{(f)}$ – коэффициент весомости j -й функциональной возможности средства РТО, принятой за базу сравнения; m – общее количество (полный набор) функциональных возможностей средства РТО, не охваченных выбором ТТХ.

Качество выполнения функций системы РТО (решения задач системой РТО) полетов авиации (таблица 1) находится в непосредственной зависимости от возможностей входящих в ее состав средств РТО [3].

Таблица 1

Функции системы РТО полетов

Индекс	Решаемые задачи
$F1$	Обеспечение выхода в район аэродрома посадки
$F2$	Обеспечение захода и расчета на посадку
$F3$	Маркирование отдельных объектов на аэродроме
$F4$	Обеспечение контроля и регулирования полетов в районе аэродромов
$F5$	Обеспечение посадки ВС в простых и сложных метеорологических условиях, днем и ночью
$F6$	Обеспечение посадки по любой криволинейной пространственно-временной линии
$F7$	Обеспечение взлета и ухода на второй круг
$F8$	Обеспечение контроля за движением на летном поле аэродрома
$F9$	Обеспечение визуального взлета и посадки

Поэтому на втором этапе оценки значений общих показателей характеризующих возможности системы РТО полетов выполнить конкретные функции (задачи) ($F1, F2, \dots, F9$) используется выражение:

$$W_{Fl} = \sum_{k=1}^{K_l} W_{K_l} \cdot \underline{\omega}_{k_l}, \quad (6)$$

где K_l – множество средств РТО, непосредственно участвующих в обеспечении решения l -ой функции системы РТО полетов; $\underline{\omega}_{k_l}$ – нормированные значения весовых коэффициентов ω_{k_l} ; ω_{k_l} – весовые коэффициенты средств РТО, которые применяются для решения конкретной l -ой функции системы РТО полетов, определяются экспертным путем на порядковой шкале «Градации качества».

Обобщенный показатель качества системы РТО полетов авиационной базы W_{PTO} носит характер функциональной зависимости от показателей W_{Fl} , где $F_l = \{F_1, F_2, F_3, F_4, F_5, F_6, F_7, F_8, F_9\}$.

Обобщенный показатель качества системы РТО полетов авиационной базы рассчитывается по формуле:

$$W_{PTO} = \sum_{l=1}^L W_{Fl} \cdot \omega_{Fl}, \quad l \in \{1, 2, \dots, 9\}, \quad (7)$$

где ω_{Fl} – весовые коэффициенты функций F_l , определяются экспертным путем на порядковой шкале «Градации качества» экспертами.

Таким образом, в статье предложенная методика оценки качества системы РТО полетов авиационной базы позволяющая производить сравнительную оценку различных возможных построений систем РТО полетов и обосновывать рекомендации по их совершенствованию. Рассмотренный подход к оценке качества системы РТО может быть использован в интеллектуальных системах поддержки принятия решений должностными лицами органов управления связи и РТО. При применении методов визуализации данных и результатов анализа, позволяющих наглядно отображать полученные результаты, рассмотренная методика может быть применена для создания у экспертов или руководителей единого мнения (картины ситуации) о различных вариантах построения систем РТО полетов.

ЛИТЕРАТУРА

- 1 Федеральные авиационные правила «Радиотехническое обеспечение полетов воздушных судов и авиационная электросвязь». М.: 2007. – 124 с.
- 2 Кузьмин Б.И. Сети и системы авиационной цифровой электросвязи: учеб. пособие / Под ред. В. А. Сарычева. – Санкт-Петербург: «Агентство «ВиТ-прит». Ч.3., 2003. – 480 с.
- 3 Воробьев В.А., Прудов М.М. Эффективность комплекса технических средств радиотехнического обеспечения полетов государственной авиации // Сборник научных статей VII международной научно-технической конференции, посвященной Дню образования войск связи «Современное состояние и перспективы развития систем связи и РТО в управлении авиацией» (24-25 октября 2018 г.) - Воронеж: ВУНЦ ВВС «ВВА», 2018. – 440 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Василевский Александр Анатольевич. Слушатель.
ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: usirto@tut.by

Россия, 394064, г. Воронеж, ул. Старых Большевиков, д.54 а.

Телефон мобильный: 8-980-556-10-54.

Стафеев Михаил Александрович. Старший преподаватель, кандидат технических наук.

ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: usirto@tut.by

Россия, 394064, г. Воронеж, ул. Старых Большевиков, д.54 а.

Телефон мобильный: 8-920-444-12-96.

Vasileuski Aliksandr. Listener.
MILITARY AIR FORCE "VVA Professor N.E. Zhukovsky and Y.A. Gagarin» (Voronezh).

E-mail: usirto@tut.by

Russia, 394064, Voronezh, street. Old Bolsheviks, d. 54 a.

Mobile phone: 8-980-556-10-54.

Stafeev Mihail. Senior Lecturer, candidate of technical sciences.
MILITARY AIR FORCE "VVA Professor N.E. Zhukovsky and Y.A. Gagarin» (Voronezh).

E-mail: usirto@tut.by

Russia, 394064, Voronezh, street. Old Bolsheviks, d. 54 a.

Mobile phone: 8-980-556-10-54.

Ключевые слова: методика оценки качества состояния системы радиотехнического обеспечения авиационного базиса.

Key words: quality estimation System State radio ensure aviation base.

УДК 629.7.054.07

Галуза Максим Андреевич;
Климов Александр Иванович,
доктор технических наук, доцент;
Кузнецов Анатолий Васильевич

МЕТОДИКА ПРОЕКТИРОВАНИЯ ПОЛОСКОВОЙ АНТЕННЫ ВЫТЕКАЮЩЕЙ ВОЛНЫ С НИЗКИМ УРОВНЕМ БОКОВОГО ИЗЛУЧЕНИЯ

DESIGN TECHNIQUE OF A STRIP LEAKY WAVE ANTENNA WITH A LOW SIDE RADIATION LEVEL

Приведено краткое описание новой методики проектирования плоской антенны вытекающей волны нормального излучения, содержащей экранированный диэлектрический волновод с полосковой дифракционной решеткой, с пониженным уровнем боковых лепестков диаграммы направленности в E- и H-плоскостях.

A brief description of a new design technique for a planar leaky wave antenna of normal radiation containing a shielded dielectric waveguide with a strip diffraction grating, with a lowered level of side lobes of the radiation pattern in the E and H planes is given.

В работах [1, 2] была рассмотрена задача снижения уровня бокового излучения плоских антенн вытекающей волны (АВВ) СВЧ или КВЧ диапазона, содержащих диэлектрический волновод (ДВ) и полосковую дифракционную решётку (ДР). На рис. 1 показаны известные (базовые) модели АВВ нормального излучения, использованные для разработки антенн с пониженным уровнем боковых лепестков диаграммы направленности (УБЛ ДН). На рис. 1 обозначено: 1 – экранированный ДВ с размерами $L_x \times L_y \times h$, из материала с относительной диэлектрической проницаемостью ε , с отражающими металлическими стенками на левом и правом торцах; 2 – две одномерно-периодических подрешетки из параллельных металлических полосок с варьируемой шириной w , расположенных с периодом d_x ; 3 – устройство возбуждения ДВ, в АВВ (а) выполненное в виде гребенчатой полосковой линии (ГПЛ) с шириной полоски W и боковыми выступами с варьируемой длиной s , фиксированной шириной w_l и периодом d_y , в АВВ (б) – в виде волноводно-щелевого делителя мощности (ВЩДМ), изготавливаемого по технологии SIW (Substrate Integrated Waveguide) с шириной полоски W и парами металлических столбиков, замыкающих полосу на экран, расположенных с фиксированным расстоянием между столбиками w_p и периодом d_y , с короткозамыкающими перемычками на концах полоски.

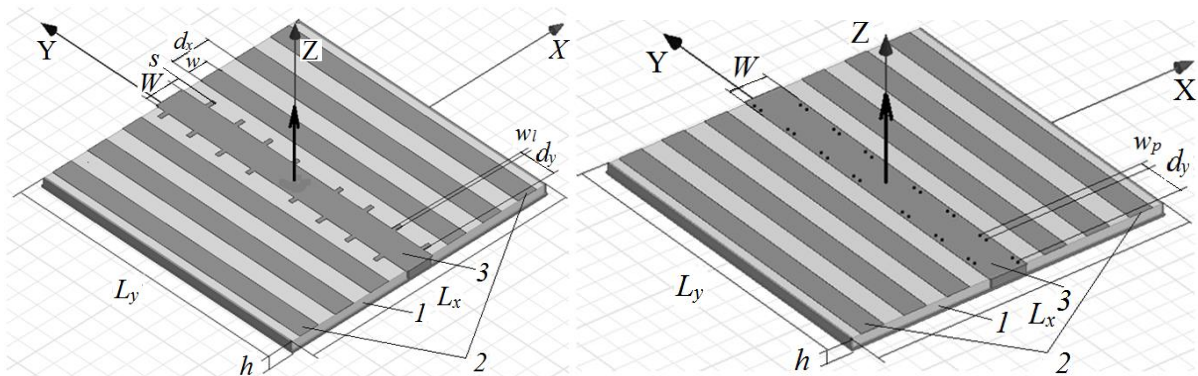


Рис. 1. Базовые АВВ с ГПЛ (а) и АВВ с ВЩДМ (б)

Особенность новых аналоговичных АВВ (рис. 2), но с пониженным УБЛ ДН состоит в том, что для упрощения и ускорения проектирования выбраны конструкции с фиксированными значениями шага элементов ДР излучающего раскрыва и устройств возбуждения.

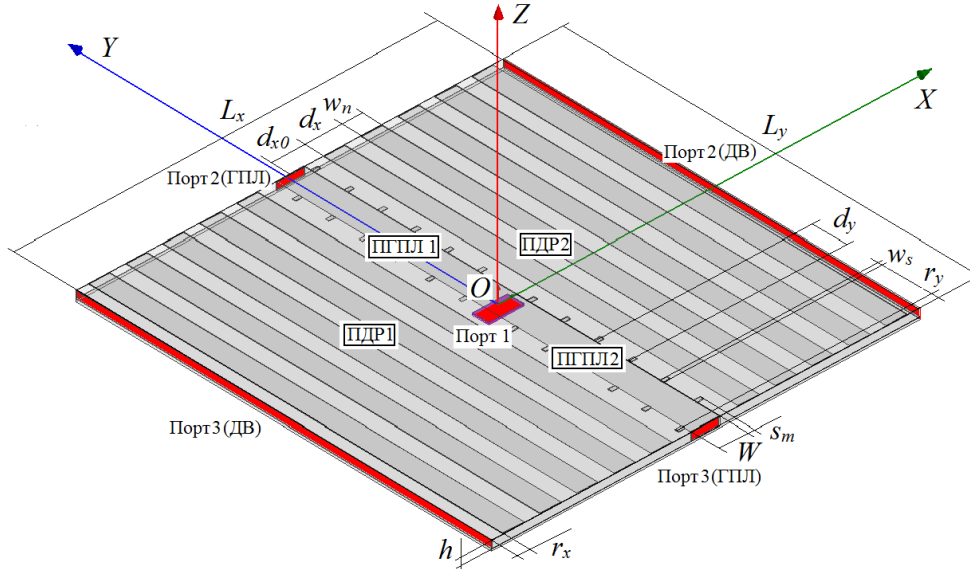


Рис. 2. Полная модель АВВ для имитационного моделирования

С одной стороны, это должно вести к снижению КНД при вариациях размеров элементов, с другой – представляет интерес в плане достижимых значений коэффициента использования поверхности (КИП) раскрыва и ответа на вопрос, стоит ли решать ресурсоемкую задачу фазирования всех излучающих элементов (что, вообще говоря, возможно только на одной частоте). В данной работе изложена новая упрощенная методика проектирования плоской АВВ нормального излучения с Н-поляризацией, с одномерно-периодической ДР из двух симметричных подрешеток и параллельно-последовательным возбуждением с помощью ГПЛ, с пониженным УБЛ ДН, содержащая следующие процедуры:

1. Оценку размеров раскрыва $L_x \times L_y$ по заданному КУ(G) и эффективности ($\mathcal{E} = \eta \nu$) антенны на нижней рабочей частоте; η – коэффициент полезного действия (КПД), ν – КИП.
2. Выбор амплитудных распределений $A(x)$ и $A(y)$, обеспечивающих требуемый УБЛ ДН антенны в Е- и Н-плоскостях и оценку полного КИП антенны.
3. Определение зависимостей коэффициентов ослабления $\alpha(x)$ и $\alpha(y)$, обеспечивающих амплитудные распределения $A(x)$ и $A(y)$, например, для Е-плоскости

$$\alpha(x) = \frac{1}{2} \frac{|A(x)|^2}{\int_x^L (|A(x)|^2) dx + \frac{P_L}{P_0 - P_L} \int_0^L (|A(x)|^2) dx}, \quad (1)$$

где $P_0=1$ – мощность на входе; P_L – мощность на конце антенны длиной L .

4. Выбор материала ДВ (по относительной диэлектрической проницаемости ϵ и тангенсу угла диэлектрических потерь $\tan \delta$).
5. Определение толщины ДВ h , ширины полосок ДР w и периода их расположения d_x , обеспечивающих нормальное излучение вдоль оси OZ на средней рабочей частоте в симметричной структуре с параллельно-последовательным возбуждением, по

результатам расчетов дисперсионных характеристик (ДХ) структуры ДВ+ДР с последовательным возбуждением (рис. 3).

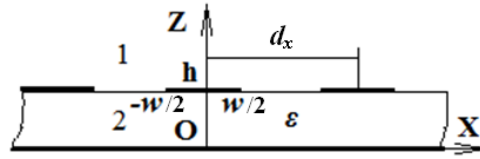


Рис. 3. Фрагмент структуры АВВ

ДХ строятся путем решения дисперсионного уравнения для бесконечно-протяженной структуры и определения частотной зависимости постоянной распространения основной ПГ типа ТМ₀ $\beta = \beta_0 - j\alpha$; β_0 – коэффициент фазы, α – коэффициент ослабления за счет излучения. Дисперсионное уравнение относительно β :

$$\text{Det}[\mathbf{G}] = 0, \quad (2)$$

где $[\mathbf{G}]$ – квадратная матрица размером $M \times M$ (M – число базисных функций $J_{xm}(x)$, например, в виде полиномов Чебышева, для разложения плотности поверхностного

тока $J_x(x) = \sum_{m=1}^M \alpha_m J_{xm}(x)$ на полосках ДР), составленная из элементов

$$G_{ij} = \sum_{n=-N}^N K_n J_{jn} J_{in}^*, \quad K_n = -\gamma_n / [j\epsilon\gamma_n / (\eta_n \tan \eta_n h) - 1];$$

ϵ – относительная диэлектрическая проницаемость, h – толщина ДВ; $\beta_n = \beta + 2\pi n/d_x = \beta_0 - j\alpha + 2\pi n/d_x$ – продольная постоянная распространения n -й ПГ; d_x – период ДР; $\gamma_n = (k_0^2 - \beta_n^2)^{1/2}$ и

$\eta_n = (k_0^2 \epsilon - \beta_n^2)^{1/2}$ – поперечные постоянные распространения n -й ПГ над структурой и в ДВ; $k_0 = 2\pi/\lambda_0$ – волновое число свободного пространства; λ_0 – длина волны;

$$J_{xmn} = \frac{1}{d_x} \int_{-w/2}^{w/2} J_{xm}(x) \exp(j\beta_n x) dx$$

– n -я компонента разложения плотности тока $J_x(x)$ в ряд Фурье по ПГ.

Направление максимального излучения в пл. XOZ для -1 -й ПГ:

$$\theta_n = \arcsin(\text{Re}\{\beta_n/k_0\}) = \theta_{-1} = \arcsin(p(\lambda_0) - \lambda_0/d_x), \quad (3)$$

где $\beta_0/k_0 = c/v_{\phi}(\lambda_0) = p(\lambda_0)$ – замедление фазовой скорости поверхностной волны ДВ. Не смотря на то, что в силу ограниченных размеров реальных ДВ в них возбуждаются гибридные волны типа ЕН, данная модель дает приемлемые результаты при определении частоты резонансной дифракции Брэгга второго порядка уже при размерах структуры порядка 6–7 длин волн.

6. Определение параметров переменного-фазной ГПЛ, обеспечивающих возбуждение в ДВ поверхностных волн, на средней рабочей частоте распространяющихся в направлениях $\pm OX$ при фиксированных значениях периода ГПЛ d_y .

7. Имитационное моделирование АВВ (рис. 2) с поочередным выделением в ее составе одной из двух симметричных трехпортовых структур с полной длиной L_x и L_y и расчета их матриц рассеяния $\mathbf{S}$: 1) вход (порт 1) – торцы ДВ, без ДР и с ДР из двух подрешеток ПДР 1,2 с варьируемой шириной полосок w_n , при возбуждении ДВ с помощью ГПЛ с параметрами из п. 6; 2) вход (порт 1) – концы ГПЛ из двух подрешеток ПГПЛ 1,2, без боковых выступов и с выступами с варьируемой длиной s_m , при наличии полосковой ДР. Получение данных о зависимости коэффициента ослабления $\alpha(w)$ для излучающего раскрытия и зависимости $\alpha(s)$ для ГПЛ. Расчет α выполняется по найденным значениям модуля коэффициента передачи s_{21} :

$$\alpha = (2/L_{x,y}) \ln(|s_{21}|). \quad (4)$$

По зависимости $\alpha(w)$ для подрешетки ДР из N полосок выбираются значения w_n ($n=1 \dots N$), реализующие выборки α_{xn} из $\alpha(x)$, а по $\alpha(s)$ для подрешетки ГПЛ из M выступов – значения s_m ($m=1 \dots M$), реализующие выборки α_{ym} из $\alpha(y)$.

8. Имитационное моделирование антенны (в частности, с помощью программы HFSS) с новыми значениями конструктивных параметров, расчет ДН и проверка УБЛ, при необходимости принятие мер по согласованию входа антенны и коррекции размеров, включая r_x и r_y .

В таблице приведены результаты имитационного моделирования новых плоских АВВ (рис. 1), но с низким уровнем боковых лепестков диаграммы направленности, рассчитанных для использования в полосе частот 60,5–61,5 ГГц.

Результаты имитационного моделирования АВВ

Характеристики	АВВ 1 с ГПЛ	АВВ 2 с ГПЛ	АВВ с ВЦДМ
Размеры раскрыва $L_x \times L_y$, мм ²	43,6×43,6	43,6×44,6	43,6×45,0
Заданная форма $A(x)$	$\Delta + (1-\Delta)\cos(\pi x/L_x)$ $\Delta=0,316$	$\Delta + (1-\Delta)\cos(\pi x/L_x)$ $\Delta=0,316$	$\Delta + (1-\Delta)\cos(\pi x/L_x)$ $\Delta=0,316$
Заданная форма $A(y)$	$\Delta + (1-\Delta)\cos(\pi y/L_y)$ $\Delta=0,316$	$1-2 y /L_y$	$1-2 y /L_y$
КНД D_{max}/D_{min} , дБ	27,9/27,68	27,52/27,13	27,77/27,34
КСВ _{max} /КСВ _{min}	1,69/1,18	1,4/1,02	1,84/1,02
КУ G_{max}/G_{min} , дБ	27,8/27,54	27,43/27	27,62/27,25
УБЛ ДН (Е/Н), дБ	–21/–22	–22/(–25,5)	–21/–26
КИП _{теор} /КИП _{реал} .	0,874/0,625	0,701/0,56	0,61/0,575

Из приведенных в таблице данных следует, что новые антенны имеют ДН с УБЛ в Е- и Н-плоскостях не более –20 дБ и реализованный КИП на средней частоте 61 ГГц более 0,5 (у базовой АВВ УБЛ в среднем –15 дБ и КИП 0,65), хотя и меньше теоретического, рассчитанного для непрерывных синфазно возбужденных раскрывов. Очевидно, что основными причинами этого (помимо погрешностей определения конструктивных параметров) служат отклонения реализованных амплитудных распределений от заданных из-за дискретности структуры АВВ, пространственного разнеса подрешеток ДР и ГПЛ, наличия паразитного излучения устройств возбуждения, а также заранее ожидаемого эффекта нарушения фазирования излучений элементов раскрыва при использовании периодических ДР и устройств возбуждения.

Тем не менее, антенны, разработанные по новой методике проектирования, по своим характеристикам превосходят известные аналоги и могут рассматриваться как довольно перспективные для использования, например, в охранных устройствах, измерительной технике и аппаратуре систем радиосвязи диапазонов СВЧ и КВЧ.

ЛИТЕРАТУРА

1. Кузнецов А. В. Плоская антенная решетка диапазона КВЧ с высоким коэффициентом усиления / Д.А. Ерошенко, А.И. Климов, А.В. Кузнецов // Вестник Воронежского института МВД России. – 2017. – № 4. – С. 175–181.
2. Кузнецов А. В. Плоские антенны вытекающей волны СВЧ и КВЧ с пониженным уровнем бокового излучения / А. В. Кузнецов // Проблемы техники и технологий телекоммуникаций: сборник трудов XVIII Международной научно-технической конференции (20–24 ноября 2017 г.). В 2-х томах. – Казань : 2017. – Т. 2. – С. 154–157.

СВЕДЕНИЯ ОБ АВТОРАХ

Галуза Максим Андреевич. Адъюнкт.
Воронежский институт МВД России.
E-mail: q0mezon@gmail.com
Россия, 394065, г. Воронеж, Проспект Патриотов, 53.
Тел. (473)200-52-65

Климов Александр Иванович. Профессор кафедры инфокоммуникационных систем и технологий. Доктор технических наук, доцент.
Воронежский институт МВД России.
E-mail: alexserkos@inbox.ru
Россия, 394065, г. Воронеж, Проспект Патриотов, 53.
Тел. (473)200-52-65

Кузнецов Анатолий Васильевич. Генеральный директор АО «Воронежское центральное конструкторское бюро «Полюс».
E-mail: polus@vckb.ru
Россия, 394019, г. Воронеж, ул. Краснодарская, 16Б.
Тел/Факс: (473) 276-24-60.

Galuza Maksim Andreevich. Adjunct.
E-mail: q0mezon@gmail.com
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473)200-52-65

Klimov Alexander Ivanovich. Professor of the Chair of Infocommunication Systems and Technologies. Doctor of Sciences (Radio Engineering), Assistant Professor.
E-mail: alexserkos@inbox.ru
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473)200-52-65

Kuznetsov Anatoly Vasilyevich. General Director of JSC "Voronezh Central Design Bureau "Polyus".
E-mail: polus@vckb.ru
Work address: Russia, 394019, Voronezh, Krasnodonskaya, 16B.
Tel./Fax: (473) 276-24-60.

Ключевые слова: антенна вытекающей волны, диаграмма направленности, уровень боковых лепестков, методика проектирования, моделирование.

Key words: leaky wave antenna, radiation pattern, sidelobe level, design technique, simulation.

УДК 621.396.67

**Гилев Игорь Владимирович;
Канавин Сергей Владимирович,**
кандидат технических наук

**ТИПОВАЯ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ РАДИОСВЯЗИ
СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ В УСЛОВИЯХ ИНФОРМАЦИОННОГО
КОНФЛИКТА**

**TYPICAL MODEL OF THE FUNCTIONING OF THE SYSTEM OF RADIO
COMMUNICATION OF SPECIAL PURPOSE IN THE CONDITIONS OF
INFORMATION CONFLICT**

Статья посвящена оценке функционирования систем связи специального назначения в условиях информационного конфликта.

The article is devoted to the evaluation of the functioning of special-purpose communication systems in conditions of information conflict.

В современном мире правоохранительные и военные системы управления, наполнены элементами критической инфраструктуры и сложными аппаратно-техническими и электронными компонентами, что с одной стороны повышает их эффективность, но одновременно с этим увеличивает их уязвимость. Выявление критически значимых элементов и их вывод из строя злоумышленниками при помощи примитивных аппаратно-программных средств могут вызвать негативные последствия, общий ущерб от которых сопоставим с результатами применения стратегического оружия. При этом низкая стоимость производства и приобретения подобных устройств делает их доступными для кустарного производства не имеющими современной научно-технической и производственной базы людьми, а также для преступных организаций [1-3]. Вышеуказанное обуславливает обеспечение функционирования критической инфраструктуры систем связи специального назначения (СС СН) в условиях информационного конфликта.

Под информационным конфликтом будем понимать разновидность конфликтного противоборства, ведущегося за контроль над информационными потоками, за завоевание информационного пространства и использование его в своих интересах и целях при одновременном блокировании или подавлении интересов правонарушителя и недопущении осуществления им своих информационных целей [4]. Проблема оценки устойчивости СС СН в конфликтных условиях стоит как в теоретическом, так и в практическом плане. Для этого введем вероятностную модель функционирования СС СН в условиях информационного конфликта, приведен на рис.1.

Приемная и передающая станции СС СН состоят из следующих элементов с известными параметрами: элемент 1 и элемент 4 являются приемниками, элемент 2 и элемент 5 – передатчиками СС СН, элемент 3 и 6 – антенными элементами (антенны, фидеры, тракты). Станция воздействия злоумышленника включает в себя элемент N, параметры которого неизвестны. В качестве критерия выберем такой показатель, как устойчивость функционирования.

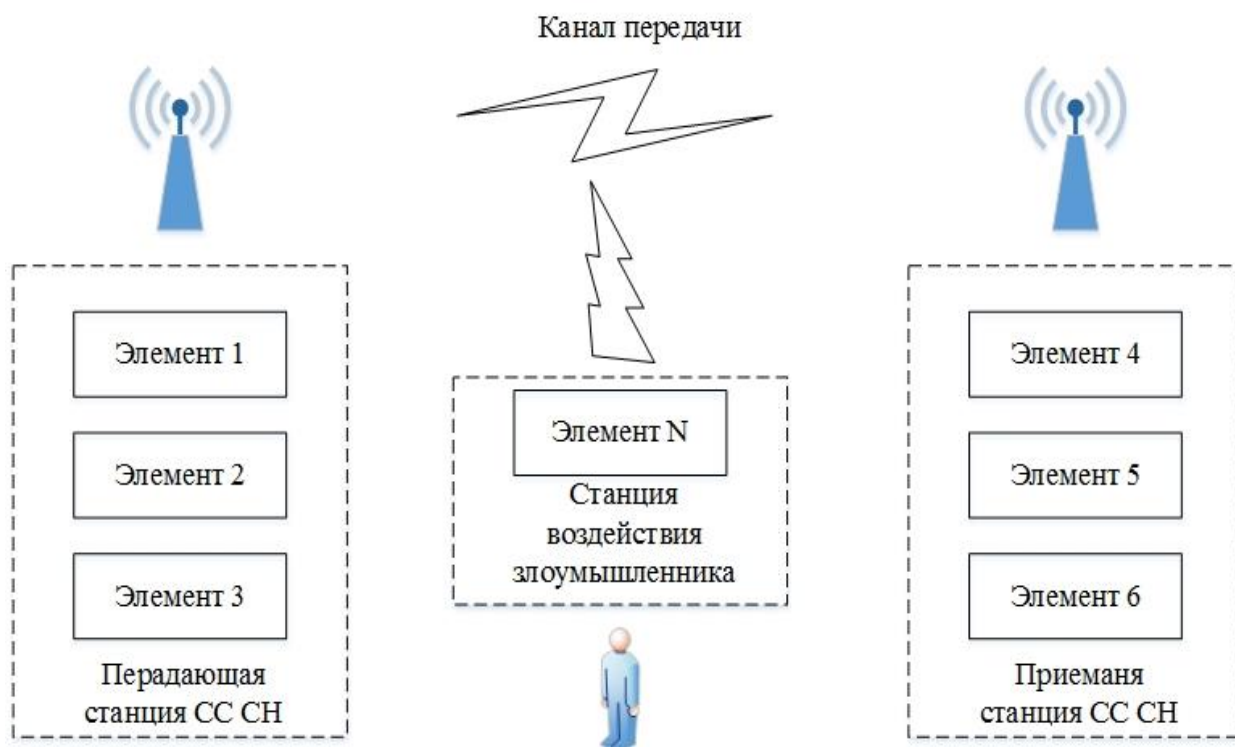


Рис. 1. Модель функционирования системы связи специального назначения в условиях информационного конфликта

Под устойчивостью будем понимать способность СС СН выполнять свои функции при влиянии деструктивных воздействий. Для количественной оценки устойчивости введем в рассмотрение непрерывные дифференцируемые функции $F_1(t), \dots, F_M(t)$, характеризующие текущие функциональные возможности каждого элемента СС СН, включая элементы, оказывающие воздействие. M – общее количество элементов СС СН, t – текущее время [5].

Для характеристики этих функций и придания им физического смысла введем ранжирование $[0;1]$ со следующими градациями: $[0;K_1)$, $[K_1;K_2)$, $[K_2;K_3)$, $[K_3;1]$. Если $F_i(t) \in [0;K_1)$, то i -й элемент СС СН не функционирует; если $F_i(t) \in [K_1;K_2)$, то i -й элемент СС СН выполняет свою функцию частично, но осуществить обмен сообщениями невозможно; если $F_i(t) \in [K_2;K_3)$, то i -й элемент СС СН выполняет свою функцию частично, осуществить обмен сообщениями возможно с некоторыми потерями; если $F_i(t) \in [K_3;1]$, то i -й элемент СС СН выполняет свою функцию в полном объеме. Пусть $\mu_{1i}(t)$ – вероятность того, что $F_i(t) \in [0;K_1)$; $\mu_{2i}(t)$ – вероятность того, что $F_i(t) \in [K_1;K_2)$; $\mu_{3i}(t)$ – вероятность того, что $F_i(t) \in [K_2;K_3)$; $\mu_{4i}(t)$ – вероятность того, что $F_i(t) \in [K_3;1]$, $\mu_{1i}(t) + \mu_{2i}(t) + \mu_{3i}(t) + \mu_{4i}(t) = 1$.

Таким образом критерий устойчивости функционирования СС СН в условиях информационного конфликта выглядит следующим образом:

- 1) если $\frac{1}{M} \sum_{i=1}^M \mu_{4i} = 1$ и $\frac{1}{M} \sum_{i=3}^M \mu_{3i} = 1$, то СС СН является устойчивой,

несмотря на деструктивные воздействия, она способна выполнять заложенные в нее функции;

2) если $\frac{1}{M} \sum_{i=1}^M \mu_{1i} = 1$ и $\frac{1}{M} \sum_{i=2}^M \mu_{2i} = 1$, то СС СН является уязвимой к воздействиям в условиях информационного конфликта, и не может выполнять возложенные на нее функции;

Задача оценки устойчивости СС СН сводится к определению текущих значений $F_i(t)$ в условиях информационного конфликта. Указанные значения определяются решением системы из M уравнений:

$$\begin{cases} \frac{dF_i(t)}{dt} = F_i \rho_i (1 - \sum_{j=1}^N c_{ij} F_j(t)) (i = \overline{1, M}) \\ F_i(t_0) = F_i^0 (i = \overline{1, M}). \end{cases} \quad (1)$$

,где ρ_i – коэффициент, характеризующий инерционные возможности i -го элемента системы связи ($0 < \rho_i < 1$); F_i^0 – стартовые функциональные возможности i -го элемента системы связи в момент времени t_0 ($0 < F_i^0 < 1$); c_{ij} – коэффициенты, служащие мерой относительного влияния элементов СС СН друг на друга ($-1 \leq c_{ij} \leq 1$).

Таким образом, в статье показана модель функционирования системы связи специального назначения в условиях информационного конфликта, сформулированы критерии устойчивости функционирования при которых системы связи функционирует нормально, не выполняет возложенные на нее функции и выполняет функции частично. Указанная модель может использоваться в дальнейшем для формирования ответных мер применительно к правонарушителям и разработке алгоритмов противодействия разрушению информации в СС СН.

ЛИТЕРАТУРА

1. Хохлов Н. С., Канавин С. В., Гилев И. В. Широкополосные и сверхширокополосные воздействия, как средство нарушения функциональной безопасности радиоэлектронных средств // Охрана, безопасность, связь – 2018 : материалы международной научно-практической конференции. – Воронеж : Воронежский институт МВД России, 2018. – С. 165–167.
2. Хохлов Н. С., Канавин С. В., Гилев И. В. Методы и средства воздействия на систему широкополосного доступа специального назначения // Охрана, безопасность, связь – 2018 : материалы международной научно-практической конференции. – Воронеж : Воронежский институт МВД России, 2018. – С. 168–170.
3. Хохлов Н. С., Канавин С. В., Гилев И. В. Типовые модели деструктивных широкополосных и сверхширокополосных сигналов, воздействующих на системы связи специального назначения // Вестник Воронежского института МВД России. – 2019. – № 1. – С. 91–101.
4. Новосельцев В. И. Системный анализ: современные концепции // Воронеж : Кватра, 2003. – С. 360.
5. Новосельцев В. И., Кочедыков. С. С., Орлова Д. Е. Тензорный анализ Крона и его приложения // Воронеж : Научная книга, 2017. – С. 260.

СВЕДЕНИЯ ОБ АВТОРАХ

Гилев Игорь Владимирович. Адъюнкт.
Воронежский институт МВД России.
E-mail: gileviv@bk.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.
Тел. +7 (473) 200-52-28.

Канавин Сергей Владимирович. Старший преподаватель кафедры инфокоммуникационных систем и технологий. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: skanavin@mvd.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.
Тел. +7(473) 2005-229.

Gilev Igor Vladimirovich. Post-graduate cadet.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: gileviv@bk.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. +7 (473) 200-52-28.

Kanavin Sergey Vladimirovich. Senior Lecturer of the chair infocommunication systems and technologies. Candidate of Technical Sciences.
Voronezh Institute of Russian Ministry of Internal Affairs.
E-mail: skanavin@mvd.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. +7 (473) 2005-229.

Ключевые слова: модель системы радиосвязи специального назначения, информационный конфликт, критерии устойчивости функционирования.

Keywords: model of a special purpose radio communication system, information conflict, requirements of sustainability of functioning.

УДК 654.16

Головченко Евгений Викторович,
кандидат технических наук;
Афанасьев Алексей Дмитриевич;
Баев Константин Сергеевич

МОДЕЛЬ СИСТЕМЫ УПРАВЛЕНИЯ АВИАЦИОННОГО ФОРМИРОВАНИЯ

MODEL OF CONTROL SYSTEM OF AVIATION FORMATION

В статье предложена модель системы управления авиационного формирования, основанная на теоретико-множественном представлении структуры и поведения системы управления с использованием системного подхода и сетевого планирования. Предложен показатель оценки эффективности функционирования системы связи, являющейся технической основой системы управления авиационного формирования.

The article proposes a model of the control system of aviation formation, based on the set-theoretical representation of the structure and behavior of the control system using a systematic approach and network planning. The indicator of an assessment of efficiency of functioning of the communication system which is a technical basis of control system of aviation formation is offered.

Реализация боевых возможностей авиационным формированием во многом зависит от эффективности управления им. При этом под эффективностью управления понимается наиболее общее, определяющее свойство управления авиационным формированием, раскрывающееся через категорию цели и объективно выражающееся степенью

достижения цели с учетом затрат ресурсов и времени [1]. Оценку эффективности управления необходимо проводить заблаговременно, при этом необходимо учитывать как особенности строения системы управления авиационного формирования, так и особенности ее функционирования.

Для решения данной задачи необходимо построение модели системы управления и процесса управления авиационным формированием. Предлагается использовать теоретико-множественное описание, рассматривающее два аспекта системы управления: ее строение и поведение [2].

Под строением системы управления понимается состав элементов и организация их в единое целое. Элементами системы управления являются [3]:

$\mathbf{Сб} = \{сб_1, сб_2...сб_i ...\}$ – множество субъектов управления;

$\mathbf{Об} = \{об_1, об_2...об_k ...\}$ – множество объектов управления;

$\mathbf{Эл} = \{эл_1, эл_2...эл_s ...\}$ – множество элементов системы связи.

Под организацией системы управления понимаются взаимосвязи и взаимодействия между ее элементами, обеспечивающие объединение элементов в конкретную систему управления:

$\mathbf{Упр}_{ik} = \{упр_{ik}^1, упр_{ik}^2...упр_{ik}^n... \}$ – множество управляющих воздействий на k -й объект управления со стороны i -го субъекта управления;

$\mathbf{Усл}_{ik} = \{усл_{ik}^1, усл_{ik}^2...усл_{ik}^p... \}$ – множество услуг связи, используемых при управлении k -м объектом управления i -м субъектом управления.

Множество всевозможных подсистем управления, образующих систему управления авиационного формирования формируется путем перемножения множеств элементов системы с учетом наличия связей и взаимодействия между элементами:

$$\mathbf{СУ} = \{су_u \in \mathbf{Сб} \times \mathbf{Об} \times \mathbf{Эл} | \mathbf{P}(су_u)\} = \{..(сб_i, об_k, эл_s)..\}, \quad (1)$$

где $\mathbf{P}(су_u): \forall сс_{су_u} = 1$ – множество предикатов, истинность которых свидетельствует о наличии в подсистеме управления $су_u$ связей и управляющих воздействий между соответствующими объектом и субъектом управления. То есть множество $\mathbf{СУ}$ представляет собой всевозможные информационные направления, функционирующие в системе управления авиационного формирования.

Модель строения подсистемы управления $су_u$ можно представить в виде многоуровневой структуры (рисунок 1).

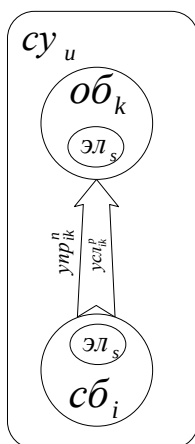


Рис. 1. Модель строения подсистемы управления

Под поведением системы управления понимается изменение ее состояния в процессе функционирования. Поведение принято описывать в терминах входов и выходов [2]. При этом под входами системы управления понимаются:

$\text{СОБ} = \langle \text{ФОБ}, \text{УО}, \text{Рес}, \text{Зад}, \text{Упр} \rangle = \{ \text{соб}_1, \text{соб}_2 \dots \text{соб}_l \dots \}$ – множество состояний объектов управления;

$\text{ССб} = \langle \text{ФСб}, \text{УО}, \text{Рес}, \text{СОБ}, \text{Упр}, \text{Усл} \rangle = \{ \text{ссб}_1, \text{ссб}_2 \dots \text{ссб}_m \dots \}$ – множество состояний субъектов управления;

$\text{СЭл} = \langle \text{ФЭл}, \text{УО}, \text{Рес}, \text{ССб}, \text{Усл}, \text{Сп} \rangle = \{ \text{сел}_1, \text{сел}_2 \dots \text{сел}_x \dots \}$ – множество состояний элементов системы связи,

где **ФОБ**, **ФСб**, **ФЭл** – множества функций, выполняемых объектами управления, субъектами управления и элементами системы связи соответственно;

Рес – множество ресурсов различной природы (материальных, временных, информационных и др.), затрачиваемых при выполнении задачи;

УО – множество значений элементов условий обстановки, в которых функционирует система управления и которые оказывают на нее воздействие;

Зад – множество задач, выполняемых объектами управления;

Сп – множество способов построения системы связи авиационного формирования.

Под выходом системы управления понимается результат ее функционирования, то есть состояние, в которое переходит объект управления, и, следовательно, вся система управления в целом (рисунок 2).

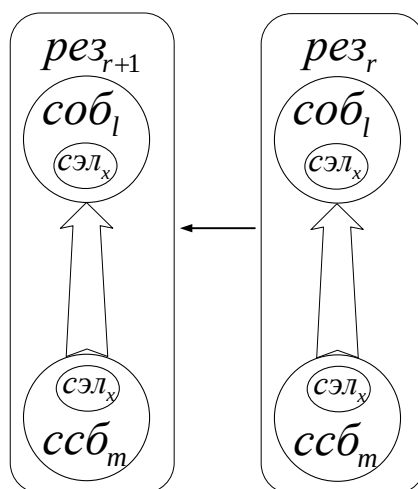


Рис. 2. Модель поведения подсистемы управления

В связи с тем, что условия обстановки носят стохастический характер, то их влияние на элементы системы управления предопределяют случайный характер результата функционирования системы:

$$\text{Рез} \subset \text{СОБ} \times \text{ССб} \times \text{СЭл} = \{ \dots (\text{соб}_i, \text{ссб}_m, \text{сел}_x) \dots \} = \{ \text{рез}_1, \text{рез}_2, \dots \text{рез}_r \dots \} \quad (2)$$

Целью функционирования системы управления и, соответственно, управления авиационным формированием является достижение требуемого результата. С точки зрения системы связи данным результатом может быть:

формирование управляющего воздействия (определяется состоянием субъекта управления);

доведение управляющего воздействия до объекта управления для перевода его в требуемое состояние (определяется состояниями элемента системы связи и объекта управления).

Для оценки качества функционирования предлагается критерий пригодности результата: включение элементов множества **Рез** во множество требуемых состояний:

$$\mathbf{Рез} \subset \mathbf{Рез}_{mp} = \{рез_t^{mp} \in \mathbf{СОБ} \times \mathbf{ССб} \times \mathbf{СЭл} \mid \mathbf{P}(рез_t^{mp})\} = \{рез_1^{mp}, рез_2^{mp} \dots рез_t^{mp} \dots\}, \quad (3)$$

где $\mathbf{P}(рез_t^{mp}) : \bigcap_{y=1}^Y (\text{пок}_{рез_t^{mp}}^y \in \mathbf{Пок}_{mp})$ – множество предикатов, истинность которых свидетельствует о принадлежности множества Y показателей t -го результата управления к множеству требуемых значений показателей $\mathbf{Пок}_{mp}$.

Показателем эффективности управления авиационным формированием может выступать вероятность достижения цели управления:

$$\mathbf{Эф} = P(\mathbf{Рез} \subset \mathbf{Рез}_{mp}). \quad (4)$$

Задачей повышения эффективности управления авиационным формированием является разработка способов построения системы связи авиационного формирования, удовлетворяющего одному из критериев: оптимальности (5) или пригодности (6).

$$\mathbf{Сп} : \max P(\mathbf{Рез} \subset \mathbf{Рез}_{mp}); \quad (5)$$

$$\mathbf{Сп} : P(\mathbf{Рез} \subset \mathbf{Рез}_{mp}) \geq P_{mp}. \quad (6)$$

Динамика функционирования системы управления авиационного формирования может быть описана с использованием системного подхода, позволяющего осуществить декомпозицию функционирования системы управления по этапам выполнения задачи авиационным формированием с выделением элементов системы управления, необходимых на каждом этапе, и по времени выполнения этапа. При этом функционирование системы управления может быть представлено с использованием метода сетевого планирования и управления [4].

Сетевое планирование и управление представляют собой комплекс расчетных методов, организационных мероприятий и контрольных приемов и является эффективным инструментом управления. Использование данного метода позволяет должностным лицам органов управления связью, контролировать планируемый процесс в целом со всеми существенными связями. В сетевой модели все мероприятия и действия представлены в их логической и технологической последовательности. Именно в этом заключается сущность метода, которая не позволит упустить детали или нарушить порядков планирования и управления связью, а система связи обеспечит управления авиационным формированием с требуемым качеством [4].

В соответствии с вышеизложенным подходом, разработана модель системы управления условного авиационного формирования (рисунк 3).

На модели представлен графический план выполнения задачи авиационным формированием по этапам с указанием:

- задачи авиационного формирования;
- базирования авиации при подготовке и в ходе выполнения задачи;
- элементов системы управления;
- элементов системы связи;
- элементов воздействия противника на систему связи.

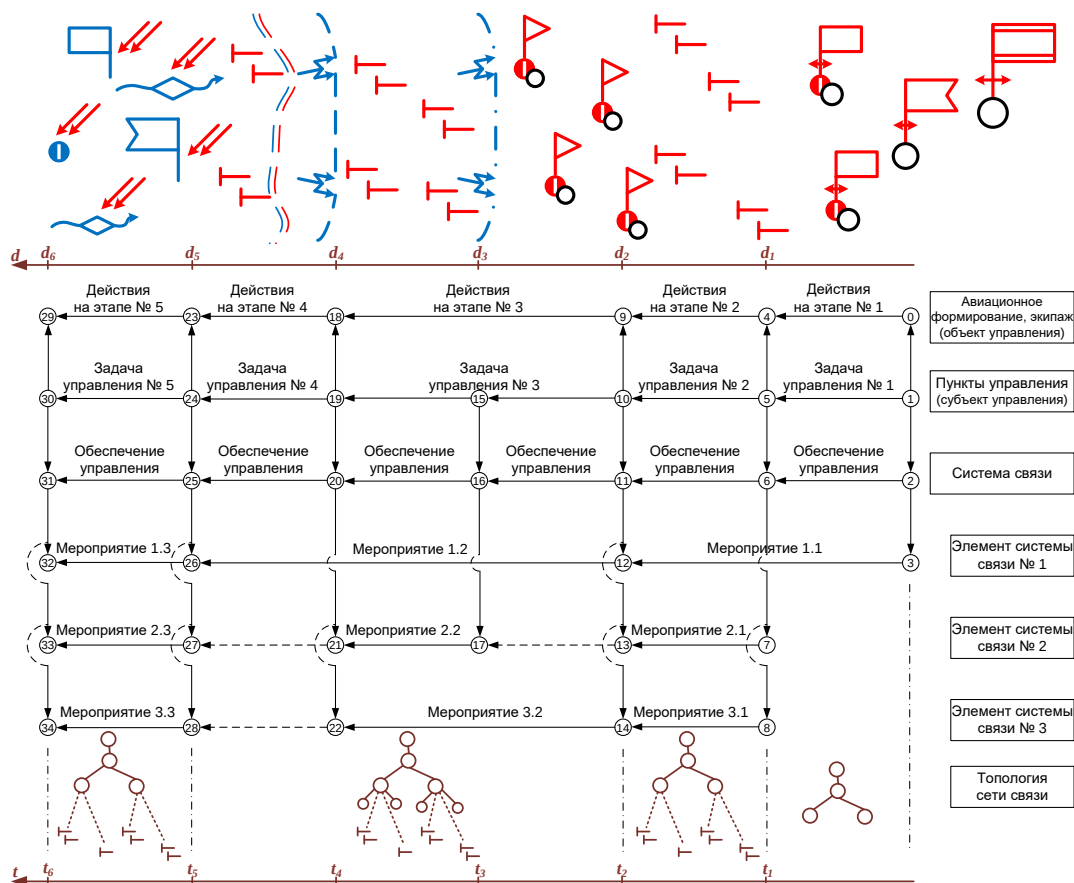


Рис. 3. Модель системы управления авиационного формирования

К графическому плану «привязаны» подсистемы управления, функционирующие на определенном этапе выполнения задачи. Действия, задачи и мероприятия, выполняемые элементами подсистем управления (обозначены стрелками), а так же их состояния (обозначены кружками), в которые переходят элементы подсистем управления в результате функционирования системы управления на данном этапе.

Каждому из этапов соответствует определенная топологии инфокоммуникационной сети авиационного формирования.

Для учета масштаба и динамики действий в модели осуществлена их привязка к пространственной и временной шкалам.

Привязка сетевой модели к графическому плану позволяет рассматривать проводимые мероприятия как во времени, так и в пространстве, что дает возможность представлять их в целом, находить узкие места и уже на стадии планирования устранять их.

Предложенная модель позволяет дифференцированно оценить качество и эффективность управления на каждом из этапов выполнения задачи и и всей задачи в целом.

ЛИТЕРАТУРА

1. Колесников Г.М. Прикладные аспекты теории деятельности человека. Монография. – Монино: Военно-воздушная академия, 2010. – 505 с.
2. Морозов Л.М., Петухов Г.Б., Сидоров В.Н. Методологические основы теории эффективности. Учебное пособие. – Ленинград: Военный инженерный краснознаменный институт, 1982. – 236 с.
3. Боговик А.В. и др. Теория управления в системах военного назначения. Учебник. – М: МО, 2001. – 320 с.

4. Тараканов К.В. Математика и вооруженная борьба. – М.: Воениздат, 1974. – 240 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Головченко Евгений Викторович. Старший преподаватель кафедры (управления воинскими частями связи и РТО авиации). Кандидат технических наук.

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия».

E-mail: evvigo@mail.ru. Тел. 8-910-245-57-06.

Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А.

Афанасьев Алексей Дмитриевич. Преподаватель кафедры (управления воинскими частями связи и РТО авиации).

Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия».

E-mail: usy_2001@mail.ru. Тел. 8-919-187-93-68.

Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54А.

Баев Константин Сергеевич. Заместитель командира батальона управления.

Войсковая часть 40963.

Email: evdokimova0101@mail.ru. Тел. 8-910-640-02-86.

Россия, 172383, Тверская обл., г. Ржев, ул. Челюскинцев, 8/22.

Golovchenko Evgeniy Viktorovich. Senior teacher of chair (management of military units of communication and aircraft RTO).

Military educational and scientific center of the Air Force Military « Air Force Academy».

E-mail: evvigo@mail.ru

Russia, 394064, Voronezh, St. Old Bolsheviks, 54A.

Afanfs'ev Aleksey Dmitrievich. Teacher of chair (management of military units of communication and aircraft RTO).

Military educational and scientific center of the Air Force Military « Air Force Academy».

E-mail: usy_2001@mail.ru

Russia, 394064, Voronezh, St. Old Bolsheviks, 54A.

Baev Konstantin Sergeevich. The deputy commander of a battalion control.

Troop unit 40963.

Email: evdokimova0101@mail.ru

Work address: Russia, Tver region, Rzhev, Chelyuskincev str., 8/22.

Ключевые слова: система управления, система связи, теоретико-множественное описание, модель.

Key words: control system, communication system, set-theoretic description, model.

УДК 623.61

Данилов Роман Михайлович,
кандидат технических наук;
Рыбак Александр Владимирович,
кандидат технических наук, доцент

ГЛОБАЛИЗАЦИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В РОССИИ

LOCAL AND GLOBAL COMPUTER NETWORKS

В статье проведен анализ актуальности использования в современном мире локальных и глобальных компьютерных сетей, а также обсуждаются задачи, решаемые с помощью локальных и глобальных компьютерных сетей.

In the article, actuality of the use of local and global computer networks is analysed presently. Tasks that can be decided by means of local and global computer networks come into question.

На современном этапе неоспоримо не просто влияние, а приоритет локальной и глобальной компьютерной сети для развития всех сфер общественной жизни: экономики, политики, социальной сферы и сферы культуры. От ИКТ-компетенцией каждого члена общества на прямую зависит скорость технического прогресса.

Уровень прогресса глобальной компьютерной сети в целом определяется развитием IT технологий.

Необходимость внимания к данной проблеме в век, когда информация становится ведущим фактором производства, лидирующим экономическим ресурсом, приобретает первостепенное значение.

В эпоху высочайшей скорости обновления информации именно локальная и глобальная компьютерная сеть призвана в первую очередь, реагировать на вызовы времени, увлекая за собой другие экономические ресурсы.

Глобальная вычислительная сеть Интернет – это мощное средство совершенствования глобальных процессов и наиболее яркий пример социальной интеграции. Согласно данным ИТАПР-ТАСС полугодовая аудитория интернета в крупных российских городах, по оптимистическим оценкам, достигнет в 2018 году 83% от всего населения страны. В городах, где проживает менее 100 тысяч человек, по оптимистическому сценарию, в 2018 году аудитория интернета составила 80%, в селах - 69%. Сейчас ФОМ оценивает объем интернет-аудитории в России в 57% от всего населения страны [1].

Создание новых сервисов Интернета открывает новые возможности для социальных коммуникаций и организации виртуальных социальных сред. Различны интересы людей, их принадлежность к учебным заведениям, место жительства и т.д. Тем не менее, в настоящее время в Интернете очевиден феномен локализации пользователей. Если еще несколько лет назад пользователь, несмотря на малую пропускную способность каналов связи, за сеанс посещал более десятка различных сайтов, то в настоящее время, несмотря на значительный рост пропускной способности каналов связи, значительная часть пользователей ограничивается посещением только одного ресурса – социальной сети. Локализации пользователей несомненно будет содействовать введение национальных алфавитов в доменное пространство Интернета. Имеется тенденция возникновения слабосвязанных сегментов Интернета, так как происходит дальнейшая стратификация пользователей. Это приведёт к вырождению глобальной сети Интернета в 11 (по числу введенных языков) региональных сетей. В связи с этим, можно предположить, будет возрастать значение локальных вычислительных сетей как основных ячеек Интернета.

Сейчас не существует выраженной границы между локальными и глобальными сетями, благодаря высокоскоростным каналам связи. Следует отметить, что современные глобальные сети имеют удобный доступ к ресурсам. Все это обеспечивает надежность и качественное функционирование каналов связи.

Удаленность локальных сетей друг от друга позволяет им успешно взаимодействовать в современных условиях. Для связи локальных сетей применяются всевозможные средства связи. Разный уровень помех у разных средств связи определяет их неодинаковую надёжность.

Разная пропускная способность линий влечет за собой и разницу в скорости передачи информации, что находит отражение в стоимости пользования линией. Качество пропускной линии определяет цену на нее. Но преимущество дорогой линии - прохождение больше данных в единицу времени. Соединение сетей образует глобальную компьютерную сеть.

Соответственно глобальная сеть имеет более сложную структуру, которая основана на трех принципах:

- наличие единого центра, который координирует работу сети;
- использование системы маршрутизации. Это система обеспечивает продвижение сообщения по узлам сети. Человек в этот процесс не вмешивается;
- применение единой стандартной адресации. Эта адресация делает сеть «понятной» для других сетей.

Надо понимать, что глобальная сеть состоит из других сетей, включает локальные сети, а также объединяет компьютеры, которые к ней подключены [3].

Глобальные сети подразделяются на четыре основных вида [3]:

1. Городские. Это сети, обеспечивающие обслуживание внутри города.
2. Региональные, то есть сети, обслуживающие регионы.
3. Национальные. Сети, осуществляющие связь внутри отдельной страны.
4. Транснациональные. Сети, объединяющие информацией весь мир.

Глобальные сети, как правило, оказывают платные услуги. Они создаются крупными компаниями. Подобные сети называют еще публичными. Поставщика услуг называют провайдером.

Гораздо реже глобальная сеть используется для реализации внутренних потребностей организации. Но такие примеры есть - Транснефть. Это частная сеть. На практике чаще всего встречается другой вариант, когда корпоративная сеть пользуется услугами или оборудованием общественной сети. Но в таком случае она добавляет туда свои услуги.

Существенным различием между сетями является то, что локальная компьютерная сеть обслуживает определенное количество абонентов и обеспечивает связь на сравнительно небольшой территории, а глобальная компьютерная сеть служит источником информации для неограниченного числа потребителей в масштабах всей Земли. Различие между локальной и глобальной сетями также определяется неодинаковыми принципами организации передачи информации и доступа к данным.

Следует отметить, что все локальные компьютерные сети объединяются глобальной сетью, что объясняет их некоторую схожесть, при этом не объединяя их в одну категорию.

Совершенствование условий труда и повышение его производительности – это одно из основных предназначений компьютерных сетей, что рождает заинтересованность как государственных, так и частных коммерческих структур, и организаций в сетевом подключении. Каждому сотруднику независимо от расположения его рабочего места обеспечивается высокоскоростной доступ к общей или корпоративной информации [4].

Также локальные и глобальные сети позволяют автоматизировать производство, они помогают управлять сложными механизмами, объединяя их и делая доступными для операторов и других участников процессов.

Информации глобальной и локальной компьютерных сетей служит источником дальнейшей автоматизации производства, так как их данные позволяют совершенствовать технологические процессы и создавать новые сегменты в производстве на новейшей технической основе. Локальные компьютерные сети объединяют вычислительные машины, расположенные на расстоянии нескольких километров. Так как локальная компьютерная сеть охватывает небольшую территорию, круг ее пользователей ограничен, а также ограничены масштабы однородных задач, решаемых этими пользователями. Типичный пример локальной сети - сеть образовательного учреждения конкретного региона. Круг пользователей данной сети ограничен только преподавателями и студентами. Объем задач, решаемых данной сетью определяется образовательными целями данного учреждения. К локальным вычислительным сетям относятся также так называемые корпоративные вычислительные сети. Зона распространения данных сетей может быть обширна. Например, корпоративная вычислительная сеть коммерческого банка охватывать территорию протяженностью в несколько тысяч километров. При этом, число абонентов данной сети ограничен банковскими служащими, а диапазон решаемых вопросов – финансовыми задачами.

Глобальные компьютерные сети соединяют в единое целое компьютеры, находящиеся в разных странах мира, на разных континентах [5]. Люди в разных частях планеты ежеминутно потребляют информацию из глобальной международной сети, ежедневно пользуются ей миллионы жителей разных континентов. Велик масштаб решаемых ими задач.

Совокупность глобальных сетей, локальных сетей, объединенных единым протоколом TCP/IP, и называют Интернет [6]. Ресурсы и возможности, предоставляемые Интернетом своим пользователям, имеют планетарный характер.

Таким образом, Интернет – это глобальная компьютерная сеть, включающая в себя локальные, региональные, корпоративные сети, и миллионы компьютеров. Большое количество линий связи и гарантирует её надежность, а значит, масштабную и долговременную востребованность.

Костяк Интернета составляет большое количество серверов, имеющих постоянное подключение к сети. Глобальные сети предлагают в основном транспортные услуги. Они переносят данные между локальными сетями или компьютерами. Таким образом, современный мир невозможно представить без локальной, региональной, корпоративной и, соответственно, глобальной компьютерной сетей, поставляющих в этот мир информацию – первостепенный источник развития общества и совершенствования производства.

ЛИТЕРАТУРА

1. Фонд общественное мнение / Интернет-ресурс <http://www.fom.ru>. (дата обращения 01.06.2019)
2. RUMЕТРИКА / Интернет-ресурс <http://rumetrika.rambler.ru>.
3. Дурнева Е.Е., Прончев Г.Б., Лонцов В.В. Феномен регионализации пользователей Интернета в условиях глобализации / в кн. «Мир и Россия: регионализм в условиях глобализации: Материалы III Международной научно-практической конференции». Часть I, Москва, 11 – 12.
4. Михасев В.Г., Прончев Г.Б. Компьютерные сети, Интернет и мультимедиа технологии, – М.: МИПК им. И. Федорова, 2007, 120 С.

5. Прончев Г. Б., Фесенко В. В., Брутов В. В., Михасев В. Г., Воробьев С. Г. Об актуальности локальных вычислительных сетей в настоящее время // Молодой ученый. — 2010. — №12. Т.1. — С. 53-56. — URL <https://moluch.ru/archive/23/2441/> (дата обращения 15.05.2019).

6. Прончев Г.Б., Брутов В.В. Организация сетевой инфраструктуры в узлах коммутации Интернета / в сб. Математическое моделирование социальных процессов. Выпуск 10 / под ред. А.П. Михайлова. – М.: КДУ, 2009, С. 301 – 316.

СВЕДЕНИЯ ОБ АВТОРАХ

Рыбак Александр Владимирович. Профессор кафедры информационного и технического обеспечения органов внутренних дел.

Дальневосточный юридический институт МВД России.

Кандидат технических наук, доцент.

E-mail: rybak_2908@mail.ru

Россия, 680020, Хабаровск, ул. Дикопольцева, д.11, кв.3.

Тел. 8-962-503-62-05.

Данилов Роман Михайлович. Доцент кафедры информационного и технического обеспечения органов внутренних дел.

Дальневосточный юридический институт МВД России.

Кандидат технических наук.

E-mail: danilovroman@mail.ru.

Россия 680018, г. Хабаровск ул. Краснофлотская, д.11 кв.67.

Тел. 8-924-311-17-66.

Rybak Alexander Vladimirovich. Professor of the Department of information and technical support of internal Affairs.

Far Eastern law Institute of the Russian interior Ministry.

Candidate of technical Sciences, associate Professor.

E-mail: rybak_2908@mail.ru

Russia, 680020, Khabarovsk, St. Dikopoltseva, d.11, sq.3.

Phone 8-962-503-62-05.

Danilov Roman Mikhailovich. Associate Professor of the Department of information and technical support of internal Affairs.

Far Eastern law Institute of the Russian interior Ministry.

Candidate of technical Sciences.

E-mail: danilovroman@mail.ru.

Russia, 680018, Khabarovsk, St. Krasnoflotskay, d.11, sq.67.

Phone 8-924-311-17-66.

Ключевые слова: интернет, компьютер, сеть, локальная и глобальная компьютерная сеть, скорость передачи информации.

Keywords: the internet, computer, network, local and global computer network, speed of information transfer.

УДК 004.7

Дмитриев Сергей Александрович,
кандидат технических наук, доцент;
Бредихина Елена Владимировна

СПЕЦИАЛЬНЫЙ КОМПЛЕКС ШИРОКОПОЛОСНОЙ РАДИОСВЯЗИ

SPECIAL COMPLEX BROADBAND RADIOCOMMUNICATIONS

Работа посвящена разработке специального комплекса широкополосной радиосвязи, который позволяет повысить эффективность использования широкополосного канала связи при его использовании для связи между объектами аэродрома и обеспечения безопасности полетов.

The work is devoted to the development of a modern broadband radio communications complex, which allows to increase the efficiency of using a broadband communication channel when using it for communication between aerodrome facilities and ensuring flight safety.

Актуальность данной темы в том, что в современных условиях, все чаще возникает необходимость в передаче больших объемов информации с большими скоростями, особенно актуально это становится при использовании видеоконференцсвязи.

Для решения этих задач был разработан комплекс широкополосной радиосвязи, который показывает, что современные системы связи, могут быть намного доступнее, мобильнее и эффективнее, чем их предшественники и давать намного больше возможностей при выполнении главной задачи связи – управлении войсками, вооружением и военной техникой.

Область применения комплекса широкополосной радиосвязи достаточно обширна:

- охрана удаленных объектов аэродрома;
- выдача видеопотока на автоматизированное рабочее место группы руководства полетами для оценки состояния воздушного судна, заходящего на посадку;
- использование видеорегистрации посадки воздушного судна в интересах обучения летчиков и должностных лиц ГРП, а также анализа причин летных происшествий;
- создание доступной единой сети видеонаблюдения на территории воинской части для повышения уровня безопасности военной службы;
- передача данных между объектами аэродрома внутри локальной вычислительной сети.

На рисунке 1 представлен вариант размещения комплекса широкополосной радиосвязи на аэродроме. На рисунке представлена часть схемы типового аэродрома, расположение оборудования комплекса и показаны линии связи для передачи информации между объектами.

Вся информация, проходящая между абонентами внутри локальной вычислительной сети с одного из элементов комплекса, поступает в центр обработки информации, в котором находится сервер, следящий за общим состоянием всей системы и криптомаршрутизатор, который шифрует канал связи и создает так называемые VPN туннели для передачи информации. Далее с центра обработки информации, данные поступают на оконечное устройство, которым может являться, как компьютер, так автоматизированное рабочее место, построенное на базе комплекса широкополосной радиосвязи.

Комплекс широкополосной радиосвязи построен на базе отечественного одноплатного компьютера Module MB 77.07, который обеспечивает необходимый уровень производительности, поддерживает все современные интерфейсы, обладает высокопроизводительным графическим процессором, а также имеет блок криптообработки, позволяющий

уменьшить вычислительную нагрузку на центральный процессор и увеличить скорость шифрования и дешифрования данных. Также в комплексе широкополосной радиосвязи предусмотрен блок видеокамеры, использующий датчики движения и инфракрасную подсветку, для обеспечения хорошей видимости в условиях плохой освещенности. Данный блок используется при передаче видеоизображения между объектами аэродрома.

В качестве приемо-передающего устройства используется FPV приемо-передатчик, работающий в диапазоне 5.8 ГГц, а также встроенный в Module MB 77.07 передатчик, работающий в диапазоне 2.4 ГГц. Для связи между объектами аэродрома используется микрополосковая антенна, работающая в диапазоне 5.8 ГГц с коэффициентом усиления равным 17.12 dB. Это позволяет обеспечить как пространственное, так и частотное разнесение сигнала, за счет узкой диаграммы направленности антенны, а также необходимый уровень электромагнитной совместимости. FPV передатчик, при использовании направленной антенны, позволяет создать радиомост дальностью более 5 км. Внутри помещений для облегчения задачи по интеграции комплекса в систему связи, предлагается использовать антенны двойной квадрат и штыревую, работающие в диапазоне 2.4 ГГц, поддержку которого имеют все современные ЭВМ и другие мультимедийные устройства. Все разработанные антенны были смоделированы в программной среде «mmapa-gal».

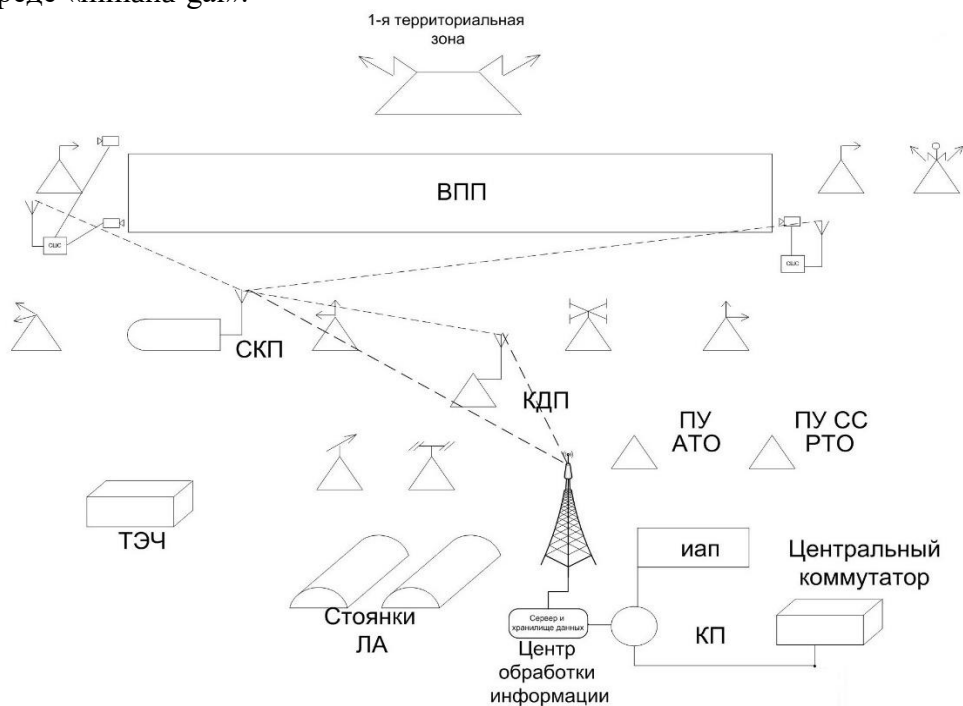


Рис. 1. Вариант размещения комплекса широкополосной радиосвязи на аэродроме

В качестве приемо-передающего устройства используется FPV приемо-передатчик, работающий в диапазоне 5.8 ГГц, а также встроенный в Module MB 77.07 передатчик, работающий в диапазоне 2.4 ГГц. Для связи между объектами аэродрома используется микрополосковая антенна, работающая в диапазоне 5.8 ГГц с коэффициентом усиления равным 17.12 dB. Это позволяет обеспечить как пространственное, так и частотное разнесение сигнала, за счет узкой диаграммы направленности антенны, а также необходимый уровень электромагнитной совместимости. FPV передатчик, при использовании направленной антенны, позволяет создать радиомост дальностью более 5 км.[1] Внутри помещений для облегчения задачи по интеграции комплекса в систему связи, предлагается использовать антенны двойной квадрат и штыревую, работающие в

диапазоне 2.4 ГГц, поддержку которого имеют все современные ЭВМ и другие мультимедийные устройства. Все разработанные антенны были смоделированы в программной среде «mmana-gal».

В качестве операционной системы в комплексе широкополосной радиосвязи используется «motion eye os» - бесплатная система семейства Linux с открытым исходным кодом. Одним из существенных преимуществ данной операционной системы следует отметить встроенные алгоритмы распознавания движения, поддержку более 100 одновременно работающих в одной сети устройств [2].

Таким образом, использование данного комплекса широкополосной радиосвязи совместно с разработанными антеннами, позволяет обеспечить взаимодействие между объектами аэродрома и действиями дежурных сил на качественно новом уровне, а также повысить эффективность управления войсками и выполнение мероприятий по обеспечению безопасности полетов.

ЛИТЕРАТУРА

1. Андруевич Л.К., Ищук А.А., Лайко К.А. Антенны и распространение радиоволн. Новосибирск.: НГТУ, 2006. 364 с.
2. Пуртов А.М. Системы и сети передачи данных. Омск: СибАДИ, 2010. 72 с.
3. Рошан П., Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11. М.: Издательский дом «Вильямс», 2003. 304 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Бредихина Елена Владимировна, Преподаватель 123 кафедры передающих и приемных радиоустройств (средств связи и РТО).

ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: strikecolder@gmail.com

Россия, 394064, Воронеж, ул. Старых Большевиков, 54а.

Тел. (999) 720-67-65.

Дмитриев Сергей Александрович. Доцент 123 кафедры передающих и приемных радиоустройств (средств связи и РТО). Кандидат технических наук, доцент.

ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: dsa_tambov@mail.ru

Россия, 394074, Воронеж, ул. Старых Большевиков, 54а.

Тел. (951) 549-35-25.

Bredikhina Yelena Vladimirovna. Tutor.

Military Air Academy named after prof. N.E. Zhukovsky and Yu.A. Gagarin, Voronezh.

Work address: Russia, 394064, Voronezh, st. Old Bolsheviks, 54a.

Tel. (999) 720-67-65.

Dmitriev Sergey Alexandrovich. Candidate of Technical Sciences, Associate Professor.

Military Air Academy named after prof. N.E. Zhukovsky and Yu.A. Gagarin, Voronezh.

Work address: Russia, 394064, Voronezh, ul. Old Bolsheviks, 54a.

Tel. (951) 549-35-25.

Ключевые слова: аэродром, безопасность полетов, широкополосная радиосвязь, Module MB 77.07, микрополосковая антенна.

Key words: airfield, flight safety, broadband radio communication, Module MB 77.07, microstrip antenna.

УДК 621.396

ПРОГРАММНЫЕ ПРОДУКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

SOFTWARE PRODUCTS TO ENSURE THE SECURITY OF VIRTUAL PRIVATE NETWORKS

Одной из первоочередных задач, возникающих после того как безопасность сайта поднята на должный уровень, является решение проблемы обеспечения безопасности самому программному обеспечению. Разработчики реализовали несколько мощных функций защиты в последнем поколении программ для работы в сети интернета.

One of the priorities that arise after the security of the site is raised to the proper level is to solve the problem of ensuring the security of the software itself. The developers have implemented several powerful protection features in the latest generation of programs for work on the Internet.

Наибольшее распространение получили два защищенных протокола: SHTTP (Secure HyperText Transfer Protocol — защищенный протокол передачи гипертекста) и SSL (Secure Sockets Layer — слой защищенных сокетов). Важная особенность этих протоколов заключается в том, что они позволяют клиенту и серверу договориться о приемлемом уровне безопасности для определенной транзакции или определенного сеанса. Клиент и сервер могут согласовывать разные методы сетевой защиты. В большинстве случаев используется какая-либо разновидность шифрования с открытым ключом. Если веб-серверу и веб-клиенту известны открытые ключи друг друга, безопасный обмен сообщениями и информацией гарантируется.

Консорциум Terisa Systems разработал набор инструментальных средств, предназначенный для разработчиков защищенного серверного программного обеспечения. Образование консорциума Terisa Systems ускорило появление стандартизованных функций защиты серверов.

Собирающейся создать собственный веб-сайт компании следует приобрести пакет веб-сервера, поддерживающий оба протокола SHTTP и SSL. Список таких пакетов велик и продолжает увеличиваться.

Устанавливая веб-сервер и соединяя его с Интернетом, компания подвергает себя риску подслушивания, вторжения, похищения и даже изменения данных. Ответственность за защиту от всех этих угроз полностью лежит на компании. Если что-либо подобное случится, апеллировать будет не к кому.

Проблема усложняется тем фактом, что культура Интернета, под которой понимается открытость, простота доступа, отсутствие контроля, легко проникает в компании, подключающиеся к Интернету. Зачастую отделы информационных систем корпораций не участвуют в планировании и реализации веб-проектов.

Потенциальные проблемы, относящиеся к безопасности, в подобных случаях очевидны. Данные веб-сайты могут работать на системах, соединенных локальными и глобальными сетями с другими вычислительными средствами корпорации. Тем не менее, ответственность за безопасность веб-сайта лежит на локальной группе, управляющей веб-сайтом, являющимся потенциальной точкой входа во всю информационную систему корпорации. Отсюда следует очевидный вывод: корпоративная информационная служба должна проявлять находчивость в вопросах, относящихся к Интернету, должна понимать

необходимость защиты веб-приложений и разбираться в соответствующих средствах защиты, а также должна проводить в жизнь политику веб-безопасности во всей компании.

В сегодняшней распределенной компьютерной среде виртуальная частная сеть (Virtual Private Network, VPN) предлагает сетевым администраторам привлекательное решение проблемы сетевой безопасности. На каждом корпоративном сайте рабочие станции, серверы и базы данных соединены одной или несколькими локальными сетями. Локальные сети управляются сетевым администратором и могут настраиваться и конфигурироваться в целях обеспечения высокого соотношения производительность/цена. Использование Интернета или другой общедоступной сети для соединения сайтов позволяет снизить финансовые затраты, по сравнению с использованием частной сети, а также переложить бремя ответственности за управление глобальной сетью на общественного поставщика сетевых услуг. Та же самая общественная сеть предоставляет доступ удаленным пользователям и мобильным сотрудникам для регистрации в корпоративной системе. Однако перед системным администратором стоит фундаментальное требование безопасности. Использование общественной сети делает корпоративный трафик уязвимым для подслушивания, а также предоставляет точки доступа для неавторизованных пользователей. Для решения этой проблемы системный администратор может выбирать самые разные схемы шифрования и аутентификации. Применение фирменных схем связано с рядом проблем. Во-первых, насколько надежным является та или иная схема? В технической литературе может быть мало сведений об уровне защиты, предоставляемом фирменными схемами шифрования и аутентификации. Вторым вопросом является совместимость. Ни один системный администратор не хочет зависеть от системы безопасности при выборе рабочих станций, серверов, маршрутизаторов, брандмауэров и т. д.

Спецификация IPSec позволяет обезопасить взаимодействие в локальной сети, а также при передаче данных через частные и общественные глобальные сети, и Интернет. Основная особенность спецификации IPSec, обеспечивающая поддержку всех этих приложений, заключается в том, что она позволяет шифровать и аутентифицировать *весь* трафик на уровне протокола IP.

Виртуальные частные сети обычно дешевле реальных частных сетей, развернутых на частных линиях, но основаны на тех же системах шифрования и аутентификации на обоих концах. Шифрование может осуществляться программным обеспечением брандмауэра или маршрутизаторами.

ЛИТЕРАТУРА

1. О связи : федеральный закон от 07.07.2003 №126-ФЗ : (с изм. и доп.) // СПС «КонсультантПлюс». — URL: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 17.10.2017).
2. Столлингс В.В. / Передача данных. 4-е изд. — СПб.: Питер, 2004. — 750с.
3. ETS 300 113. Европейский телекоммуникационный стандарт [Электронный ресурс]. — URL: <http://www.eroocdb.dk/Docs/doc98/Official/Pdf/DEC9607E.pdf>.

СВЕДЕНИЯ ОБ АВТОРАХ

Жайворонок Денис Александрович. Доцент кафедры инфокоммуникационных систем и технологий. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: d.zh007@bk.ru

Россия, 394065, Воронеж, пр-кт Патриотов, 53. Тел. (473) 200-52-24.

Zhayvoronok Denis Alexandrovich. Associate Professor of the Department of Infocom-
munication Systems and Technologies. Candidate of Technical Sciences, Associate Professor.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: d.zh007@bk.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-24.

Ключевые слова: программные продукты, обеспечение безопасности, вирту-
альные частные сети, приложения, трафик, аутентификация, спецификация.

Key words: software products, security, virtual private networks, applications, traffic,
authentication, specification.

УДК 621.396.62

Жуков Михаил Михайлович,

кандидат технических наук,

Удалов Валерий Петрович,

кандидат физико-математических наук, доцент

ПОСТРОЕНИЕ МАТРИЦЫ ЧУВСТВИТЕЛЬНОСТИ РИСКОВ ДЛЯ КОМПОНЕНТ РАСПРЕДЕЛЕННОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ, УЩЕРБЫ В КОТОРЫХ ИМЕЮТ РАСПРЕДЕЛЕНИЕ ПАРЕТО

CREATION OF THE MATRIX OF SENSITIVITY OF RISKS FOR THE COMPONENT OF THE DISTRIBUTED TECHNICAL SYSTEM IN WHICH DAMAGES HAVE PARETO'S DISTRIBUTION

*Получена матрица чувствительности рисков для компонент распределенной техниче-
ской системы, ущерба в которых имеют распределение Парето.*

*The matrix of sensitivity of risks for a component of the distributed technical system in
which damages have Pareto's distribution is received.*

Определим дифференциальные чувствительности риска для компонент распреде-
ленной технической системы, ущерба в которых в результате дестабилизирующих факто-
ров имеют распределение Парето. Для этого случай функция риска имеет вид [1, 2]:

$$Risk(u, q, U_m) = u\varphi(u) = \frac{qU_m^q}{u^q}$$

где: u – ущерб, q, U_m - параметры распределения плотности вероятности наступления
ущерба [5].

$$\varphi(u, q, U_m) = \frac{qU_m^q}{u^{q+1}} \quad q > 0, U_m > 0, u \geq U_m$$

Математическое ожидание:

$$M_{Risk}(q, U_m) = \frac{1-q}{2-q} U_m$$

Дисперсия:

$$D_{Risk}(q, U_m) = \frac{(1+2q)(1-q)}{(2-q)^2(3-q)} U_m^2$$

Проведем расчет коэффициентов дифференциальной чувствительности по параметру q [3,4]:

$$S_q^{Risk} = \frac{\partial(Risk(u))}{\partial q} = \frac{\partial\left(\frac{qU_m^q}{u^q}\right)}{\partial q} = \frac{\partial\left(q\left(\frac{U_m}{u}\right)^q\right)}{\partial q} = \left(\frac{U_m}{u}\right)^q + q\left(\frac{U_m}{u}\right)^q \ln\left(\frac{U_m}{u}\right).$$

$$S_q^{M(Risk)} = \frac{\partial\left(\frac{1-q}{2-q}U_m\right)}{\partial q} = \frac{-1}{2-q}U_m + \frac{1-q}{(2-q)^2}U_m.$$

$$S_q^{D(Risk)} = \frac{\partial\left(\frac{(1+2q)(1-q)}{(2-q)^2(3-q)}U_m^2\right)}{\partial q} = \frac{\partial\left(\frac{1+q-2q^2}{12-10q+5q^2-q^3}U_m^2\right)}{\partial q} = \left(\frac{1-4q}{12-10q+5q^2-q^3} + \frac{1+q-2q^2}{(10-10q+3q^2)(12-10q+5q^2-q^3)^2}\right)U_m^2 =$$

Для параметра U_m получаем:

$$S_{U_m}^{Risk} = \frac{\partial(Risk(u))}{\partial U_m} = \frac{\partial\left(\frac{qU_m^q}{u^q}\right)}{\partial U_m} = \frac{q^2}{u^q}U_m^{q-1}.$$

$$S_{U_m}^{M(Risk)} = \frac{\partial\left(\frac{1-q}{2-q}U_m\right)}{\partial U_m} = \frac{1-q}{2-q}.$$

$$S_{U_m}^{D(Risk)} = \frac{\partial\left(\frac{(1+2q)(1-q)}{(2-q)^2(3-q)}U_m^2\right)}{\partial U_m} = 2U_m \frac{(1+2q)(1-q)}{(2-q)^2(3-q)}.$$

Рассчитаем коэффициенты относительной чувствительности риска для компонент распределенной технической системы, ущерба в которых в результате дестабилизирующих факторов имеют распределение Парето.

Для параметра q получаем:

$$S_q^{Risk\_ln} = \frac{q}{\frac{qU_m^q}{u^q}} \left(\left(\frac{U_m}{u}\right)^q + q\left(\frac{U_m}{u}\right)^q \ln\left(\frac{U_m}{u}\right) \right) = 1 + q \ln\left(\frac{U_m}{u}\right)$$

$$S_q^{M(Risk\_ln)} = \frac{q}{\frac{1-q}{2-q}U_m} \cdot \left(\frac{-1}{2-q}U_m + \frac{1-q}{(2-q)^2}U_m \right) = \frac{-q}{1-q} + \frac{q}{2-q}$$

$$S_q^{D(Risk\_ln)} = \frac{q}{\frac{1+q-2q^2}{12-10q+5q^2-q^3}U_m^2} \cdot$$

$$\cdot \left(\frac{1-4q}{12-10q+5q^2-q^3} + \frac{1+q-2q^2}{(10-10q+3q^2)(12-10q+5q^2-q^3)^2} \right) U_m^2 = \frac{q-4q^2}{1+q-2q^2} + \frac{q}{(10-10q+3q^2)(12-10q+5q^2-q^3)}$$

Для параметра U_m , соответственно, имеем:

$$S_{U_m}^{Risk\_ln} = \frac{U_m}{\frac{qU_m^q}{u^q}} \cdot \frac{q^2}{u^q} U_m^{q-1} = q.$$

$$S_{U_m}^{M(Risk\_ln)} = \frac{U_m}{\frac{1-q}{2-q} U_m} \cdot \frac{1-q}{2-q} = 1$$

$$S_{U_m}^{D(Risk\_ln)} = \frac{U_m}{\frac{(1+2q)(1-q)}{(2-q)^2(3-q)} U_m^2} \cdot 2U_m \frac{(1+2q)(1-q)}{(2-q)^2(3-q)} = 2$$

Матрица чувствительности риска для компонент распределенной системы, ущерба в которых в результате дестабилизирующих факторов имеют распределение Парето, имеет вид:

$$S^{Risk} = \begin{pmatrix} S_{U_m}^{Risk\_ln} \\ S_q^{Risk\_ln} \end{pmatrix} = \begin{pmatrix} q \\ 1 + q \ln\left(\frac{U_m}{u}\right) \end{pmatrix}$$

Таким образом, получена матрица чувствительности риска для компонент распределенной системы, ущерба в которых в результате дестабилизирующих факторов имеют распределение Парето.

ЛИТЕРАТУРА

1. Ермилов Е.В. Построение динамической риск-модели для компонент распределенной платежной системы на основе заданного закона распределения ущерба / Е.В. Ермилов, М.М. Жуков, О.Н. Чопоров, А.В. Бабурин // Информация и безопасность. – ВГТУ. – 2012. – № 4. – С. 449-460.
2. Остапенко А.Г. Функция возможности в оценке рисков, шансов и эффективности систем. / А.Г. Остапенко // Информация и безопасность: Регион. науч-техн. журнал. – Воронеж. 2010. Вып. 1., с. 17-20.
3. Остапенко А.Г. Исследование компьютерной преступности на основе статистического риск-анализа / А.Г. Остапенко [и др.] // Информация и безопасность: Регион. науч-техн. журнал. – Воронеж. 2010. Вып. 2., с. 185-202.
4. Остапенко Г.А. Способы регулирования рисков распределенных систем / Г.А. Остапенко [и др.] // Информация и безопасность: Регион. науч-техн. журнал. – Воронеж. 2010. Вып. 3., с. 435-438.
5. Кендалл М. Теория распределений / М. Кендалл, А. Стьюарт. – М.: Наука, 1966. – 590 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Жуков Михаил Михайлович. Начальник кафедры радиотехники и электроники. Кандидат технических наук.

Воронежский институт МВД России.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-5254.

Удалов Валерий Петрович. Доцент кафедры радиотехники и электроники. Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-5257.

Zhukov Mikhail Mikhailovich. The chef of the radio engineering and electronics department. A Candidate of sciences (technical).

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Phone: (473) 200-5254.

Udalov Valery Petrovich. The assistant professor of the radio engineering and electronics chair. A Candidate of sciences (physics and mathematics), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Phone: (473) 200-5257.

Ключевые слова: риск, безопасность, ущерб.

Key words: the risk, safety, damage.

УДК 624.3

Зарубин Сергей Владимирович,
кандидат технических наук;
Перминов Геннадий Вадимович,
кандидат технических наук

НЕКОТОРЫЕ АСПЕКТЫ ОПТИМИЗАЦИИ НАСТРОЕК КОМПОНЕНТА ПЛАНИРОВАНИЯ ЗАЩИЩЕННОЙ СЕТИ VIPNET ADMINISTRATOR

VIPNET ADMINISTRATOR: SOME ASPECTS OF SETTINGS OPTIMIZATION OF SECURITY NETWORK PLANNING COMPONENT

В статье рассматриваются вопросы оптимизации настроек программного компонента ViPNet Administrator, позволяющие наиболее эффективно управлять территориальными сегментами защищенных сетей ViPNet.

The article discusses the issues of optimizing the settings of the ViPNet Administrator software component, which allow the most efficient management of the territorial segments of the protected ViPNet networks.

Особенности построения сети ViPNet для территориального сегмента ИМТС МВД России зависят от задач, стоящих перед конкретными подразделениями. Как правило, в центрах территориальных сегментов ОВД располагается компонент администратора, который создаёт в соответствии с имеющимися инструкциями адресную и прикладную структуру будущей сети ViPNet, настраивает криптографические связи, а также генерирует ключи для пользователей.

Администрируемый территориальный сегмент обычно представляет собой телекоммуникационную сеть ОВД определенного региона Российской Федерации, которая находится на периферии относительно ядра телекоммуникационной сети ИМТС МВД России, находящегося в городе Москва. Компонент администрирования любого регио-

нального сегмента располагается в областном центре и, как правило, представляет собой автоматизированное рабочее место ViPNet Administrator, находящееся в составе центра информационных технологий, связи и защиты информации.

В настоящее время в территориальных сегментах продолжается процесс подключения сотрудников к единой системе информационно-аналитического обеспечения деятельности МВД России (ИСОД), поэтому подходы к планированию и администрированию уже существующей сети ViPNet вполне могут быть скорректированы с учётом оптимизации настроек компонентов этой сети для повышения эффективности её работоспособности и защищенности.

Анализ базовых настроек территориальных сетей показывает наличие следующих проблем:

1. Настройки в компоненте ЦУС ViPNet Administrator выставлены по-умолчанию: автоматически регистрируются типы коллективов и пользователи с именем абонентского пункта, что вносит определенные неудобства в дальнейшее администрирование сети.

2. В виду того, что включение пользователя в коллектив означает, что пользователь может расшифровать конфиденциальную информацию, отправленную этому коллективу или любому пользователю этого коллектива и того, что в каждом коллективе на автоматизированных рабочих местах работает, как правило, более одного пользователя, это создаёт условия несанкционированного ознакомления одними пользователями с конфиденциальной информацией других пользователей, работающих за тем же АРМ.

3. Отсутствуют сетевые группы, которые позволяют снизить нагрузку криптографических преобразований и упростить администрирование сегментов сети, автоматизированные рабочие места которых обрабатывают информацию одного уровня конфиденциальности.

4. Отсутствуют скрытые коллективы, позволяющие руководителям подразделений иметь доступ к информации своих подчинённых.

5. Присутствует классическая полносвязная схема между всеми созданными типами коллективов, что создаёт предпосылки для максимальных нагрузок на криптографическую подсистему поддерживающего функционирование сети ViPNet Coordinator HW 1000.

6. Задана жёсткая привязка пользователей к своим абонентским пунктам через тип коллектива. Один пользователь – один тип коллектива. Это накладывает определённые ограничения для сотрудников Управления, которым в виду своих должностных обязанностей приходится работать на нескольких автоматизированных рабочих местах.

7. Несмотря на персонализацию по подразделениям, в именовании пользователей отсутствует персонификация и наглядность, которая позволила бы администратору сети осуществлять более простой, невдумчивый аудит сети.

8. Отсутствуют возможности для оперативного масштабирования и модификации сети в части касающейся добавления, удаления, переименования большого количества пользователей, абонентских пунктов и типов коллектива.

Исходя из имеющихся проблем, разберём подходы по оптимизации текущих параметров сети ViPNet.

Автоматичность действий с одной стороны упрощает работу администратора, с другой – создаёт ему дополнительную работу впоследствии: приходится вручную переименовывать уже существующие многочисленные записи пользователей и типов коллектива, которые схожи с именами создаваемых абонентских пунктов, а также создаёт связи между всеми типами коллективов. Связи между всеми созданными в системе типами коллективов, как уже говорилось, приводит к предпосылкам создания максимальных нагрузок на существующий сервер-маршрутизатор.

Для самостоятельной и изначально правильной регистрации имён новых типов коллективов и пользователей, а также для возможности более гибкой настройки связей

между типами коллективов, видится более оптимальным снять чекбоксы со всех опций в верхней части настроек «по умолчанию».

Это позволит администратору:

- планировать политику именования элементов сети ViPNet;
- планировать связи между типами коллективов, то есть защищенные криптографические каналы.

Учитывая специфику служебной деятельности в каждом из представленных исследуемых подразделений, сложившаяся ситуация носит разный характер. И если для подразделений, не связанных с обработкой персональных данных и прочей информации, носящей строго конфиденциальный характер, и занимающихся вопросами сопровождения деятельности территориального органа (таких, как службы тыла и т.д.) это не является проблемой, то в случае с такими подразделениями, как ЦИТСиЗИ, управлений по работе с личным составом, центров финансового обеспечения УМВД – персонализация защиты информации каждого отдельного сотрудника (пользователя ViPNet) необходима.

Поэтому предлагается закрепить в подразделениях, обрабатывающих персональные данные и прочую конфиденциальную оперативно-служебную информацию, принцип «1 тип коллектива – 1 пользователь». Таким образом, мы оптимизируем сеть, уходя от классической конфигурации по-умолчанию: «1 тип коллектива – 1 абонентский пункт». Такая оптимизация в некотором роде усложняет изначальную настройку элементов сети, но в конечном итоге многократно повышает общий уровень её защищенности.

Это позволит:

- защитить критически важную информацию, циркулирующую между автоматизированными рабочими станциями, на которых работает несколько сотрудников;
- создать условия для более гибкого планирования криптографических каналов связи персонально между сотрудниками подразделения (например, в части касающейся упразднения связей между пользователями, ведущими обычный, не конфиденциальный, информационный обмен).

Таким образом, несанкционированный доступ к информации со стороны других пользователей, работающих совместно с получателем конфиденциальной информации за одним автоматизированным рабочим местом, исключается.

ЛИТЕРАТУРА

1. Зарубин, С.В. К вопросу защиты информации в системах безопасности [Текст] / С.В. Зарубин, В.С. Зарубин // сборник материалов XIII Всероссийской научно-практической конференции «Математические методы и информационные средства». – Краснодар: Краснодарский университет МВД России. – 2018. – С. 39-45.
2. Зарубин, С.В. К вопросу оценки показателя защищенности информационных процессов в автоматизированной системе безопасности [Текст] / А.А. Савинков, С.В. Зарубин, В.С. Зарубин // Вестник Воронежского института ФСИИ России. – Воронеж: Воронежский институт ФСИИ России. – 2018. – № 1. – С. 42-46.
3. Зарубин, С.В. К вопросу решения задачи разработки моделей и алгоритмов синтеза комплекса показателей защищенности автоматизированной системы безопасности и охранного мониторинга критически важных объектов [Текст] / С.В. Зарубин, В.С. Зарубин // сборник материалов международной научно-практической конференции «Общественная безопасность, законность и правопорядок в III тысячелетии». – Воронеж: Воронежский институт МВД России. – 2018. – С. 31-35.
4. Перминов, Г.В. Определение объема репрезентативной выборки в целях получения трасологической статистики стеганографических программ [Текст] / А.Н. Копылов, Р.А. Солодуха, Г.В. Перминов // сборник материалов международной научно-

практической конференции «Охрана, безопасность, связь – 2011». – Воронеж: ВИ МВД России. – 2011. – С. 138-140.

5. Перминов, Г.В. Технические аспекты интеграции потребителей услуг вневедомственной охраны в информационную систему отдела вневедомственной охраны [Текст] / Р.А. Солодуха, Г.В. Перминов // Вестник Воронежского института МВД России. – 2009. – № 1. – С. 144-151.

6. Перминов, Г.В. Вычислительный эксперимент по проверке свойств критерия динамической эффективности контроля целостности программной среды эталонной АДИС [Текст] / Г.В. Перминов, С.В. Родин, С.С. Кочедыков // Вестник Воронежского института МВД России. – 2015. – № 1. – С. 263-270.

СВЕДЕНИЯ ОБ АВТОРАХ

Зарубин Сергей Владимирович. Старший преподаватель кафедры информационной безопасности. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: zarubin.sv@mail.ru

Россия, 394065, г. Воронеж, пр. Патриотов, 53. Тел. (473) 200-52-42.

Перминов Геннадий Вадимович. Старший преподаватель кафедры информационной безопасности. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: perminovgv@mail.ru

Россия, 394065, г. Воронеж, пр. Патриотов, 53. Тел. (473) 200-52-42.

Zarubin Sergey Vladimirovich. Senior Lecturer of the chair of Information Security. Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-42.

Perminov Gennadiy Vadimovich. Senior Lecturer of the chair of Information Security. Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-42.

Ключевые слова: виртуальная частная сеть, шифрование, защита информации.

Key words: virtual private network, encryption, information security.

УДК 004.056

К ВОПРОСУ ОБ ОПИСАНИИ СТРУКТУРНО-ПАРАМЕТРИЧЕСКОЙ МОДЕЛИ ЭРГАТИЧЕСКИХ СИСТЕМ

TO THE QUESTION OF DESCRIPTION THE STRUCTURAL-PARAMETRIC MODEL OF ERGATIC SYSTEMS

В настоящей статье описывается подход к описанию структурно-параметрической модели эргатических систем, на основе использования взвешенных гиперграфов.

This article describes an approach to the description of a structural-parametric model of an ergatic systems based on the use of weighted hypergraphs.

Эргатические системы нашли своё применение тех областях, где вмешательство человека-оператора в работу является необходимым условием обеспечения их успешного функционирования. В общем смысле эргатическими называются системы, функционирование которых невозможно без вмешательства человека-оператора [1]. Примерами указанных систем могут являться диспетчерские службы аэропортов, вокзалов, системы управления самолетом и тому подобное. Для эффективного функционирования и возможности оперативного решения возникающих при работе нештатных ситуаций необходимо производить оценку живучести таких систем [2], то есть способности сохранять состояние работоспособности при внешних или внутренних воздействиях на систему.

Каждая эргатическая система содержит элементы (подмножества элементов), которые в результате взаимодействия обеспечивают с некоторой вероятностью выполнение возложенных на систему функций. При этом следует учитывать, что выполнение некоторых функций подразумевает взаимосвязь высокого уровня, то есть взаимосвязь более двух элементов [3].

Эффективность функционирования эргатической системы во многом определяется не только эффективностью отдельных её элементов, но и возможностью их взаимодействия.

В этой связи при описании эргатической системы в качестве структурно-параметрической модели целесообразно использовать взвешенный гиперграф [4], который имеет вид:

$$\Gamma = (S, E, P, K). \quad (1)$$

Его вершины (S) отображают элементы системы, ребра (E) характеризуют взаимосвязь между элементами, веса вершин и ребер (P и K) отражают степень возможности выполнения возложенных на них функций, и степень возможности осуществления взаимосвязи соответственно.

Параметры P и K из (1) могут принимать значения в диапазоне от нуля до единицы. Их значение, равное нулю, показывает выход из строя элемента или полное отсутствие связи между элементами (подмножествами элементов). Значение, равное единице, свидетельствует о том, что элемент функционирует в штатном режиме или взаимосвязь осуществляется между элементами (подмножествами элементов) в полном объеме.

Значения параметров P и K могут быть заданы численно. Тогда в качестве характеристики функциональных возможностей эргатической системы выступает функция $F(\Gamma)$, которая имеет вид:

$$F(\Gamma) = \sum_{i=1}^n \alpha_i p_i + \sum_{j=1}^m \beta_j k_j. \quad (2)$$

Здесь α_i – важность (вклад в общую эффективность системы) элемента системы s_i , а β_j – важность (вклад в общую эффективность системы) взаимосвязи e_j . При функционировании системы в штатном режиме $F(\Gamma) = 1$.

Однако при анализе эргатических систем не стоит забывать о возможном присутствии так называемого «человеческого фактора». В этой связи при описании их функциональных возможностей необходимо использовать нечеткое представление параметров из (2), а, следовательно, описанное выше выражение принимает вид:

$$F(\Gamma) = S\left[\bigcup_{i=1}^n S(T(\mu_{\alpha_i}, \mu_{p_i})), \bigcup_{j=1}^m S(T(\mu_{\beta_j}, \mu_{k_j}))\right]. \quad (3)$$

Здесь параметрам из (2) поставлены в соответствие их функции принадлежности $\mu_{\alpha_i}, \mu_{p_i}, \mu_{\beta_j}, \mu_{k_j}$, а операции агрегирования представлены в виде T- и S-норм [5, 6].

Явный вид для описанных выше операций агрегирования определяется с учетом специфики предметной области.

В заключении хотелось бы отметить, что указанный подход к описанию структурно-параметрической модели эргатических систем применим для их широкого класса. Отдельно из них можно выделить системы критического применения, которые характеризуются наличием в своей структуре организационных элементов, имеющих возможность выполнения альтернативных задач при изменении внешних условий функционирования. Примером таких систем выступают системы управления силовых ведомств при возникновении чрезвычайных ситуаций [7].

ЛИТЕРАТУРА

1. Малафеев, С. И. Надежность технических систем. Примеры и задачи / С. И. Малафеев, А. И. Копейкин – Москва : Горная книга, 2012. – 299 с.
2. Зверев, Г. И. Об одном подходе к оценке живучести эргатических систем / Г. И. Зверев, В. В. Меньших // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции (Воронеж, 14-15 февраля 2019 г.). – Воронеж, 2019. – С. 1138-1140.
3. Меньших, В.В. Структурно-параметрическое моделирование гетерогенных систем в интересах обеспечения их безопасности / В. В. Меньших, Н. Е. Спиридонова // Проблемы управления и моделирования в сложных системах. Труды XXI Международной конференции. В 2-х томах. (Самара, 03-06 сентября 2019 г.). – Самара, 2019. – С. 289-292.
4. Меньших, В.В. Моделирование оценки живучести эргатических систем на основе использования взвешенных гиперграфов / В. В. Меньших, Г. И. Зверев // Проблемы управления и моделирования в сложных системах. Труды XXI Международной конференции. В 2-х томах. (Самара, 03-06 сентября 2019 г.). – Самара, 2019. – С. 388-391.
5. Зак, Ю. А. Принятие решений в условиях нечетких и размытых данных: Fuzzy-технологии / Ю. А. Зак. – Москва : Книжный дом «ЛИБРОКОМ», 2013. – 352 с.
6. Нечеткие множества в моделях управления и искусственного интеллекта / А. Н. Аверкин [и др.] – Москва : Книга по Требованию, 2013. – 312 с.
7. Меньших, В. В. Моделирование коллективных действий сотрудников органов внутренних дел: монография / В. В. Меньших, А. Ф. Самороковский, Е. Н. Середа, В. В. Горлов – Воронеж : Воронежский институт МВД России, 2017. – 236 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Зверев Георгий Игоревич. Научный сотрудник научно-исследовательского отдела.
Воронежский институт МВД России.
E-mail: gzverev2@mvd.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.
Тел. (473) 200-51-28.

Zverev Georgiy Igorevich. Scientific employee of the research department.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-28.

Ключевые слова: эргатические системы, графовая модель, гиперграф.
Key words: ergatic systems, graph model, hypergraph.

УДК 004.5, 519.17.

Истомин Станислав Александрович;
Коратаев Павел Дмитриевич,
кандидат технических наук;
Пакляченко Марина Юрьевна,
кандидат технических наук

ТОЧНОСТНЫЕ ХАРАКТЕРИСТИКИ АППАРАТУРЫ ГЛОБАЛЬНЫХ НАВИГАЦИОННЫХ СПУТНИКОВЫХ СИСТЕМ

ACCURACY CHARACTERISTICS OF GLOBAL POSITIONING SYSTEM EQUIPMENT

В статье приводятся итоги научного исследования, посвященного повышению целостности навигационных определений двусистемной аппаратуры потребителей глобальных навигационных спутниковых систем. Проведены расчеты для аппаратуры потребителя в штатных условиях навигационных приемников, работающих по сигналам ГЛОНАСС и GPS по типовым данным для разработанной имитационной модели устройства мультисистемного навигационного приемника.

The article deals with the results of a scientific research on improving the navigation definitions of two-system equipment integrity of global navigation satellite systems consumers. Calculations for consumer dual-system equipment under standard conditions of navigation receivers operating on GLONASS and GPS signals according to input data for the developed simulation model of a multisystem navigation receiver device are presented.

Приоритетное значение среди средств навигации летательных аппаратов занимают глобальные навигационные спутниковые системы (ГНСС). В настоящее время одними из устройств навигации отечественного производства, используемыми в комплексе пилотажно-навигационных средств и систем гражданской авиации воздушных судов, является аппаратура потребителей спутниковой системы навигации ГНСС БПСН-2 [1], ПСН-2001 различных модификаций [2].

Для более корректного определения навигационных параметров указанные системы работают как с сигналами отечественных комплексов глобальной навигационной спутниковой системы (ГЛОНАСС), так и с сообщениями, формируемыми системой глобального позиционирования Global Positioning System (GPS, США).

Применение однотипных датчиков однородной навигационной информации направлено на повышение точностных характеристик навигационных приемников. В условиях агрессивной политики США в отношении значительного количества государств функционирование аппаратуры потребителя (АП) ГНСС обусловлено следующими факторами:

- отключение сигналов ГНСС GPS в определенных частях мира, в соответствии с политическим решением правительства США;

- искусственное загробление точности излучаемых сигналов ГНСС GPS.

В условиях отключения системы GPS, АП ГНСС будет использовать сигналы системы ГЛОНАСС, что негативно скажется на точностных характеристиках навигационных приемников, относительно АП работающей одновременно с сигналами двух ГНСС [3]. В условиях искусственного загробления точности излучаемых сигналов ГНСС GPS погрешности при определении координат местоположения объекта становятся значительными и могут оказать существенное влияние на воздушную навигацию.

На основе вышеизложенного возникает противоречие между выбором АП ГНСС, работающий по сигналам только ГНСС ГЛОНАСС, и двусистемных навигационных приемников, работающих в условиях искусственного загробления сигналов. Следовательно, определение точностных характеристик аппаратуры потребителей глобальных навигационных спутниковых систем в условиях искусственного загробления сигналов является на сегодняшний день актуальной и практически значимой задачей.

Целью научных исследований и разработок в данном аспекте является повышение целостности навигационных определений двусистемной аппаратуры потребителей глобальных навигационных спутниковых систем.

Для уменьшения точности установления координат системы GPS, несанкционированным потребителям министерство обороны США вводит режим выборочного (ограниченного или селективного) доступа Selective Availability (SA/ВД), в котором в навигационный сигнал умышленно вводятся искаженные данные о поправках к системному времени и орбитах космического аппарата, что очевидно приводит к некорректности навигационных спецификаций.

Селективный доступ будет представлен суммированием двух эффектов:

- Epsilon - манипулирование данными («ложные» эфемериды изменяется очень медленно с периодом около часа);

- Dither - варьирование часами, которое предполагает циклическую вариацию (для одного цикла - от 4 до 15 минут).

При разработке имитационной модели предлагается рассмотреть эффект Dither, для различного варьирования временем, а именно: 4, 8, 12 и 15 минут соответственно.

В программной среде разработана имитационная модель устройства вторичной обработки навигационной информации мультисистемного навигационного приемника. С использованием разработанной модели проведен расчет примера для двусистемной АП ГНСС в штатных условиях навигационных приемников, работающих по сигналам ГЛОНАСС и GPS в условиях искусственного загробления точности излучаемых сигналов ГНСС GPS по типовым исходным данным:

- состав орбитальных группировок ГНСС GPS, ГЛОНАСС взят по данным реальных эфемерид (данные со спутников, параметры спутника от 01.03.2019 г.);

- расчет произведен для орбитальной группировки GPS в составе 28-ми навигационных спутников, ГЛОНАСС в составе 27-ми навигационных спутников. Время наблюдения за орбитальной группировкой составило 24 часа с шагом 1 секунда;
- координаты точки наблюдения: 50° с.ш. и 40° в.д.

При проведении расчета предполагалось, что координаты ГНСС GPS, ГЛОНАСС и точки наблюдения в совмещенной АП программным способом приведены к единой шкале времени и системе координат (рис.1).

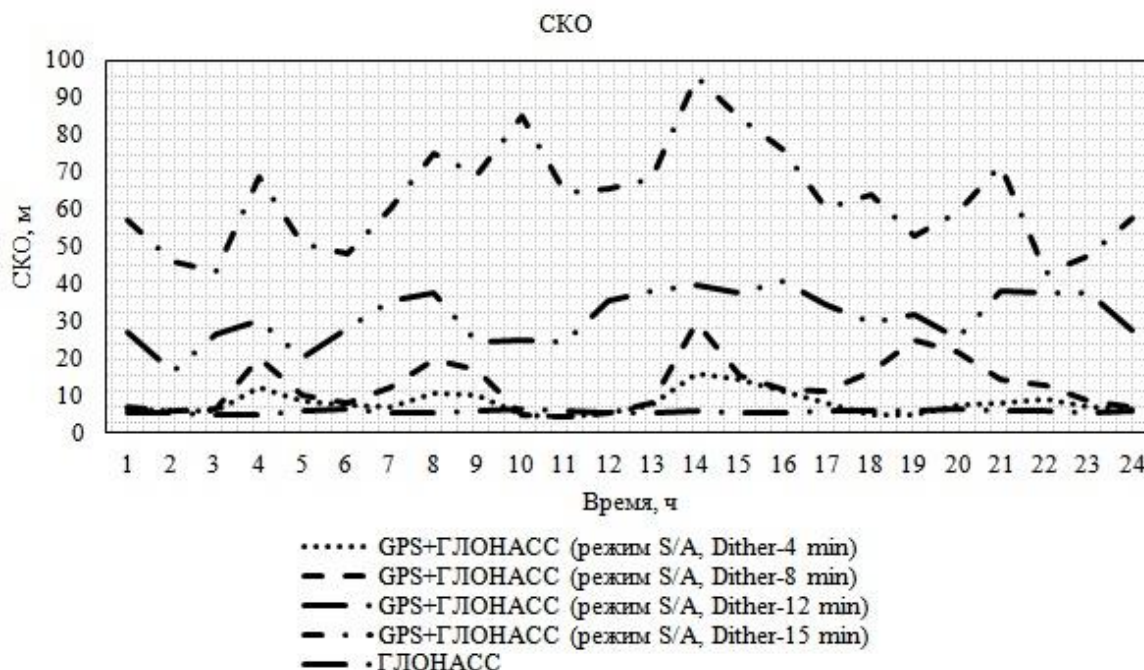


Рис. 1. Среднее квадратическое отклонение (СКО) АП ГНСС при введении режима ограниченного доступа (для различных вариантов эффекта Dither)

Анализ полученных результатов показывает, что наихудшими точностными характеристиками обладает АП ГНСС, работающая по сигналам систем GPS+ГЛОНАСС в условиях ограниченного доступа при варьировании часами в 15 минут (СКО достигает 95 м). В тоже время в односистемной АП ГНСС, работающей по сигналам ГНСС ГЛОНАСС, ошибка определения координат составляет 9-10 м.

Из имеющихся результатов можно сделать вывод, что при введении правительством США режима ВД в определенных областях земного шара, необходимо в двусистемной АП ГНСС переходить от использования сигналов GPS и ГЛОНАСС к функционированию навигационных приемников по сигналам только российской системы ГЛОНАСС.

ЛИТЕРАТУРА

1. Акционерное общество «Конструкторское бюро навигационных систем» АО «КБ НАВИС» [Электронный ресурс]. – Режим доступа: <https://navis.ru/ru> (дата обращения: 20.05.2019).
2. Электронное периодическое издание «ГЛОНАСС-Портал» [Электронный ресурс]. – Режим доступа: <http://www.glonass-portal.ru> (дата обращения: 20.05.2019).
3. Неровный В. В. Помехоустойчивость мультисистемной аппаратуры потребителей ГНСС : монография / В. В. Неровный. – Воронеж : Научная книга, 2018. – 230 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Истомин Станислав Александрович. Курсант факультета авиационного радио-электронного оборудования.

ВУНЦ ВВС ВВА им. Профессора Н.Е. Жуковского и Ю.А. Гагарина.

E-mail: istiom_st@mail.ru

Россия, 394064, г. Воронеж, ул. Ст. Большевиков, 54а.

Тел. 8-928-416-05-01.

Istomin Stanislav Aleksandrovich. Cadet of the Faculty of Aviation Radioelectronic Equipment.

Federal State Official Military Educational Institution of Higher Education «Military Educational and Scientific Centre of the Air Force N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh) the Ministry of Defence of the Russian Federation.

E-mail: istiom_st@mail.ru

Russia, 394064, Voronezh, St. Bolsheviks, 54a. Tel. 8-928-416-05-01.

Коратаев Павел Дмитриевич. Преподаватель кафедры авиационных систем и комплексов радионавигации и радиосвязи. Кандидат технических наук.

ВУНЦ ВВС ВВА им. Профессора Н.Е. Жуковского и Ю.А. Гагарина.

E-mail: korataev2015@mail.ru

Россия, 394064, г. Воронеж, ул. Ст. Большевиков, 54а. Тел. 8-920-412-47-17.

Korataev Pavel Dmitrievich. Teacher of the chair of Aviation Systems and Radio Navigation and Radio Communication Systems. Candidate of sciences (technical).

Federal State Official Military Educational Institution of Higher Education «Military Educational and Scientific Centre of the Air Force N.E. Zhukovsky and Y.A. Gagarin Air Force Academy» (Voronezh) the Ministry of Defence of the Russian Federation.

E-mail: korataev2015@mail.ru

Russia, 394064, Voronezh, St. Bolsheviks, 54a. Tel. 8-920-412-47-17.

Пакляченко Марина Юрьевна. Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: marina_lion@mail.ru

Россия, 394065, г. Воронеж, пр. Патриотов, 53. Тел. 8-920-440-38-45.

Paklyachenko Marina Yurievna. Senior teacher of the chair of radiotechnical systems and security monitoring complexes. Candidate of sciences (technical).

Voronezh institute of Ministry of the Interior of Russia.

E-mail: marina_lion@mail.ru

Russia, 394065, Voronezh, pr. Patriotov, 53. Tel. 8-920-440-38-45.

Ключевые слова: глобальные навигационные спутниковые системы; двусистемная аппаратура потребителей; ГЛОНАСС; GPS; моделирование.

Key words: global positioning system; two-system equipment of consumers; GLONASS; GPS modelling.

УДК 621.396.98

АКТУАЛЬНЫЕ ВОПРОСЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ УЧРЕЖДЕНИЙ И ОРГАНОВ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

ACTUAL QUESTIONS OF ENGINEERING AND TECHNICAL SUPPORT OF THE PENAL SYSTEM

Рассматриваются основные направления развития инженерно-технического обеспечения учреждений и органов уголовно-исполнительной системы. Указываются перспективные технологии, применяемые в уголовно-исполнительной системе.

The main directions of development of engineering and technical support of institutions and bodies of the penitentiary system are considered. Promising technologies used in the penal system are indicated.

В 2010 году распоряжением Правительства РФ от 14.10.2010 № 1772-р была утверждена «Концепция развития уголовно-исполнительной системы Российской Федерации до 2020 года» (далее – Концепция развития УИС). Основная задача Концепция развития УИС состояла в изменении структуры УИС и создании новых видов учреждений, осуществляющих исполнение наказаний в виде лишения свободы. Предполагался переход на два основных вида исправительных учреждений: тюрьмы (общего, усиленного и особого режимов) и колонии-поселения (с обычным и усиленным наблюдением).

Основой принятого решения по изменению структуры УИС стало вступление России в 1996 году в Совет Европы и как результат возникшая необходимость выполнения взятых Россией на себя обязательств, в том числе и по приведению уголовного, уголовно-исполнительного законодательства в соответствие с международными нормами. Одним из таких направлений стало реформирование уголовно-исполнительной системы. Были разработаны модели поэтапного перехода и перепрофилирования исправительных учреждений в учреждения нового типа.

Однако, в мае 2013 года возникло понимание того, что необходимо корректировать Концепцию развития УИС. В итоге, в 2015 г. распоряжением Правительства Российской Федерации от 23 сентября 2015 г. № 1877-р в Концепцию УИС Российской Федерации до 2020 года были внесены изменения, которые закрепили:

- 1) отказ от перехода на тюремные условия содержания осужденных (основная, первоначальная идея Концепция развития УИС);
- 2) обозначение в качестве приоритетного направления развития уголовно-исполнительной системы – обеспечение прав и законных интересов осужденных и лиц, содержащихся под стражей, развитие системы уголовных наказаний, альтернативных лишению свободы, гуманизация условий отбывания наказаний.

В 2018 году научно-исследовательским институтом (НИИ) ФСИН России был подготовлен аналитический обзор анализа достигнутых результатов и целей Концепции развития УИС до 2020 года. В том же году Академией ФСИН России, а также НИИ ФСИН России были подготовлены проекты Концепции развития уголовно-исполнительной системы на период до 2030 года. Однако новая концепция развития УИС так и не была принята.

Одной из важных задач на современном этапе развития УИС является внедрение современных технологий и технических средств в практику исполнения наказаний, в том числе, совершенствование технических средств охраны и надзора.

Целями применения технических средств охраны и надзора в учреждениях УИС являются предупреждение побегов и других преступлений, нарушений установленного порядка отбывания наказания, а также получение необходимой информации о поведении лиц, содержащихся под стражей.

Применение современных информационных технологий и подходов в частности определено Приказом Министерства юстиции РФ от 17 июня 2013 г. № 94 «О внесении изменений в приказ Министерства юстиции Российской Федерации от 4 сентября 2006 г. № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы». В этом документе предусматривается «...создание системы противодействия преступному поведению осужденных на основе применения современных инженерно-технических средств охраны и надзора, новых технологий и подходов к организации безопасности объектов уголовно-исполнительной системы, а также формирование единой технической политики в области их оснащения комплексами инженерно-технических средств охраны и надзора, оснащение всех следственных изоляторов и исправительных учреждений современными интегрированными системами безопасности».

Таким образом, основной тенденцией развития современных технических средств охраны и надзора является интеграция различных технических средств и систем в единый программно-аппаратный комплекс – интегрированную систему безопасности.

Можно дать следующее определение: интегрированная система безопасности (ИСБ) объекта УИС – это совокупность технических средств охраны и надзора и программного обеспечения, объединенных в единую систему в целях обеспечения физической защиты объекта от внешних и внутренних источников опасности. ИСБ обеспечивает комплексную безопасность объекта охраны путем интеграции различных подсистем (охранного телевидения, охранно-тревожной и пожарной сигнализаций, контроля и управления доступом, оперативно-диспетчерской связи, громкоговорящей связи, сбора и обработки информации) на основе единой программно-аппаратной платформы.

Рассмотрим наиболее важные с практической точки зрения и перспективные направления применения и развития современных технологий и инженерно-технических средств обеспечения учреждений и органов УИС.

1 Совершенствование систем видеонаблюдения. Развитие средств видеоаналитики.

Осенью 2018 года на заседании Совета при президенте РФ по правам человека и развитию гражданского общества первый заместитель директора Федеральной службы исполнения наказаний генерал-лейтенант Рудый А. А. заявил о создании новых систем видеонаблюдения в СИЗО и тюрьмах. По его словам на 1 июля 2018 года в учреждениях УИС использовались 116 774 видеокамер и 18 158 единиц переносных видеорегистраторов. Сейчас ФСИН России необходимо более 28 тыс. комплектов переносных видеорегистраторов, 34 473 единицы камер видеонаблюдения систем охранного телевидения, а также дополнительное оборудование для хранения видеозаписей на срок до одного года, что потребует порядка 15 млрд руб. дополнительных вложений.

При этом не стоит забывать, что после 20 минут наблюдения за множеством видеокамер оператор теряет из виду до 90 % происходящего. Поэтому в настоящее время на объектах ФСИН России активно вводятся в эксплуатацию современные системы видеонаблюдения, построенные с применением алгоритмов видеоаналитики. Под видеоаналитикой в узком смысле слова понимается программное обеспечение для обработки видеоизображений.

На сегодняшний день на охраняемых объектах УИС востребованы следующие функции видеоаналитики:

1) видеодетекция движения объектов и людей на периметре и прилегающей территории учреждения;

2) обнаружение необходимых лиц и объектов на территории учреждения и за ее пределами, а также сопровождение их при попадании в поле зрения камеры в соответствии с выделенными зонами;

3) распознавание и регистрация номеров транспортных средств выезжающих и выезжающих с автотранспортного шлюза;

4) контроль качества видео – детекторы определяют причины неработоспособности видеокамеры (закрытие объектива, засвет матрицы, туман в поле зрения камеры, загрязнение объектива и т. д.);

5) мониторинг активности персонала – предназначен для контроля несения службы часовыми на постах. Детектор определяет состояние контролируемого в заданной зоне активен или пассивен. Если часовой малоподвижен (спит, читает книгу) или отсутствует, то система идентифицирует его как отсутствующего;

6) интеллектуальный поиск в архиве. В архив накладывается критерий поиска по направлению пересечения линии, соответственно уменьшается количество фрагментов, также можно накладывать фильтры скорости, цвета и времени нахождения в зоне. Поиск в архиве по лицам: в базу данных загружают фото и система выдаст похожих лиц (система выдаст информацию в каком месте и в какое время находился сотрудник).

2 Тепловизионное видеонаблюдение.

Совершенствование технологий получения и обработки изображений в настоящее время позволяет применять видеонаблюдение не только в видимом диапазоне, но и в инфракрасном, причем с точным определением температуры различных точек объекта. Применять тепловизионные видеокамеры эффективно при плохих погодных условиях (дождь, туман и т. д.). При этом тепловизионные видеокамеры не заменяют традиционных, а дополняют их.

В учреждениях УИС возможно применение тепловизионных устройств (тепловизоров и тепловизионных видеокамер) в следующих направлениях:

1) организации охраны учреждения как во внутренней запретной зоне периметра и на территории учреждения, так и за пределами учреждения для наблюдения за наружными объектами (леса, болота, поля и т. д.);

2) в системах контроля управления доступом – распознавание людей по картинкам распределения температур лица человека при его пропуске через контрольно-пропускные пункты учреждений;

3) своевременное обнаружение и устранение неполадок в системах питания, выявление перегрева мест некачественного соединения кабелей оборудования;

4) досмотр автотранспорта, осуществляющих въезд/выезд в учреждения.

Следует отметить, что современное тепловизионное оборудование легко интегрируется в другие системы видеонаблюдения так, как имеют внешний интерфейс, позволяющий подключаться к стандартным сетям питания и передачи видеоизображений, поскольку передача информации осуществляется по протоколу ТСР/IP. Наиболее эффективно использовать тепловизионные видеокамеры совместно со средствами видеоналитики. Такие решения уже предлагают различные производители.

3 Применение современных систем контроля и управления доступом (СКУД).

Находит свое применение видеоналитика и в СКУД. Комплексное применение видеоналитики и систем контроля и управления доступом позволяет решать широкий спектр задач от распознавания личности на основе различных биометрических показателей (отпечатки пальцев, изображение лица (2D и 3D), изображение радужной оболочки глаза, голос, рисунок вен, геометрия ладони, походка и многое другое) до интеграции с досмотровым оборудованием автотранспорта и системами идентификации автотранспорта по регистрационным знакам.

4 Современные технологии досмотра вещей и людей.

С целью обеспечения безопасности и осуществления режима на контрольно-пропускных пунктах исправительных учреждений применяется различное оборудование досмотра людей и вещей. Однако, с развитием современных технологий совершенствуются методы и способы досмотра людей и вещей. Для осуществления процессов досмотра вещей и людей применяются две группы устройств:

- 1) металлодетекторы (металлоискатели портативные и стационарные);
- 2) рентгентелевизионные установки (рентгеновские интроскопы – досмотр вещей, рентгеновские системы досмотра или системы рентгеновского контроля (СРК) – досмотр людей).

5 Использование новых видов интеллектуальных охранных извещателей.

Особое хотелось бы отметить внедрение на объектах ФСИН России современных средств обнаружения нарушителя, основанных на различных физических принципах действия, например, инфракрасного и вибрационного и т. д. Актуально также применение интеллектуальных охранных извещателей, информирующих о дальности до места нарушения на периметре объекта. Кроме того, некоторые современные охранные извещатели имеют возможность точной подстройки параметров под характеристики объекта охраны в ручном режиме с помощью пульта настройки или персонального компьютера по интерфейсу RS-485. Также возможна интеграция комплекса охранных извещателей с периметральной подсистемой видеонаблюдения

6 Системы нелетального электрошокового воздействия.

Одним из интересных направлений совершенствования инженерно-технических средств, используемых на периметре объекта охраны является применение систем нелетального электрошокового воздействия (СНЭВ). СНЭВ объединяет в себе функции труднопреодолимого инженерного барьера, средства обнаружения и электрошокового воздействия на человека при попытках его преодоления. Принцип действия состоит в поражении нарушителя импульсами высокого напряжения при попытке преодоления электризуемого ограждения. Воздействие импульсов на инстинктивном уровне вынуждает нарушителя прекратить попытки преодоления, а испытываемый болевой шок предупреждает повторение последующих попыток.

7 Беспилотные летательные аппараты (БПЛА) или квадрокоптеры.

Применительно к задачам, стоящим перед подразделениями УИС, применение БПЛА позволяют:

- проводить детальное обследование территории, относящейся к объекту УИС;
- проводить корректировку действий сотрудников при возникновении чрезвычайных обстоятельств и массовых беспорядков;
- проводить наглядное обучение, тренировки;
- прорабатывать вводные с абсолютным контролем действий, а также возможностью разбора отдельных действий и команд;
- реализовывать контроль за службой караулов по охране учреждений и их объектов.

8 Навигационно-информационные системы контроля передвижения людей и спецтранспорта.

Введение в эксплуатацию в России системы ГЛОНАСС (глобальной навигационной спутниковой системы) подстегнуло развитие навигационно-информационных систем для УИС.

Система электронного мониторинга подконтрольных лиц (СЭМПЛ) ФСИН России обеспечивает дистанционный надзор за осужденными и контроль выполнения предписанных им ограничений путем индивидуальной идентификации и контроля местонахождения в установленных местах. Как показала практика, применение электронных средств надзора

и контроля позволяет сотрудникам уголовно-исполнительных инспекций более эффективно осуществлять надзор за соблюдением ограничений подконтрольными лицами и незамедлительно применять меры взыскания к нарушителям.

Другим широко внедряемым направлением в этой области является применение системы контроля транспортных средств УИС. Эта система позволяет оперативно отслеживать и управлять процессами транспортировки осужденных в спецавтомобилях и спецвагонах. При этом обеспечивается своевременное информирование о возникновении нестандартных ситуаций с целью выработки соответствующих оперативных решений.

9 Ситуационные центры.

В последние годы в рамках совершенствования инженерно-технического обеспечения подразделений ФСИН России актуальной становится задача организации ситуационных центров в территориальных органах. Идея заключается в том, чтобы вся информация с исправительных учреждений поступала в ситуационный центр территориального органа и оперативно обрабатывалась, в результате чего принимались решения.

В заключение хотелось бы отметить, что совершенствование инженерно-технического обеспечения подразделений УИС направленное на повышение информативности, оперативности и достоверности результатов контроля, на автоматизацию и интеллектуализацию процессов охраны и реагирования и программно-аппаратную интеграцию средств различных производителей позволит нивелировать негативные факторы, снижающие уровень безопасности в учреждениях, повысить в них эффективность охраны и надзора.

СВЕДЕНИЯ ОБ АВТОРЕ

Кобзистый Сергей Юрьевич. Доцент кафедры технических комплексов охраны и связи. Кандидат технических наук, доцент.

Воронежский институт ФСИН России.

E-mail: kobzuk@yandex.ru.

Россия, 394072, г. Воронеж, ул. Иркутская 1-а. Тел. 89056581936.

Kobzistyy Sergei Yurievich. Associate professor of chair technical complexes of safety and communication. Candidate of technical sciences. Associate professor.

Voronezh institute of Russian Federal Penitentiary Service.

E-mail: kobzuk@yandex.ru.

Work address: Russia, 394072, Voronezh, St. Irkutsk, 1A. Tel. 89056581936.

Ключевые слова: уголовно-исполнительная система; инженерно-техническое обеспечение; современные технологии.

Key words: penal system; engineering support; modern technologies.

УДК 343.8.

Колтаков Евгений Викторович;
Стафеев Михаил Александрович,
кандидат военных наук

**МЕТОДИКА ОЦЕНКИ УПРАВЛЯЕМОСТИ СИСТЕМЫ СВЯЗИ
И РАДИОТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ АВИАЦИОННОГО
ОБЪЕДИНЕНИЯ**

**METHODS FOR ASSESSING THE CONTROLLABILITY OF A
COMMUNICATION SYSTEM AND RADIO TECHNICAL SUPPORT FOR
AVIATION FORMATION**

В данной работе разработан подход оценки управляемости системы связи и радиотехнического обеспечения по показателю продолжительности цикла управления.

In this paper, we developed an approach to assess the controllability of a communication system and radio technical support in terms of the control cycle duration.

Являясь технической основой системы управления авиационного формирования, система связи и РТО представляет собой сложную организационно-техническую структуру. От способности изменять своё состояние (при управленческих воздействиях на неё органа управления системой связи и РТО) во всех условиях обстановки зависит эффективность реализации боевых возможностей не только подразделений связи и РТО но и авиационного формирования в целом.

В настоящее время действия авиации характеризуются высокой динамичностью, значительным пространственным размахом и быстрым изменением обстановки, с другой стороны своевременное планирование связи и РТО, оперативное принятие решений и доведение задач до подчиненных, уровень внедрения и использования средств автоматизации на пунктах управления системой связи и РТО авиационного формирования, не обеспечивает требуемого качества по управляемости системы связью и РТО.

Таким образом, объективно существует противоречие заключающееся в следующем, с одной стороны для обеспечения устойчивости, непрерывности, оперативности и скрытности системы управления авиационного формирования необходима качественная техническая основа, с другой стороны управляемость системы связи и РТО не в полной мере обеспечивает требуемое качество управления связью и РТО авиационного формирования.

На основе вышесказанного, актуальным является проведение исследования по вопросам повышения управляемости системы связи и РТО авиационного формирования.

Целью работы является повышение управляемости системы связи и РТО авиационного формирования.

Показателями управляемости системы связи и РТО являются:
вероятность перевода системы из одного состояния в другое (требуемое);
продолжительность цикла управления системой (подсистемой, элементами) связи и РТО.

Критерии оценки управляемости системы связи и РТО по представленным показателям:

по вероятности перевода - значение вероятности должно быть не ниже требуемого;
по продолжительности цикла управления - значение времени должно быть не больше требуемого.

Предлагается оценку управляемости системы связи и РТО авиационного формирования осуществлять по показателю продолжительности цикла управления – время цикла оперативного управления ($T_{\text{цоу}}$):

$$T_{\text{цоу}} = t_{\text{к}} + t_{\text{сб}} + t_{\text{об}} + t_{\text{пр}} + t_{\text{фки}} + t_{\text{д}}, \quad (1)$$

где: $t_{\text{к}}$ – время контроля элемента системы связи и РТО:

$$t_{\text{к}} = t_{\text{обн}} + t_{\text{фис}} + t_{\text{оби}}, \quad (2)$$

$t_{\text{обн}}$ – время обнаружения несоответствия параметров контроля элемента системы связи и РТО (линии, канала, связи) требуемым (допустимым) значениям;

$t_{\text{фис}}$ – время формирования информации состояния и ее передачи на пункт управления элементом системы связи и РТО;

$t_{\text{оби}}$ – время обобщения информации состояния, ее обработки и передачи информации на пункт оперативного управления;

$t_{\text{сб}}$ – время сбора информации о состоянии системы (элемента, сети) связи и РТО; $t_{\text{об}}$ – время обработки информации состояния органом управления; $t_{\text{пр}}$ – время принятия решения по сложившейся ситуации;

$t_{\text{фки}}$ – время формирования командной информации органом управления; $t_{\text{д}}$ – время доведения командной информации до исполнителей.

Таким образом, возможности системы управления связью и РТО характеризуются временем ее реакции на изменение состояния системы связи и РТО, то есть оперативностью выполнения основных функций управления связью и РТО:

контроля состояния элементов системы связи и РТО;

сбора и обработки информации об их состоянии;

принятия решения по сложившейся ситуации и доведения его до исполнителей [1].

ЛИТЕРАТУРА

1. Ермишян, А. Г. Теоретические основы построения систем военной связи в объединениях и соединениях : учебник для слушателей войск связи / А. Г. Ермишян. – СПб. : МО, 2005. – 740 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Колтаков Евгений Викторович. Слушатель.

ВУНЦ ВВС «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: evgenij.koltakov@mail.ru

Россия, 394064, г. Воронеж, ул. Старых Большевиков, д.54 а.

Тел.8-999721-10-68.

Стафеев Михаил Александрович. Старший преподаватель, кандидат военных наук.

ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: usirto@tut.by

Россия, 394064, г. Воронеж, ул. Старых Большевиков, д.54 а.

Телефон мобильный: 8-920-444-12-96.

Koltakov Evgenij Viktorovich. Listener.
MILITARY AIR FORCE "VVA Professor N.E. Zhukovsky and Y.A. Gagarin» (Voronezh).

Work address: Russia, 394064, Voronezh, street. Old Bolsheviks, d. 54 a.
Mobile phone: 8-999721-10-68.

Stafeev Mikhail Aliksandrovich. Senior Lecturer, candidate of military sciences.
MILITARY AIR FORCE "VVA Professor N.E. Zhukovsky and Y.A. Gagarin» (Voronezh).

Work address: Russia, 394064, Voronezh, street. Old Bolsheviks, d. 54 a.
Mobile phone: 8-980-556-10-54

Ключевые слова: оценка управляемости системы связи и радиотехнического обеспечения; продолжительность цикла управления.

Key words: assessment of controllability of a communication system and radio technical support; control cycle time.

УДК 623.618.5

Костин Сергей Викторович,
кандидат технических наук;

Мишин Дмитрий Станиславович,
кандидат юридических наук;

Сотников Александр Александрович

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ НЕЙРОННОЙ СЕТИ ХОПФИЛДА В БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

PROSPECTS OF APPLICATION OF THE HOPFIELD NEURAL NETWORK IN BIOMETRIC IDENTIFICATION

В данной статье рассматриваются структура, принцип работы, математический аппарат, алгоритм функционирования, способ реализации, достоинства и недостатки нейронной сети Хопфилда, а также перспективы прикладного применения ее для предоставления доступа в охраняемые помещения.

This article discusses the structure, principle of operation, mathematical apparatus, algorithm, method of implementation, advantages and disadvantages of the Hopfield neural network, as well as prospects for its application to provide access to protected areas.

Нейронная сеть Хопфилда основана на идее создания связей(аксонов) между нейронами, их взаимодействии, которое проявляется в использовании памяти для запоминания признаков изображения и их дальнейшей обработки. Одной из областей применения данного метода и является идентификация изображений.

Принцип реализации нейронной сети Хопфилда

Чтобы разобраться в принципе работы данного метода необходимо обратить внимание на его название, которое отсылает нас к анатомии человека, к строению головного мозга.

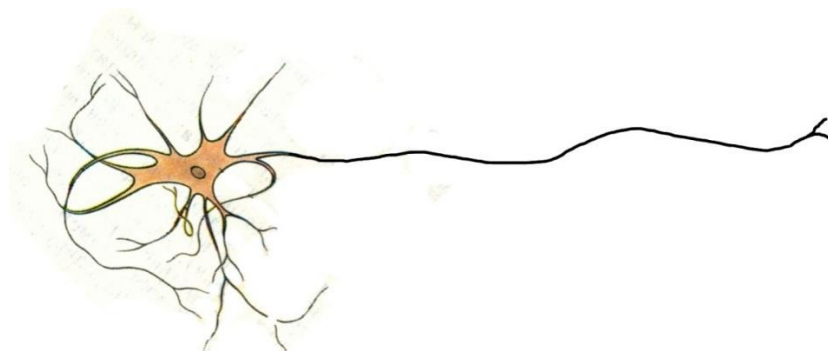


Рис. 1. Изображение нейрона

Изображение нейрона представлено на рисунке 1. Нейроном называется клетка, которая обрабатывает, хранит и передает информацию с помощью электрических и химических сигналов. Она взаимодействует с себе подобными, образуя целую систему[1]. Схема нейронной сети Хопфилда, представленная на рисунке 2, наглядно демонстрирует реализацию одного «слоя» нейронов, который является элементом логики. Он включают в себя: входы, количество которых равно числу выходов; весовые коэффициенты; сумматор и нелинейный преобразователь. Взаимодействие осуществляется посредством синапсов (мест контакта между двумя нейронами), при том что входит сигнал в один нейрон через один синапс, а выходные сигналы сформированы на аксонах.

В целом нейронной сети Хопфилда может быть представлена и охарактеризована такими составляющими как: архитектура сети, функциональные способности отдельных нейронов, способы их взаимодействия и образования связей[2].

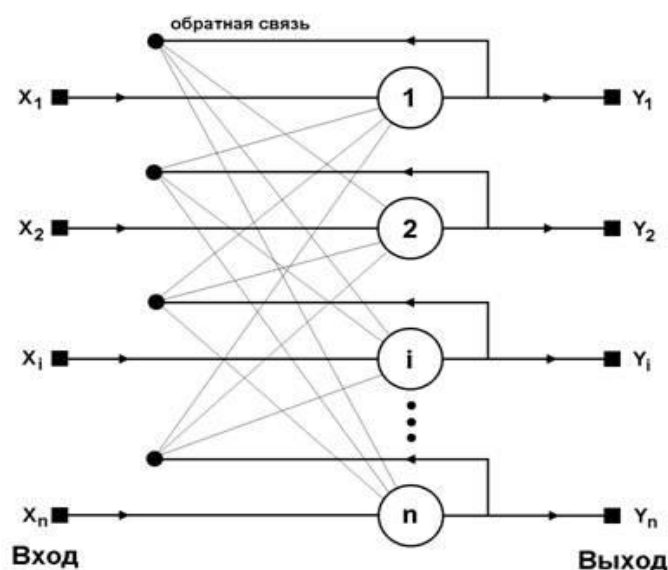


Рис.2. Структурная схема функционирования нейронной сети Хопфилда

Принцип работы нейронной сети Хопфилда также может быть описан математической моделью, основа которой состоит из матрицы коэффициентов и векторов.

Входной двоичный сигнал описывается вектором $X = (x_1 \dots x_n)$, где n определяется числом нейронов и размерность входных и выходных векторов. При этом каждый нейрон находится в одном из двух состояний: $x_n(t) \in [-1; +1]$.

Пусть на вход подается вектор, который описывает m -ный образец с помощью X^m , а его составляющие- X_i^m , где $m=0 \dots z-1$, где z - число образцов.

Взаимодействие между нейронами, которые ввиду биполярности также называют спинами, обуславливается особенностью структурной схемы и характеризуется следующим выражением:

$$E = \frac{1}{2} \sum_{i,j=1}^N \omega_{ij} X_i X_j, \quad (1)$$

где ω_{ij} — элементы матрицы взаимодействий W , состоящей из весовых коэффициентов связей между нейронами, куда и заносятся эталонные образы. При этом стоит отметить, что матрица связей симметрична, а диагональные элементы равны нулю для исключения воздействий нейронов самих на себя.

Установка весовых коэффициентов производится по следующему принципу:

$$\omega_{ij} = \begin{cases} \sum_{m=0}^{n-1} X_i^m X_j^m, & i \neq j \\ 0, & i = j \end{cases}, \quad (2)$$

где i - коэффициент предсинаптического нейрона, j — коэффициент постсинаптического нейрона, а $X_i^m X_j^m$ — i и j элементы вектора m -го образца. При этом коэффициенты изменяются исходя из параметров, архитектуры сети и правилами ее обучения.

Далее выходные значения попадают на сумматор, где складываются в одно число, которое на нелинейном преобразователе сравнивается с определенным пороговым значением, установленным заранее. Если значение выше порогового, то нейрон пропускает сигнал, если нет, то сигнал будет равен 0.

Для наглядности и упрощения понимания функционирования нейронной сети Хопфилда данный процесс можно представить в виде алгоритма, изображенном на рисунке 3.

На первом этапе происходит подача сигнала и установка аксонов $y_i(0) = x_i$, $i=0 \dots n-1$ (3)

Далее рассчитывается новое состояние нейронов:

$$s_j(p+1) = \sum_{i=0}^{n-1} \omega_{ij} y_i(p), j = 0 \dots n-1, \quad (4)$$

где p - номер итерации

и новое состояние аксонов:

$$y_i(p+1) = f[s_j(p+1)], \quad (5)$$

где f — функция, характеризующая единичный скачок.

В завершение идет проверка изменения состояния аксонов за последнюю операцию. При положительном ответе происходит возвращение к расчету нового состояния, в противном случае, работа прекращается, имея на выходе эталонный образец схожий со входным вектором.

Таким образом, при подаче исходного изображение на вход возможны два исхода:

1. Нейронная сеть верно идентифицирует изображение, исправляя при необходимости пораженные составляющие без добавления ошибок.
2. Произойдет обнаружение нескольких схожих изображений с искомым, вследствие чего пороговое число циклов будет превышено, и не будет никакого результата.



Рис.3. Алгоритм работы нейронной сети Хопфилда

Если говорить о машинной реализации, то данный метод использует не просто ассоциативную память (в ходе алгоритма обращение к ячейкам памяти происходит по содержимому последних, а не по конкретному адресу, что реализуется на ассоциативных запоминающих устройствах, такие как запоминающий массив, регистры ассоциативных признаков, маски и индикаторов адреса со схемами сравнения), а автоассоциативную, которая способна завершить работу или изменить образ, но не способна ассоциировать полученный образ с другим[3]. Также характерной особенностью сети является наличие обратных связей, образованных соединением аксонов каждого нейрона с дендритами остальных нейронов, а веса синоптических связей рассчитываются в начале работы и не изменяются.

Достоинства метода нейронных сетей Хопфилда:

- отсутствие громоздких вычислительных операций (весовые коэффициенты изначально рассчитаны по одной формуле);
- высокая точность (свыше 90%);

-высокая устойчивость работы, обусловленная асинхронный режимом работы и отсутствия работы нейронов на себя (задается матрицей связей).

Недостатки метода нейронных сетей Хопфилда:

- главным недостатком является малая емкость запоминаемых эталонов, которая определяется выражением:

$$G \cong \frac{N}{2 \log_2 N}, \quad (5)$$

где N- число нейронов. Примерно получается около 15% от общего количества нейронов;

- возможность заклинивания при распознавании обусловленная схожестью объектов;

-наличие перекрестных ассоциаций при большом объеме выборки образцов.

Для улучшения функционирования данного метода разумно использовать различные модификации. Например, применение ортогонального преобразования, которое поможет работать с сильно коррелированными изображениями, преобразуя начальное множество в дуальную совокупность векторов, к которой он способен обращаться при обработке похожих изображений. Также уместно использование гибридных методов, которые основываются на достоинствах их составных частей, нивелируя недостатки.

Применение нейронной сети Хопфилда для биометрической идентификации может быть представлено в следующем виде. Процесс распознавания начинается с детектирования лица. После изображение дифференцируется на кластеры, совокупность нескольких пикселей (2x2, 5x5 и др.), количество которых задается разработчиком. Это будет входной слой, поступающий на сеть слоев-фильтров с наборами признаков разной сложности и различного размера. Выделенные признаки попадают на классификатор, представленный обычно в виде многослойного персептрона [4]. Далее происходит передача данных сигналов от слоя к слою, при этом параллельно рассчитываются весовые коэффициенты синапсов. Они суммируются, заключая в себе информацию об отдельных фрагментах лица. По завершении работы будем иметь конкретный набор коэффициентов, который сравнивается с матрицей весов, сформированной по правилу Хэбба [5]. Основной задачей является подбор этих коэффициентов для уменьшения выходной ошибки.

Примером среды реализации метода являются программы Recognition, компании Adobe Systems Incorporated, где при подаче некоторого искаженного образа на вход нейронная сеть его идентифицирует посредством соотношения с одним из хранимых образов или же, в случае неудачи, выдает «химеру» (неаутентичный образ) [6]. Одной из самых распространенных является программа DellFastAccess 3.0 FacialRecognition, которая находится в открытом доступе, на сайте этой компании. Она позволяет предоставлять доступ лишь ограниченному кругу лиц, причем базу данных формирует сам владелец ПК или устройства, на которое она установлена.

ЛИТЕРАТУРА

1. Асадуллаев Р.Г. Нечеткая логика и нейронные сети. Учебное пособие. — Белгород: БелГУ, 2017. - 309с.
2. Тадеусевич Р., Боровик Б., Гончаж Т., Леппер Б. Элементарное введение в технологию нейронных сетей с примерами программ. Перевод с польск. И.Д. Рудинского. — М.: Горячая линия - Телеком, 2011. - 410с.
3. Каллан Роберт. Основные концепции нейронных сетей. Пер. с англ. — М.: Издательский дом "Вильямс", 2001. — 287 с.
4. Хайкин С. Нейронные сети: полный курс, 2-е изд., испр., исправленное — М.: ООО "И.Д. Вильямс", 2006.-1104с.

5. Терехов С.А. Лекции по теории и приложениям искусственных нейронных сетей, 2004.

6. EfremovaN., AsakuraN., InuiaT., AbdikeevN. TheNeuralNetworkforView-InvariantObjectRecognitionandClassification (Additional Details) – 2012.

СВЕДЕНИЯ ОБ АВТОРАХ

Мишин Дмитрий Станиславович. Доцент кафедры информационных технологий в деятельности ОВД. Кандидат юридических наук.

Орловский юридический институт МВД России имени В.В. Лукьянова.

E-mail: mishinds@mail.ru

Россия, 302027, г. Орел, ул. Игнатова, 2. Тел. 8-903-880-23-45.

Костин Сергей Викторович. Кандидат технических наук.

Академия ФСО России.

Адрес: 302027, г. Орел, ул. Приборостроительная, 35.

Сотников Александр Александрович.

Академия ФСО России.

Адрес: 302027, г. Орел, ул. Приборостроительная, 35.

Mishin Dmitriy Stanislavovich. Assistant professor. Candidate of science (jurisprudence /law).

Orel Law Institute of the Ministry of the Interior of the Russian Federation named after V.V. Lukianov

Russia, 302027, Orel, st. Ignatov, 2.Tel. 8-903-880-23-45.

Kostin Sergey Viktorovich. Candidate of Technical Sciences.

Russian Academy of FSO

Address: 302027, Orel, st. Instrument-35.

Sotnikov Alexander Alexandrovich

Russian Academy of FSO

Address: 302027, Orel, st. Instrument-35.

Ключевые слова: нейронная сеть Хопфилда, структура, принцип работы, математический аппарат, алгоритм функционирования, способ реализации, достоинства и недостатки, биометрическая идентификация, перспективы применения.

Key words: Hopfield neural network, structure, principle of operation, mathematical apparatus, functioning algorithm, method of implementation, advantages and disadvantages, biometric identification, application prospects.

УДК 004

**АНАЛИЗ ОСОБЕННОСТЕЙ ПРОЦЕССОВ ПРИНЯТИЯ РЕШЕНИЙ В
СИСТЕМАХ УПРАВЛЕНИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ПРИ
ВОЗНИКНОВЕНИИ ЧРЕЗВЫЧАЙНЫХ ОБСТОЯТЕЛЬСТВ**

**ANALYSIS OF THE PECULIARITIES OF DECISION MAKING PROCESSES
IN MANAGEMENT SYSTEMS OF SPECIAL PURPOSE IN CASE OF EMERGENCY**

В данной работе представлена статистика чрезвычайных обстоятельств и сравнительный анализ их особенностей, которые необходимо учитывать в процессе принятия решения при их ликвидации.

This paper presents statistics on emergency and a comparative analysis of their features, which must be taken into account in the decision making process during their liquidation.

В настоящее время в Российской Федерации в значительной степени сохраняется высокая опасность возникновения и развития чрезвычайных обстоятельств различного характера, т. е. в соответствии с существующей официальной терминологией [1, 2] событий, существенно влияющих на жизнедеятельность людей и общества и требующих принятия специальных мер по защите жизни, здоровья, прав и свобод граждан, материальных и иных ценностей от уничтожения, повреждения и по восстановлению нормальной работы.

Примером этого могут служить такие виды чрезвычайных обстоятельств, как чрезвычайные ситуации техногенного, природного, биолого-социального характера и крупные террористические акты, которые фигурируют в официальной статистике Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.

В таблице 1 на основе этой статистики [3 - 6] собрана информация об общих количественных характеристиках последствий (числе пострадавших, погибших и оценке материального ущерба) указанных чрезвычайных ситуаций за период 2015-2018 г.г. Анализ приведённых данных свидетельствует о сохраняющихся ежегодно огромных негативных последствиях, к которым они приводят.

Аналогичные данные имеются и по другим видам чрезвычайных обстоятельств.

Предотвращением и ликвидацией чрезвычайных обстоятельств в основном занимаются силовые ведомства Российской Федерации (Министерство по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС), Министерство обороны, Министерство внутренних дел, Федеральная служба безопасности, Росгвардия, Федеральная служба исполнения наказаний (ФСИН) и др.), в которых для этой цели используются системы управления специального назначения (СУ СН).

В значительном числе случаев планирование действий по предотвращению и ликвидации чрезвычайных обстоятельств связана с обработкой конфиденциальной информации, поэтому среди всех СУ СН выделяются системы, выработка управляющих воздействий в которых осуществляется с учётом требований обеспечения жёстких мер информационной безопасности, нарушение которых может существенно влиять на ход и исход процесса ликвидации чрезвычайных обстоятельств.

Таблица 1

Количество и последствия чрезвычайных ситуаций				
Характеристики \ Годы	2015	2016	2017	2018
Всего ЧС	257	299	257	266
Количество погибших	699	788	556	717
Количество пострадавших	20785	130959	36402	57477
Общий материальный ущерб (млн. руб.)	8505,899	9000,002	11232,975	11227,028

Следствием этого является разделение массивов обрабатываемой информации (логическое или даже физическое), а также специалистов по уровню доступа к ней. С учётом данного обстоятельства специалисты могут в различной степени оценивать важность тех или иных действий по принятию решений.

Главным образом такая ситуация относится к чрезвычайным обстоятельствам криминального характера, а также техногенного и природного характера, если возникает вероятность массовой гибели или заражения людей для недопущения случаев панического поведения населения.

К СУ СН такого вида, в частности, относятся системы управления Федеральной службы исполнения наказаний, обеспечивающие предотвращение и ликвидацию чрезвычайных обстоятельств в уголовно-исполнительной системе, под которыми в соответствии с [7] понимаются особо опасные события, происшедшие (происходящие) в учреждениях уголовно-исполнительной системы, вызванные явлениями криминального свойства и требующие принятия незамедлительных мер для их пресечения или ликвидации.

Число чрезвычайных обстоятельств, наиболее характерным для пенитенциарной системы России в соответствии с официальной статистикой ФСИН за период 2015-2018 г.г. [8] приведено в таблице 2.

Таблица 2

Количество чрезвычайных обстоятельств в учреждениях ФСИН				
Виды ЧО \ Годы	2015	2016	2017	2018
Действия, дезорганизующие работу исправительных учреждений	13	8	6	13
Побеги	123	101	106	103
Захваты заложников	2	0	1	0

Особенностью чрезвычайных обстоятельств на объектах ФСИН России является то, что несвоевременные и неправильные действия сотрудников могут привести в дальнейшем к причинению вреда здоровью, гибели людей, излишним материальным затратам.

Кроме того, следует отметить, что специфика чрезвычайных обстоятельств такова, что в их предотвращении и ликвидации участвуют объекты (функциональные группы, подразделения силовых ведомств), выполняющие существенно различающиеся задачи, требующие для организации их работы привлечения специалистов, обладающих специфическими узкопрофессиональными знаниями. Естественно, что у специалистов, отвечающих за различные аспекты принятия решений в СУ СН в процессе предотвращения и ликвидации чрезвычайных обстоятельств, может существенно различаться представление о значимости тех или иных действий, осуществляемых в процессе принятия решений.

Главным образом описанные ситуации относятся к сложным чрезвычайным ситуациям техногенного и природного характера.

Таким образом, задача совершенствования процессов принятия решений с использованием СУ СН указанного вида является актуальной.

ЛИТЕРАТУРЫ

1. Организация защиты населения и территорий от чрезвычайных ситуаций : учебник / В. А. Седнев, С. И. Воронов, И. А. Лысенко и др. – 3-е изд., перераб. и доп. – М. : Акад. ГПС МЧС России, 2014. – 229 с.
2. Ямалов И. У. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуациях / И. У. Ямалов. – М. : Лаборатория базовых знаний, 2012. – 288 с.
3. Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2015 году» / — М.: МЧС России. ФГБУ ВНИИ ГОЧС (ФЦ), 2016, 390 с.
4. Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2016 году» / МЧС России. М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2017, 360 с.
5. Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2017 году» / – М.: МЧС России. ФГБУ ВНИИ ГОЧС (ФЦ), 2018, 376 с.
6. Государственный доклад «О состоянии защиты населения и территорий Российской Федерации от чрезвычайных ситуаций природного и техногенного характера в 2018 году» / М.: МЧС России. ФГБУ ВНИИ ГОЧС (ФЦ), 2019, 344 с.
7. Антонов И. А. Деятельность ФСИН России в условиях чрезвычайных обстоятельств: понятие, задачи, подготовка кадров / И. А. Антонов, В. А. Антонов / Вестн. Санкт-Петербург. ун-та МВД России. – 2007. – № 4. С. 107–112.
8. Федеральная служба исполнения наказаний [Электронный ресурс]. – М., 2003–2019. – Режим доступа: <http://фсин.рф> (дата обращения: 02.08.2019 г.).

СВЕДЕНИЯ ОБ АВТОРЕ

Меньших Татьяна Валерьевна. Преподаватель кафедры математики и естественно-научных дисциплин.

Воронежский институт ФСИН России.

E-mail: tasay94@rambler.ru

Россия, 394072, г. Воронеж, ул. Иркутская, д.1-а. Тел. (473) 260-68-20.

Menshikh Tatyana Valerevna. Lecturer in the Department of Mathematics and Natural Sciences.

Voronezh institute of Russian Federal Penitentiary Service.

E-mail: tasay94@rambler.ru

Work address: Russia, 394072, Voronezh, Irkutskaya Str., 1-a.

Tel. (473) 260-68-20.

Ключевые слова: чрезвычайные обстоятельства, системы управления специального назначения, принятие решений.

Key words: emergency, management systems of special purpose, making decisions.

УДК 004.942:681.5

Мишин Дмитрий Станиславович,
кандидат юридических наук;
Еременко Владимир Тарасович,
доктор технических наук, профессор;
Паньков Сергей Леонидович

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ВНЕДРЕНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

ACTUAL PROBLEMS OF INTRODUCTION OF CLOUD COMPUTING IN LAW ENFORCEMENT

В предлагаемой статье рассматриваются основные понятия облачных технологий и облачных вычислений, направления и модели использования облачных сервисов в правоохранительных органах. Также проанализированы угрозы, препятствующие использованию и хранению данных в облачных структурах, а также выявлены перспективы нейтрализации угроз использования облачных вычислений в системе МВД России.

The article deals with the basic concepts of cloud technologies and cloud computing, directions and models of cloud services in law enforcement. Also analyses the threats that hinder the use and storage of data in the cloud structures as well as identified the prospects of the neutralization of threats of the use of cloud computing in the Ministry of interior of Russia.

В современном обществе можно наблюдать повсеместное развитие и широкое использование средств вычислительной техники и инфокоммуникационных технологий. Подобные процессы позволили обеспечить информационный обмен между пользователями на различном удалении друг от друга. Одновременно с этим проявились проблемы, требующие расширения границ администрирования, а также систематизации и обслуживания данных по запросам различных пользователей, направляемых посредством стандартизированного программного обеспечения. Особую актуальность эта тенденция стала приобретать в процессе значительного роста совокупных инфокоммуникационных ресурсов, что требует закупки существенного количества аппаратных средств, хотя потребность в них зачастую спорна.

В органах внутренних дел использование информационных технологий развивается также стремительно, и в настоящее время существует устойчивая тенденция расширения использования информационной системы обработки данных в практической деятельности. При этом следует отметить, что интеллектуальность систем постоянно повышается. Наибольшая востребованность информационных ресурсов наблюдается в процессе выполнения служебных обязанностей на определенном удалении от стационарных пунктов, что обусловило развитие мобильности для доступа к системе.

Постоянный рост объемов используемых информационных ресурсов и усложнение структуры информационных систем имеют положительные и отрицательные моменты. С одной стороны, усложнение системы позволяет повысить ее функциональность, а с другой стороны, повышается сложность обслуживания системы и растут затраты на поддержание ее в работоспособном состоянии[1]. Все это создает препятствия дальнейшему развитию информационных систем в правоохранительных органах. Решение данной проблемы возможно посредством объединения ресурсов на базе единой информационной системы.

Одним из актуальных направлений использования информационных и телекоммуникационных технологий в России, которые указаны в «Стратегии развития отрасли информационных технологий в РФ на 2014-2020 гг. и на перспективу до 2025» [2], выступает развитие культуры средств массовой информации, а также медиа- и управленческой среды. В связи с данными тенденциями особую актуальность приобретают пер-

спективы процесса организации документационного обеспечения и управления деловой коммуникацией в учреждениях, организациях, ведомствах, в том числе в подразделениях системы МВД России.

Таким образом, в настоящее время теория и практика исследования вопросов внедрения информационно-телекоммуникационных технологий, а также средств мультимедийной электроники и иных ресурсов сферы ИТ, направлена на такую сферу как организация документооборота в субъектах различных сфер правоотношений, в том числе с использованием облачных технологий и вычислений. В целом, понятие облачных технологий тождественно понятию облачных вычислений (CloudComputing) и представляет собой особый сервис для удаленного использования средств обработки и хранения информации.

В научной литературе «облачные вычисления» определены как особая технология, предназначенная для распределенной обработки данных, в которой ресурсы и мощности компьютерного устройства предоставляются пользователям как интернет-сервисы [4, с.40]. В обобщенном понятии «облако» используется только как метафора, которая имеет основание – изображение сети «Интернет» и представляет собой образ сложной структуры, объединяющей в себе комплекс технических средств и деталей.

При помощи использования облачных сервисов открываются возможности по получению доступа к информационным ресурсам, происходит деление прав групп пользователей данными ресурсами, используя при этом только подключение к Интернету и веб-браузер.

Модели развертывания информации, хранящейся в облачных интерфейсах, в настоящее время представлены следующими характеристиками:

- во-первых частное «облако» (Privatecloud) является ИТ-инфраструктурой, создаваемой и эксплуатируемой в масштабах одной организации и размещаемой в служебных помещениях. Особенностью данной системы является достаточно высокий уровень безопасности. В масштабах информационной системы обработки данных подобное «облако» может быть развернуто в масштабах службы, управления, департамента. Примером использования таких частных облачных инфраструктур могут быть модели, используемые, например, одним следственным отделом территориального органа внутренних дел. При этом, местоположение частного информационного пространства может находиться не только в управлении органа внутренних дел, но и у третьих лиц;

- во-вторых, публичное «облако» (Publiccloud) представляет собой ИТ-инфраструктуру, используемую пользователями различных организаций, при этом управлять и обслуживать систему может только владелец, то есть информация находится в юрисдикции поставщика этой информации. Особенностью публичного «облака» является невысокий уровень безопасности используемых информационных ресурсов. Например, хранящиеся на подобном ресурсе данные могут быть доступны для ознакомления пользователям официального сайта МВД России.

- в-третьих, разделяемое «облако» (Communitycloud) представляет собой симбиоз специальных публичных «облачных» инфраструктур, которые предназначены для определенных групп пользователей. Подобная реализация может быть использована государственными организациями в связи со спецификой требований этой группы. Например, доступ к данным предоставляется только конкретным подразделениям системы МВД России. Кроме того, целесообразно отметить, что подобное облако может эксплуатироваться как одним, так и несколькими подразделениями, а также выходить за пределы юрисдикции владельца данной информации;

- в-четвертых, гибридное «облако» (Hybridcloud) представляет собой комплекс наиболее эффективных свойств публичного и частного «облака». Особенностью данного облака является возможность перераспределения вычислительных мощностей в пе-

риод пиковой нагрузки. Подобное «облако» предусматривает возможность совместного использования предыдущих моделей.

Отметим, что в качестве преимуществ, которые раскрываются перед пользователями облачных технологий, в т. ч. применяемых в системе МВД России, можно назвать возможность управления большим объемом данных, обеспечение высокого уровня безопасности использования информации, отсутствие зависимости подключения к данным от модификации компьютерных устройств и программного обеспечения устройства. Однако, существует и ряд недостатков использования облачных технологий, например, зависимость пользования и управления данными от наличия и качества канала связи, риски технических сбоев и организация правового регулирования использования информации, хранящейся в облачных сервисах.

В настоящее время большое распространение получили такие облачные хранилища информации, как Amazon, Google, Microsoft, Savvis, Verizon и др.

Как отмечают современные исследователи, в настоящее время прослеживается тенденция, связанная с ростом количества облачных сервисов, в том числе и тех, которые ориентированы на предоставление услуг по хранению и обработке данных.

Как полагаем, такая тенденция связан, прежде всего, с тем обстоятельством, что при использовании облачных хранилищ значительно снижаются затраты на себестоимость работ по консолидации ресурсов, также расширяются возможности по их масштабированию, кроме того, предусматривается возможность доступа к данным из любой географической точки. Таким образом, использование облачных сервисов позволяет значительно повысить эффективность ИТ-инфраструктуры.

В современной научной литературе встречаются исследования, предметом которых выступают угрозы, с которыми сталкиваются организации, при использовании облачных технологий. Среди таковых, например, принято выделять [3, с.50]:

1. Угрозы потери и утечки информации, которых хранятся и обрабатываются в облачном хранилище. Причинами существования таких видов угроз в рассматриваемой сфере могут быть как действия мошенников, так и сбои в работе самих серверов, при которых может произойти потеря или утечка данных.

2. Угрозы компрометации учетных регистров и возникновение путей для обхода аутентификации пользователей облачного сервиса. Причинами возникновения данного вида угроз выступают: небрежное отношение владельца хранилища данных к механизму организации системы, отвечающей за проверку подлинности зашифрованных данных, использование односложных паролей, а также ненадлежащий порядок управления механизмом шифрования и сертификации.

3. Угрозы хакерских атак на интерфейсы отдельных пользователей, групп пользователей (взлом интерфейсов). Во избежание подобных угроз необходимо, в первую очередь, детально проработать механизм контроля доступа, предусмотреть возможность шифрования.

4. Угрозы утечки данных об учетных записях пользователей, содержащихся в облачных хранилищах (фишинг, мошенничество и пр.). К данной группе угроз целесообразно отнести угрозы, связанные с неправомерными действиями мошенников, направленными на изменение данных зарегистрированных пользователей, манипулирование их транзакциями как в рамках облачного хранилища, так и за его пределами.

5. Угрозы недостаточной осведомленности, заключающиеся в недостаточном осознании рисков и возможностей, которые открываются при использовании облачных технологий организациями, преследующими снижение затрат на себестоимость, но, в свою очередь, не учитывающих возможность наступления угроз в рассматриваемой сфере.

6. Угроза Dos и DDoS-атаки. Развитие облачных технологий сделало DoS и DDoS-атак более распространенными, в результате возникновения которых происходит замедление, а в некоторых случаях и полное прекращение, работы отдельных сервисов.

7. Угрозы совместных технологий, обобщенные риски. В данном случае возможно наступление цепной реакции, при которой уязвимость одного элемента облачной технологии порождает уязвимость другого структурного элемента и т.д.

Применяя вышеуказанные угрозы информационной безопасности облачного хранения и использования данных к вычислительным системам органов внутренних дел Российской Федерации, В.В. Киселев и Д.Б. Парыгин [3, с.52-53] провели экспертный анализ рассматриваемых угроз применительно к органам внутренних дел Российской Федерации.

Результатом проведенного анализа явилось заключение наличия в вычислительных системах МВД России всех необходимых механизмов для обеспечения информационной безопасности на достаточном уровне. В тоже время необходимо обеспечить их грамотное внедрение и применение, как в организационном, так и в методическом плане. Кроме того, отсутствие специальных навыков в области обеспечения безопасности информации у определенного количества пользователей создают предпосылки реализации известных угроз в вычислительных системах органов внутренних дел Российской Федерации.

Так, к примеру, при проведении исследования В.В. Киселев и Д.Б. Парыгин [3, с.52-53], указали, что наиболее значимыми угрозами для органов внутренних дел Российской Федерации выступают:

- угроза компрометации учетных записей;
- обход аутентификации, в частности проникновение в информационные системы вредоносного кода.

В Единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России) в целях минимизации подобных угроз предусмотрено формирование технологической инфраструктуры антивирусной защиты и многофакторной аутентификации.

То есть, с учетом прогресса использования облачных технологий в системе органов внутренних дел Российской Федерации, актуальным направлением является разработка системы устранения угроз инсайдеров-злоумышленников и компрометация учетных данных.

В целях минимизации угроз использования и хранения данных органов внутренних дел Российской Федерации в системе облачных вычислений, прежде всего, необходимо ставить акцент на неукоснительном соблюдении дисциплины в сфере информационной безопасности при работе с вычислительными системами, в том числе с использованием облачных технологий, например, ИСОД МВД России.

Как полагаем, строгое соблюдение и выполнение правил обеспечения безопасности информационной безопасности при работе с вычислительными системами, в том числе с использованием облачных технологий должно обеспечиваться со стороны каждого сотрудника ОВД, который является пользователем и имеет соответствующий доступ к данным, хранящимся и обрабатываемым на облачном сервисе.

ЛИТЕРАТУРА

1. Монахов Д.Н. и др. Облачные технологии. Теория и практика/ Монахов Д.Н., Монахов Н.В., Прончев Г.Б., Кузьменков Д.А. — М.: МАКС Пресс, 2013. — 128 с.

2. Распоряжение Правительства РФ от 01.11.2013 N 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на

2014 - 2020 годы и на перспективу до 2025 года» (ред. от 18.10.2018) //СЗ РФ. 2013. №46. Ст.5954.

3. Киселев В.В., Парыгин Д.Б. Анализ угроз облачных вычислений органов внутренних дел Российской Федерации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2018. № 1. С. 47-55.

4. Малюхова В.А., Глебова Р.В. Компьютерные информационные технологии в документационном обеспечении управления учебно-методический комплекс/ В.А. Малюхова, Р.В. Глебова. Йошкар-Ола: МОСИ, 2012. 115 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Мишин Дмитрий Станиславович. Доцент кафедры информационных технологий в деятельности ОВД. Кандидат юридических наук.

Орловский юридический институт МВД России имени В.В. Лукьянова.

E-mail: mishinds@mail.ru

Россия, 302027, г. Орел, ул. Игнатова, 2. Тел. 8-903-880-23-45.

Еременко Владимир Тарасович, Заведующий кафедрой информационной безопасности. Доктор технических наук, профессор.

Орловский государственный университет имени И.С. Тургенева

302026, г. Орел, ул. Комсомольская д. 95.

Тел.: 8-920-812-65-64.

Паньков Сергей Леонидович. Начальник научно-исследовательского и редакционно-издательского отдела.

Орловский юридический институт МВД России имени В.В. Лукьянова.

Тел.: 8-953-619-99-82.

Россия, 302027, г. Орел, ул. Игнатова, 2.

Mishin Dmitriy Stanislavovich. Assistant professor. Candidate of science (jurisprudence /law).

Orel Law Institute of the Ministry of the Interior of the Russian Federation named after V.V. Lukianov.

E-mail: mishinds@mail.ru

Russia, 302027, Orel, st. Ignatov, 2. Tel. 8-903-880-23-45.

Eryomenko Vladimir Tarasovich

Head of the Department of Information Security. Doctor of Technical Sciences, Professor.

Orel state University named after I. S. Turgenev.

Pankov Sergey Leonidovich. Head of the Research and publishing department.

Orel Law Institute of the Ministry of the Interior of the Russian Federation named after V.V. Lukianov

Russia, 302027, Orel, st. Ignatov, 2. Tel. 8-953-619-99-82.

Ключевые слова: документационное обеспечение, облачные вычисления, облачные технологии, органы внутренних дел, IT-технологии.

Keywords: documentation support, cloud computing, cloud technologies, internal Affairs bodies, IT-technologies.

УДК 004

ОСОБЕННОСТИ ПОСТРОЕНИЯ ДЕМОДУЛЯТОРОВ СИГНАЛОВ С ФАЗОРАЗНОСТНОЙ МАНИПУЛЯЦИЕЙ

FEATURES OF CONSTRUCTION OF SIGNAL DEMODULATORS WITH PHASE DIFFERENTIAL MANIPULATION

Статья посвящена исследованию демодуляторов сигналов с фазоразностной манипуляцией.

The article is devoted to the study of signal demodulators with phase difference manipulation.

В настоящее время в области радиотехники широкое распространение получили системы радиосвязи с фазовой (ФМ) и относительно фазовой (ОФМ) манипуляцией, так как известно, что они обладают высокой помехоустойчивостью.

Фазоразностная манипуляция основана на использовании конечных разностей функций, которые нашли применение в радиотехнике и связи при решении задач дискретной аппроксимации сигналов, при построении алгоритмов специализированных вычислителей, при разработке адаптивных систем обработки информации и систем передачи информации по каналам связи.

Рассмотрим представление конечных разностей в виде рекуррентного соотношения:

$$\Delta_n^K f = \Delta_n^{K-1} f - \Delta_{n-1}^{K-1} f. \quad (1.1)$$

Соотношение (1.1) наряду с формулой для вычисления разности первого порядка

$$\Delta_n^1 f = f(t_n) - f(t_{n-1}), \quad (1.2)$$

Можно использовать также представление конечных разностей непосредственно через отсчеты функций:

$$\Delta_n^K f = \sum_{i=0}^K (-1)^{K-i} C_K^i f(t_{n-K+i}), \quad (1.3)$$

где, C_K^i - число сочетаний из i .

Аппарат конечных разностей имеет вид

$$\widetilde{f(t)} = f(t_0) + \sum_{K=1}^N \frac{\Delta^K f}{K! (\delta t)^K} (t - t_0) [t - (t_0 - \delta t)] \times \dots \times [t_0 + (K - 1) \delta t] \quad (1.4)$$

Причем погрешность представления $f(t)$ многочленом (1.4) равна

$$\frac{\widetilde{f(t)} - f(t)}{(N+1)!} = \left(\frac{\Delta^K f}{\Delta t^K} \right) \frac{(t - t_0) [t - (t_0 - \delta t)] \dots [t - (t_0 - N \delta t)]}{(N+1)!}, \quad (1.5)$$

где $(\Delta^K f / \Delta t^K)$ – условное обозначение так называемой разделенной конечной разности K -го порядка, являющейся аналогом K -й производной функции.

Известно выражение разделенной разности через конечную разность того же порядка

$$\left(\frac{\Delta^K f}{\Delta t^K} \right) = \frac{\Delta^K f}{K! (\delta t)^K}, \quad (1.6)$$

откуда вытекает следующее важное соотношение:

$$\Delta^K f = (\delta t)^K \frac{d^K f(t)}{dt^K} \Big|_{t=\tau} \quad (1.7)$$

Выражения 1.1 -1.6 дают возможность сформулировать два важных свойства дискретно-разностного преобразования:

1) свойство линейности, вытекающее из 1.3:

$$\begin{aligned} \Delta^K (S_1 + S_2) \\ = \Delta^K S_1 + \Delta^K S_2 \end{aligned} \quad (1.8)$$

2) свойство инвариантности, вытекающее из 1.7

$$\begin{aligned} \Delta^K S = 0, \quad \text{если} \quad \frac{d^K S(t)}{dt^K} \\ \equiv 0 \end{aligned} \quad (1.9)$$

Отсюда следует, что если имеется аддитивная смесь полезного сигнала $S(t)$ и мешающего воздействия $\xi(t)$: $x(t) = S(t) + \xi(t)$, и последнее таково, что

$$d^K \xi(t)/dt^K \equiv 0 \quad (1.10)$$

то согласно 1.6 и 1.7

$$\Delta^K x = \Delta^K (S + \xi) = \Delta^K S + \Delta^K \xi = \Delta^K S = \text{invar} \xi \quad (1.11)$$

Два основных алгоритма модуляции и демодуляции конечных разностей строятся на базе 1.1 и 1.3.

Первый рекуррентный алгоритм, основанный на использовании соотношения 1.1.

Структурная схема передающей части системы с разностной модуляцией K -го порядка представлена на рис.1.1.

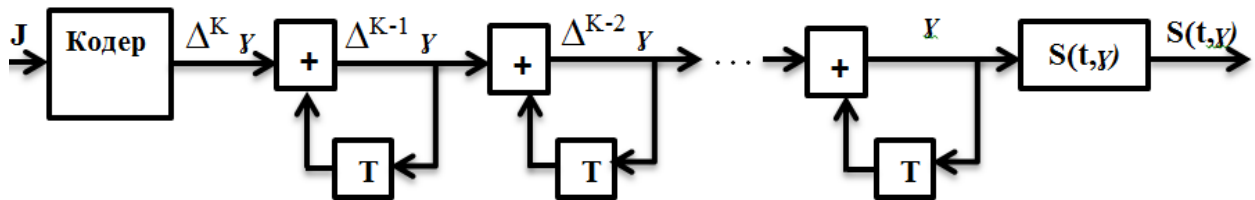


Рис.1.1. Структурная схема передающей части системы с разностной модуляцией K -го порядка

Принятый сигнал J с помощью кодера преобразуется в значения K -й разрядности $\Delta^K y$ параметра y . Далее в результате K последовательно включенных преобразователей, содержащих суммирующее устройство и запоминающее устройство на время T , вычисляются значения параметра y , и в формирователе сигнала образуются соответствующие этим значениям посылки принимаемого сигнала. В случае системы ПДИ кодер представляет собой преобразователь, в данном случае двоичных кодовых комбина-

ций в значение К-й разности модулируемого параметра, а формирователь сигнала – манипулятор соответствующего параметра несущего колебания.

Структурная схема приемной части системы, соответствующая рекуррентному алгоритму представлена на рис.1.2.

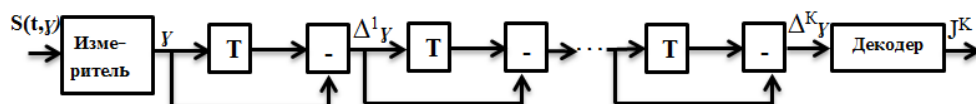


Рис.1.2. Структурная схема приемной части системы с разностной модуляцией К-го порядка

Приемная часть включает в себя измеритель параметра y и K последовательно включенных равнозначных преобразователей, содержащих запоминающее устройство на время T и вычитающее устройство, вычисляющие конечные разности от первого до К-го порядка. Последним элементом в схеме является декодер, где выносятся решение и соответствии вычисленной разности $\Delta^K y$ информационного символа J . В системе ПДИ декодер преобразует значение разности в двоичную кодовую комбинацию. Данная структура может быть представлена не только в аналоговом, но и в цифровом виде, для этого измеритель параметра y должен включать в себя аналого-цифровой преобразователь.

Существуют еще один подход при решении задачи модуляции и демодуляции конечных разностей, который основан на выражении 1.3, и имеет следующий вид

$$\Delta_n^K y = (-1)^{K-i} C_{K-i}^i y_{n-K+i} \quad (1.12)$$

Отличительной чертой такого подхода является то, что К-я разность вычисляется в данном случае напрямую через значения параметра y в $(K+1)$ отсчетных точках, без операции вычисления разностей.

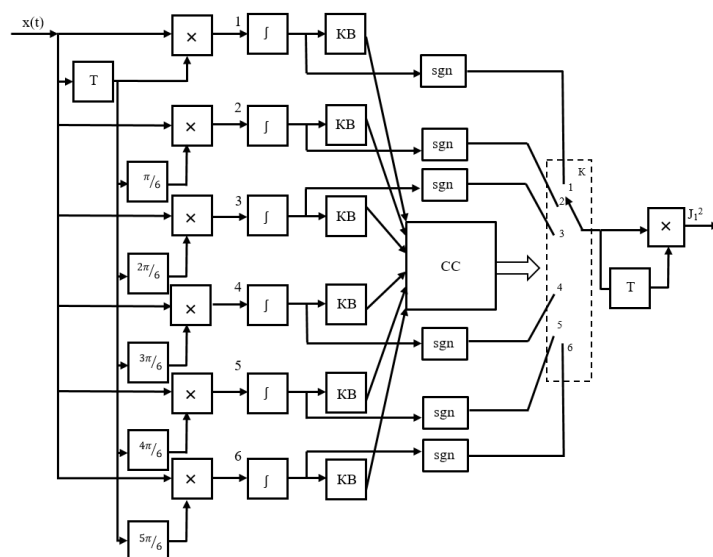


Рис.1.3. Структурная схема демодулятора сигналов с однократной ФРМ второго порядка

Поступивший сигнал обрабатывается параллельно в нескольких автокорреляторах (АК), состоящих каждый из фазовращателя (ФВ), перемножающего устройства (ПУ) и интегрирующего устройства (ИУ). На рис.1.3 представлен вариант с шестью АК, имеющими сдвиги фаз между прямым и задержанным сигналами; $0, \pi/6, 2\pi/6, 3\pi/6, 4\pi/6, 5\pi/6$, соответственно. Отсчеты с выходов ИУ всех шести АК возводятся в квадрат

и подаются на сравнивающее устройство (СУ), где принимается решение о выборе большего значения из них. СУ управляет далее работой коммутатора К, к выходной части демодулятора присоединяется только один АК с наивысшим значением по уровню выходным сигналом. Таким образом удастся вычислить знак второй разности фаз в результате перемножения знаков соседних отсчетов сигнала на выходе АК, тем самым достичь повышения помехозащищенности демодулятора.

На основе быстрых цифровых алгоритмах, предложенных в 5, проводятся исследования возможности применения данного алгоритма к демодуляции сигналов с фазоразностной манипуляцией второго и третьего порядка.

ЛИТЕРАТУРА

1. Финк Л.М. Теория передачи дискретных сообщений / Л.М. Финк. – М.: Советское радио, 1970. – 728 с.
2. Федоров И.Б. Информационные технологии в радиотехнических системах: учеб. пособие / под ред. И.Б. Федорова. – 3-е изд. перераб. и доп. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2011. – 846 с.
3. Лайонс Р. Цифровая обработка сигналов / Р. Лайонс. – М.: ООО Бином Пресс, 2006. – 656 с.
4. Richard W. Middlestead. Digital communications with Emphasis on data modems. John Wiley & Sons, Inc., 2017, 792 p.

СВЕДЕНИЯ ОБ АВТОРЕ

Оболонская Алёна Владимировна. Старший преподаватель-методист адъюнктуры.
Воронежский институт МВД России.
E-mail: alena.obolonskaja2017@yandex.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.
Тел. +7 (473) 200-51-71.

Obolonskaya Alena Vladimirovna. Senior Lecturer.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: alena.obolonskaja2017@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. +7 (473) 200-51-71.

Ключевые слова: демодулятор, фазоразностная манипуляция, быстрый цифровой алгоритм, разностная модуляция.

Keywords: phase difference manipulation, fast digital algorithm, difference modulation.

УДК 621.376

Перминов Геннадий Вадимович,
кандидат технических наук;
Зарубин Сергей Владимирович,
кандидат технических наук

АНАЛИЗ АКТУАЛЬНОСТИ ПРОБЛЕМЫ ПАССИВНОГО ПЕРЕХВАТА ТРАФИКА В СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

THE ANALYSIS OF THE RELEVANCE OF THE PROBLEM OF PASSIVE INTERRUPTION OF TRAFFIC IN MODERN COMPUTER NETWORKS

Статья посвящена анализу методов пассивного перехвата трафика в компьютерных сетях, построенных на основе концентраторов типа switch. Также приводятся рекомендации по предотвращению пассивного перехвата трафика.

The article is devoted to the analysis of methods for passive traffic interception in computer networks based on switch-type hubs. It also provides recommendations to prevent passive traffic interception.

Технология Ethernet, на основе которой построены практически все современные проводные компьютерные сети, подразумевает соединение компьютеров в топологию типа «звезда». В центре звезды находится концентратор, от которого к каждому компьютеру в сети протянут отдельный провод. Концентраторы могут быть двух видов: hub и switch.

Hub является более простым и, в настоящее время, устаревшим устройством, которое использовалось на заре развития сетевых технологий. Получив пакет данных на один свой порт он усиливает сигнал и отправляет этот пакет во все свои оставшиеся порты. В результате все участники сети получают этот пакет. Далее сетевые карты сравнивают MAC-адрес, указанный в качестве адреса назначения пакета с собственным. На основе этого сравнения сетевая карта компьютера принимает решение удалить этот пакет из памяти сетевой карты или передать его для обработки прикладному ПО.

Как видим, использование концентраторов типа hub позволяет успешно функционировать локальному сегменту компьютерной сети, но имеет ряд недостатков.

Первый из них – снижение скорости работы сети. Дело в том, что концентратор типа hub создает для участников сети общую разделяемую среду передачи данных. Разделение осуществляется по времени. Это значит, что одновременно только один участник сети может передавать информацию. Остальные должны ждать, когда общая разделяемая среда передачи данных освободится. Возможны ситуации, когда несколько компьютеров в сети одновременно убедившись в том, что сеть свободна, одновременно начнут передачу информации в сеть. Такая ситуация называется коллизия. Понятно, что чем больше в сети участников, тем больше время ожидания и тем выше вероятность возникновения коллизий.

Однако, снижение скорости работы сети – не единственная и не самая опасная проблема, связанная использованием концентраторов типа hub. Как было показано выше, отправленный в сеть пакет будет доставлен всем участникам сети, которые самостоятельно принимают решение об уничтожении или дальнейшей обработке пакета. Существует специальное программное обеспечение, которое отключает такую проверку, то есть переводит сетевую плату в так называемый неразборчивый режим. Целый класс такого ПО объединен общим названием – sniffеры (от англ. sniff – вынюхивать). Такой sniffер, который переводит сетевую карту компьютера в неразборчивый

режим и никаким образом не сказывается на работе компьютерной сети, называется пассивным. Следует отметить, что, во-первых, пассивный сниффер является эффективным с точки зрения перехвата информации, так как позволяет контролировать трафик целого сегмента сети, во-вторых, из-за того, что он никак не вмешивается в работу сети, то его трудно обнаружить.

Дальнейшее развитие сетевых технологий привело к возникновению концентраторов типа switch. Они используются в настоящее время. Switch. Когда switch впервые включается в сеть, он фактически работает так же, как hub. Но при этом находится в режиме обучения. То есть, получив пакет на один свой порт он также усиливает сигнал и отправляет его во все свои оставшиеся порты. Но при этом анализирует заголовки пакетов и, в частности, анализирует MAC-адреса отправителей и сохраняет их в своей таблице маршрутизации. В результате через короткое время switch накапливает информацию о MAC-адресах всех компьютеров, подключенных к соответствующим портам. Далее switch переходит из режима обучения в рабочий режим.

В рабочем режиме switch, получив пакет, анализирует MAC-адрес назначения и, усилив сигнал, направляет его только в один свой порт, к которому подключен компьютер-получатель. Такая схема работы сети позволяет решить оба недостатка, связанные с использованием концентраторов типа hub. Во-первых, одновременно несколько участников сети могут обмениваться информацией, если их направления не пересекаются, снижается вероятность возникновения коллизий и появляется возможность объединять в один сегмент сети большее количество компьютеров. Во-вторых, пакет, отправленный в сеть, будет доставлен не всем участникам сети, а только нужному получателю. Это делает невозможным пассивный перехват трафика в сегменте сети.

Следует отметить, что использование концентраторов типа switch полностью не решает проблему перехвата трафика. Существует ряд методов, позволяющих перенаправлять трафик в таких сетях, таким образом, чтобы он проходил через компьютер разведчика. Такие методы объединены общим названием активный сниффинг, так как они влияют на работу сети. Однако методы активного сниффинга выходят за рамки данной статьи.

В настоящее время устройства типа hub потеряли актуальность и не используются. Однако, актуальность проблемы пассивного сниффинга по-прежнему актуальна. Это связано с тем, что пассивный сниффинг более эффективен в сравнении с активным и его значительно труднее обнаружить.

Рассмотрим методы пассивного сниффинга, которые могут применяться в сетях, построенных на концентраторах типа switch.

Первый связан с тем фактом, что некоторые устройства типа switch в периоды пиковой нагрузки переходят в режим hub. Разведчику следует только вывести работу компьютерной сети в такой режим. Это можно сделать, например осуществив атаку типа DoS или DDoS, то есть атака на отказ в обслуживании или распределенная атака на отказ в обслуживании. Следует сказать, что такая атака значительно сказывается на скорости работы сети и достаточно быстро может быть обнаружена и нейтрализована администратором сети. Поэтому этот метод может применяться только в короткие промежутки времени.

Другой способ связан с использованием так называемых портов зеркалирования. Это специальные порты, которые встроены в маршрутизаторы и концентраторы типа switch высокого уровня, в которые перенаправляется весь трафик, передаваемый в сегменте сети независимо от отправителя и адресата. Порты зеркалирования обычно используются для диагностики сети. Однако, если разведчик сможет получить физический доступ к порту зеркалирования, то он сможет получить доступ ко всему трафику, передаваемому через концентратор. Такое подключение может быть не обнаружено в течение длительного времени, так как концентраторы могут устанавливаться под

подвесными потолками, или под стенными панелями, или в других скрытых местах. Тогда несанкционированное подключение может быть обнаружено в период планового технического обслуживания сетевой аппаратуры. Разведчик также может использовать радиопередающие устройства для передачи перехваченного с порта зеркалирования трафика. Это позволит усложнить задачу его обнаружения.

Еще один метод пассивного перехвата трафика в компьютерных сетях, построенных на основе концентраторов типа switch, связан с тем, что сетевые кабели обычно также прокладываются в скрытых местах. С одной стороны, это сделано из соображений эстетики, с другой, это позволяет злоумышленнику осуществить несанкционированное подключение непосредственно к кабелю. При этом никаких специальных технических средств не требуется. Достаточно только обрезать сетевой провод, установить на получившиеся концы коннекторы и соединить их при помощи концентратора типа hub. В результате мы получаем сегмент сети, описанный выше. Такой способ подключения позволяет контролировать трафик только одного участника сети, но зато весь трафик, передающийся к/от данного компьютера доступен злоумышленнику и такое подключение может быть не обнаружено длительное время, так как сетевые провода не нуждаются в плановом техническом обслуживании и не контролируются. Также разведчик может использовать радиопередающие устройства для усложнения задачи своего обнаружения.

Возможно, приведенный перечень методов не является исчерпывающим и автору не известны другие существующие методы пассивного перехвата трафика в сетях, построенных на основе концентраторов типа switch. Однако, проведенный анализ позволяет сделать вывод о том, что пассивный перехват трафика в современных компьютерных сетях является актуальной проблемой, требующей внимания.

В качестве мер по борьбе с методами пассивного перехвата трафика следует выделить следующие:

1. Концентраторы и маршрутизаторы следует устанавливать таким образом, чтобы можно было легко осуществлять их визуальный контроль, но при этом не допустить к ним физический доступ со стороны посторонних лиц. Это можно сделать, например, с помощью прозрачных коробов, устанавливаемых в коридорах и запирающихся на ключ с опломбированием.

2. Сетевые кабели следует укладывать таким образом, чтобы либо иметь возможность их визуального контроля, либо исключить возможность доступа к ним со стороны посторонних лиц, например, укладывать их в штробу в кирпичной кладке. Однако, контроль целостности проводных линий связи – это очень сложная и дорогостоящая задача.

3. Наиболее эффективным методом защиты информации, передаваемой по каналам связи является защита с помощью ее криптографического преобразования.

Таким образом, в статье рассмотрены актуальные методы пассивного перехвата трафика в современных компьютерных сетях и предложены способы его предотвращения.

ЛИТЕРАТУРА

1. Перминов, Г.В. Определение объема репрезентативной выборки в целях получения трасологической статистики стеганографических программ [Текст] / А.Н. Копылов, Р.А. Солодуха, Г.В. Перминов // сборник материалов международной научно-практической конференции «Охрана, безопасность, связь – 2011». – Воронеж: ВИ МВД России. – 2011. – С. 138-140.

2. Перминов, Г.В. Технические аспекты интеграции потребителей услуг вневедомственной охраны в информационную систему отдела вневедомственной охраны [Текст] / Р.А. Солодуха, Г.В. Перминов // Вестник Воронежского института МВД России. – 2009. – № 1. – С. 144-151.

3. Перминов, Г.В. Вычислительный эксперимент по проверке свойств критерия динамической эффективности контроля целостности программной среды эталонной АДИС [Текст] / Г.В. Перминов, С.В. Родин, С.С. Кочедыков // Вестник Воронежского института МВД России. – 2015. – № 1. – С. 263-270.

4. Зарубин, С.В. К вопросу защиты информации в системах безопасности [Текст] / С.В. Зарубин, В.С. Зарубин // сборник материалов XIII Всероссийской научно-практической конференции «Математические методы и информационные средства». – Краснодар: Краснодарский университет МВД России. – 2018. – С. 39-45.

5. Зарубин, С.В. К вопросу оценки показателя защищенности информационных процессов в автоматизированной системе безопасности [Текст] / А.А. Савинков, С.В. Зарубин, В.С. Зарубин // Вестник Воронежского института ФСИИ России. – Воронеж: Воронежский институт ФСИИ России. – 2018. – № 1. – С. 42-46.

6. Зарубин, С.В. К вопросу решения задачи разработки моделей и алгоритмов синтеза комплекса показателей защищенности автоматизированной системы безопасности и охранного мониторинга критически важных объектов [Текст] / С.В. Зарубин, В.С. Зарубин // сборник материалов международной научно-практической конференции «Общественная безопасность, законность и правопорядок в III тысячелетии». – Воронеж: Воронежский институт МВД России. – 2018. – С. 31-35.

СВЕДЕНИЯ ОБ АВТОРАХ

Перминов Геннадий Вадимович. Старший преподаватель кафедры информационной безопасности. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: perminovgv@mail.ru

Россия, 394065, г. Воронеж, пр. Патриотов, 53. Тел. (473) 200-52-42.

Зарубин Сергей Владимирович. Старший преподаватель кафедры информационной безопасности. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: zarubin.sv@mail.ru

Россия, 394065, г. Воронеж, пр. Патриотов, 53. Тел. (473) 200-52-42.

Perminov Gennadiy Vadimovich. Senior Lecturer of the chair of Information Security. Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-42.

Zarubin Sergey Vladimirovich. Senior Lecturer of the chair of Information Security. Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-42.

Ключевые слова: компьютерные сети, перехват трафика, защита информации.

Key words: computer networks, traffic interception, information protection..

УДК 004.056

УВЕЛИЧЕНИЕ ВРЕМЕНИ РАБОТЫ СРЕДСТВ РАДИОСВЯЗИ, СТОЯЩИХ НА ВООРУЖЕНИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

INCREASE OF WORK TIME OF RADIO COMMUNICATION FACILITIES STANDING ON ARMAMENT IN INTERNAL AFFAIRS

В статье рассматриваются вопросы увеличения времени работы средств радиосвязи, стоящих на вооружении в органах внутренних дел для оперативности принятия решений и повышения качества несения службы

The article discusses the issues of increasing the working hours of radio communications equipment in service in the internal affairs bodies for speedy decision-making and improving the quality of service

Портативные средства радиосвязи появились на вооружении органов внутренних дел в конце 60-х годов прошлого века. Использование носимых радиостанций при обеспечении охраны общественного порядка, проведении оперативно-розыскных, массовых мероприятий, ликвидации последствий чрезвычайных ситуаций и стихийных бедствий позволило существенно сократить время реагирования нарядов и повысило управленческий потенциал дежурных частей органов внутренних дел. Появление у пеших нарядов полиции возможности использования федеральных, региональных баз данных, сервисов ИСОД МВД России для осуществления проверки граждан и автотранспорта повысило качество несения службы и оперативность принятия решений.

Таким образом, от срока автономной работы аккумуляторных батарей портативных средств связи, напрямую зависит эффективность работы сотрудника полиции, что делает вопрос обеспечения работоспособности средств радиосвязи, при несении службы сотрудниками органов внутренних дел, особенно актуальным.

На снижение времени работы средств радиосвязи, влияют несколько факторов: эффективность работы усилительных элементов, интенсивность ведения радиообмена (передачи информации), температура окружающей среды, срок эксплуатации аккумуляторной батареи.

Самым очевидным и в тоже время одним из самых финансово затратным способом увеличения времени автономной работы средств радиосвязи, является замена элементов питания, в связи с чем, необходимо принятие организационных мер для соблюдения правил эксплуатации и заряда аккумуляторных батарей в зависимости от материала питающего элемента.

Для никель-кадмиевым NiCd и в меньшей степени никель-металл-гидридных NiMH аккумуляторов, применяемых в парке радиостанций «Гранит», «Альтавия», «Эрика», «Kenwood» и т.д. свойственен «Эффект памяти». Причина этого явления заключается в том, что в процессе эксплуатации с каждым новым циклом заряда-разряда рабочее вещество внутри и NiMH NiCd аккумуляторов постепенно изменяет свою структуру, уменьшая площадь активной поверхности, а это ведет к уменьшению реальной емкости. Такой эффект развивается от того, что аккумуляторы на основе никеля заряжаются не полностью разряженные, а сильнее всего это проявляется в никель-кадмиевых аккумуляторах. Никель-металл-гидридные аккумуляторы подвержены эффекту памяти в меньшей степени.

В процессе эксплуатации рации, потребители обычно не дожидаются полной разрядки аккумулятора перед очередным зарядом. Это вполне естественно, когда от-

существует запасной аккумулятор. Но в результате такой практики через несколько месяцев (в зависимости от частоты заряда, глубины разряда, условий эксплуатации, качества аккумулятора и фирмы-изготовителя) реальная емкость аккумулятора заметно уменьшается, сокращается время заряда.

Возникновения «эффекта памяти» можно избежать применяя «тренировку» аккумуляторов. «Тренировка» аккумулятора – это процесс периодического (3-4 раза) цикла зарядов и последующих разрядов [1]. Выполнение тренировочных циклов возможно непосредственно в радиостанции, но для этого требуется значительно больше времени, что менее эффективно, поскольку рация отключиться раньше, чем аккумулятор полностью разрядится, поэтому «тренировку» выполняют на стационарных зарядных устройствах, с функцией разряда. Для никель-кадмиевых аккумуляторов рекомендуется осуществлять «тренировку» не менее одного раз в месяц, а для никель-металл-гидридных раз в три месяца.

В парке носимых радиостанция «Такт», «Волна», «Вихрь», «Icom» и др. активно используются литий-ионных (Li-Ion) аккумуляторы, практически не подвергающиеся «эффекту памяти», но предпочитающие заряженное состояние разряженному. Их можно неограниченно держать в зарядном устройстве (ЗУ) и ставить на заряд в любой момент, так как ЗУ для данного типа батарей снабжены схемой автоматического отключения после окончания заряда. Важно, чтобы ЗУ было предназначено для заряда литиевых аккумуляторов именно этого производителя, в противном случае аккумулятор может быть либо недозаряжен, либо испорчен. При эксплуатации литиевых аккумуляторов также наблюдается снижение емкости, что ведет к снижению времени автономной работы аккумулятора, в связи с чем, перед эксплуатацией нового аккумулятора рекомендуется произвести цикл полного заряда и полного разряда аккумулятора несколько раз — в этом случае аккумулятор примет свою максимально возможную емкость [1].

Ещё одним способом увеличения времени автономной работы средств радиосвязи, является снижение мощности передатчика. Анализ маршрутов и схем патрулирования нарядов, эксплуатирующих средства связи, позволяет снизить мощность излучения передатчика не ухудшая качество связи. Несмотря на то, что на дальность связи больше влияют чувствительность приемника, конструкция антенны, диапазон рабочих частот, радиочастотное окружение, рельеф местности и городская застройка, снижение мощности передатчика ведет к снижению дальности связи. Данная проблема решается применением ретрансляционного оборудования, при этом существенно увеличивает качество связи, но требуется задействование дополнительных технических средств и дополнительного финансирования.

Рассматривая вопрос увеличения времени работы средств радиосвязи, более детально, стоит отметить, что в цифровых радиосетях органов внутренних дел циркулируют высоко эффективные сигналы в связи с чем, существует ряд особенностей, связанных с их усилением. В средствах радиосвязи стандарта APCO-25 применяется непрерывная квадратурная фазовая модуляция, с одновременной модуляцией фазы и амплитуды сигнала для обеспечения минимальной ширины занимаемой полосы частот. В стандарте TETRA – четырехпозиционная дифференциальная фазовая модуляция ($\pi/4$ DQPSK). Данные виды модуляции не обеспечивают постоянство формы огибающей и, как следствие, требуют применения усилителей с высокой линейностью [2].

Любой усилитель мощности по своей сути является энергетическим преобразователем. Энергия постоянного тока от источника питания преобразуется с помощью усилительного прибора в энергию радиочастотного колебания требуемой частоты и формы. Усилитель, как и любой преобразователь энергии подчиняется фундаментальным законам физики, а в частности это закон сохранения энергии и второе начало тер-

динамики. Следовательно, не вся затраченная энергия преобразуется в полезную и у любого усилительного прибора коэффициент полезного действия меньше 1.

Как правило, лучшей линейности усилителей добиваются за счет увеличения мощности выходного каскада. Однако при этом эффективность усиления падает, следовательно, рассеивается больше тепла, что, в конечном счете, увеличивает энергопотребление системы и уменьшает время работы портативного устройства [3]. Более того, обеспечить необходимые условия линейности возможно только при применении усилителя класса А, с присущим ему недостатком – очень низким КПД. Для получения высоких КПД транзисторные усилители мощности должны работать в режиме с отсечкой тока, то есть в классе АВ или С. Поэтому современные СВЧ-усилители включают в свою схему несколько типов компенсации нелинейных искажений, от регулировки рабочей точки до обратных и прямых связей компенсации [4].

Многообразие этих систем можно разделить на несколько типов это система с петлей обратной связи (ОС), система с прямой связью, система с предискажениями.

Рассмотрим системы с обратной связью на примере обратной связи в декартовой системе координат представленной на рис.1. Особенностью данной схемы является присутствие демодулятора в цепи ОС.

Входными сигналами системы служат синфазная $I(t)$ и квадратурная $Q(t)$ составляющие (декартовы координаты) амплитудно-фазового модулированного колебания.

$$V(t) = A(t) \sin(\omega_c(t) + \varphi(t)) = Q(t) \cos(\omega_c(t)) + I(t) \sin(\omega_c(t)), \quad (1)$$

где $A(t)$, $\varphi(t)$, ω_c – огибающая, фаза и несущая частота модулированного сигнала соответственно,

$$I(t) = A(t) \cos[\varphi(t)], \quad Q(t) = A(t) \sin[\varphi(t)]. \quad (2)$$

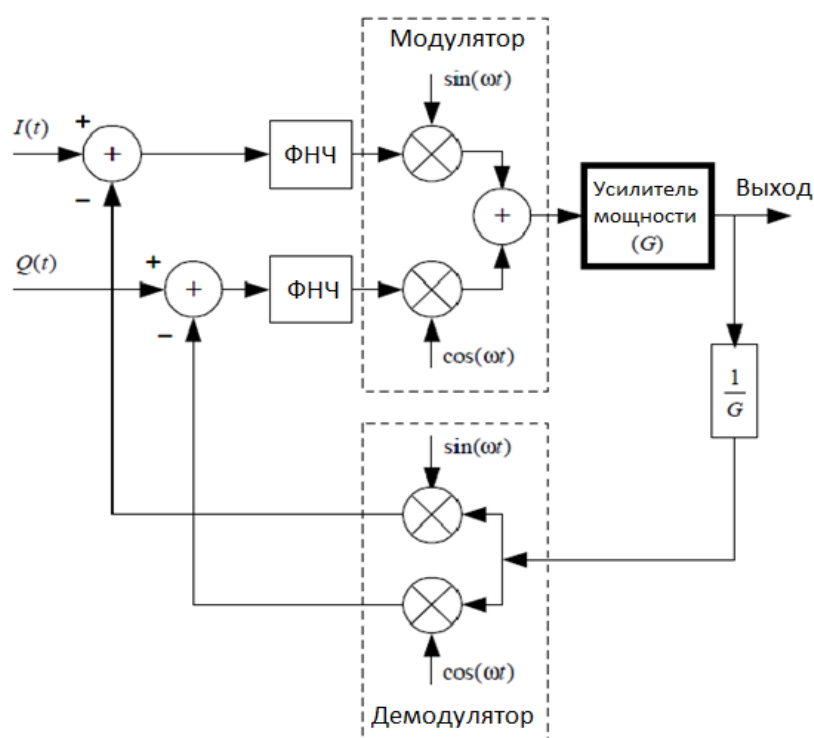


Рис. 1. Система усиления с декартовой обратной связью

Посредством декартовой ОС изменения температуры, напряжения питания и нагрузки влияют на характеристики усилителя. Применение цифровой обработки сигналов предоставляет новые возможности для аппаратной реализации рассматриваемой системы усиления. Ключевой проблемой метода декартовой ОС является сохранение устойчивости

системы в условиях, когда нелинейный усилитель создает фазовые сдвиги сигналов в широкой полосе частот, а смесители демодулятора ОС порождают нелинейные эффекты [5].

Система усиления с прямой связью представлена на рис.2. Она содержит два замкнутых цикла обработки сигналов [5]. Выходной сигнал первого цикла – сигнал ошибки – результат вычитания из задержанного нелинейно усиленного сигнала. Во втором замкнутом цикле сигнал ошибки, усиленный в «усилителе искажений», вычитается из выходного, задержанного сигнала усилителя.

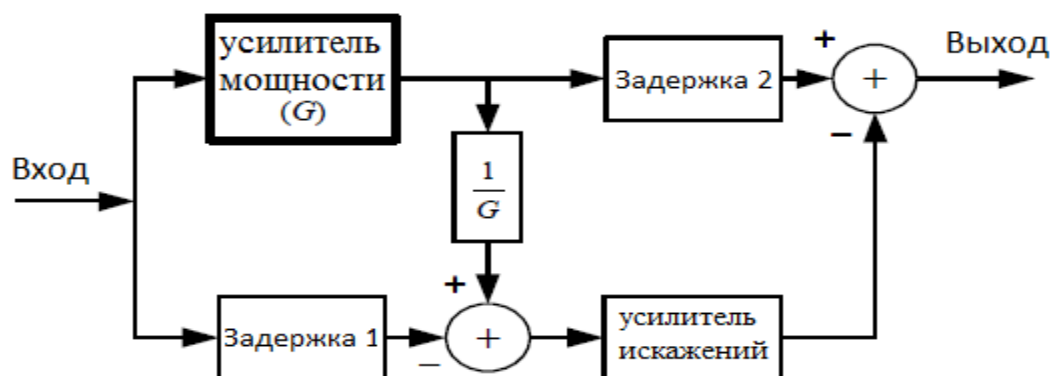


Рис. 2. Система усиления с прямой связью

Таким образом, на выходе системы формируется усиленный сигнал без нелинейных искажений.

Достоинствами данного метода является то, что система усиления без обратной связи всегда устойчива; коэффициент усиления системы не уменьшается, как это происходит в системе с ОС; система усиления является широкополосной; мощность усилителя искажений существенно меньше мощности главного усилителя.

К недостаткам системы относятся: отсутствие влияния многих факторов (изменения температуры, старения усилителя и т. д.) на характеристики усилителя; чувствительность к согласованию схемных элементов; большие аппаратные затраты на синтез системы по сравнению с методами обратной связи [5].

На рис. 3 представлен еще один тип линейризации – система с предискажением. Блоки ЦАП, АЦП – цифроаналоговый и аналого-цифровой преобразователи соответственно; преобразователи, повышающий и снижающий частоту сигнала. При построении предискажителя необходимо найти компромисс между точностью линейризации усилителя, аппаратными затратами на синтез предискажения и быстродействием системы. На точность работы влияют помехи, источниками которых служат неидеальные преобразователи из аналоговой области системы передачи данных.

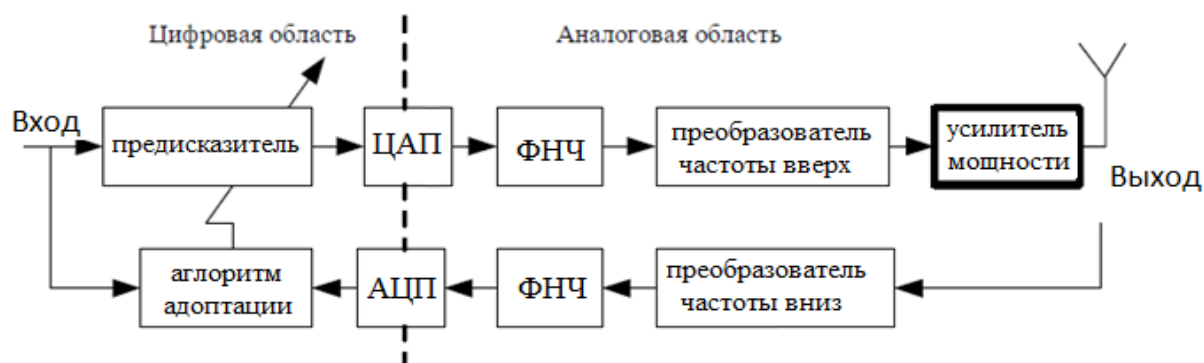


Рис. 3. Система линейризации с предискажением.

Таким образом, для решения вопроса, увеличения времени работы средств радиосвязи, стоящих на вооружении в органах внутренних дел возможно принятие организационных, инженерно-технические и схемотехнических решений.

ЛИТЕРАТУРА

1. Как продлить срок службы аккумулятора у портативной радиостанции? [Электронный ресурс]. – Режим доступа: URL: <http://www.radiosila.ru/lastnews/943-2015-05-28-13-16-59.html> (дата обращения: 04.04.2019)
2. Сравнение систем DMR и TETRA. [Электронный ресурс]. – Режим доступа: URL: <http://www.mptsrv.com/wp-content/uploads/2014/10/> (дата обращения: 05.04.2019)
3. Пол Р. Повышение линейности и эффективности РЧ-усилителей // Время электроники: сайт. – URL: <http://www.russianelectronics.ru/leader-r/review/intergal/doc/50528/> (дата обращения: 05.04.2019)
4. Курушин А., Недера В. Усилители мощности с высокой линейностью для базовых станций беспроводной связи // ChipNews №7, 2002. URL: <http://www.chipinfo.ru/literature/chipnews/200207/2.html> (дата обращения: 05.04.2019)
5. Соловьева Е. Б. Методы линеаризации характеристик усилителей мощности // Санкт-Петербургский государственный электротехнический университет им. В. И. Ульянова (Ленина) – Санкт-Петербург : СПбГЭТУ «ЛЭТИ», 2015. – № 9.

СВЕДЕНИЯ ОБ АВТОРЕ

Печников Сергей Сергеевич. Аспирант кафедры инфоком-муникационных систем и технологий. Воронежский институт МВД России.

E-mail: orl_os@mail.ru

Россия, 394065, г. Воронеж, пр-т Патриотов, 53. Тел. +7(473) 200-52-31.

Pechnikov Sergey Sergeevich. Post-graduate cadet of the chair of communication systems and technologies. Voronezh Institute of the Ministry of the Interior of Russia.

E-mail orl_os@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. +7 (473) 200-52-31.

Ключевые слова: увеличения времени работы средств радиосвязи, аккумуляторная батарея, цифровая радиосвязь, сигналы с высокой спектральной эффективностью, линеаризация усилителей мощности.

Keywords: increasing the working hours of radio communications equipment, storage battery, digital radio communication, signals with high spectral efficiency, linearization of power amplifiers.

УДК 621.396

Рыбак Александр Владимирович,
кандидат технических наук, доцент

ВОПРОСЫ КАДРОВОГО ОБЕСПЕЧЕНИЯ ТЕРРИТОРИАЛЬНЫХ ОРГАНОВ МВД РОССИИ

STAFFING ISSUES OF TERRITORIAL ORGANIZATION OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

В статье на основе анализа нормативных документов и материалов статистики, посвященных кадровой политике и кадровой работе в ОВД, рассматриваются возможности математического моделирования кадрового обеспечения территориальных подразделений МВД России. Автор предлагает применить для решения этой задачи метод системной динамики, позволяющий использовать динамическое равновесие основных элементов оперативной обстановки «преступность - ресурсы - эффективность» для определения кадровой потребности основных территориальных подразделений МВД России. Это позволит решать задачу прогнозирования кадровой потребности подразделений в зависимости от изменения оперативной обстановки.

In the article on the basis of the analysis of normative documents and materials of statistics devoted to personnel policy and personnel work in the police Department, the possibilities of mathematical modeling of personnel support of territorial divisions of the Ministry of internal Affairs of Russia are considered. The author proposes to use the method of system dynamics to solve this problem, allowing using the dynamic balance of the main elements of the operational situation "crime - resources - efficiency" to determine the staffing needs of the main territorial divisions of the Ministry of internal Affairs of Russia. This will allow solving the problem of forecasting the personnel needs of units depending on the changes in the operational environment.

Изучение оперативной обстановки за период, прошедший после начала реформирования ОВД, а также опыт работы со слушателями дополнительного профессионального образования, в первую очередь с руководителями следственных подразделений, а также с сотрудниками, выдвинутыми в резерв руководителей территориальных органов на районном уровне, позволили выявить как позитивные, так и проблемные моменты в управленческой деятельности ОВД.

В качестве позитивных результатов следует отметить – улучшение имиджа органов внутренних дел, очищение его от негатива и тем самым повышение уровня доверия населения к сотрудникам МВД, активизация борьбы с коррупцией среди работников органов внутренних дел; улучшение материального положения сотрудников МВД. Эти положительные сдвиги в работе органов внутренних дел происходят на фоне стабильного уменьшения количества зарегистрированных преступлений в целом по России (за исключением небольшого повышения в 2015 году).

В то же время следует обратить внимание на ряд негативных тенденций, которые проявляются в последнее время в деятельности ОВД и вступают в противоречие с отмеченными позитивными результатами.

Прежде всего, наблюдается достаточно высокий некомплект сотрудников по территориальным подразделениям уголовного розыска, дознания, следствия, участковых пунктов полиции. При этом высокий уровень ротации по этим подразделениям неуклонно ведет к снижению профессионализма.

Это противоречие имеет как объективные, так и субъективные корни и формирует основу для нарастания проблемы снижения эффективности деятельности ОВД в целом.

В качестве объективных причин можно отметить то, что одной из основных задач проводимой реформы системы МВД России являлось снижение «затратности» органов внутренних дел на основе сокращения количества сотрудников. Но количество и качество кадрового состава ОВД в основном определяют интенсивность выявленных, раскрытых и расследованных преступлений. Когда общая интенсивность преступности превышает возможности территориальных подразделений по ее «переработке» наступает состояние коллапса, при котором резко повышается уровень латентности преступлений, а обнаруженные «лишние» преступления различными путями переводятся либо в статус отказных, либо укрываются с нарушением учетно-регистрационной дисциплины.

Таким образом, каждое территориальное подразделение обладает предельным уровнем так называемой «пропускной способности» и предельным уровнем нагрузки на специалистов, превышение которых объективно приводит к невозможности качественного решения поставленных служебных задач и, как следствие, к снижению мотивации к работе.

В качестве субъективной причины можно отметить воинствующий волонтаризм многих руководителей подразделений, когда повышение денежного содержания (при том, что большую его часть за прошедшие восемь лет «съела» инфляция) воспринимается, как право отнимать у подчиненных право на отдых и личную жизнь.

Таким образом, увеличение нагрузки на сотрудников территориальных подразделений, резко авторитарный стиль управления в совокупности с ужесточением требований к физическому и психическому здоровью кандидатов на службу в ОВД привели к ситуации, когда при сравнительно высоком уровне денежного довольствия наблюдается значительный некомплект сотрудников по основным подразделениям ОВД.

В этих условиях ряд проблемных вопросов относятся к сфере кадровой политики и кадровой работы в органах внутренних дел и требуют своего решения.

Кадровая политика в системе МВД России осуществляется в целях формирования профессионального состава кадров, сохранения, воспроизводства, укрепления, развития, рационального и эффективного использования кадрового потенциала органов внутренних дел в интересах оперативно-служебной деятельности. Поставленные цели определяют кадровую работу как многоаспектную управленческую деятельность по решению целого комплекса экономических, социальных, нравственных, правовых, психологических и иных задач. Одним из главных показателей организации кадровой работы является уровень соответствия кадровой обеспеченности подразделений ОВД требованиям реальной криминологической обстановки на обслуживаемой ими территории. При этом кадровая работа должна строиться с учетом необходимости поддержания баланса интересов сотрудников, с одной стороны, и органов внутренних дел, в целом, с другой. Без создания гибкого мотивационного механизма решение этой задачи невозможно. Все это должно обеспечивать эффективную реализацию конституционных прав и свобод сотрудника как профессионала, гражданина и личности в единстве с целями и задачами, поставленными перед органами внутренних дел.

В настоящее время деятельность системы кадрового обеспечения регламентирована набором приказов МВД России инструкциями, нормативами, и т.п. Так для определения кадровой потребности подразделений дознания, участковых уполномоченных полиции, уголовного розыска и ряда других служит примерный норматив численности подразделений, изложенный в приказе МВД России от 6 октября 2014 г. № 859 «Об утверждении примерных нормативов численности подразделений органов внутренних дел Российской Федерации».

Основными критериями, определяющими в нем норму численности подразделений в зависимости от направления деятельности, являются:

а) привязка к количеству сельского или городского населения, проживающего на обслуживаемой территории (подразделения, участковых уполномоченных полиции, патрульно-постовой службы);

б) привязка к количеству уголовных или административных дел в производстве

(подразделения дознания, уголовного розыска, исполнения административного законодательства).

Здесь просматривается ряд требующих решения задач.

Во-первых, привязка штатной численности территориальных подразделений к количеству населения, проживающего на обслуживаемой ОВД территории, даже дифференцированная по городу и сельской местности, не является достаточно объективной. Криминальная активность населения зависит от множества факторов, таких как средний образовательный уровень, менталитет населения, уровень его занятости, уровень развития промышленного потенциала территории и пр. В целом эти факторы определяют уровень преступности, доминирующие виды преступлений, трудоемкость их раскрытия и расследования, а значит – кадровую потребность ОВД.

Во-вторых, количество уголовных дел в производстве не в полной мере определяет кадровую потребность в силу того, что трудоемкость раскрытия и расследования даже одинаковых по квалификации преступлений часто бывает различна.

В-третьих, расчет кадровой потребности осуществляется в лучшем случае на основе изучения криминологической обстановки за прошедший период и не предусматривает количественных и тем более структурных ее изменений в будущем.

В этом направлении особый интерес представляют собой методы, которые позволяют количественно оценить изменение уровня преступности в зависимости от результативности деятельности ОВД и эффективности использования своих ресурсов.

В основе таких методик лежит динамическое равновесие элементов системы «преступность–ресурсы» – весьма важное понятие с точки зрения разработки математических моделей кадрового обеспечения органов внутренних дел, представленное В.А. Минаевым в работе «Кадровые ресурсы органов внутренних дел: современные подходы к управлению» [4].

В преобразованном виде эту зависимость можно записать, как:

$$\alpha = \frac{\gamma \cdot R}{V} \cdot \left(1 - e^{-\frac{V}{\gamma \cdot R}}\right) \quad (1)$$

где α – рассматривается, как показатель эффективности использования подразделением своих ресурсов, в том числе и кадровых;

γ – показатель оптимальной или предельной (в зависимости от поставленной задачи) «пропускной способности» одного сотрудника подразделения;

R – реальная численность сотрудников подразделения;

V – реальная нагрузка на подразделение в виде количества уголовных дел в производстве у следственного подразделения или подразделения дознания, либо количество поручений у сотрудников подразделения уголовного розыска и пр. за определенный период.

Определяющим элементом этой математической модели является γ – показатель «пропускной способности», который рассчитывается на основе экспертной процедуры. В процессе проведения экспертизы решаются следующие задачи:

а) все уголовные дела U , зарегистрированные на территории подразделения за прошедший период, классифицируются на категории по степени трудоемкости их обработки различными подразделениями, допустим, на k категорий;

б) определяется доля каждой категории в общем количестве преступлений за прошедший период, например, $d_1, d_2, \dots, d_k$;

в) по каждой категории определяется норма ее обработки: количество соответствующих этой категории уголовных дел, которое должен обработать один сотрудник подразделения в течение, допустим, одного года, например, $n_1, n_2, \dots, n_k$.

г) определяется γ , как средневзвешенная величина: сумма произведений доли каждой категории на норму ее обработки.

$$\gamma = d_1 * n_1 + d_2 * n_2 + d_3 * n_3 + \dots + d_k * n_k \quad (2)$$

Таким образом, определив γ , мы получаем возможность применить выражение (1) для определения кадровой потребности территориального подразделения **R**. Для этого необходимо решить две задачи:

1. Задать уровень эффективности α . Для следственного подразделения им является желательный коэффициент расследованных преступлений, для уголовного розыска - коэффициент раскрытых преступлений и т.п.

2. Рассчитать прогноз количества преступлений на период определения кадровой потребности.

В итоге, используя динамическое равновесие компонентов оперативной обстановки, представленное в выражении (1), находим **R** – кадровую потребность подразделения на заданный период с учетом динамики оперативной обстановки и нагрузки на подразделение.

Подобная технология может быть применена для территориальных подразделений любого профиля. Различие заключается лишь в объектах обработки, которые могут быть представлены в виде расследованных уголовных дел, раскрытых уголовных дел, административных протоколов, заявлений и обращений граждан и т.п.

Таким образом, возможность прогнозирования кадровой потребности территориальных подразделений в зависимости от изменения оперативной обстановки позволит более эффективно использовать кадровые ресурсы в борьбе с преступностью.

ЛИТЕРАТУРА

1. Об утверждении примерных нормативов численности подразделений органов внутренних дел Российской Федерации: Приказ МВД России от 06. 10.2014. № 859. Доступ из справ.-правовой системы «Консультант Плюс».

2. Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации: Приказ МВД России от 31.12.2013 № 1040. Доступ из справ.-правовой системы «Консультант Плюс».

3. Об утверждении Типового положения о штате территориального органа Министерства внутренних дел Российской Федерации: приказ МВД России от 26.10.2017 №808. Доступ из справ.-правовой системы «Консультант Плюс».

4. Минаев В.А. Кадровые ресурсы органов внутренних дел: современные подходы к управлению. Монография. – М.: Академия МВД СССР, 1991.С. 47-57.

5. Рыбак, А.В. Оценка эффективности деятельности следственных подразделений на основе применения методов системной динамики: метод. реком. – Хабаровск: ДВЮИ МВД России, 2016.

6. Москалев М.А. Аналитическая деятельность штабных подразделений территориальных органов МВД России на региональном уровне: – М.: Спутник, 2012.

7. Рыбак А.В., Бондарь К. М., Скрипко П. Б., Дунин В.С., Рыбак А.А. Применение модели системной динамики для оценки эффективности деятельности следственных подразделений // Власть и управление на Востоке России. 2017. № 4 (81). С. 151–156.

8. Рыбак А.В. Применение методов системной динамики при формировании государственного заказа на подготовку кадров в образовательных учреждениях МВД России // Вестник ДВЮИ МВД России. 2014. № 1 (5/7).

9. Рыбак А.В. Оценка эффективности деятельности следственных подразделений на основе применения методов системной динамики // Научный портал МВД России. 2016. № 3 (35). С. 99-103.

СВЕДЕНИЯ ОБ АВТОРЕ

Рыбак Александр Владимирович. Профессор кафедры информационного и технического обеспечения органов внутренних дел.

Дальневосточный юридический институт МВД России.

Кандидат технических наук, доцент.

E-mail: rybak_2908@mail.ru

Россия, 680020, Хабаровск, ул. Дикопольцева, д.11, кв.3.

Тел. 89625036205.

Rybak Alexander Vladimirovich. Professor of the Department of information and technical support of internal Affairs.

Far Eastern law Institute of the Russian interior Ministry.

Candidate of technical Sciences, associate Professor.

E-mail: rybak_2908@mail.ru

Russia, 680020, Khabarovsk, St. Dikopoltseva, d. 11, sq. 3.

Phone 89625036205.

Ключевые слова: кадровая политика и кадровая работа; система кадрового обеспечения, оперативная обстановка; метод системной динамики; динамическое равновесие элементов системы «преступность-ресурсы-эффективность»; «пропускная способность»; статистический показатель.

Keywords: Personnel policy and HR management; the system of staffing, and the operational environment; the method of system dynamics; dynamic equilibrium of the elements of the system "crime resource efficiency"; "capacity"; statistic.

УДК 332.1:352

Рыбокитов Андрей Евгеньевич

РИСК-МОДЕЛИ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ САМООРГАНИЗУЮЩИХСЯ СЕТЯХ СВЯЗИ

RISK MODELS OF INFORMATION SECURITY VIOLATION IN MOBILE SELF-ORGANIZING COMMUNICATION NETWORKS

В статье рассмотрены риск-модели нарушения информационной безопасности в самоорганизующихся сетях связи. Построение данных моделей и действия после введения в эксплуатацию систем противодействия угрозам нарушения информационной безопасности.

The article discusses the risk model of information security breaches in self-organizing communication networks. The construction of these models and actions after the commissioning of systems to counter threats to information security breaches.

Для безопасного функционирования каждой системы необходимо спланировать и построить систему противодействия угрозам и рискам, которые могут возникнуть при эксплуатации системы. Необходимость знания всех используемых ресурсов, сроков их эксплуатации и то, против каких именно угроз они используются, очень важный фактор. Так для противодействия рискам нарушения информационной безопасности в самоорганизующихся системах будут построены риск-модели [1].

Угрозы можно разделить на несколько подгрупп:

- 1) угрозы физического воздействия;
- 2) угрозы информационного воздействия.

После разделения моделей на подгруппы, необходимо работать с каждой подгруппой в отдельности и с использованием особенностей каждой. Для противодействия угрозам физического воздействия необходимо определить, какие элементы системы могут физически уничтожены, повреждены или выведены из строя другим путём. Необходимо определить, какие из выбранных элементов имеют большую значимость для функционирования системы в нормальном режиме и наибольшую стоимость. После чего разработать систему мер противодействия угрозам физического воздействия на элементы системы. Произвести оценку остаточных рисков [2] и принять решение, что необходимо делать с ними, ввести дополнительные элементы в систему безопасности, для их уничтожения, принять или передать ответственность за них. При введении системы в действие, необходимо следить за её работоспособностью и постоянно оптимизировать.

Для противодействие угрозам информационного воздействия на начальном этапе также необходимо определить, какие элементы системы могут быть подвержены угрозам данного типа. После чего, определяем какие угрозы нарушения информационной безопасности могут возникнуть в системе. На несколько элементов системы может воздействовать одна угроза. Определив все угрозы в системе необходимо принять решение, что с ними требуется сделать [3]: уничтожить, используя доступные ресурсы и вводя в систему новые, уменьшить вероятность их реализации до требуемого уровня или разработать план по противодействию им. После чего произвести оценку системы безопасности и оценить остаточные риски и выбрать, что необходимо сделать с ними. При эксплуатации системы требуется постоянно проводить её анализ, на сколько она актуальна и в случае необходимости производить её модернизацию [4].

Для построения модели нарушения информационной безопасности введём переменные: $D = \{d_1, \dots, d_n\}$ – возможные угрозы нарушения информационной безопасности, $T = \{t_1, \dots, t_n\}$ – события происходящие с сети связи, $I = \{i_1, \dots, i_n\}$ – сценарии нарушения информационной безопасности в самоорганизующейся сети связи [5]. Используя переменные можно построить модель нарушения информационной безопасности, так при событии t_n в сети связи, используя угрозы нарушения информационной безопасности d_1 и d_n , злоумышленники реализуют сценарий нарушения i_n (рис. 1).



Рис. 1. Нарушение информационной безопасности

При использовании системы контрмер, вероятность реализации угрозы нарушения информационной безопасности уменьшается, в следствии чего, сложнее реализовать сценарий нарушения информационной безопасности.

Так, используя теорию графов, построим граф [6], вершиной которого будет успешная реализация сценария нарушения информационной безопасности (рис. 2).

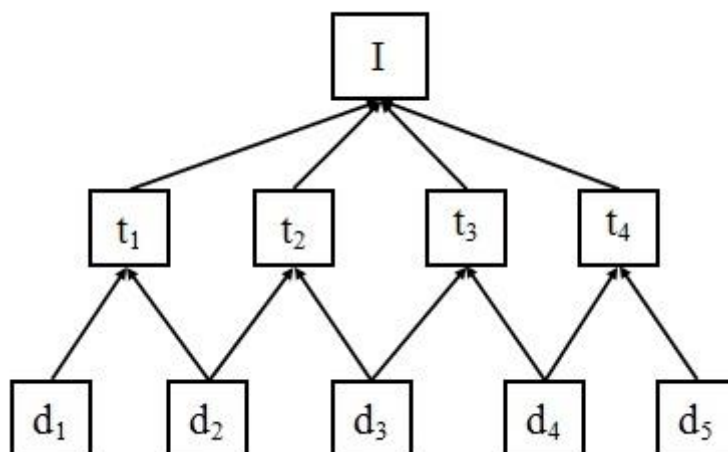


Рис. 1. Реализация нарушения информационной безопасности

При этом видно, что если при анализе сети связи и выявлении угроз безопасности ввести систему контрмер, шансы на успешную реализацию сценария нарушения информационной безопасности значительно уменьшаются, из-за того, что нет возможности начала для атаки.

При построении мобильной самоорганизующейся сети связи необходимо учитывать все угрозы нарушения информационной безопасности, разделять их на классы по определённым признакам и выстраивать систему безопасности учитывая имеющиеся ресурсы и особенности сети связи.

ЛИТЕРАТУРА

1. ГОСТ Р 61508-2-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. – Введ. 2012-29-10. – Москва : Стандартинформ, 2012. – 86 с.
2. ГОСТ Р ИСО/МЭК 27001–2012. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Введ. 2012-24-09. – Москва : Стандартинформ, 2014. – 104 с.
3. Рыбокитов А.Е. Анализ угроз нарушения информационной безопасности для предупреждения преступлений в мобильных системах специального назначения // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: материалы всероссийской научно-практической конференции. – Воронеж : Воронежский институт МВД России, 2018. – С. 107–111
4. Хохлов Н.С., Канавин С.В., Рыбокитов А.Е. Анализ рисков в управлении информационной безопасностью самоорганизующихся мобильных беспроводных сетей специального назначения // Охрана, безопасность, связь – 2018 : материалы международной научно-практической конференции. – Воронеж : Воронежский институт МВД России, 2018. – С. 109–113.
5. Репин М.М. Модели риска возникновения нарушений информационной безопасности в платежной системе // История и архивы. 2016. №3 (5) [электронный ресурс]. – URL: <https://cyberleninka.ru/> (дата обращения: 24.06.2019).
6. Теория графов. Основные понятия и виды графов / [электронный ресурс]. URL: <http://kvodo.ru> (дата обращения: 24.06.2019).

СВЕДЕНИЯ ОБ АВТОРЕ

Рыбокитов Андрей Евгеньевич. Научный сотрудник научно-исследовательского отдела.

Воронежский институт МВД России.

E-mail: AERybokitov@yandex.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-51-28.

Rybokitov Andrey Evgenievich. Researcher of the research Departmen.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: AERybokitov@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-51-28.

Ключевые слова: самоорганизующиеся сети, риски нарушения информационной безопасности.

Key words: self-organizing networks, information security risks.

УДК. 519.17

Спешилов Эдуард Вадимович

К ВОПРОСУ О ЦИФРОВЫХ СИСТЕМАХ ФАЗОВОЙ АВТОПОДСТРОЙКИ (PLL)

TO THE QUESTION ABOUT DIGITAL SYSTEMS OF PHASE LOCKED LOOP (PLL)

В статье рассмотрен принцип работы простейшей схемы цифровой фазовой автоподстройки и ее модификации.

In article deals with the principle of operation of the simplest digital phase-locked loop and its modifications.

В свете современного развития цифровой техники широкое применение получили цифровые системы фазовой автоподстройки (ФАП). ФАП это система управления, которая генерирует выходной сигнал, фаза которого связана с фазой входного сигнала. Петли фазовой синхронизации широко используются в радиосвязи, телекоммуникациях и других электронных приложениях. Они могут использоваться для демодуляции сигнала, восстановления сигнала из зашумленного канала связи, генерации стабильной частоты при кратных значениях входной частоты (синтез частоты) или распределения точно синхронизированных тактовых импульсов в цифровых логических схемах (ПЛИС), таких как микропроцессоры. В частности, они используются для выделения гармонического сигнала из шума, в демодуляторах ФМ и ЧМ сигналов, в устройствах тактовой синхронизации [1, 2].

Первые петли фазовой синхронизации были реализованы в начале 1930-х годов французским инженером де Беллескизом. Однако, они стали широко применяться тогда, когда интегрированные ФАП стали доступны в качестве относительно недорогих компонентов в середине 1960-х годов [5].

Цифровые системы ФАП имеют хорошие технологические показатели, высокую надежность. Под цифровыми системами ФАП будем понимать такие системы, в которых все координаты дискретизируются по времени и по уровню, а информация в цепях управления и обратной связи передается или обрабатывается в цифровой форме. Системы, в которых дискретизация осуществляется только по времени, называются дискретными.

На рис. 1 представлена блок-схема цифровой ФАП. Допустим, что на вход такой системы поступает периодический сигнал той или иной формы. Фазы сигналов с эталонного и цифрового генераторов сравниваются в фазовом детекторе и вырабатывается комбинация из кодов, которая соответствует разности фаз в момент сравнения (дискретизация по времени). Этот момент можно определить либо эталонным сигналом, либо сигналом ПГ.

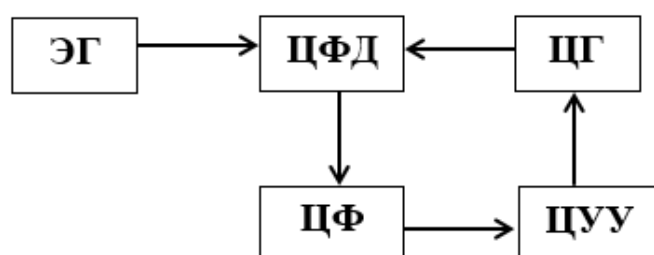


Рис. 1. Схема цифровой ФАП

Дискретизация по уровню достигается в ЦФД, который является основным звеном любых цифровых систем ФАП. Цифровой фильтр (ЦФ) фильтрует выходной сигнал ЦФД.

Устройство, на выходе которого мгновенная или средняя частота сигнала принимает одно из возможных дискретных значений называется цифровым генератором. Выходной сигнал ЦГ это, как правило, последовательность импульсов с постоянной амплитудой. Цифровые системы ФАП являются разновидностью систем синхронизации, построенных на основе принципа дискретной коррекции фазы (частоты) цифрового генератора.

Известны [1] разновидности цифровых систем ФАП, среди которых выделяются две основные: с управляемым кодом синтезатором частот и с устройством добавления-вычитания (УДВ). Первая работает по принципу дискретного регулирования частоты ЦГ, а вторая корректирует фазу этого генератора. На рис. 2 показана цифровая система ФАП с УДВ.

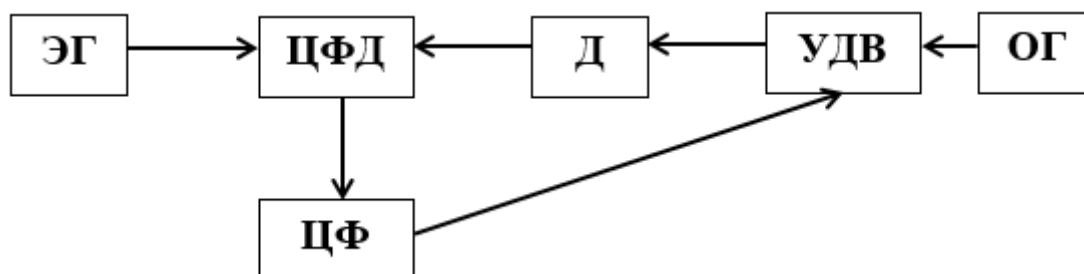


Рис. 2. Цифровая система ФАП с УДВ

Отличие второго вида ЦФАП заключается в наличие УДВ, которое вычитает и/или добавляет к опорной импульсной последовательности с частотой $\omega_{ог}$ опорного генератора (ОГ) то или иное число импульсов за период коррекции. Добавление одного импульса равносильно увеличению, а вычитание – уменьшению фазы на 2π . Делитель частоты Д уменьшает скачки фазы на выходе пропорционально уменьшению частоты. Совокупность УДВ и делителя частоты можно рассматривать как некоторый дискретный фазовращатель.

ЛИТЕРАТУРА

1. Шахгильдян В.В. Системы фазовой автоподстройки частоты с элементами дискретизации / В.В. Шахгильдян [и др.] М.: Связь, 1979. – 224 с.
2. Цифровые системы фазовой синхронизации / В. А. Прасолов [и др.]; под ред. М. И. Жодзишского. — М. : Сов. Радио, 1980. — 208 с.
3. Шахгильдян В.В., Ляховкин А.А. Системы фазовой автоподстройки частоты. М.: Связь, 1972.
4. Шахгильдян В.В. Системы фазовой синхронизации с элементами дискретизации. – 2-е изд., доп. и перераб. / В.В. Шахгильдян [и др.]; под ред. В.В. Шахгильдяна. – М.: Радио и связь, 1989. – 320 с.
5. Collins, Ian. Integrated PLLs and VCOs for Wireless Applications. Radio Electronics, 2010.

СВЕДЕНИЯ ОБ АВТОРЕ

Спешилов Эдуард Вадимович. Адъюнкт.
Воронежский институт МВД России.
E-mail: eduard.speshilov@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.
Тел. (473) 2005227.

Speshilov Eduard Vadimovich. Post-graduate cadet.
E-mail: eduard.speshilov@yandex.ru
Voronezh Institute of the Ministry of Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 2005227.

Ключевые слова: обработка сигналов, цифровые устройства приема и обработки информации, помехоустойчивость, фазовая автоподстройка.

Key words: signals processing, digital devices for receiving and processing information, noise immunity, phase-locked looped.

УДК: 621.396.962.21

Терентьев Александр Андреевич;
Пьянков Олег Викторович,
доктор технических наук, доцент

ВИЗУАЛИЗАЦИЯ РЕЗУЛЬТАТОВ ОБРАБОТКИ ЭКСПЕРТНЫХ ОЦЕНОК ПО СТЕПЕНИ ПРЕДПОЧТЕНИЯ ОБЪЕКТОВ

VISUALIZATION OF THE TREATMENT RESULTS OF EXPERT ASSESSMENTS BY THE DEGREE OF OBJECT PREFERENCE

Рассматриваются вопросы применения графических способов представления результатов обработки экспертных оценок в ситуационных центрах органов внутренних дел при подготовке управленческих решений.

The article discusses the use of graphical ways of presenting the results of processing expert assessments in the situational centers of the internal affairs bodies when preparing an effective management decision.

В связи с реализацией Указа Президента Российской Федерации от 25 июля 2013 г. № 648 «О формировании системы распределённых ситуационных центров работающих по единому регламенту взаимодействия», Приказа МВД России от 16.11.2018 г. № 775 «Об утверждении Положения о Ситуационном центре Министерства внутренних дел Российской Федерации и Регламента работы Ситуационного центра Министерства внутренних дел Российской Федерации», а также со служебной необходимостью в органах внутренних дел активно развиваются, создаются специализированные внештатные подразделения – ситуационные центры.

Ситуационный центр – это наукоемкий комплекс программно-технических средств обработки и отображения информации, информационно-аналитических систем и информационных ресурсов, информационно-телекоммуникационных сетей, технических и программных средств обеспечения необходимого уровня информационной безопасности, а также специально подготовленный персонал [1].

Такие центры используются во всех органах исполнительной власти. Особое значение СЦ имеют для силовых структур, для таких как МВД, МЧС, ФСБ, ФСО, потому что применение таких центров позволяет немедленно принимать эффективное управленческое решение, направленное на защиту общества и государства от противоправных посягательств.

Ситуационный центр Министерства внутренних дел Российской Федерации является постоянно действующим внештатным подразделением, предназначенным для информационно-аналитического и телекоммуникационного обеспечения решения задач управления силами и средствами подразделений центрального аппарата Министерства внутренних дел Российской Федерации, территориальных органов МВД России, образовательных, научных, медицинских (в том числе санаторно-курортных) организаций системы МВД России, окружных управлений материально-технического снабжения системы МВД России, заграничного аппарата МВД России, организаций культуры, физкультурно-спортивных организаций, редакций печатных и электронных средств массовой информации, а также иных организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел, осуществляющим информационно-аналитическую поддержку реализации государственной политики в сфере внутренних дел, оперативное взаимодействие с федеральными органами исполнительной власти, иными государственными органами и организациями, в

том числе в составе системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия, как в повседневном режиме, так и в режиме повышенной готовности или кризисной ситуации, в том числе при непосредственной подготовке к переводу и переводу на работу в условиях военного времени [2].

Для выполнения всех поставленных целей, каждый ситуационный центр обязан быть оборудован современной многофункциональной техникой, но СЦ при помощи одной только техники не смогут решать поставленные перед ними задачи, поэтому важным связующим звеном является персонал. Состав персонала состоит не только из компетентных сотрудников органов внутренних дел, а также экспертов различных предметных областей. Привлечение экспертов к решению задач органов внутренних дел является важным условием повышения эффективности принимаемых решений и всей деятельности ситуационного центра органов внутренних дел.

В связи с этим функционирование ситуационного центра, основывается на слиянии технологий передачи информации и представлении ее в реальном времени, методов анализа и оценки ситуаций, а также организации коллективной работы экспертов непосредственно в процессе решения задач.

Эксперт вынужден работать с большим объемом данных, что значительно замедляет его работу, вследствие чего могут возникать различные неблагоприятные последствия, в связи с этим несомненным плюсом является возможность представлять данные в графическом виде путем их визуализации с помощью средств и методов, реализуемых аппаратом Exploratory Data Analysis (EDA) [3].

Exploratory Data Analysis (исследовательский анализ данных) — это подход для анализа данных, который использует различные более 100 графических методов для:

1. Максимизирования понимания набора данных.
2. Раскрытия основной структуры данных.
3. Извлечения главных переменных.
4. Обнаружения выбросов и аномалий.
5. Проверки основных гипотез.
6. Разработки упрощенных моделей.

Среди графических методов EDA имеются:

1. Star Plot;
2. Spectrum;
3. Linear Slope Plot;
4. Histogram;
5. Box Plot и др.

В процессе деятельности ситуационного центра органов внутренних дел, у эксперта могут появляться задачи, когда необходимо сравнивать объекты между собой, и выдавать результат о степени предпочтения этих объектов. Для облегчения анализа полученных результатов, а также для наилучшей наглядности предлагается использовать визуализацию данных. Визуальное исследование позволяет эксперту представить отчет в виде таблиц, диаграмм, графиков, карт, гистограмм, статистик и т.п., что способствует выбору оптимального решения поставленных задач органов внутренних дел.

В качестве примера представим работу компьютерной программы «Расчет вектора приоритетов с использованием slice-матриц» [4]. Данная программа создана для обработки экспертных оценок с большим количеством сравниваемых объектов [5].

Расчет вектора приоритетов с использованием slice-матриц

Количество slice-матриц: Размерность slice-матрицы:

Сlice-матрица № 1 Slice-матрица № 2

	1	2	3	4	5	6
1	1	3	4	5	6	7
2	0,333	1	3	4	5	6
3	0,25	0,333	1	3	4	5
4	0,2	0,25	0,333	1	3	4
5	0,167	0,2	0,25	0,333	1	3
6	0,143	0,167	0,2	0,25	0,333	1

Необходимо вводить:
 $1/2 = 0,5$
 $1/3 = 0,333$
 $1/4 = 0,25$
 $1/5 = 0,2$
 $1/6 = 0,167$
 $1/7 = 0,143$
 $1/8 = 0,125$
 $1/9 = 0,111$
Ввод дробных чисел осуществлять через запятую!

Результаты расчета вектора приоритетов:

	Вектор приоритетов
1	0,432472364009
2	0,202
3	0,091
4	0,041
5	0,018
6	0,009
7	0,114
8	0,053
9	0,024
10	0,011
11	0,005
12	0,000

Общая сумма (Σ):

Рис. 1. Интерфейс программы «Расчет вектора приоритетов с использованием slice-матриц»

Результаты расчета вектора приоритетов приведен в таблице 1.

Таблица 1

Результаты расчета вектора приоритетов	
№ объекта	Значения элементов вектора приоритетов
Объект № 1	0,43
Объект № 2	0,20
Объект № 3	0,09
Объект № 4	0,04
Объект № 5	0,018
Объект № 6	0,008
Объект № 7	0,114
Объект № 8	0,053
Объект № 9	0,024
Объект № 10	0,011
Объект № 11	0,005

Количество сравниваемых объектов может быть достаточно велико, а значения вектора приоритетов малы, поэтому табличное представление результатов будет нецелесообразно использовать. В связи с этим будем использовать графический метод представления данных (рис. 2).



Рис. 2. Графическое представление вектора приоритетов

Представленный графический способ (рис. 2) представления экспертных оценок наглядно показывает все значения вектора приоритетов по степени приоритетности сравниваемых объектов.

Стоит отметить, что в настоящее время разрабатывается новая программа для расчета вектора приоритетов с использованием slice-матриц для группы экспертов, где комплекс визуализации данных будет внедрен. Структура данной программы приведена на рис. 3.

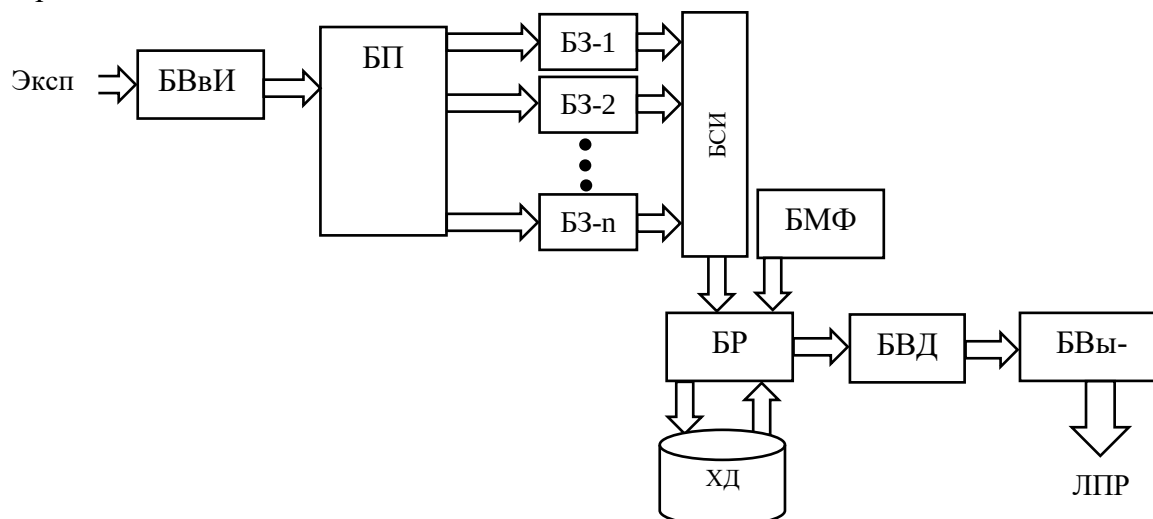


Рис. 3. Структура предлагаемой проблемно-ориентированной программы для группы экспертов: Эксп. – эксперт; БВВИ – блок ввода информации; БП – блок построение Slice-матриц; БЗ – блок заполнение Slice-матриц; БМФ – блок математических функций; БР – блок расчета; БВД – блок визуализации данных; БВЫИ – блок вывода информации; ЛПР – лицо, принимающее решение; ХД – хранилище данных; БСИ – блок сбора информации

В заключении следует отметить, что кроме рассмотренного графического способа в виде диаграммы, выше представленные методы EDA также можно использовать для визуализации данных при решении задач, возникающих в процессе функционирования ситуационных центров органов внутренних дел.

ЛИТЕРАТУРА

1. Ильин Н. И., Демидов Н. Н., Новикова Е. В. Ситуационные центры. Опыт, состояние, тенденции развития / Н. И. Ильин, Н. Н. Демидов, Е. В. Новикова – Москва : МедиаПресс, 2011. – 336 с.
2. Об утверждении Положения о Ситуационном центре Министерства внутренних дел Российской Федерации и Регламента работы Ситуационного центра Министерства внутренних дел: приказ МВД России № 775 от 16.11.2018 г.
3. Exploratory Data Analysis. Engineering Statistics Handbook, 2006. – 3118 с.
4. Терентьев А. А. Разработка информационной технологии обработки экспертных оценок / А. А. Терентьев // Информационные технологии в моделировании и управлении: Подходы, методы, решения. – 2019. – Ч.2. – С. 289-295.
5. Пьянков О. В. Разработка численного метода определения весов конфликтных взаимодействий / О.В. Пьянков, А. А. Терентьев // Вестник Воронежского института МВД России. – 2019. – № 1. – С. 69-74.

СВЕДЕНИЯ ОБ АВТОРАХ

Терентьев Александр Андреевич. Адъюнкт.
Воронежский институт МВД России.
E-mail: Alextt02021993@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473)200-52-24.

Пьянков Олег Викторович. Заместитель начальника кафедры инфокоммуникационных систем и технологий. Доктор технических наук, доцент.
Воронежский институт МВД России.
E-mail: Olegic79@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473)200-52-33.

Pyankov Oleg Viktorovich. Deputy Head of the Department of Infocommunication Systems and Technologies. Doctor of Technical Sciences, Associate Professor.
Voronezh Institute of the Ministry of the Interior of Russia
E-mail: Olegic79@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-52-33.

Terentyev Alexandr Andreevich. Adjunct.
Voronezh Institute of the Ministry of the Interior of Russia
E-mail: Alextt02021993@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-52-24.

Ключевые слова: Ситуационный центр, расчет вектора приоритетов с использованием slice-матриц, визуальное представление данных

Key words: Situation center, calculation of vector of priorities using slice-matrices, visual presentation of data

УДК 519.67

Удалов Валерий Петрович,
кандидат физико-математических наук, доцент;
Жуков Михаил Михайлович,
кандидат технических наук

ОСОБЕННОСТИ ЭКСПЕРТНОГО ОЦЕНИВАНИЯ ПАРАМЕТРОВ НАДЕЖНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

FEATURES OF EXPERT ESTIMATION OF RELIABILITY PARAMETERS OF THE SECURITY SYSTEM OF THE OBJECT OF INFORMATIZATION

Предложен алгоритм применения метода экспертных оценок при расчете параметров модели надежности системы безопасности объекта информатизации. Для полученной модели надежности показаны особенности экспертной оценки параметров предложенной модели.

The algorithm of application of method of expert evaluations when calculating parameters of model of reliability of a security system of an object of informatization is offered. For the received model of reliability, features of expert assessment of parameters of the offered model are shown.

На этапе моделирования будущей технической системы обеспечения безопасности и на протяжении всего периода ее эксплуатации возникает вопрос повышения ее надежности. Этот вопрос требует пристального внимания и является актуальным, так как необходимо исключить возможные ошибки в работе многокомпонентных систем безопасности, вызванные отказами отдельных подсистем (компонентов).

Наиболее востребованными, с точки зрения полноты реализуемых охранных функций, в настоящее время являются интегрированные системы безопасности (ИСБ), объединяющие различные подсистемы. С целью обеспечения защиты объекта охраны необходимо создание математической модели надежности ИСБ.

В качестве примера возьмем охраняемый объект, на котором установлено N различных подсистем из схемы надежности [1]. Каждая подсистема в отдельности определяет групповые параметры надежности (ГПН) ИСБ.

Рассмотрим экспертную оценку надежности ИСБ, состоящего из 17 подсистем, комиссией из 5 экспертов. В результате работы комиссии проставлены баллы каждому из ГПН системы в соответствии с уровнем значимости соответствующего компонента в обеспечении надежности охраны объекта (табл. 1) [2].

Как правило, обработка результатов деятельности экспертной комиссии производится путем вычисления средних величин с помощью среднего арифметического значения. В то же время такой способ будет не вполне математически корректным, поскольку выставленные баллы, являющиеся исходными данными, по факту являются последовательностью порядковой шкалы. Представляется более корректным осуществлять расчет медиан вместо среднего арифметического значения [3].

Проведем сравнение указанных методов расчета итоговых экспертных оценок применительно к модели надежности ИСБ охраняемого объекта.

Таблица 1

Результаты экспертного оценивания

№ группового параметра надежности	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Эксперт 5
1	2	1	3	4	2
2	1	3	4	2	3
3	4	2	2	1	1
4	3	4	1	5	5
5	6	7	5	3	4
6	8	6	8	6	9
7	9	10	11	12	10
8	15	12	13	11	13
9	12	13	12	10	11
10	14	17	15	16	17
11	10	11	9	8	7
12	7	5	6	7	8
13	13	12	11	14	12
14	5	8	7	9	6
15	13	14	16	14	15
16	17	16	17	15	14
17	11	9	10	13	12

При применении метода средних арифметических рангов происходит подсчет суммы рангов, присвоенных ГПН. Рангом называют номер объекта экспертизы в упорядоченном ряду. По рангам строится итоговая ранжировка ГПН. В ранжировке используется следующий принцип: чем меньше средний ранг, тем выше значимость ГПН для ИСБ (табл. 2, столбцы 3 и 4).

В методе медиан выставленные экспертами баллы (ранги) располагают в порядке возрастания. Далее медианы вычисляются как среднее арифметическое центральных баллов в ряду. В случае нечетного числа экспертов (и, соответственно, количества выставленных баллов) медианой является балл, расположенный в центре полученного ряда. Полученные результаты представлены в виде таблицы (табл. 2, столбцы 5 и 6).

Сравнение методов среднего арифметического рангов и медиан рангов показывает их схожесть в целом, но в то же время наблюдаются отличия в присвоенных рангах (табл. 2) у отдельных подсистем ИСБ.

Из анализа данных таблицы 2 следует, что особенно существенным является различие оценок 1 и 2 мест для ГПН 1 и ГПН 3. Их ранги позволяют сделать выводы о существенной значимости обоих ГПН для надежности ИСБ и только сравнение двух методов ранжировок дает возможность сказать о превосходстве ГПН 3 над ГПН 1. Что касается различий в выставленных рангах для ГПН 8 (13 и 14 места по разным методам), ГПН 13 (13 и 15 места) и ГПН 15 (15 и 14 места), то нам следует сделать вывод, что указанные ГПН находятся почти в конце ранжировочного списка и превосходство того или другого элемента ИСБ при разработке системы в целом не является существенным и может не приниматься во внимание.

Таблица 2

Ранжированные данные по методам средних рангов и медиан рангов

	Среднее арифметическое рангов	Итоговый ранг по среднему арифметическому	Медианы рангов	Итоговый ранг по медианам
(ГПН 3)	2	1	2	1,5
(ГПН 1)	2,4	2	2	1,5
(ГПН 2)	2,6	3	3	3
(ГПН 4)	3,6	4	4	4
(ГПН 5)	5	5	5	5
(ГПН 12)	6,6	6	7	6
(ГПН 14)	7	7	7	7
(ГПН 6)	7,4	8	8	8
(ГПН 11)	9	9	9	9
(ГПН 7)	10,4	10	10	10
(ГПН 17)	11	11	11	11
(ГПН 9)	11,6	12	12	12
(ГПН 13)	12,4	13	16	15
(ГПН 8)	12,8	14	13	13
(ГПН 15)	14,4	15	14	14
(ГПН 10)	15,8	16,5	16	16,5
(ГПН 16)	15,8	16,5	16	16,5

Таким образом, существуют особенности в обработке данных экспертизы, позволяющие выявить наиболее существенные групповые параметры надежности интегрированной системы безопасности. Рассмотренный пример позволяет сделать вывод о необходимости рассмотрения одновременно нескольких методов обработки данных для получения более объективных выводов по работе экспертной комиссии.

ЛИТЕРАТУРА

1. ГОСТ Р 53704–2009. Системы безопасности комплексные и интегрированные. Общие технические требования. – М. : «Стандартинформ», 2010. – 72 с.
2. Булгаков О.М., Удалов В. П. Применение метода экспертного оценивания при разработке модели надежности системы безопасности объекта информатизации // Вестник Воронежского института МВД России. – 2018. – №2. – С.56 – 64.
3. Орлов А. И. Организационно-экономическое моделирование в 3 ч. / А. И. Орлов. – М.: Изд-во МГТУ им. Н. Э. Баумана. Ч. 2 : Экспертные оценки. – 2011. – 486 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Удалов Валерий Петрович. Доцент кафедры радиотехники и электроники. Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-5257.

Жуков Михаил Михайлович. Начальник кафедры радиотехники и электроники. Кандидат технических наук.

Воронежский институт МВД России.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-5254.

Udalov Valery Petrovich. The assistant professor of the radio engineering and electronics chair. A Candidate of sciences (physics and mathematics), assistant professor.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Phone: (473) 200-5257.

Zhukov Mikhail Mikhailovich. The chef of the radio engineering and electronics department. A Candidate of sciences (technical).
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Phone: (473) 200-5254.

Ключевые слова: модель надежности, вероятность безотказной работы, экспертная оценка.

Key words: reliability model, probability of non-failure, expert assessment.

УДК 624.381

Хворов Руслан Александрович,
кандидат технических наук;
Безрядин Владислав Анатольевич,
кандидат технических наук

ФОРМИРОВАНИЕ ТЕОРЕТИЧЕСКОЙ ОСНОВЫ МЕТОДИКИ ВЫЯВЛЕНИЯ ВРЕМЕННОГО РЕЗЕРВА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ РАДИОКОНТРОЛЯ

THE FORMATION OF THEORETICAL BASIS METHODS TO IDENTIFY SLACK OF THE AUTOMATED SYSTEM OF RADIO CONTROL

В статье сформулированы и доказаны положение для формирования теоретической основы методики выявления временного ресурса АС РК с целью использования его для реализации средств защиты информации.

The article formulates and proves position for the formation theoretical basis of the methodology for identifying the temporary resource of the ASRC in order to use it for the implementation of information security tools.

Эффективное функционирования автоматизированной системы радиоконтроля (АС РК) сопряжено с рядом особенностей, одним из которых является возможности противника по деструктивному воздействию. Исходя из этого, реализация защитных механизмов сопряжена с необходимостью выделения ресурса АС РК.

С целью формирования теоретической основы методики выявления временного ресурса АС РК сформулируем и докажем теоретическое положение, о том что существует аналитическая зависимость между показателем эффективности защиты информации от воздействия угроз ее безопасности и величиной используемого в интересах защиты временного ресурса АС РК.

Введем следующие обозначения:

$\wp^{(u)} = \{\rho_i^{(u)} \mid i = 1, 2, \dots, |\wp^{(u)}|\}$ - упорядоченное множество программных модулей, реализующих процедуры обработки информации;

$\wp^{(3)} = \{\rho_j^{(3)} \mid j = 1, 2, \dots, |\wp^{(3)}|\}$ - упорядоченное множество программных модулей, реализующих механизмы защиты информации.

С целью доказательства сформулированного положения рассмотрим детально механизм защиты от воздействий угроз безопасности информации. Для защиты от воздействия угроз осуществляется разбиение множеств $\wp^{(u)}$ и $\wp^{(3)}$ на K непересекающихся подмножеств (фрагментов) $\wp_k^{(u)}$ и $\wp_k^{(3)}$, соответственно. При этом в каждом фрагменте $\wp_k^{(u)}$ формируется один значимый признак, контролируемый средствами защиты информации, а в соответствующем ему фрагменте $\wp_k^{(3)}$ – операции по защите на основе анализа корректности такого признака.

Представим показатель эффективности защиты информации k -го, $k = 1, 2, \dots, K$ фрагмента как вероятность обнаружения и устранения последствий воздействия угроз безопасности информации соответствующим механизмом защиты в виде [1]:

$$p_k = \begin{cases} \frac{v_k^{(3)}}{v_k^{(u)}} & , \text{при } v_k^{(3)} < v_k^{(u)} , \\ 1 & , \text{при } v_k^{(3)} \geq v_k^{(u)} \end{cases} \quad (1)$$

где $v_k^{(u)}$ - программный объем множества $\wp_k^{(u)}$; $v_k^{(3)}$ - программный объем множества $\wp_k^{(3)}$.

Примем в качестве характеристики вычислительного ресурса АС РК количество информации, обрабатываемое в единицу времени, и определим ее, используя базовые положения теории Шеннона [2], а так же методы программной метрики Холстеда [3]:

$$W = \log_2 \frac{a}{\Delta t} ,$$

где a – количество операторов программного обеспечения АС РК, реализуемых за время Δt .

Тогда выражение (1) можно записать в виде:

$$p_k = \frac{\log_2 a_k^{(3)}}{\log_2 a_k^{(u)}} ,$$

в котором $a_k^{(u)}$ - количество операторов программ обработки информации, реализуемых k -м фрагментом; $a_k^{(3)}$ - количество операторов программ защиты информации, реализуемых k -м фрагментом.

При условии, что воздействия угроз нарушения безопасности информации являются равновероятными событиями, а все множество $\wp = \wp^{(u)} \cup \wp^{(3)}$ реализуемых в АС РК процедур обработки информации является потенциально возможной областью формирования значимых признаков, показатель эффективности защиты информации на всем множестве $\wp$ определяется согласно выражению:

$$E_{(3u)} = 1 - \prod_{k=1}^K (1 - p_k) = 1 - \prod_{k=1}^K \left(1 - \frac{\log_2 a_k^{(3)}}{\log_2 a_k^{(u)}} \right). \quad (2)$$

Тогда, при равномерном разбиении этого множества на контролируемые фрагменты количество операторов программ обработки информации определяется согласно выражению:

$$A^{(u)} = K \cdot a^{(u)} ,$$

где $a^{(u)} = a_1^{(u)} = a_2^{(u)} = \dots = a_k^{(u)} \dots = a_K^{(u)}$ – количество операторов, реализуемых одним фрагментом.

При условии, что средство защиты информации реализует набор операций анализирующих один параметр, количество операторов программного обеспечения защиты информации, реализующих множество процедур $\wp^{(3)}$ определяется согласно выражению:

$$A^{(3)} = K \cdot a^{(3)},$$

где $a^{(3)} = a_1^{(3)} = a_2^{(3)} = \dots = a_k^{(3)} \dots = a_K^{(3)}$ – количество операторов, реализуемых одним средством защиты. В этом случае выражение (2) представляется в виде:

$$E_{(zu)} = 1 - \prod_{k=1}^K (1 - p_k) = 1 - \left(1 - \frac{\log_2 a_k^{(3)}}{\log_2 a_k^{(u)}} \right)^K,$$

Представим выражение для определения уровня временного резерва в виде:

$$U = \frac{T^{(3)}}{T^{(u)}} = \frac{\gamma \cdot A^{(3)}}{\gamma \cdot A^{(u)}} = \frac{K \cdot a^{(3)}}{A^{(u)}}, \quad (3)$$

где $T^{(3)}$ – временной ресурс АС РК, используемый для реализации процедур защиты информации; $T^{(u)}$ – временной ресурс АС РК, используемый для реализации процедур обработки информации; γ – быстродействие вычислительной среды АС РК, откуда K определяется как:

$$K = U \frac{A^{(u)}}{a^{(3)}}.$$

Тогда выражение (2) можно представить в виде:

$$E_{(zu)} = 1 - \left(1 - \frac{\log_2 a^{(3)}}{\log_2 a^{(u)}} \right)^K = 1 - \left(1 - \frac{\log_2 a^{(3)}}{\log_2 a^{(u)}} \right)^{U \frac{A^{(u)}}{a^{(3)}}}. \quad (4)$$

С учетом того, что время $T^{(3)}$ для средств защиты информации будет соответствовать величине $\Delta\tau$ используемого в интересах защиты временного резерва, выражение (3) для определения его уровня можно представить в виде:

$$U = \frac{\Delta\tau}{T^{(u)}} = \frac{\gamma \cdot \Delta\tau}{A^{(u)}}. \quad (5)$$

Подставив выражение (5) для уровня временного резерва U в (4) получим аналитическую зависимость между показателем эффективности защиты информации в АС РК и величиной используемого в интересах защиты временного ресурса:

$$E_{(zu)} = 1 - \left(1 - \frac{\log_2 a^{(3)}}{\log_2 a^{(u)}} \right)^{U \frac{A^{(u)}}{a^{(3)}}} = 1 - \left(1 - \frac{\log_2 a^{(3)}}{\log_2 a^{(u)}} \right)^{\frac{\gamma \cdot \Delta\tau}{a^{(3)}}}, \quad (6)$$

что и требовалось доказать.

Таким образом, полученные при помощи данной методики варианты реализации временного ресурса могут быть использованы в дальнейшем для формирования управленческих решений по использованию конкретных программных и технических средств при обеспечении безопасности информации в АС РК.

ЛИТЕРАТУРА

1. Вентцель Е.С. Исследование операций. – М.: Советское радио, 1972. – 552 с.
2. Шеннон К. Математическая теория связи / В сб.: Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – 94 с.
3. Холстед М.Х. Начала науки о программах / Пер. с англ. – М.: Финансы и статистика, 1981. – 128 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Хворов Руслан Александрович, слушатель кафедры (управления воинскими частями связи и РТО авиации).

Кандидат технических наук.

ВУНЦ ВВС «Военно-воздушная академия им.проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: khvoroff@rambler.ru

Россия, 394064, Воронеж, ул. Старых Большевиков, 54а.

Тел.: 8919 180 60 30.

Безрядин Владислав Анатольевич, старший преподаватель кафедры (управления воинскими частями связи и РТО авиации).

Кандидат технических наук.

ВУНЦ ВВС «Военно-воздушная академия им.проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж).

E-mail: bezrvlad@mail.ru

Россия, 394064, Воронеж, ул. Старых Большевиков, 54а.

Тел.: 8 910 34677 14.

Khvorov Ruslan Aleksandrovic. Learner department management of military units of communication and RTS aviation).

Candidate of technical Sciences.

«Air force academy named by prof. N.E. Zhukovski and U.A. Gagarin» (с. Voronezh).

Work address: Russia, 394064, Voronezh, St. Bolshevikov st., 54a.

Tel. 8-919-180-60-30.

Bezryadin Vladislav Anatol'evich, Senior lecturer department (management of military units of communication and RTS aviation).

Candidate of technical Sciences.

«Air force academy named by prof. N.E. Zhukovski and U.A. Gagarin» (с. Voronezh).

Work address: Russia, 394064, Voronezh, St. Bolshevikov st., 54a.

Tel. 8 910 346 77 14.

Ключевые слова к статье: автоматизированная система радиоконтроля, безопасность информации, временной резерв.

Keywords: automated radio monitoring system, information security, time reserve.

УДК 621.39

Шерстюков Сергей Анатольевич,
доктор технических наук, доцент;
Печников Сергей Сергеевич

ПРОБЛЕМЫ ТЕХНИЧЕСКОГО СОПРЯЖЕНИЯ СТАНДАРТОВ СИСТЕМ РАДИОСВЯЗИ В ПРЕДМОДУЛЯЦИОННОМ И УСИЛИТЕЛЬНОМ ТРАКТАХ

PROBLEMS PAIRING THE TECHNICAL STANDARDS OF RADIO COMMUNICATION SYSTEMS IN PREMODULATION AND THE AMPLIFYING PATHS

В статье рассмотрен способ сопряжения оборудования радиосвязи различных стандартов и диапазонов посредством межсистемных шлюзов и негативные последствия, возникающие в результате данных преобразований.

The article deals with the method of interfacing radio equipment of different standards and ranges by means of intersystem gateways and the negative consequences arising from these transformations.

Основу системы радиосвязи Министерства внутренних дел Российской Федерации (Министерства) составляют как аналоговые, так и цифровые стандарты, функционирующие в основном по методам множественного доступа с частотным и частотно-временным разделением каналов. В аналоговых системах радиосвязи широкое применение нашли носимые радиостанции ОВЧ и УВЧ диапазонов: «Эрика-310 П23», «Волна-302.03 П23», «Волна-302 П23», «Альтавия-301 П23», «Гранит-303.01 П23», «Радон-301 П23», «Kenwood ТК-3160», стационарные и возимые радиостанции ОВЧ и УВЧ диапазонов: «Эрика-111С П23», «Эрика-211 П23», «Волна-101 П23», «Волна-201 П23», «Альтавия-101 П23», «Альтавия-201 П23», «Гранит-102 П23», «Гранит-202 П23», «Радон-101 П23», «Радон-201 П23», «Kenwood ТК-8160.01» [1].

Цифровая ведомственная радиосвязь представлена профессиональными транкинговыми системами радиосвязи APCO25 и IDAS, стандартами цифровой конвенциональной радиосвязи DMR и «Альфа». В рамках межведомственного взаимодействия может использоваться системами радиосвязи стандарта TETRA.

Несмотря на разнообразие в парке средств радиосвязи, при использовании аналогового режима работы с классической частотной модуляцией, как правило, не возникает проблем электромагнитной совместимости при их эксплуатации. Данный факт обусловлен существующими нормативами классов излучения, которые необходимо соблюдать производителям средств радиосвязи [2]. В тоже время, в связи с особенностями работы подразделений органов внутренних дел, в ряде случаев существует необходимость организации работы аналоговых средств радиосвязи с цифровыми или цифровых радиосредств стандартов APCO25 и DMR, однако, в настоящее время вопросам сопряжения оборудования с различными классами излучения уделяется недостаточно внимания.

Проведенный анализ радиочастотного спектра, выделенного для использования Министерству в различных субъектах Российской Федерации, показал его высокую загруженность, в связи с чем возникает необходимость применения межсистемных шлюзов для сопряжения как используемого связного оборудования, так и вновь вводимого в эксплуатацию.

Одним из известных и оптимальным техническим решением по соотношению «цена-качество» является применение аппаратно-программного комплекса (АПК)

«Форком», предназначенного для коммутации локальных систем радиосвязи, управления базовыми радиостанциями и передачи голоса по ведомственным локальным сетям.

Существуют и зарубежные производители аналогичного оборудования, например универсальный шлюз MotoBridge, от компании Motorola. Оборудование обладает большими функциональными возможностями, в том числе диспетчерское управление через IP, VoIP телефония и голосовые конференции, связь радио с абонентом телефонной сети. Но производитель гарантирует поддержание этих сервисов при использовании радиооборудования Motorola, а в парке ОВД эксплуатируется большое количество радио средств различных производителей, в связи с чем, в данной области необходимо проведение дополнительных исследований. Кроме того стоимость универсального шлюза MotoBridge составляет 450 000 руб., что существенно дороже аналогичного отечественного оборудования.

Базовым принципом работы АПК «Форком-Р», как и универсального шлюза MotoBridge является использование радио приемо-передатчиков и RoIP шлюза для связи в одну радиосеть отдельных групп радиосредств. Данный подход исключает прямую связь абонентского оборудования различного стандарта и диапазона между собой.

Предположим, что на приемо-передающую часть радио оборудования *Радиосети №1* поступает высокочастотный радиосигнал с частотой определенной для радиосредств работающих в данной зоне радиопокрытия. Согласно закону модуляции, заданному для радиосредств Радиосети №1, в демодуляторе осуществляется преобразование в основную полосу частот. В результате, подключение к RoIP шлюзу №1 происходит с помощью аналогового низкочастотного сигнала, в связи с чем тип абонентского оборудования (аналогового или цифрового) не имеет значения. Также можно не учитывать диапазон рабочих частот несущего колебания и тип радиоизлучений подключаемого оборудования.

Аналого-цифровое преобразование осуществляется RoIP шлюзом №1, который конвертирует сообщение в РСМ стандарт и передает его другим известным ему компонентам системы TCP/IP пакетами посредством сети Ethernet. При получении TCP/IP пакетов RoIP шлюз №2, производит обратное цифро-аналоговое преобразование и передачу низкочастотного сигнала на вход ретрансляционного оборудования Радиосети №2, после чего в модуляторе осуществляется формирование сигнала согласно закона модуляции определенного для радиосредств Радиосети №2. Передающее устройство излучает высокочастотный сигнал в диапазоне определенном в данной зоне радиопокрытия.

На рис. 1 видно, что на вход ретранслятора Группы №1 поступает ВЧ сигнал, подвергшийся изменению в результате воздействия среды, причем для аналоговых радиосредств это будет выражено в появлении шумов и снижении слоговой разборчивости, в то время, как для цифровых средств связи это может повлечь пропадание или изменение отдельных фрагментов сообщений, что обусловлено применением различного рода вокодеров.

АЦП-ЦАП преобразованию будет подвергнут сигнал, с уже существующей долей ошибок, которые могут быть увеличены в результате данных преобразований. Также возможно внесение дополнительных ошибок связанных с потерей пакетов при передаче по каналам сети Ethernet.

Таким образом, на вход модулятора ретранслятора Радиосети №2 будет поступать преобразованный НЧ сигнал, что может привести к амплитудно-фазовым искажениям в результате модуляции и усиления радиосигнала, и, как следствие – к нарушению электромагнитной совместимости радиосредств.

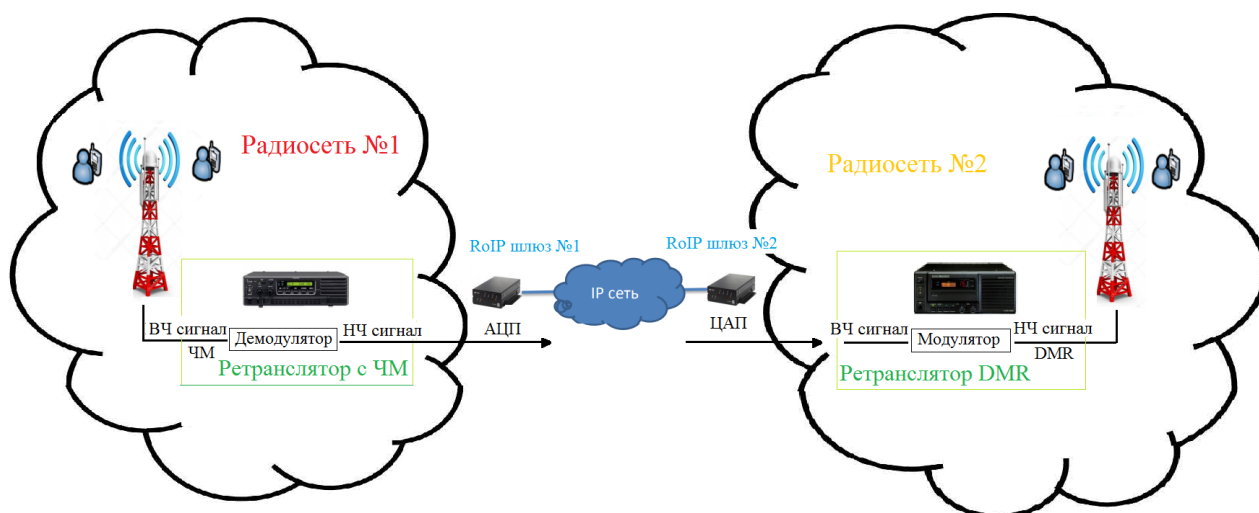


Рис.1. Схема объединения радиосетей с использованием RoIP шлюза

Согласно ГОСТ 12252-86 «Радиостанции с угловой модуляцией сухопутной подвижной службы» ширина полосы частот излучения передатчика определяется для полосы звуковых частот (на входе) от 300 до 3000 Гц, а девиация частот IP-шлюза установлена в размере от 20 до 3600 Гц, в результате ширина полосы частот будет отличаться от значений установленных ГОСТом.

Кроме того, чувствительность модуляционного входа передатчика должна соответствовать выходному уровню источника информационного сигнала, в случае несовпадения данных параметров возможно возникновение дополнительных искажений, вносящих побочные спектральные составляющие, что может привести к превышению допустимого коэффициента нелинейных искажений передатчика, для радиостанции тип 1 – 5%, для радиостанции тип 2 – 7%.

Нелинейные искажения группового сигнала в усилителях передатчиков возникают в основном из-за нелинейности статических и динамических характеристик. Эти характеристики имеют наибольшую нелинейность как при малых (работа на нижнем участке характеристик), так и при сравнительно больших токах (критический и перенапряженный режимы). Рассматривая двухтоновый равноамплитудный сигнал

$$U_{вх}(t) = 0.5U_0 \cos \omega_1 t + 0.5U_0 \cos \omega_2 t = 0.5U_0 \cos \Delta t \cos \omega_0 t \quad (1)$$

имеющий наиболее простой спектр, для сигнала с переменной амплитудой, где $\Delta = (\omega_2 - \omega_1) / 2$, $\omega_0 = (\omega_2 + \omega_1) / 2$, при линейной амплитудной характеристике усилителя (кривая 1) огибающая сигнала имеет вид коммутированной синусоиды (сплошная линия).

При нелинейности амплитудной характеристики из-за влияния нелинейности амплитудной характеристики (кривая 3) проявляются как расширение импульса огибающей и уплощение их вершин (штрих-пунктирная линия). Искажения из-за влияния нижнего сгиба статических характеристик (кривая 2) импульсы огибающей несколько сужаются (штриховая линия) [3].

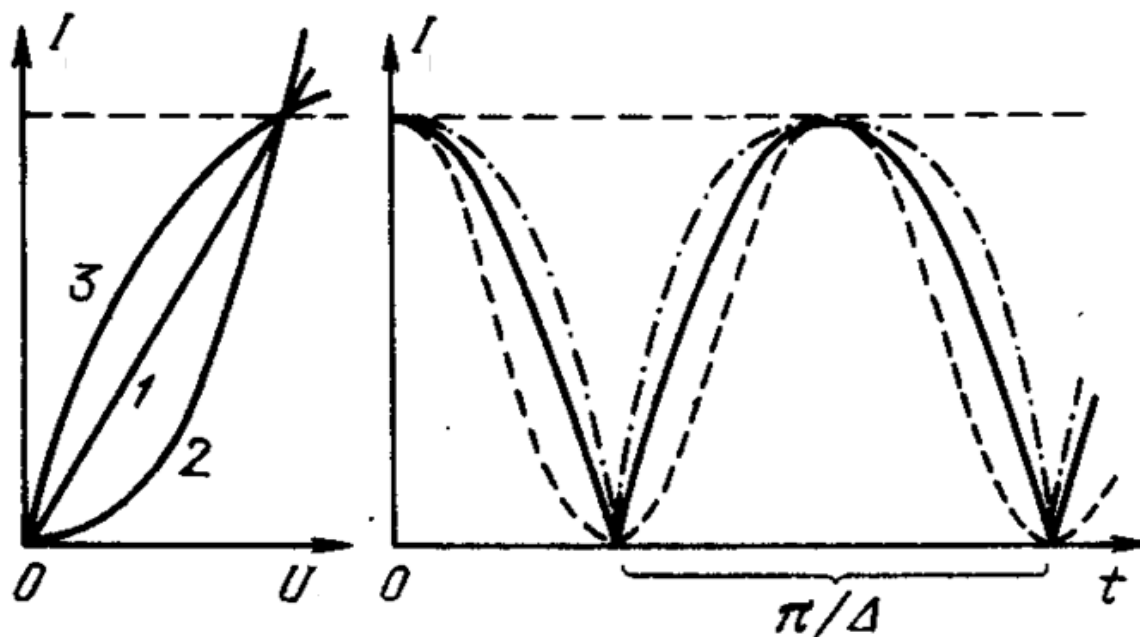


Рис. 2. Варианты модуляционных характеристик и искажений огибающей

Искажение огибающей двухтонового сигнала ведет к появлению дополнительных спектральных компонент A_3 и A_5 , которые определяют коэффициенты нелинейных искажений третьего $K_3=20\log(A_3/A_1)$ и пятого $K_5=20\log(A_5/A_1)$ порядков.

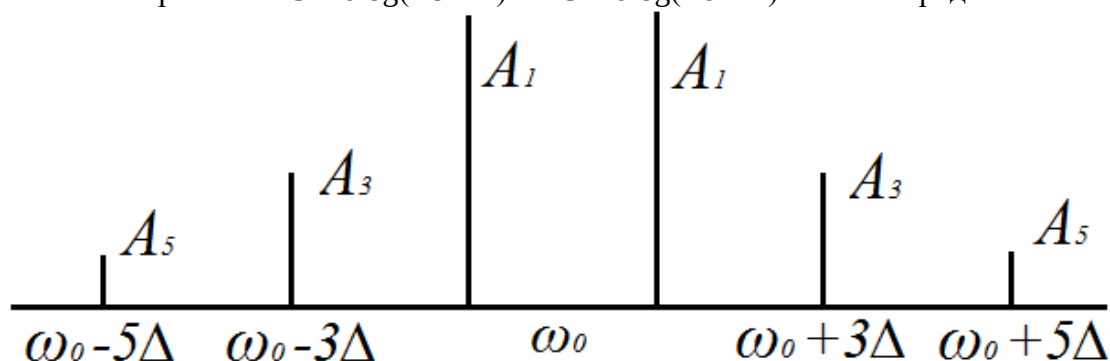


Рис. 3. Спектр двухтонового сигнала с искажением

Кроме того, искажение форм модуляционных характеристик ведет к невозможности использования энерго-эффективных режимов работы усилителя, в частности, ключевого режима работы в связи с внесением дополнительных спектральных составляющих.

Для подавления интермодуляционных искажений в выходном спектре сигналов, необходимо повышение линейности усилительного тракта применяя схемы компенсации искажений, возникающих при использовании нелинейного усиления.

ЛИТЕРАТУРА

1. Шерстюков С.А. Конфигурирование аппаратно-программного комплекса «Форком»: методические рекомендации / С.А. Шерстюков. – Воронеж: Воронежский институт МВД России, 2017. – 76 с.
2. Шерстюков С. А., Печников С. С. Повышение энергетических свойств радио-передающих устройств, формирующих высокоэффективные радиосигналы с цифровой модуляцией // Охрана, безопасность, связь – 2018 : материалы международной научно-практической конференции. – Воронеж : Воронежский институт МВД России, 2018. – С. 168 – 171.
3. Шахгильдян В.В. Радиопередающие устройства. Учебник для вузов. – 3-е изд., перераб. и доп. – В.В. Шахгильдян, В.Б. Козырев, А.А. Ляховкин, В.П. Нуянзин, В.М. Розов, М.С. Шумилин. – Москва : Радио и связь, 2003. – 560 с.
4. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра. Пер. с англ. Под ред. В.И. Журавлева. – Москва : Радио и связь, 2000. – 520 с.
5. Верещагин Е. М., Никитенко Ю. Г. Частотная и фазовая модуляция в технике связи [Текст] / Е. М. Верещагин, Ю. Г. Никитенко. - Москва : Связь, 1974. - 224 с.
6. [Электронный ресурс] // Объединение стандартов. URL: <https://cnt-radio.com/index.php/ru/ob-edinenie-standartov> (Дата обращения: 16.11.2018).
7. ГОСТ 12252-86 (СТ СЭВ 4280-83) Радиостанции с угловой модуляцией сухопутной подвижной службы. Типы, основные параметры, технические требования и методы измерений

СВЕДЕНИЯ ОБ АВТОРАХ

Шерстюков Сергей Анатольевич. Профессор кафедры инфокоммуникационных систем и технологий. Доктор технических наук, доцент.

Воронежский институт МВД России.

E-mail: sherstukov@vimvd.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

T.+7(473)200-52-26.

Печников Сергей Сергеевич. Аджункт кафедры инфокоммуникационных систем и технологий.

Воронежский институт МВД России.

E-mail: orl_os@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

T.+7(473)200-52-31.

Sherstyukov Sergey Anatolevich. Professor of the chair infocommunication systems and technologies. Doctor of Technical Sciences, assistant professor.

Voronezh Institute of Russian Ministry of Internal Affairs.

E-mail: sherstukov@vimvd.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. +7 (473) 200-52-26.

Pechnikov Sergey Sergeevich. Post-graduate cadet of the chair of communication systems and technologies.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail orl_os@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. +7 (473) 200-52-31.

Ключевые слова: радиосвязь, RoIP шлюз, сопряжение радиооборудования, искажения сигнала, спектр, линеаризация усилителей мощности.

Keywords: radio communication, RoIP gateway, the pairing of radio equipment, signal distortion, spectrum, linearization of power amplifiers

УДК 621.396.

**Шугай Оксана Евгеньевна;
Орлова Дарья Евгеньевна**

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ РИСКОВ ПРИ ВЫБОРЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ПРЕДПРИЯТИЯ УГОЛОВНО- ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ

MATHEMATICAL MODEL OF RISK ASSESSMENT IN THE CHOICE OF DIRECTION OF DEVELOPMENT OF ENTERPRISES CRIMINALLY-EXECUTIVE SYSTEM

В данной статье рассмотрен инструментарий корректной оценки производственного риска промышленного предприятия уголовно-исполнительной системы (УИС) на основе математической статистики и теории вероятности. Предложена модель оценки риска по нескольким показателям на основе расчетных значений математического ожидания, стандартного отклонения и коэффициента вариации.

In this article the tools of correct assessment of industrial risk of the industrial enterprise of penal system (MIS) on the basis of mathematical statistics and probability theory are considered. A model of risk assessment for several indicators based on the calculated values of expectation, standard deviation and coefficient of variation is proposed.

Последние годы ситуация в мировой экономике характеризуется снижением количества источников ресурсного развития. Данная тенденция не стала исключением и для УИС. Ограниченность и неординарность ресурсов в производстве УИС требует определенной специфики в управлении, позволяющей более эффективно использовать имеющийся потенциал. В этой связи проведение маркетинговых исследований рынка сбыта товаров является неотъемлемой частью процесса планирования. Предварительное сегментирование рынка позволяет выделить сегменты, в которых «ниша» планируемого к производству товара не занята конкурентами или определить конкурентные преимущества продукции предприятия УИС [3]. Тем не менее, после проведения сегментирования остается возможность возникновения непредвиденных потерь, т. е. существуют риски проектной деятельности или её отдельных параметров, имеющих временную, количественную и стоимостную оценку. Проектный риск имеет определенные источники, причины и последствия, т.е. оказывает влияние на результаты проекта [1].

Управление рисками является важнейшей частью любой программы или проекта, которая может внести большой вклад в достижение успешных результатов. В УИС механизм использования этого типа управления только начинает внедряться, несмотря

на подтвержденную многолетним опытом международного использования эффективность.

В случае предприятия УИС будем оценивать возможность получения определенного результата при производстве нескольких товаров, перечень которых определен результатами маркетинговых исследований (сегментирования) рынка сбыта [3]. Зная, что риск это некоторая вероятностная величина, будем оценивать его с помощью математической статистики и теории вероятности, анализируя величину математического ожидания и стандартного отклонения и коэффициента вариации [2].

Оценим вероятность получения заданного уровня дохода и максимальной трудозанятости заключенных с учетом возможности подготовки и профессионального обучения потенциальных работников. Данные показатели являются наиболее значимыми для системы.

Выделенные показатели будут являться дискретными величинами, вероятность возникновения которых является случайным событием. В таком случае сумма вероятностей возникновения всех возможных значений будет равна 1. Тогда среднее математическое ожидание $\overline{M(x, z)}$ заданных показателей x и z будем вычислять по формуле:

$$\overline{M(x, z)} = \frac{1}{2} \left(\sum_{i=1}^n x_i \mu_i + \sum_{j=1}^k z_j \varphi_j \right), \quad (1)$$

где x_i – количественный показатель прибыльности производства выбранного вида товара;

μ_i – вероятность получения указанной прибыли;

z_j – процент трудовой занятости заключенных;

φ_j – вероятность возникновения данной занятости.

Дальнейший анализ рисков основан на определении среднеквадратического стандартного отклонения $\overline{\sigma(x, z)}$, показывающего степень колеблемости (дисперсии) полученной величины.

$$\overline{\sigma(x, z)} = \frac{1}{2} \left(\sqrt{\sum_{i=1}^n x_i^2 \mu_i + \sum_{j=1}^k z_j^2 \varphi_j - 2(\overline{M(x, z)})^2} \right). \quad (2)$$

В случае равенства среднеквадратического отклонения нескольких проектов, на основе полученных данных рассчитываем коэффициент вариации, показывающий величину риска на каждую единицу прибыли и трудозатрат:

$$K_v = \overline{\sigma(x, z)} / \overline{M(x, z)}. \quad (3)$$

Выбор стоит делать в сторону производства товаров с наименьшим коэффициентом вариации, как возможности производства товаров с максимальной прибылью, наибольшей занятостью заключенных и минимальным риском. Достоинством данного метода является возможность оценки и анализа различных вариантов развития событий по нескольким наиболее важным для предприятий УИС показателям в рамках одного подхода.

ЛИТЕРАТУРА

1. Королев В. Ю., Бенинг В. Е., Шоргин С. Я. Математические основы теории риска. – Москва : Физматлит, 2011. – 620 с.

2. Магер В. Е., Леонова Т. И., Орлова О. Ю. Вероятностная модель рисков в системе менеджмента качества организации// Экономика и менеджмент систем управления. – 2017. – № 2. – С. 23-32.

3. Новосельцев В. И., Шугай О. Е. Алгоритм сегментирования рынка сбыта продукции, производимой предприятиями уголовно-исполнительной системы// Вестник Воронежского института ФСИИ России. – 2018. – № 3. – С. 116-121.

СВЕДЕНИЯ ОБ АВТОРАХ

Шугай Оксана Евгеньевна. Преподаватель кафедры социально-гуманитарных и финансово-правовых дисциплин.

Воронежский институт ФСИИ России.

E-mail: oks-shugaj@mail.ru

Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. 89507710556.

Орлова Дарья Евгеньевна. Начальник кабинета специальных дисциплин инженерно-технического факультета.

Воронежский институт ФСИИ России.

E-mail: dasha_scorobogat@mail.ru

Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. 89066739219.

Shugai Oksana Evgenievna. Teacher of the Department of social and humanitarian, financial and legal disciplines.

Voronezh Institute of the FSIN of Russia.

E-mail: oks-shugaj@mail.ru

Russia, 394072, Voronezh, Irkutsk str., 1A. Phone 89507710556

Orlova Daria Evgenievna. Head of the Cabinet of special disciplines of engineering and technical faculty.

Voronezh Institute of the FSIN of Russia.

E-mail: dasha_scorobogat@mail.ru

Russia, 394072, Voronezh, Irkutsk str., 1A. Tel. 89066739219.

Ключевые слова: управление рисками, оценка рисков, неопределенность, математическое ожидание, стандартное отклонение, коэффициент вариации.

Keywords: risk management, risk assessment, uncertainty, expectation, standard deviation, coefficient of variation.

УДК 519.2

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Абросимова Евгения Михайловна,
кандидат технических наук;

Иванченко Ольга Степановна,
кандидат юридических наук, доцент

ПОКАЗАТЕЛИ ЗАЩИЩЕННОСТИ И ЭФФЕКТИВНОСТИ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В СИСТЕМАХ БЕЗОПАСНОСТИ ОВД

THE SECURITY METRICS AND THE EFFECTIVENESS OF THE IMPLEMENTATION OF INFORMATION PROCESSES IN SYSTEMS SECURITY OVD

В статье непосредственно рассматриваются принципы формирования показателя эффективности защиты информации с учетом ряда особенностей механизмов реализации этой функции при осуществлении ими двух основных этапов процесса защиты информации: устранение угроз нарушения целостности и доступности сведений и устранение их последствий.

The article deals with the principles of formation of the indicator of information security effectiveness taking into account a number of features of protection mechanisms in the implementation of two main stages of the information security process: elimination of threats to the integrity and availability of information and elimination of their consequences.

Информационным процессом непосредственно от объекта (источник) к ПЦО (приёмник) является преобразование сведений в автоматизированной системе ПЦО, зависящее от происходящего на объекте. Любая обработка информации внутри информационной системы происходит непосредственно с помощью данных потоков.

Утечка сведений также происходит только с помощью потоков информации, а значит есть необходимость непосредственно уметь разделять потоки на разрешенные (безопасные, не приводящие к утечке данных) и запрещенные (небезопасные, потенциально ведущие к утечке).

Повышение эффективности защиты процессов распространения информации, передаваемой по каналам связи, используемым непосредственно при организации охраны с помощью технических средств, рассредоточенных в пределах одного населенного пункта объектов, достигается непосредственно за счет сокращения количества используемых линий проводной связи, количества аппаратуры систем централизованного наблюдения, размещаемой на технологических площадках автоматизированных телефонных станций, а так же непосредственно реализации комплекса мер по защите данных при использовании современных каналов передачи.

При формировании непосредственно показателя эффективности защиты данных учитывается ряд особенностей механизмов защиты при реализации ими непосредственно двух основных этапов процесса защиты информации:

- 1) устранение угроз нарушения целостности и доступности информации;
- 2) устранение их последствий.

Непосредственно реализация этапа устранения угроз нарушения целостности и доступности данных определяется условием:

$$\tau_{(y)} \leq \tau_{(cy)}, \quad (1)$$

в котором $\tau_{(y)}$ определяется в соответствии с выражением:

$$\tau_{(y)} = \tau_{(k)} * \tau_{(ov)} * \tau_{(oi)} * \tau_{(pi)}, \text{ где}$$

$\tau_{(k)}$ – время, непосредственно затрачиваемое на контроль подверженности информационного процесса угрозам нарушения целостности и доступности данных;

$\tau_{(ov)}$ – время, непосредственно затрачиваемое на обнаружение воздействий угроз;

$\tau_{(oi)}$ – время, непосредственно затрачиваемое на обнаружение источников угроз;

$\tau_{(pi)}$ – время, непосредственно затрачиваемое на подавление источников угроз;

$\tau_{(cy)}$ – время существования угрозы нарушения целостности и доступности данных.

Непосредственно своевременность устранения последствий определяется условием:

$$\tau_{(n)} \leq \tau_{(tr)}, \quad (2)$$

в котором $\tau_{(n)}$ определяется в соответствии с выражением:

$$\tau_{(n)} = \tau_{(ap)} * \tau_{(vi)} * \tau_{(pr)}, \text{ где}$$

$\tau_{(ap)}$ – время, непосредственно затрачиваемое на анализ последствий воздействия угроз нарушения целостности и доступности данных;

$\tau_{(vi)}$ – время, непосредственно затрачиваемое на восстановление целостности вычислительной среды;

$\tau_{(pr)}$ – время, непосредственно затрачиваемое на принятие решения о продолжении реализации процесса передачи данных;

$\tau_{(tr)}$ – требуемое время восстановления данного процесса.

С учетом изложенного, непосредственно можно сделать вывод о том, что вероятность $P_{(y)}$ выполнения условия (1):

$$P_{(y)} = P(\tau_{(y)} \leq \tau_{(cy)}) \quad (3)$$

является достаточно полной характеристикой своевременной реализации функций устранения угроз нарушения целостности и доступности данных, а непосредственно вероятность $P_{(n)}$ выполнения условия (2):

$$P_{(n)} = P(\tau_{(n)} \leq \tau_{(tr)}) \quad (4)$$

является достаточно полной характеристикой своевременной реализации процедур защиты данных от угроз нарушения ее непосредственно целостности и доступности.

С целью формирования показателя эффективности реализации процессов передачи данных в условиях обеспечения их защищенности представим время $\tau_{(ип)}$ реализации процедур передачи данных в виде:

$$\tau_{(ип)} = [\tau_{(n)} + (\tau_{(k)} + \tau_{(ov)} + \tau_{(oi)})] + P_{(n)} * [(\tau_{(pi)} + \tau_{(ap)} + \tau_{(vi)} + \tau_{(pr)}) + (1 - E_{(зи)}) * \tau_{(y)}] \quad (5)$$

где $\tau_{(n)}$ – непосредственно потенциальное время реализации процессов обработки информации;

$\tau_{(y)}$ – непосредственно время, в течение которого сегмент ПЦО вследствие нарушения целостности и доступности его информации является нерабочим (убыток, нанесенный воздействием угрозы).

В общем случае время $\tau_{(y)}$ представляет собой комбинацию непосредственно двух случайных величин:

$$\tau_{(y)} = \tau_{(yц)} \circ \tau_{(yд)} \quad (6)$$

- временных потерь $\tau_{(yц)}$ вследствие нарушения целостности данных и временных потерь $\tau_{(yд)}$ непосредственно вследствие нарушения их доступности.

С учетом изложенного можно сделать вывод о том, что непосредственно вероятность $P(\tau_{(ип)} \leq \tau_{(д)})$ достаточно полно характеризует своевременность реализации процессов передачи данных в условиях обеспечения их защиты, что дает непосредственно возможность использовать их как соответствующий показатель эффективности E , т.е.

$$E = P(\tau_{(ип)} \leq \tau_{(д)}) \quad (7)$$

ЛИТЕРАТУРА

1. Оценка защищенности информационных процессов в территориальных ОВД: модели исследования: монография / под ред. С.В. Скрыля – Воронеж: Воронежский институт МВД России, 2010. – 213 с.
2. Проблемы организации защиты информации в интегрированных системах безопасности / В.С. Зарубин, В.В. Гайфулин, С.В. Петрушков, А.Р. Фамильнов // Информация и безопасность. – Воронеж: Воронежский государственный технический университет, 2009. Вып. 1. – С. 95 – 98.
3. Юдин Д.В. Модели и алгоритмы синтеза комплекса показателей защищенности информационных ресурсов федеральной системы мониторинга критически важных объектов: Диссертация канд. техн. наук – Воронеж: Воронежский институт МВД России, 2012. – 135 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Абросимова Евгения Михайловна. Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: chip_ik@mail.ru

Россия, 394065, Воронеж, Проспект патриотов, 53.

Тел. (919) 185-00-36.

Иванченко Ольга Степановна. Доцент кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: iskorka@yandex.ru

Россия, 394065, Воронеж, Проспект патриотов, 53.

Тел. (906) 584-99-09.

Abrosimova Evgeniya Mikhailovna. Lecturer of the Department of radio systems and security monitoring systems.

Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: chip_ik@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-85.

Ivanchenko Olga Stepanovna. Associate Professor of radio engineering systems and security monitoring systems.

Candidate of law, associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: iskorka@yandex.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-85.

Ключевые слова: информационный процесс, утечка информации, защита информационных процессов, показателя эффективности защиты информации.

Key words: information process, information leakage, protection of information processes, efficiency of information protection.

УДК 621

Бороненков Александр Иванович,
кандидат технических наук;
Саваровский Алексей Борисович

ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ СОВРЕМЕННОМУ ТЕРРОРИЗМУ КАК СПОСОБ БОРЬБЫ С ЕГО ПРОЯВЛЕНИЯМИ

INFORMATION COUNTERACTION OF MODERN TERRORISM, AS A METHOD OF STRUGGLE AGAINST HIS MANIFESTATIONS

В статье рассмотрены понятие терроризма, его сущность и причины появления. Информационный терроризм: среда Интернет как главный фактор его возникновения. Представлены рекомендации для общества, которые направлены на противодействие информационному терроризму в сети Интернет.

The article deals with the concept of terrorism, its essence and causes. Information terrorism: the Internet environment as the main factor of its occurrence. Recommendations for the society aimed at combating information terrorism on the Internet are presented.

Иногда войну с терроризмом называют третьей мировой войной, но это лишь метафора. Терроризм во всех своих формах стал глобальной проблемой, с которой общество столкнулось в XXI веке.

В истории современной России немало грустных страниц, связанных с массовой гибелью граждан в результате террористических актов. Одна из них произошла 1 сентября 2004 года в школе №1 города Беслана. Террористы сделали своими заложниками 1300 человек. В результате этого жестокого теракта погибло 333 человека, среди них более половины – это дети. Ещё пятьсот человек оказались ранеными. Данный бесчеловечный противоправный акт должен быть переосмыслен с научной точки зрения для устранения причин и условий, способствующих его совершению.

Современное общество столкнулось с огромной бедой – терроризмом, на данном этапе развития жизни, для которой до сих пор нет чётких ответов и решений.

Федеральный закон «О противодействии терроризму» даёт чёткое понятие терроризма – это идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий [1]. Но это только одно из 100 понятий терроризма. Поэтому даже данное определение не будет являться однозначным.

Каковы причины терроризма? Это один из волнующих вопросов общества.

Причины:

- политические, то есть политическая нестабильность или же недостаток мер по обеспечению безопасности населения;
- социальные – упадок уровня жизни в стране;
- экономические, то есть терроризм – это доход, способный приносить пользу своим организаторам;
- религиозные – наличие религиозных течений, пропагандирующих насилие;
- духовные – кризис общества, искажение правовых и общечеловеческих ценностей.

Современная жизнь не только связана с реальными событиями, но и с виртуальностью. Интернет для людей стал частью жизни и поэтому зачастую люди, не понимающие, как правильно пользоваться интернетом попадают на уловки мошенников, тем самым страдают. Например, для достижения поставленных целей террористы воздействуют на людей различными способами (электронные письма, картинки, посты), меняющих созна-

ние человека и угрожающих их жизни и здоровью. Регулярное общение в среде Интернет способствует возникновению информационного терроризма.

Прежде всего, смысл определения «информационный терроризм» вытекает из его названия, а именно подразумевает форму деструктивного воздействия на человека, социум и государство в целом, при помощи различной пропагандисткой информации. Целью данного воздействия является изменение сознания человека до такой степени, чтобы мнение личности соответствовало агитационной тематике, а впоследствии общественному восприятию.

Информационный терроризм – новая разновидность террористической деятельности, основанная на последних достижениях науки и техники в области компьютерных и информационных технологий [2].

Известный американский профессор факультета коммуникаций университета Хайфы Габриэль Вейман выделяет восемь способов использования Интернет террористами:

- 1) проведение психологической войны;
- 2) поиск информации;
- 3) обучение террористов;
- 4) сбор денежных средств;
- 5) пропаганда;
- 6) вербовка;
- 7) организация сетей;
- 8) планирование и координирование террористических действий [3].

Интернет имеет много возможностей, поэтому служит источником для совершения своих действий террористическими организациями. Террористы часто используют обширные средства массовой информации, чтобы захватить большую аудиторию людей не для вымогательства денег, а для выполнения своих политических целей. Одно из средств массовой информации является СМИ, с помощью которого регулируется общественное мнение.

Информационные технологии всё больше внедряются в обыденную жизнь человека, число пользователей Интернет постоянно возрастает, сфера электронных услуг представляется всё шире.

Для предупреждения и профилактики преступных проявлений, связанных с террористической угрозой, требуется:

- в образовательных учреждениях, различных организациях проводить специальные лекции по избеганию информационного террора;
- усилить работу служб информационной безопасности;
- родителям детей и подростков быть бдительными, постоянно проводить с ними беседы на тему: «Как не стать жертвой информационной пропаганды терроризма».

В настоящее время молодежь является объектом террористического воздействия так как у данного социального слоя не в полной мере прошёл процесс социализации. Террористы пользуются наивностью детей и подростков для осуществления своих целей. Приведём пример из жизни: в 2015 году появилась игра «Синий кит», под благовидными целями и предложениями скрывалась цель по доведению детей и подростков до самоубийства. В результате данной завуалированной террористической атаки погибло примерно 130 подростков.

Таблица 1

Противодействие терроризму

Противодействие (профилактика) информационному терроризму в среде Интернет	
1	2
молодежь	взрослое поколение
- Проведение профилактических мероприятий для улучшения правосознания молодых граждан Российской Федерации	- Передача жизненного опыта младшему поколению
- Поддержание традиционного общественного мнения о социальных процессах	
- Воздействие на мнение граждан через профессиональные союзы, общественные объединения, профессиональные студенческие комитеты	
- Воспитание у молодежи соблюдения законности	
- Формирование правил социального поведения, принятого в гражданском обществе	
- Повышение толерантности с использованием института семьи	
- Контроль над информационным пространством, оказывающее пагубное воздействие на воспитание, образование, мнение, психологию молодежи	
- Необходимо предложить меры по ужесточению законодательства, в части касающиеся экстремистских и террористических преступлений, а также за подстрекательские действия в этой сфере	

Противодействие террористическим угрозам в информационной среде выражается в действиях и решениях, способствующих формированию позитивной правовой психологии и правового сознания. Нужно развернуть меры по реализации в обществе мер правовой пропаганды для информирования населения о методах защиты от террористических угроз и профилактики самих преступных террористических проявлений [4]. При этом должны осуществляться мероприятия, которые сказаны выше, но в этот же момент предполагать надёжную защиту и эффективное использование своих собственных информационных ресурсов. Также люди должны быть готовы к тому, что могут возникнуть новые вызовы и угрозы информационного терроризма, для которых будут необходимы быстрые решения и их реализация. Результативные решения этой задачи требуют совместных усилий, опирающихся на общедоступный обмен информацией, как отдельных государств, так и мирового сообщества в целом.

Человек волен сам распоряжаться собственной жизнью. Но, чтобы его жизнь протекала размеренно, спокойно и прекрасно, в первую очередь он должен обеспечить себе безопасное существование. То есть быть внимательнее и аккуратнее при использовании коммуникаций, не терять свою бдительность, реальность жизни, а к тому же своё сознание.

Предугадать негативные последствия террористической атаки на информационную сферу представляется зачастую невозможным, а исход таких атак может быть катастрофическими. Поэтому, чтобы избежать трагедий люди должны быть предупреждены и готовы, ведь общество - это динамическая система, которую возможно изменить как в лучшую, так и в худшую сторону.

ЛИТЕРАТУРА

1. О противодействии терроризму: Федеральный закон РФ от 06.03.2006 N 35-ФЗ (в ред. от 18.04.2018) (дата обращения 28.03.2019).
2. Россошанский А.В. Риски и угрозы информационного терроризма в России [Электронный ресурс]. - URL: <https://cyberleninka.ru/article/n/riski-i-ugrozy-informatsionnogo-terrorizma-v-rossii> (дата обращения 24.04.2019).
3. Вейман Г. Как современные террористы используют Интернет. Специальный доклад №116 [Электронный ресурс]. - URL: scienceport.ru/library/-literature/5170-spetsialnyi-doklad-no-116-kak-sovremennyye-terroristy-ispolzuyut-internet/ (дата обращения 23.04.2019).
4. Вельможина Н.В. Профайлинг как метод профилактики и борьбы с терроризмом / Н.В. Вельможина, Д.Н. Черников - Сборник материалов «Преступность в СНГ: проблемы предупреждения и раскрытия преступлений», 2018 г. – с.87-89.

СВЕДЕНИЯ ОБ АВТОРЕ

Бороненков Александр Иванович. Кандидат технических наук.
Воронежский институт МВД России.
E-mail: boronenkovai@vimvd.ru
Россия, 394006, г. Воронеж, ул. проспект Патриотов, 53.
Тел. (473) 200-56-28.

Саваровский Алексей Борисович,
Воронежский институт МВД России.
E-mail: savrovskyab@vimvd.ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-56-31.

Boronenkov Alexander Ivanovich. Candidate of technical Sciences.
E-mail: boronenkovai@vimvd.ru
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-56-28.

Swarovski Mr Miller,
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
E-mail: savrovskyab@vimvd.ru
Tel. (473) 200-56-31.

Ключевые слова: терроризм; информационный терроризм; интернет; информационные технологии; информационного противодействия терроризму.

Key words: terrorism; information terrorism; the Internet; information technology; information counter terrorism.

УДК 351.865

РАЗРАБОТКА СИСТЕМ КОНТРОЛЯ ДОСТУПА ОХРАНЯЕМОГО ОБЪЕКТА

DEVELOPMENT OF ACCESS CONTROL SYSTEM FOR THE PROTECTED FACILITY

В данной работе в ходе анализа существующих систем контроля доступа предназначенных для охраны объектов, подтверждена актуальность постоянной модернизации систем контроля доступа, ввиду постоянного роста уязвимостей в системах контроля доступа. Предложена структура системы контроля управления доступом для режимного помещения.

In this work, while analyzing existing access control systems designed to protect objects, the relevance of continuous modernization of access control systems is confirmed, due to the constant growth of vulnerabilities in access control systems. The structure of the access control system for secure premises is proposed.

Согласно установленной классификации ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом» технические требования и методики испытаний выделяет в СКУД следующие типы: по виду объектов контроля; числу контролируемых точек доступа; способу управления; уровню защищенности системы от несанкционированного доступа (НСД).

В настоящее время можно выделить основные компоненты, входящие в обобщенную схему СКУД: идентификатор пользователя (ключ, биометрия), устройства идентификации, контроллер, персональный компьютер, исполнительное устройство.

Наиболее часто на режимных объектах применяется сетевая распределенная автоматическая система контроля и управления доступом с распределенными правами и возможностью подтверждения идентификации. Рассмотрим предполагаемый охраняемый объект с требованиями к повышенной безопасности – хранилище ювелирного магазина.

Цель: защита материальных ценностей, находящихся в помещении, повышение лояльности посетителей, защита жизни обслуживающего данное помещение персонала, обеспечение усиленного контроля доступа к помещению (рис.1).

Задачи: регистрация всех событий оператора по управлению доступом к помещению, возможностью автоматической полной блокировки доступа к объекту, доступ в помещение без постоянного пропуска по разрешению оператора службы безопасности., обеспечение стабильного доступа к помещению зарегистрированного персонала в автоматическом режиме при минимальной задержке, создание двух точек контроля доступа к охраняемому помещению.

Предполагаемая СКУД повышенной безопасности включает следующие компоненты (рис.2):

1) Двери в режимное помещение. Дверь в помещении оснащена датчиком прохода, индикаторами состояния двери, электронным замком и датчиками прохода. Вход осуществляется в автоматическом режиме по предъявлению зарегистрированного ключа. Выход через вторую дверь доступен при закрытой входной двери, для зарегистрированных пользователей осуществляется в автоматическом режиме, а для посетителей с разовыми пропусками при подтверждении оператора доступа к помещению.

2) Считыватель ключей доступа. Устанавливается с двух сторон каждой из дверей. При наличии посетителя внутри внешние считыватели заблокированы.

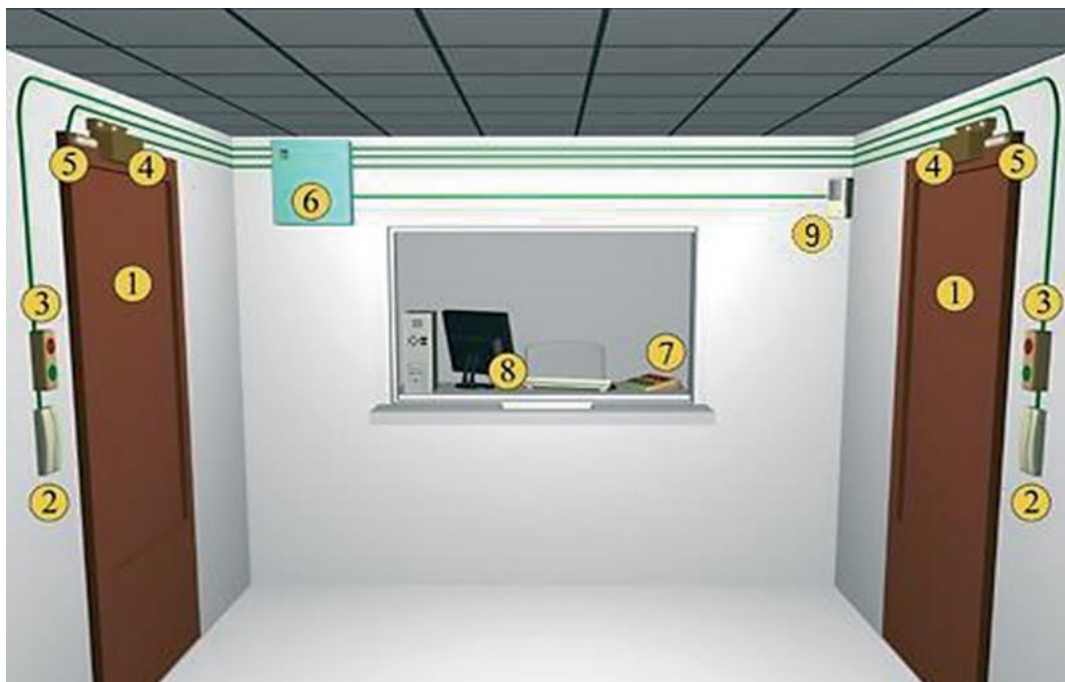


Рис.1. Схема режимного помещения

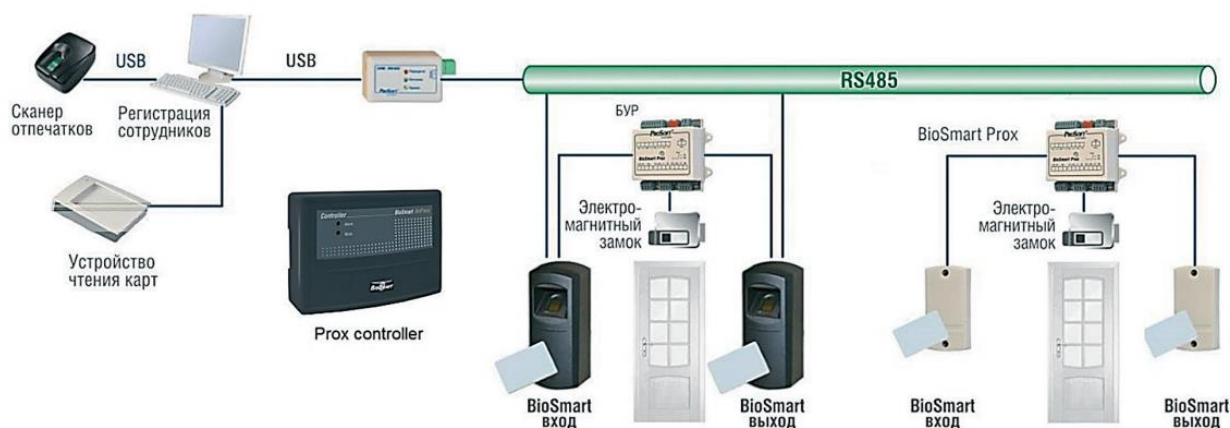


Рис. 2. Структурная схема системы контроля управления доступом

3) Индикатор состояния. Выводит информацию о состоянии замка контроля на двери, показывая тем самым разрешен проход посетителю или нет. После прохода, дверь автоматическим закрывается доводчиком. По срабатыванию магнитоконтактного дверного датчика, замок включается и блокирует дверь.

4) Электромагнитный или электромеханический замок. После входа дверь закрывается доводчиком. При срабатывании магнитно-контактного извещателя двери, замок автоматически блокирует дверь.

5) Датчик открывания двери. Выполняет функцию детектирования прохода в помещение.

6) Контроллер СКУД - центральный элемент управления работой режимного помещения. Выполняет роль связующего элемента необходимого количества считывателей в системе.

7) Пульт ручного предоставления доступа. Дает возможность охраннику предоставлять доступ посетителям по разовым пропускам, не имея постоянного допуска.

8) АРМ оператора. Представляет собой персональный компьютер, с установленным программным обеспечением поставщика оборудования контроля доступом НА него выводится вся необходимая служебная информация, может выполнять роль сервера базы данных.

9) Датчик присутствия. Регистрирует факт нахождения посетителя внутри помещения.

Вывод: В статье предложен эффективный подход к организации системы контроля управления доступом, позволяющий использовать современные компоненты, обеспечивающие надежную защиту охраняемого объекта с целью минимизации программно-аппаратных затрат на реализацию автоматической СКУД.

ЛИТЕРАТУРА

1. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия - Телеком, 2010. – 272 с.: ил.
2. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – М.: Стандартинформ, 2008.
3. Крахмалев А.К. Перспективы развития ИСБ. Платформы интеграции. // SS. Системы безопасности. СПб., 2010, апрель-май. С.146-148.
4. Синилов В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации : учебник для нач. проф. образования / В. Г. Синилов. — 5-е изд., перераб. и доп. — М. : Издательский центр «Академия», 2010. — 512 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Герасименко Евгений Сергеевич.

Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежского института МВД России.

E-mail: jenya35353@yandex.ru

Россия, 394065 г. Воронеж, проспект Патриотов, 53.

Тел. +7-919-241-66-18.

Gerasimenko Evgeny Sergeevich.

Lecturer of the Department of radio engineering systems and complexes of security monitoring.

Voronezh Institute of the Russian interior Ministry

E-mail: jenya35353@yandex.ru

Russia, 394065 Voronezh, prospect Patriots, 53.

Tel. +7-919-241-66-18.

Ключевые слова: система контроля и управления доступом, безопасность, охрана.

Key words: access control and management system, security, security.

УДК 004.03

Голиков Алексей Анатольевич,
кандидат технических наук;
Толстых Ольга Владимировна,
кандидат технических наук

НЕКОТОРЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ В РОССИИ И МИРЕ

SOME ASPECTS OF ROAD SAFETY IN RUSSIA AND THE WORLD

Рассматривая принимаемые во всем мире усилия по обеспечению безопасности на дорогах, сохранению жизни, здоровья людей, материальных ресурсов государственными, общественными и международными институтами, анализируются результаты этой деятельности на территории Российской Федерации.

The results of these activities on the territory of the Russian Federation are analyzed, considering the efforts made all over the world to ensure road safety, preservation of life, human health, material resources by state, public and international institutions.

Человеческая жизнь - величайшая ценность и первоочередная задача любых государственных и международных надгосударственных институтов выявлять и бороться с источниками угроз для неё. Дорожно-транспортный травматизм является одной из 3-х основных причин гибели людей в возрасте от семи до сорока пяти лет. И в случае неприятия действенных и скорейших мер станет по прогнозам ученых, пятой основной причиной смерти на планете, каждый год на более чем два с половиной миллиона человек сокращающей численность населения в мире.

Недостаточное совершенствование стратегий обеспечения дорожной безопасности и планирования землеприродопользования, и в какой-то мере стремительно увеличивающееся количество используемых человечеством транспортных средств, является косвенной причиной этого явления.

Последствия дорожно-транспортных происшествий для экономики государств по разным оценкам составляют один, два процента от совокупного валового национального продукта государств планеты и в денежном выражении достигают величины более тридцати триллионов рублей.

Для дальнейшего развития человечества, плодотворного сотрудничества и процветания на планете, необходимо сокращение смертности и травматизма на автодорогах. Число дорожно-транспортных происшествий не уменьшается, проблемы безопасности дорожного движения растут год от года, увеличивается и количество автотранспорта на дорогах стран по всему миру. И как бы ни улучшали качество жизни по различным направлениям, отрицательную динамику подпитывают именно проблемы дорожно-транспортного травматизма.

И только в начале XXI века под эгидой Организации Объединенных Наций был реализован механизм международного сотрудничества, объединивший международные и государственные организации занимающиеся проблемами безопасности дорожного движения. В сферу глобальной политики эти вопросы попали благодаря кропотливой работе различных международных организаций и институтов Организации Объединенных Наций, собиравших и анализировавших информацию по транспортному травматизму и гибели людей при автоавариях.

Как результат этой работы в марте 2010 г. на сессии Генеральной Ассамблеи Организации Объединенных Наций была принята резолюция «Десятилетие действий по обеспечению безопасности дорожного движения 2011–2020 гг.» (А/64/255).

В результате уже в самих странах участницах, благодаря такому мощному толчку, развернулось движение за сохранение жизни на дорогах путем улучшения дорожной инфраструктуры, пропаганде безопасного поведения на автодорогах и грамотных действий участников дорожного движения при дорожно-транспортных происшествиях. На дорогах нашей страны за 12 месяцев 2018 г. всего совершено 168099 (-0,8%) ДТП, в которых погибло 18214 (-4,6%) и ранено 214853 (-0,2%) человека. В результате в одном из 9 ДТП зарегистрирован погибший.

В 2018 году девять из десяти (88,1%) ДТП в Российской Федерации произошли в результате нарушения Правил дорожного движения (ПДД) водителями транспортных средств. Всего совершено 148142 (+3,3%) таких ДТП, в которых погибло 15279 (-2,5%) и ранено 196653 (+2,6%) человека.

За предыдущий год, как и ранее, основными видами ДТП являлись столкновение транспортных средств (42,3%) и наезд на пешехода (29,1%). Наибольшей тяжестью последствий характеризовались наезд на гужевой транспорт (20,5) и опрокидывание ТС (10,6).

По итогам 2018 года в результате нарушения ПДД водителями ТС произошло 148142 ДТП, в которых погибли 15297 и получили ранения 196653 человека. По сравнению с аналогичным периодом прошлого года при незначительном увеличении количества ДТП на 3,3 % и числа раненых на 2,6%, отмечалось снижение числа погибших на 2,5%.

Увеличились показатели количества ДТП и числа раненых из-за нарушения ПДД водителями, находившимися в состоянии опьянения. Всего совершено 15166 (+1,3%) таких ДТП, в которых погибло 4296 (-0,9%) и ранено 20629 (+1,6%) человек. Тяжесть последствий ДТП составила 17,2.

В 2018 году снизились основные показатели дорожно-транспортной аварийности с участием пешеходов. Количество таких ДТП сократилось на 5,7%, число погибших и раненых – на 8,3% и 5,5% соответственно. Всего совершено 50207 ДТП, в которых погибло 5299 и получили ранения 47144 человека.

Девять из десяти (92,5%) ДТП с участием пешеходов совершено на улицах и дорогах городов и населенных пунктов. В 46441 (-5,1%) таком ДТП погибло 3687 (-6,8%) и ранено 44805 (-5,0%) человек. Тяжесть последствий ДТП составила 7,6, что почти в шесть раз меньше аналогичного показателя на автомобильных дорогах (вне городов и населенных пунктов) (40,8).

За 12 месяцев 2018 года произошло 48814 (-5,8%) наездов на пешеходов, в которых погибло 5155 (-8,5%) и получили ранения 45666 (-5,6%) человек. Более половины (68,4% или 3525 чел.) участников таких ДТП погибло в темное время суток, при этом тяжесть последствий (17,0) в три раза выше аналогичного показателя в светлое время суток (5,4).

Зафиксирован рост всех основных показателей аварийности в результате наезда на пешеходов из-за нарушения ПДД водителями (32966 (+5,5%) ДТП; 2418 (+0,9%) погибли; 32239 (+5,5%) ранены). Тяжесть последствий ДТП составила 7,0.

Более трети (38,9%) всех наездов на пешеходов произошло из-за нарушения ПДД самими пешеходами (18987 ДТП, (-9,0%)), при этом каждое пятое такое ДТП – со смертельным исходом (3455 чел., (-9,7%)). Тяжесть последствий таких ДТП крайне высока (17,8).

Почти треть (28,7%) наездов на пешеходов совершалось на регулируемых пешеходных переходах (5203 ДТП; -5,8%). Стоит отметить, что за отчетный период произо-

шло снижение трех основных показателей аварийности в этих ДТП, особенно числа погибших. В таких ДТП погибло 243 (-19,3%) и ранено 5225 (-4,5%) человек. Более половины (62,7%) из этих ДТП произошло в светлое время суток, при этом тяжесть последствий составила 3,2, что в два раза ниже аналогичного показателя в темное время суток (6,6).

Именно перечисленные дорожно-транспортные происшествия чаще всего становятся скрытыми. И хотя в настоящее время количество скрывшихся с места аварий водителей снизилось почти в два раза, число таких происшествий все еще довольно существенно. Причиной падения общего числа подобных нарушений стало, как считают эксперты: введение европротокола, его широкое применение участниками дорожного процесса. Возможность оформить все необходимые бумаги на дороге без участия сотрудников Госавтоинспекции привлекает с каждым годом все большее количество участников дорожно-транспортных происшествий своей оперативностью и относительной простотой. Потому как, иной раз, дожидаться приезда наряда дорожно-патрульной службы, особенно в «час пик» или на удаленном от мегаполиса участке автодороги, в «глуши», достаточно затратно по времени. А подготовить необходимые документы, так чтобы у страховой компании не возникло оснований отказать в выплате страхового возмещения, можно не только при помощи аварийных комиссаров, но и самостоятельно, изучив этот вопрос на огромном количестве сайтов в сети «Интернет», где подробно описывается список всех необходимых действий, в такой ситуации.

Кроме того законодатели в последнее время регулярно с подачи МВД ужесточают законодательство в области безопасности дорожного движения, в том числе и вводя более суровые меры препятствующие, такому противоправному поведению. Широкое использование получают средства мониторинга транспортных средств, а почти повсеместное использование автолюбителями средств видеофиксации – видеорегистраторов, наличие которых в автомобилях из диковинки давно превратилось в один из обязательных атрибутов. Позволяет на основании записей сделанных участниками дорожного движения не только увидеть наиболее полную картину происшествия, но и по характерным приметам, разыскать виновника дорожно-транспортного происшествия.

Однако остроты проблемы по розыску таких транспортных средств указанные обстоятельства полностью не снимают. И бурно развивающиеся сегодня технические средства обеспечения безопасности дают видимый по результатам анализа эффект.

ЛИТЕРАТУРА

1. Сизоненко А.Б. Специальная техника органов внутренних дел: учебник: часть 1. / А.Б. Сизоненко [и др.]. – Москва : ДГСК МВД России, 2014. – ч.1. – 264с.
2. Рыков С.А., Бурковский В.Л., Голиков А.А. Управление гетерогенными распределенными объектами информационных систем реального времени // монография. Воронеж, 2012. – С. 140.
3. Винокуров С. А. Организация комплексных систем мониторинга объектов охраны/ С.А. Винокуров, С.А. Гречаный, Д.Ю. Калков, М.В. Таравков. – Воронеж: ВИ МВД России, 2018. - 68с.
4. Сайт нцбдд.мвд.рф/ресурсы/обзоры-аварийности

СВЕДЕНИЯ ОБ АВТОРАХ

Голиков Алексей Анатольевич. Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: galexey@yandex.ru

Россия, 394065, г. Воронеж, Проспект Патриотов, 53.

Тел. (473) 200-52-08.

Толстых Ольга Владимировна. Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: tov48@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-08.

Golikov Aleksey Anatolyevich. Senior lecturer of the department of radio engineering systems and complexes of security monitoring. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

E-mail: galexey@yandex.ru

Tel. (473) 200-52-08.

Tolstykh Olga Vladimirovna. Senior lecturer of the department of radio engineering systems and complexes of security monitoring. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: tov48@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-08.

Ключевые слова: безопасность, дорожное движение, мониторинг транспорта.

Key words: safety, traffic, transport monitoring.

УДК 656.09

Данилова Ольга Юрьевна,
кандидат физико-математических наук, доцент;
Попов Алексей Вячеславович

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ПОЛИНОМИАЛЬНЫХ КОДОВ ПРИ ПЕРЕДАЧЕ СООБЩЕНИЙ В ПОДРАЗДЕЛЕНИЯХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

TO THE QUESTION ON THE USE OF POLYNOMIAL CODES WHEN TRANSFERING MESSAGES IN THE UNITS OF INTERNAL AFFAIRS

Информация играет важную роль в современном мире. Поэтому проблема защиты информации становится все более актуальной. Такую защиту можно осуществлять при помощи кодирования. В статье рассматриваются полиномиальные коды, которые являются одним из классов помехоустойчивых кодов, и их применение для кодирования сообщений в подразделениях органов внутренних дел.

Information plays an important role in the modern world. Therefore, the problem of information security is becoming increasingly important. Such protection can be implemented using coding. The article deals with polynomial codes, which are one of the classes of noise-resistant codes, and their application for encoding messages in the departments of the internal affairs bodies.

Введение. В органах внутренних дел кодированию и декодированию информации отводится определённое место. От целостности и правильности переданных данных зависит очень многое: личные данные как граждан, так и сотрудников; планы обороны различных объектов; расположение постов; тактика действий при возникновении чрезвычайных обстоятельств и т.д. С целью защиты информации используются различные методы кодирования, а так же шифрование и стеганография [1] – [3]. Кодирование не только выполняет защитную функцию, но и способствует более удобному использованию данных, упрощает процесс обработки и хранения информации (рисунок 1).

В процессе кодирования отождествляется буквенные или символьные знаки входного кода (сообщения) со знаками или группами знаков выходного кода. Обратной операцией является декодирование [4].

Построение полиномиальных кодов. В данной работе будет рассматриваться один из методов помехоустойчивого кодирования, т.е. кодирования, позволяющего найти и исправить ошибки, возникающие при передаче и декодировании исходного сообщения.

Комбинации, используемые в исходном коде, называют разрешенными, а неиспользуемые – запрещенными. Число разрешенных комбинаций принято называть «мощностью кода».

Основной задачей помехоустойчивого кодирования является подбор определенного количества разрешенных комбинаций с достижением наименьшей избыточности. Большая избыточность увеличивает время передачи сообщения, приводит к большим энергозатратам и усложнению обрабатывающих устройств (кодеров/декодеров).



Рис. 1. Кодирование информации с целью обеспечения информационной безопасности

Полиномиальные коды, которые мы будем рассматривать в данной работе, относятся к числу блочных кодов, схема которых представлена на рисунке 2.

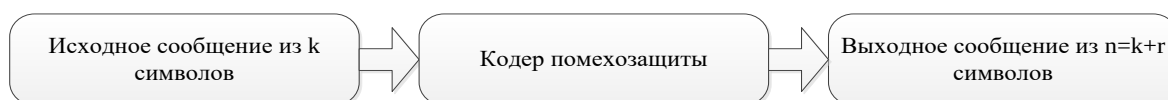


Рис. 2. Схема блочного кодирования

Из схемы видно, что в выходном сообщении присутствует переменная r , обозначающая число проверочных символов, не несущих информации, но служащих для поиска и исправления ошибок в исходном сообщении.

Полиномиальный код в свою очередь является разновидностью линейных кодов, называемой циклическими кодами. Относятся полиномиальные коды к семейству помехоустойчивых кодов. За счет их использования обеспечивается более гибкая реализация кодов со способностью исправления и обнаружения ошибок.

Основное свойство: если последовательность символов $(a_1 a_2 \dots a_{n-1} a_n)$ является разрешенной комбинацией этого кода, то и любая последовательность, полученная из нее циклической перестановкой символов $(a_2 a_3 \dots a_{n-1} a_n a_1)$, является также разрешенной комбинацией [2].

Данное свойство обуславливается тем, что символы строки порождающей матрицы кода могут быть получены циклическим сдвигом одной комбинации (образующей).

Так для кодовой комбинации 110101 циклический сдвиг выглядит следующим образом:

$$110101 \rightarrow 101011 \rightarrow 010111 \rightarrow 101110 \rightarrow 011101 \rightarrow 111010. \quad (1)$$

С помощью представления данной двоичной последовательности в виде полинома (многочлена) переменной x можно будет удобно произвести математическое описание циклического сдвига.

Приведенной комбинации будет соответствовать многочлен, который носит название образующий (порождающий):

$$P(x)=1 \cdot x^5+1 \cdot x^4+0 \cdot x^3+1 \cdot x^2+0 \cdot x^1+1 \cdot x^0=x^5+x^4+x^2+1. \quad (2)$$

Представление бинарной последовательности в виде многочленов необходимо для проведения математических операций над кодовыми комбинациями (умножение, деление, сложение и вычитание по модулю два).

Рассматриваются два случая: когда необходимо осуществить перенос 0 или 1. В первом случае циклический сдвиг происходит посредством умножения многочлена $P(x)$ на переменную x , причем важно отметить, что при переносе единицы степень многочлена не превысит допустимое значение $(n-1)$, где n -порядок многочлена.

Задан код:010111. В таком случае $P(x) \cdot x = x(x^4+x^2+x+1) = x^5+x^3+x^2+x \rightarrow 101110$.

Если же необходимо осуществить перенос 1, то при умножении на x будет превышено допустимое значение.

Если задан код 110101, то $P(x) \cdot x = x(x^5+x^4+x^2+1) = x^6+x^5+x^3+x$. Как видно из полученной формулы, x^6 превышает допустимый порядок многочлена $(n-1)$. В таком случае возникает необходимость замены x^6 на $x^0=1$. Это может быть достигнуто посредством сложения по модулю два полученного многочлена с $x^n+1=x^6+1$.

С учетом того, что $x^6 \oplus x^6 = x^6(1 \oplus 1) = x^6 \cdot 0 = 0$, следует:

$$(x^6+x^5+x^3+x) \oplus (x^6+1) = x^5+x^3+x^1+1 = 1 \cdot x^5+0 \cdot x^4+1 \cdot x^3+0 \cdot x^2+1 \cdot x^1+1 \cdot x^0 \rightarrow 101011,$$

что соответствует второй комбинации, указанной в (1).

Такой же результат будет получен, если найти остаток от деления полученного многочлена на $x^n+1 \rightarrow (x^6+x^5+x^3+x) \bmod (x^6+1) = x^5+x^3+x^1+1$.

Формулировка правила циклического сдвига звучит [5]: для произведения циклического сдвига на i разрядов необходимо умножить многочлен комбинации на x^i и выполнить приведение получившегося результата по модулю (x^n+1) .

Широкое применение полиномиальных кодов в помехоустойчивом кодировании обуславливается важнейшим свойством: многочлены, соответствующие всем разрешенным кодовым комбинациям, должны делиться без остатка на образующий многочлен $P(x)$. Обнаружение ошибок происходит по наличию остатка при делении многочлена искаженной кодовой комбинации на порождающий многочлен. Исправление возникающих ошибок производится по виду синдрома (остатка от деления).

Улучшение корректирующей способности достигается увеличением числа синдромов при делении. Доказано, что максимальное количество остатков будет образовываться в случае, когда многочлен степени g является неприводимым (делящимся только на себя и единицу). При его выборе учитываются требования к количеству остатков, которые он дает. Это необходимо для того, чтобы каждой ошибке соответствовал свой синдром. Данные многочлены представлены в таблицах, приведенных в справочных источниках.

Существует несколько способов кодирования: несистематическое циклическое кодирование, систематическое циклическое кодирование.

В первом случае, чтобы закодировать сообщение 110101, $A(x)=x^5+x^4+x^2+1$, необходимо использовать формулу:

$$B(x) = A(x) \cdot P(x), \quad (3)$$

где $P(x)$ – образующий многочлен, $B(x)$ – выходная комбинация.

Должно обязательно соблюдаться условие: $m+r < n$ ($m=k-1$ – порядок информационного многочлена, r – порядок образующего многочлена, n – количество символов в выходном сообщении).

В приведенном случае $m=5$, $r=3$, $n>3+5 \rightarrow n=9$.

Выберем образующий многочлен из перечня: $P(x) = x^3 + x^2 + 1$ (1101).

Теперь необходимо найти произведение многочленов:

$$x^5 + x^4 + 0 + x^2 + 0 + 1 \otimes x^3 + x^2 + 0 + 1 = x^8 + 0 + x^6 + 0 + 0 + x^3 + 0 + 0 + 1.$$

На выходе получается комбинация: 101001001, где подчеркнутые символы являются проверочными. Суть несистематического кодирования заключается в том, что их расположение в коде не является закономерным.

Во втором случае проверочные символы будут располагаться непосредственно после информационных и будут, соответственно, иметь наименьшие степени. Правило систематического кодирования можно описать формулой:

$$B(x) = x^r \cdot A(x) + R(x), \quad (4),$$

где $R(x)$ – остаток от деления $\frac{x^r \cdot A(x)}{P(x)}$.

Как и в первом случае закодируем комбинацию: $110101 \rightarrow A(x) = x^5 + x^4 + x^2 + 1$. Так как $r=3$, то $x^r \cdot A(x) = x^3(x^5 + x^4 + x^2 + 1) = x^8 + x^7 + x^5 + x^3$. Разделим на образующий многочлен $P(x) = x^3 + x^2 + 1$. В результате получим: $R(x) = x^2 + 1$. По формуле (4) найдем искомым многочлен: $B(x) = x^8 + x^7 + x^5 + x^3 + x^2 + 1 \rightarrow 110101101$. Три последних символа являются проверочными. Если при делении данной комбинации в остатке получается 0, значит она является разрешенной, и сообщение закодировано правильно.

Выводы. Полиномиальные коды широко применяются [6] на самых разных уровнях систем управления, обладают способностью к обнаружению и исправлению как однократных, так и многократных независимых ошибок. Их использование позволяет передавать информацию по системам передачи данных с большей надежностью, что является необходимым, особенно в структуре органов внутренних дел. Могут использоваться в протоколах Ethernet, ModBus, FlexRay. Помимо этого, обеспечивают более удобное хранение информации самых различных форматов (PNG, SCSI, MPEG-2 и т.д) и ее декодирование.

ЛИТЕРАТУРА

1. Бабаши А. В., Шанкин Г. П. Криптография. – М. : Солон-Р, 2002. – 512 с.
2. Зубов А. Ю. Совершенные шифры. – М. : Гелиос, 2003. – 160 с.
3. Данилова О.Ю., Думачев В.Н. Математические основы криптографии: учебник – Воронеж: ВИ МВД России. — 2017. — 301 с.
4. Стримова Н. С. Информационная безопасность, кодирование и декодирование данных // Молодой ученый. — 2018. — №39. — С. 16-20.
5. Понятов А.А. Теория информации и кодирования: учебное пособие / А.А. Понятов. – Москва : МИИТ, 2010. – 188 с.
6. Сапожников В.В. Полиномиальные коды в системах функционального контроля комбинационных логических схем // В.В. Сапожников, Д.В. Ефанов, Р.Б. Абдуллаев [Электронный ресурс]. – URL: <http://kitidis.tsu.ru/icam/data/uploads/abstracts/c/c38.pdf> (дата обращения 24.02.2019).

СВЕДЕНИЯ ОБ АВТОРАХ

Данилова Ольга Юрьевна. Доцент кафедры математики и моделирования систем. Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

Тел. 8-960-010-0569.

E-mail: danilova_olga@hotmail.com.

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-13.

Попов Алексей Вячеславович. Курсант.

Воронежский институт МВД России.

Тел. 8-960-010-0569.

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-13.

Danilova Olga Yur'evna. Assistant professor of the chair of mathematics and modeling systems. Candidate of physical and mathematical sciences, assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-13.

Popov Aleksey Vaycheslavovich. Cadet.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-13.

Ключевые слова: кодирование, декодирование, помехоустойчивое кодирование, полиномиальные коды.

Key words: encoding, decoding, error control coding, polynomial codes.

УДК 004.056.55

Дровникова Ирина Григорьевна,
доктор технических наук, доцент;
Арутюнова Валентина Игоревна,
кандидат технических наук;
Алфёров Владимир Павлович

**АНАЛИТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ
ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ
СВЕДЕНИЙ ПРИ РЕАЛИЗАЦИИ СЛАБО УЯЗВИМОГО РАЗГРАНИЧЕНИЯ
ДОСТУПА К ИНФОРМАЦИОННОМУ РЕСУРСУ СИСТЕМ ЭЛЕКТРОННОГО
ДОКУМЕНТООБОРОТА**

**AN ANALYTICAL MODEL EVALUATING THE PERFORMANCE OF THE
SUBSYSTEM OF PROTECTION OF CONFIDENTIAL INFORMATION WHEN
IMPLEMENTED POORLY AFFECTED ACCESS TO INFORMATION RESOURCES
ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS**

В статье предложена аналитическая модель комплексной оценки эффективности функционирования подсистемы защиты конфиденциальных сведений, являющейся объектом управления слабо уязвимым разграничением доступа штатных пользователей к информационному ресурсу систем электронного документооборота. Для комплексной оценки используется полумарковская модель, разработанная на основе графовой формализации динамики функционирования подсистемы защиты конфиденциальных сведений.

In the article the analytical model of complex estimation of efficiency of functioning of the subsystem of protection of confidential information which is the object of weakly vulnerable access control of regular users to an information resource of systems of electronic document flow is offered. The semi-Markov model developed on the basis of graph formalization of dynamics of functioning of a subsystem of protection of confidential data is used for a complex assessment.

Для решения задач комплексной оценки эффективности мероприятий по управлению слабо уязвимым разграничением доступа (РД) к информационному ресурсу (ИР) системы электронного документооборота (СЭД) в [1] разработана система показателей эффективности функционирования подсистемы защиты конфиденциальных сведений (ПЗКС). Математическое обеспечение оценки данных показателей заключается в разработке аналитической модели комплексной оценки эффективности функционирования ПЗКС, осуществляемой путём использования комплексного показателя. Оценка комплексного показателя производится через элементарные показатели, подразделяемые на качественные (показатель функциональности ПЗКС E_f , показатель эксплуатируемости ПЗКС E_o) и количественный (показатель своевременности реализации защиты ИР (ЗИР) E_c).

Характеризующие эффективность параметры E_f , E_o оцениваются с помощью проведения анализа имеющейся технической документации на программный продукт ПЗКС на основе использования качественной шкалы, позволяющей производить символическую лингвистическую оценку и, соответственно, вводить булеву независимую переменную.

Методика расчёта параметра E_c базируется на моделировании функционирования ПЗКС в реальном времени, которую можно представить, как систему массового

обслуживания [2]. Функционирование ПЗКС в режиме реального времени математически описывается на основе аппарата сетей Петри [3]. Поскольку время реализации ПЗКС защитных функций лежит в основе своевременности реализации функций ЗИР в СЭД, то в соответствии с [1] показатель E_c предлагается определять по формуле:

$$E_c = P(\tau_c \leq \tau_{\max c}), \quad (1)$$

где: τ_c — время реализации защитных функций ПЗКС; $\tau_{\max c}$ — максимально допустимое значение указанного времени (представляет собой случайно распределённую величину, аппроксимируемую экспоненциальным законом распределения со средним значением τ_m).

Параметр E_c удобно вычислять с использованием количественной шкалы для осуществления оценки с помощью действительных чисел 0 или 1.

Для того, чтобы оценить параметр E_c применимо выражение (1) с использованием графовой формализации процесса функционирования ПЗКС и разработанной на её основе полумарковской модели [4]. Используемая модель может быть описана с помощью конечного полумарковского процесса (КПМП) [5], вход в исходное и конечное состояния которого ассоциируются с обращением к ПЗКС и завершением решения подсистемой функциональных задач по конкретному обращению соответственно. Вычисление интервально-переходных вероятностей КПМП следует рассматривать в качестве основной задачи его анализа [6].

Характеризующий процесс функционирования ПЗКС КПМП можно описать с помощью полумарковской матрицы для проведения оценки параметра E_c :

$$H_c(\tau) = \|H_{cij}(\tau)\|, \quad i = \overline{1, n}, \quad j = \overline{1, n} \quad (2)$$

где $H_{cij}(\tau)$ — случайный элемент матрицы, описывающий вероятность перехода КПМП из состояния i в состояние j за промежуток времени, меньший τ .

Вычисление $H_{cij}(\tau)$ осуществляется по формуле:

$$H_{cij}(\tau) = p_{cij} G_{ci}(\tau), \quad i = \overline{1, n}, \quad (3)$$

где: p_{cij} — вероятности перехода КПМП из состояния i в состояние j ; $G_{ci}(\tau)$ — функции распределения времени нахождения КПМП в состоянии i .

Для определения вероятностей p_{cij} и $G_{ci}(\tau)$ при $i = \overline{1, n}, \quad j = \overline{1, n}$ целесообразно применение разрешающих процедур и процедур временной задержки переходов сети Петри, формально описывающей процесс функционирования ПЗКС в его динамике. При осуществлении комплексной оценки эффективности функционирования ПЗКС используются, как правило, стандартные законы распределения функций $G_{ci}(\tau)$, однако изначально отсутствует информация о точных значениях вероятностей p_{cij} , поэтому заранее известными следует считать лишь их предварительные значения. Результаты, полученные путём статистической обработки данных о параметрах реализации ПЗКС защитных функций в процессе решения сервисных задач в СЭД, позволяют осуществить коррекцию значений данных вероятностей.

Параметр E_c , позволяющий описать вероятностно-временные характеристики (ВВХ) процесса функционирования ПЗКС в его динамике, может рассматриваться как вероятность КПМП вовремя достичь конечного состояния. Поэтому в качестве основы исследования ВВХ динамики функционирования ПЗКС следует использовать систему уравнений полных вероятностей перехода КПМП из произвольных состояний в конечное состояние в течение временного интервала, меньшего τ [6]:

$$Q_{c\ i}(\tau) = p_{c\ in} \cdot G_{c\ i}(\tau) + \sum_{j=1}^{n-1} p_{c\ ij} \cdot G_{c\ i}(\tau) * Q_{c\ j}(\tau), \quad i = \overline{1, n-1}, \quad (4)$$

где $Q_{ci}(\tau)$ — имеющий вероятностный характер параметр, характеризующий возможность КППП перейти из состояния i в конечное состояние n за промежуток времени, меньший τ .

Построенная система интегральных уравнений (4) является результатом анализа системы уравнений интервально-переходных вероятностей КППП, формализовано описывающего процесс функционирования ПЗКС в его динамике, и раскрывает взаимосвязь ВВХ отдельных состояний КППП с ВВХ всего процесса в целом.

Использование преобразований Лапласа [7] позволяет упростить систему уравнений (4) для производящих функций путём преобразования её из интегральной в алгебраическую [6]:

$$q_{ci}(v) = p_{cin} \cdot g_{ci}(v) + \sum_{j=1}^{n-1} p_{cij} \cdot g_{ci}(v) * Q_{cj}(v), \quad i = \overline{1, n-1}, \quad (5)$$

где: $q_{ci}(\nu), g_{ci}(\nu)$ — преобразования Лапласа для производящих функций $Q_i(\tau)$ и $G_i(\tau)$ соответственно.

Применительно к полумарковской матрице $H_{cij}(\tau)$ используется следующее выражение для расчёта преобразования Лапласа её элементов:

$$h_{c\bar{ij}}(\nu) = p_{c\bar{ij}} \cdot q_{ci}(\nu). \quad (6)$$

Рассмотрим алгоритм расчёта величины $g_{ci}(v)$ для типовых распределений времени нахождения ПЗКС в состоянии i [7].

Если время пребывания ПЗКС в состоянии i случайным образом распределено в пределах интервала $[a_i; b_i]$ равномерно, то имеем:

$$g_{ci}(\nu) = \frac{\exp(-a_i \nu)[1 - \exp(-b_i \nu)]}{b_i \nu}. \quad (7)$$

При использовании экспоненциального закона распределения для описании времени пребывания ПЗКС в состоянии i со средним значением b_i величина $g_{ci}(\nu)$ может рассчитываться по формуле:

$$g_{ci}(v) = \frac{1}{1 + b_i v}. \quad (8)$$

В случае использования нормально распределённой случайной величины со средним значением μ_i и малой дисперсией σ_i^2 для описания времени нахождения ПЗКС в состоянии i значение $q_{ci}(\nu)$ может быть рассчитано по формуле:

$$g_{ci}(v) = \exp(-\mu_i v + \frac{1}{2} \sigma_i^2 v^2) \quad (9)$$

Приняв $h_{ij} = h_{cij}(\nu)$, $q_i = q_{ci}(\nu)$ и с учётом (6) преобразуем систему уравнений (5) к следующему виду:

[illegible]

Для решения системы уравнений (10) целесообразным является использование метода исключения Гаусса в том случае, если «ведущие» коэффициенты уравнений не принимают нулевых значений [6]. Такое ограничение выполняется для представленной системы уравнений, поскольку при $i = \overline{1, n-1}$ $h_{ji} < 1$, а следовательно, коэффициенты

Осуществив деление каждого члена 1-го уравнения на коэффициент $(1 - h_{11})$, получим приведённое уравнение:

где: $h_{1,j}^{(1)} = \frac{h_{1,j}}{1-h_{1,1}}$, $j = \overline{2, n}$.

В результате получаем следующую систему уравнений:

$$\text{где: } h_{i,j}^{(1)} = h_{i,j} + h_{i+1} h_{i,j}^{(1)}, \quad i = \overline{2, n-1}, \quad j = \overline{2, n}. \quad (13)$$

В результате многократного проведения описанных преобразований получим следующую систему приведённых уравнений:

$$\text{где: } h_{k,j}^{(k)} = \frac{h_{k,j}^{(k-1)}}{1 - h_{k,k}^{(k-1)}}, \quad h_{i,j}^{(k)} = h_{i,j}^{(k-1)} + h_{i,k}^{(k-1)} h_{k,j}^{(k)}, \quad h_{ij}^{(0)} = h_{ij}, \quad k = \overline{1, n-1}, \quad i = \overline{k+1, n-1}, \quad j = \overline{k+1, n}. \quad (15)$$

$$\left\{ \begin{array}{l} q_{n-1}=h_{n-1,n}^{(n-1)}; \\ q_{n-2}=h_{n-2,n}^{(n-2)}+h_{n-2,n-1}^{(n-2)}q_{n-1}; \\ \\ q_1=h_{1,n}^{(1)}+h_{1,n-1}^{(1)}q_{n-1}+h_{1,n-2}^{(1)}q_{n-2}+...+h_{1,2}^{(1)}q_2. \end{array} \right. \quad (16)$$
$$E_c = q_{c1}(\nu_m), \quad (17)$$

(максимальное значение) $\tau_{\max c}$; τ_m — математическое ожидание $\tau_{\max c}$.

237

зована характеристика v_m , будем придерживаться следующей методики определения указанного параметра: на первом этапе осуществляется процедура вычисления $g_i(v_m)$ по формулам (7) — (9), на втором этапе — величины $h_{ij}(v_m)$ согласно выражению (6), на третьем — коэффициентов системы уравнений (14) с использованием формулы (15). Окончательный расчёт параметра E_c , определённого (17), вычисляется на основе (16), учитывая, что $v = v_m$.

Максимальную величину любого из рассчитанных параметров можно воспринимать как оптимальное значение качества функционирования ПЗКС по данному вычисляемому параметру.

При проведении процедуры комплексной оценки эффективности эксплуатации ПЗКС в качестве управляемого объекта слабо уязвимым РД необходимо использовать комплексный параметр E_k , интегрирующий частные параметры эффективности.

Для определения интегрального E_k необходимо проанализировать частные параметры эффективности функционирования ПЗКС. Поскольку качественные показатели E_ϕ и E_γ являются булевыми значимыми переменными их не рекомендуется использовать как интегральный параметр, учитывая их ограничения:

$$E_\phi = 1; E_\gamma = 1, \quad (18)$$

которые представляют собой единое ограничение:

$$E_\phi \wedge E_\gamma = 1. \quad (19)$$

Методика расчёта параметра E_c приведена ниже. Общие требования, предъявляемые к оперативности СЭД, имеют ограничение на эксплуатацию ПЗКС, которое можно распространить и на E_c :

$$E_c \geq E_{\min c}, \quad (20)$$

где $E_{\min c}$ — наименьшее значение E_c , определённое требованиями к ПЗКС от несанкционированного доступа в технической документации на эксплуатацию СЭД.

Таким образом, окончательное выражение для вычисления интегрального параметра эффективности функционирования ПЗКС может быть представлено в виде:

$$E_k = \begin{cases} E_c, & \text{если } (E_c \geq E_{\min c}) \wedge E_\phi \wedge E_\gamma = 1, \\ 0, & \text{иначе.} \end{cases} \quad (21)$$

Выше изложенное позволяет сделать вывод о том, что разработана математическая модель для оценки показателей эффективности эксплуатации ПЗКС как объекта управления процессом слабо уязвимого РД штатных пользователей к ИР в СЭД. Комплексная оценка эффективности эксплуатации ПЗКС адекватна оценке показателя своевременности реализации ЗИР при допущении, что значение показателя E_c не будет меньшим фиксированного значения $E_{\min c}$, а оставшиеся имеющиеся частные элементарные параметры являются допустимыми. При оценке параметра E_c использована полумарковская модель, созданная на базе формальной модели динамики эксплуатации ПЗКС в СЭД в режиме реального времени.

ЛИТЕРАТУРА

1. Дровникова И.Г. Моделирование оценки эффективности функционирования подсистемы защиты конфиденциальных сведений систем автоматизированного документооборота / И.Г. Дровникова, В.П. Алфёров // Общественная безопасность, законность и правопорядок в III тысячелетии: сб. ст. Междунар. науч.-практич. конф. (Воронеж, 27 июня 2018 г.). — В. 4. — Ч. 2. — 2018. — С. 32-35.

2. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного до-

кументооборота: монография / И.И. Застрожных [и др.]. — Воронеж: Воронеж. гос. техн. ун-т, 2015. — 106 с.

3. Мараховский В.Б. Моделирование параллельных процессов. Сети Петри / В.Б. Мараховский, Л.Я. Розенблюм, А.В. Яковлев. — СПб.: Профессиональная литература, 2014. — 400 с.

4. Рогозин Е.А. Разработка модели функционирования типовой системы защиты информации от несанкционированного доступа на основе теории графов с конечным числом состояний / Е.А. Рогозин, А.Д. Попов, В.В. Конобеевских // Проблемы обеспечения надёжности и качества приборов, устройств и систем: межвуз. сб. науч. тр. — Воронеж: ВГТУ, 2017. — С. 34-40.

5. Королук В.С. Полумарковские процессы и их приложения / В.С. Королук, А.Ф. Турбин. — Киев: Наукова думка, 1976. — 184 с.

6. Авсентьев О.С. Методика управления защитой информационного ресурса системы электронного документооборота / О.С. Авсентьев, И.Г. Дровникова, И.И. Застрожных, А.Д. Попов, Е.А. Рогозин // Труды СПИИРАН. № 2 (57) (2018). — С.-Пб.: СПИИРАН, 2018. — 2018. — № 2(57). — С. 188-210. — DOI 10.15622/sp.57.8.

7. Глушко А.В. Преобразование Лапласа. Свойства и применения: пособие по спецкурсу / А.В. Глушко, В.П. Глушко. — Воронеж: ВГУ, 2004. — 59 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Дровникова Ирина Григорьевна. Профессор кафедры автоматизированных информационных систем ОВД. Доктор технических наук, доцент.

Воронежский институт МВД России.

E-mail: idrovnikova@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2005-182.

Арутюнова Валентина Игоревна. Преподаватель кафедры автоматизированных информационных систем ОВД. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: avi1101@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2005-189.

Алфёров Владимир Павлович. Соискатель кафедры конструирования и производства радиоаппаратуры.

Воронежский государственный технический университет.

E-mail: alferov_vladimir@mail.ru

Россия, 394066, Воронеж, Московский пр-т, д. 179, к. 3.

Тел. (473) 2437-706.

Drovnikova Irina Grigorevna. Professor of the chair of information systems in interior affairs department. Doctor of sciences (techniques), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: idrovnikova@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-182.

Arutynova Valentina Igorevna. Teacher of the chair of information systems in interior affairs department. Candidate of sciences (techniques).

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: avi1101@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-189.

Alferov Vladimir Pavlovich. Applicant of design and manufacture of radio equipment department.

Voronezh State Technical University.

E-mail: alferov_vladimir@mail.ru

Work address: Russia, 394065, Voronezh, Moscow Avenue, 179, h. 3.

Tel. (473) 2437-706.

Ключевые слова: система электронного документооборота, подсистема защиты конфиденциальных сведений, слабоуязвимое разграничение доступа, сети Петри, вероятностно-временные характеристики, конечные полумарковские процессы, преобразование Лапласа, метод Гаусса.

Key words: electronic document management system, the subsystem of protection of confidential information, weakly vulnerable access control, Petri nets, probabilistic-temporal characteristics, finite semi-Markov processes, Laplace transformation, Gauss method.

УДК 621.3

Дровникова Ирина Григорьевна,
доктор технических наук, доцент;
Алфёров Владимир Павлович

АЛГОРИТМИЗАЦИЯ ОЦЕНКИ ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

ALGORITHMIC ESTIMATING THE EFFECTIVENESS OF THE SUBSYSTEM OF PROTECTION OF SENSITIVE INFORMATION SYSTEM ELECTRONIC DOCUMENT CIRCULATION

Рассматриваются вопросы алгоритмизации оценки эффективности функционирования подсистемы защиты конфиденциальных сведений при реализации разграничения доступа пользователей к программно-информационному ресурсу системы электронного документооборота. Приводится схема алгоритма оценки показателя своевременности реализации защиты информационного ресурса.

The article deals with the algorithmization of evaluation of the effectiveness of the subsystem of protection of confidential information in the implementation of the differentiation of user access to the program-but-information resource of the electronic document management system. The scheme of the algorithm for assessing the timeliness of the implementation of information resource protection.

Для формирования программного обеспечения (ПО) оценки эффективности мероприятий по автоматизированному управлению разграничением доступа (РД) пользователей к программно-информационному ресурсу (ПИР) системы электронного документооборота (СЭД) необходимо разработать алгоритмы оценки элементарных (E_{Φ} —

показатель функциональности; E_c — показатель своевременности реализации защиты ИР (ЗИР); E_o — показатель эксплуатируемости) и комплексного показателей эффективности функционирования подсистемы защиты конфиденциальных сведений (ПЗКС). Комплексная оценка эффективности функционирования ПЗКС приравнивается к оценке количественного показателя E_c при условии, что его величина не меньше заданной $E_{\min c}$, а качественные показатели E_ϕ и E_o — допустимы [1].

Алгоритм оценки E_c представлен на рисунке 1. Здесь искомую величину E_c будем рассматривать в качестве вероятности своевременного достижения конечным полумарковским процессом (КПМП), моделирующим динамику функционирования ПЗКС, своего поглощающего состояния.

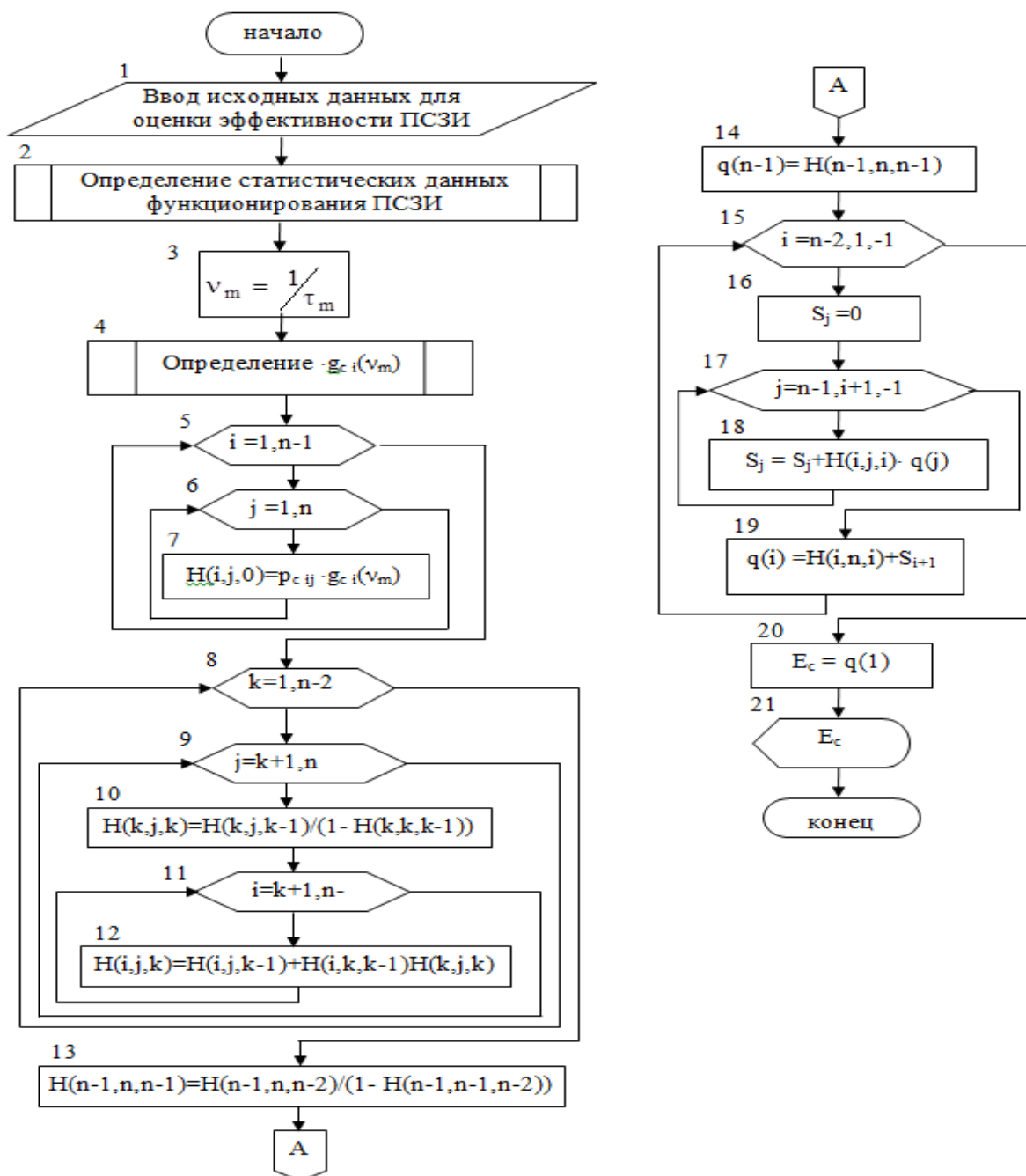


Рис. 1. Схема алгоритма оценки показателя своевременности реализации ЗИР

Указанный КППП однозначно может быть определён переменными p_{cij} и функциями $G_{ci}(\tau)$. При этом введём следующие обозначения: p_{cij} — вероятности перехода КППП из состояния i непосредственно в состояние j , если выполняется условие, что данный КППП оказался в состоянии i ; $G_{ci}(\tau)$ — функции распределения времени нахождения КППП в состоянии i ; $i = \overline{1, n}$, $j = \overline{1, n}$.

Состояние КППП, обозначенное 1, будем считать начальным, а состояние, обозначенное n — поглощающим. При выполнении условия $p_{cij} > 0$ функции $G_{ci}(\tau)$ могут однозначно определяться параметрами и идентификаторами законов распределения, при невыполнении условия $G_{ci}(\tau) = 0$. Рассмотрим содержание блоков схемы, представленной на рисунке 1.

Блок 1. Ввод исходных данных для оценки эффективности функционирования ПЗКС:

1) z_{ci} — идентификаторы закона распределения времени нахождения в состоянии i КППП, формализующего динамику функционирования ПЗКС с целью определения показателя своевременности реализации ЗИР. Указанные идентификаторы обозначим следующим образом: «Р» (для равномерного закона распределения), «Н» (для нормального закона); «Э» (для экспоненциального закона). В данном случае аппроксимация другими законами не рассматривается, хотя, следует отметить, что возможности метода не ограничиваются лишь перечисленными законами распределения;

2) τ_m — среднее значение максимально допустимого времени реализации ПЗКС своих защитных функций (устанавливается администратором ЗИР в соответствии с разделом программной документации на СЭД «Требования к подсистеме ЗИР от несанкционированного доступа (НСД)»);

3) (M, S_m, t_m) , $m = \overline{1, M}$ — список, сформированный подсистемой регистрации и учёта, (M — число зарегистрированных переходов ПЗКС между двумя произвольными состояниями, S_m — состояние, в которое перешла ПЗКС во время m -го перехода за время t_m).

Блок 2. Вычисление статистических данных функционирования ПЗКС как текущих оценок параметров переходных процессов ПЗКС. Введём следующие обозначения: p_{cij} — переходные вероятности (без учёта закона распределения); a_i , b_i — минимальное и максимальное значения времени нахождения КППП в состоянии i (при использовании равномерного закона распределения); μ_i , σ_i — среднее значение и среднее квадратическое отклонение времени нахождения КППП в состоянии i (при использовании нормального закона); b_i — среднее значение времени нахождения КППП в состоянии i (при использовании экспоненциального закона). Алгоритм текущих оценок параметров переходных процессов ПЗКС рассмотрен в [2, 3].

Блок 3. Вычисление параметра v_m по формуле $v_m = 1/\tau_m$.

Блок 4. Вычисление значений $g_{ci}(v_m)$ в точке $v = v_m$ преобразования Лапласа функции $G_{ci}(\tau)$ с учётом равномерного, нормального и экспоненциального законов распределения времени нахождения КППП в состоянии i . Алгоритм оценки значений функции $g_{ci}(v_m)$ для выше указанных законов распределения времени нахождения КППП в состоянии i рассмотрен в [2-4].

Блок 5. Начало цикла по параметру i вычисления значений функции $h_{cij}(v_m)$ преобразования Лапласа элементов полумарковской матрицы $H_{cij}(\tau)$, где $H_c(\tau) = \|H_{cij}(\tau)\|$, $i = \overline{1, n}$, $j = \overline{1, n}$ описывает КППП, моделирующий динамику функционирования ПЗКС с целью оценки показателя E_c .

Блок 6. Начало цикла по параметру j вычисления значений функции $h_{cij}(v_m)$ преобразования Лапласа элементов полумарковской матрицы $H_{cij}(\tau)$.

Блок 7. Вычисление значений функции $h_{cij}(v_m)$ в точке $v = v_m$ преобразования Лапласа элементов полумарковской матрицы $H_{cij}(\tau)$ для произвольных состояний i, j КППМ с использованием формулы $h_{cij}(v) = p_{cij} \cdot g_{ci}(v)$.

Блок 8. Начало цикла по параметру k вычисления значений коэффициентов системы приведённых уравнений для производящих функций [5].

Блок 9. Начало цикла по параметру j вычисления значений коэффициентов системы приведённых уравнений для производящих функций [5].

Блок 10. Вычисление значений коэффициентов $h_{k,j}^{(k)}$ системы приведённых уравнений для производящих функций при произвольных значениях параметров k, j , $k=\overline{1, n-2}$, $j=\overline{k+1, n}$.

Блок 11. Начало цикла по параметру i вычисления значений коэффициентов системы приведённых уравнений для производящих функций [5].

Блок 12. Вычисление значений коэффициентов $h_{i,j}^{(k)}$ системы приведённых уравнений для производящих функций при различных значениях параметров k, i, j , $k=\overline{1, n-2}$, $i=\overline{k+1, n-1}$, $j=\overline{k+1, n}$.

Блок 13. Вычисление значений коэффициентов $h_{n-1,n}^{(n-1)}$ системы приведённых уравнений для производящих функций [5].

Блок 14. Вычисление значения функции $q_{c\ n-1}(v_m)$ в точке $v = v_m$ преобразования Лапласа функции $Q_i(\tau)$ для $(n-1)$ -го состояния КППМ, присваивая ему значение коэффициента $h_{n-1,n}^{(n-1)}$, рассчитанного в блоке 13.

Блок 15. Начало цикла по параметру i вычисления значений функции $q_{ci}(v_m)$ в точке $v = v_m$ преобразования Лапласа функции $Q_i(\tau)$ из системы приведённых уравнений для производящих функций [5].

Блок 16. Начальное присвоение промежуточной функции S_j значения 0, используя все значения j ($S_j = 0$).

Блок 17. Начало цикла по параметру j вычисления значений промежуточной функции S_j .

Блок 18. Вычисление значений промежуточной функции S_j при произвольных значениях параметра j .

Блок 19. Вычисление значений функции $q_{ci}(v_m)$ в точке $v = v_m$ преобразования Лапласа функции $Q_i(\tau)$ из системы приведённых уравнений для производящих функций при произвольных значениях параметра i .

Блок 20. Вычисление величины показателя E_c , присваивая ей значения функции $q_{c\ 1}(v_m)$.

Блок 21. Вывод искомого значения E_c на дисплей администратора ЗИР.

Таким образом, разработан алгоритм оценки показателя своевременности реализации ЗИР E_c , который может служить основой для дальнейшего формирования ПО количественной оценки элементарного показателя эффективности функционирования ПЗКС как объекта управления РД, обеспечивающего возможность оценки эффективности мероприятий по управлению РД штатных пользователей к ПИР СЭД.

ЛИТЕРАТУРА

1. Дровникова И.Г. Моделирование оценки эффективности функционирования подсистемы защиты конфиденциальных сведений систем автоматизированного документооборота / И.Г. Дровникова, В.П. Алфёров // Общественная безопасность, законность и правопорядок в III тысячелетии: сб. ст. Междунар. науч.-практич. конф. (Воронеж, 27 июня 2018 г.). — В. 4. — Ч. 2. — 2018. — С. 32-35.

2. Методы и средства автоматизированного управления подсистемой контроля целостности в системах защиты информации / А.С. Дубровин [и др.]: Воронеж: Воронеж. гос. техн. ун-т, 2003. — 165 с.

3. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота: монография / И.И. Застрожных [и др.]. — Воронеж: Воронеж. гос. техн. ун-т, 2015. — 106 с.

4. Методы и средства оценки защищённости автоматизированных систем органов внутренних дел: монография [Электронный ресурс] / Е.А. Рогозин [и др.]; под ред. проф. Е.А. Рогозина. — Воронеж: Воронеж. ин-т МВД России, 2017. — 88 с.

5. Авсентьев О.С. Методика управления защитой информационного ресурса системы электронного документооборота / О.С. Авсентьев [и др.] // Труды СПИИРАН. № 2 (57) (2018). — С.-Пб.: СПИИРАН, 2018. — 2018. — № 2(57). — С. 188-210. — DOI 10.15622/sp.57.8.

СВЕДЕНИЯ ОБ АВТОРАХ

Дровникова Ирина Григорьевна. Профессор кафедры автоматизированных информационных систем ОВД. Доктор технических наук, доцент.

Воронежский институт МВД России.

E-mail: idrovnikova@mail.ru

Россия, 394065, г. Воронеж, пр-т Патриотов, 53.

Тел. (473)200-51-82, (952)558-96-10.

Алфёров Владимир Павлович. Соискатель кафедры КИПРА.

Воронежский государственный технический университет.

E-mail: alferov_vladimir@mail.ru

Россия, 394026, г. Воронеж, ул. Московский пр-т, 14. Тел. (910)281-96-19.

Drovnikova Irina Grigoryevna. Professor of the chair of Automatic Information Systems. Doctor of technical sciences, associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: idrovnikova@mail.ru

Work address: Russia, 394065, Voronezh, Patriotov Prospect, 53.

Ph. (473)200-51-82, (952)558-96-10.

Alferov Vladimir Pavlovich. Applicant of the department Design and manufacture of radio equipment.

Voronezh State Technical University

E-mail: alferov_vladimir@mail.ru

Work address: Russia, 394026, Voronezh, Moscow Avenue, 14. Ph. (910)281-96-19.

Ключевые слова: система электронного документооборота; подсистема защиты конфиденциальных сведений; информационная безопасность; награничение доступа; оценка эффективности; показатель своевременности реализации защиты информационного ресурса.

Key words: electronic document management system; the subsystem of protection of confidential information; information security; access differentiation; efficiency evaluation; indicator of timely implementation of information resource protection.

УДК 621.3

Дровникова Ирина Григорьевна,
доктор технических наук, доцент;
Етепнев Андрей Сергеевич

К ВОПРОСУ ОЦЕНКИ НАДЁЖНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

TO THE QUESTION OF THE RELIABILITY ASSESSMENT SYSTEM OF INFORMATION SECURITY OF THE AUTOMATED SYSTEM

В статье обоснована необходимость разработки классификации угроз безопасности информации, обусловленных отказами системы защиты информации, определяющих основные критерии оценки её надёжности при обеспечении целостности, конфиденциальности и доступности информации в автоматизированной системе.

The article substantiates the need to develop a classification of information security threats caused by failures of the information security system, which determine the main criteria for assessing its reliability while ensuring the integrity, confidentiality and availability of information in an automated system.

При оценке надёжности системы защиты информации (СЗИ) автоматизированной системы (АС) необходимо исходить из факторов, связывающих надёжность её математического, программного и информационного обеспечения с общим показателем безопасности информации (БИ) при обработке в АС [1]. Свойство надёжности СЗИ — не самостоятельное свойство, так как оно проявляется не только в процессе работы системы по парированию угроз БИ, но и в процессе выполнения СЗИ защитных функций по противодействию данным угрозам. Поэтому целесообразным является подход, при котором надёжность оценивается во взаимосвязи с комплексными показателями БИ АС, функционирующей по прямому назначению в условиях реализации множества угроз БИ и защиты от них с выполнением функций безопасности СЗИ. Это важно ещё и потому, что отказы СЗИ и угрозы БИ представляют собой взаимозависимые события. Взаимозависимость возникает по разным причинам, в первую очередь, из-за взаимосвязи режимов работы СЗИ с уровнем БИ, а также из-за влияния друг на друга отказов подсистем СЗИ. Вместе с тем, с целью декомпозиции задачи оценки надёжности СЗИ возможно получение отдельных оценок показателей надёжности отдельных подсистем СЗИ с последующим их объединением по схеме независимых событий. Игнорирование взаимозависимости отказов подсистем СЗИ приводит к оценке снизу для показателей надёжности СЗИ. Данный фактор необходимо учитывать для контроля общего уровня безопасности АС.

СЗИ как объект анализа и как часть АС имеет ряд особенностей.

Программы, реализующие основные программные модули СЗИ, не подвержены износу и в них отсутствуют ошибки производства: если обнаруженные в процессе отладки и опытной эксплуатации дефекты устраняются, а новые не вносятся, то интенсивность отказов СЗИ уменьшается. Надёжность СЗИ в значительной степени определяется входной информацией, обозначающей траекторию исполнения программы. Если при этом текст программы содержит первичные ошибки, то СЗИ сработает ошибочно даже при угрозе БИ. Если при возникновении ошибок их не фиксировать и не исправлять, то ошибки СЗИ будут систематически приводить к возможности реализации угроз БИ.

Надёжность СЗИ в значительной степени зависит от условий её применения: при изменении области применения СЗИ показатели надёжности могут значительно изме-

ниться без внесения изменений в код программы.

Необходимая информация о характеристиках надёжности аппаратных средств, составляющих АС, может быть определена посредством накопления и обработки статистических сведений, полученных в результате эксплуатации однотипных образцов таких устройств. Использование указанного пути для СЗИ малоприменимо, поскольку копии программы, реализующей СЗИ, идентичны и тиражирование дистрибутива СЗИ приводит к тиражированию дефектов (ошибок проектирования). При этом необходимо учитывать то, что характеристики статистики допущенных проектных ошибок являются устойчивым показателем качества работы программистов и используемых ими средств разработки [2]. Следовательно, регистрация данных о допущенных ошибках в ранее разработанных программах позволит оценить надёжность программы в новой СЗИ. В случае отсутствия сведений о статистических характеристиках допущенных ошибок в ранее разработанных программах возможно использование более общих сведений о процессах разработки программного обеспечения (ПО), а также данных о результатах отладки программы СЗИ.

Для проведения оценок надёжности по указанным данным требуется разработка модели надёжности СЗИ на каждом этапе жизненного цикла программы. На ранней стадии разработки СЗИ возможно использование описания алгоритма как «чёрного ящика» по входам и выходам либо как «белого ящика», когда структура алгоритма рассматривается в виде совокупности структурных элементов, описание каждого из которых также реализуется по входам и выходам.

В процессе отладки и эксплуатации СЗИ, когда возможен анализ статистических данных об обнаружении дефектов, исходное количество ошибок, являющееся одной из важнейших характеристик качества СЗИ, можно оценивать с использованием методов математической статистики.

Анализ архитектуры и порядка выполнения СЗИ в АС программных модулей в процессе реализации защитных функций показал, что данные программные системы предназначены для решения триединой задачи обеспечения целостности, конфиденциальности и доступности информации, являющихся основными свойствами БИ согласно нормативной документации [3-6], и в частности ГОСТ РВ 51987-2002 «Информационная технология. Комплекс стандартов на автоматизированные системы. Типовые требования и показатели качества функционирования информационных систем. Общие положения».

В соответствии с указанными свойствами целесообразно разработать классификацию угроз БИ, обусловленных отказами СЗИ, определяющих следующие основные критерии оценки надёжности СЗИ в АС:

- критерии отказов СЗИ при обеспечении целостности информации;
- критерии отказов СЗИ при обеспечении конфиденциальности информации;
- критерии отказов СЗИ при обеспечении доступности информации.

ЛИТЕРАТУРА

1. Методы и средства эволюционного и структурного моделирования при обосновании требований к программным системам защиты информации / В.А. Хвостов [и др.]. — Воронеж: Воронеж. ин-т МВД России, 2015. — 91 с.
2. Макаров О.Ю. Метод формализации процесса анализа алгоритма работы средств защиты информации. / О.Ю. Макаров [и др.] // Телекоммуникации. — 2002. — № 1. — С. 40-42.
3. Сборник действующих международных стандартов ИСО серии 9000. — Т. 1, 2, 3. — М: ВНИИКИ, 1998. — 4 с.

4. ГОСТ 27.001-81. Система стандартов «Надёжность в технике». Основные положения. — М.: Издательство стандартов, 1981. — 4 с.

5. ГОСТ 27.301-95. Надёжность в технике. Расчёт надёжности. Основные положения. — М.: Издательство стандартов, 1995. — 12 с.

6. ГОСТ 24.701-86. Надёжность. Автоматизированные системы управления технологическими процессами. Основные положения — М.: Издательство стандартов, 2009. — 12 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Дровникова Ирина Григорьевна. Профессор кафедры автоматизированных информационных систем ОВД. Доктор технических наук, доцент.

Воронежский институт МВД России.

E-mail: idrovnikova@mail.ru.

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473)200-51-82, (952)558-96-10.

Етепнев Андрей Сергеевич. Адъюнкт кафедры автоматизированных информационных систем ОВД. Воронежский институт МВД России.

E-mail: electronag@gmail.com.

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473)200-51-80, (929)007-97-37.

Drovnikova Irina Grigoryevna. Professor of the chair of Automatic Information Systems in Interior Affairs. Doctor of technical sciences, professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: idrovnikova@mail.ru.

Work address: Russia, 394065, Voronezh, Patriotov Prospect, 53.

Ph. (473)200-51-82, (952)558-96-10.

Etepnnev Andrei Sergeevich. Adjunct of the chair of Automatic Information Systems in Interior Affairs.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: electronag@gmail.com.

Work address: Russia, 394065, Voronezh, Patriotov Prospect, 53.

Ph. (473)200-51-80, (929)007-97-37.

Ключевые слова: угрозы безопасности информации, надёжность системы защиты информации, критерии оценки надёжности, автоматизированная система.

Key words: threats to information security, the reliability of the system of information protection, reliability assessment criteria, automated system.

УДК 621.3

**ПРОБЛЕМА КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ ОБЪЕКТОВ
КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

**PROBLEMS OF QUALIFICATION OF CRIMES AGAINST OBJECTS OF
CRITICAL INFORMATION INFRASTRUCTURE**

Статья посвящена рассмотрению квалификации преступлений против объектов критической информационной инфраструктуры.

The article is devoted to the consideration of the qualification of crimes against objects of critical information infrastructure.

В настоящее время метод моделирования шаг за шагом становится одним из главных средств познавательной деятельности человека, выступая в качестве одной из характеристик современного стиля мышления.

Многие годы исследования эффективности систем безопасности осуществляются с использованием различных моделей и, в частности, моделей нарушителя. Особый интерес представляет разработка модели нарушителя в зависимости от категории охраняемого объекта.

Модель нарушителя информационной безопасности представлена в работах А.П. Стефарова [1], Н.В. Гришиной [2], А.В. Богданова [3], Г.Н. Гудова [4], О.Т. Даниловой [5], В.И. Белоножкина [6].

По мнению А.П. Стефарова [1], для построения системы защиты информации необходимо рассматривать не только модель угроз, но и модель нарушителя. В статье приводится научно-обоснованное понятие модели нарушителя, создана нормированная гистограмма индекса цитирования классификации признаков информационного нарушителя.

Наиболее распространенными классификационными признаками, применяемыми при построении модели нарушителя являются:

- 1) категория;
- 2) мотив действий;
- 3) уровень квалификации;
- 4) средства атак;
- 5) уровень знаний об объектах атак;
- 6) место воздействия.

Таким образом, данные признаки способствуют созданию реалистичной модели нарушителя, что поможет наиболее вероятно оценить угрозу нападения злоумышленника.

Н.В. Гришина [2] рассматривает модель нарушителя на объекте информатизации, разграничивает понятие нарушителя на внешнего и внутреннего, приводит подробную классификацию.

А.В. Богданов [3] в исследовании рассматривает личность нарушителя, под которой понимается субъект нарушения. Построение концептуальной модели нарушителя, по мнению А.В. Богданова необходимо начинать с анализа социальных истоков преступности. Модель нарушителя по результатам исследования А.В. Богданова позволяет выявить условия, при которых может произойти формирование психологической готовности к противоправным действиям [3].

Г.Н. Гудов [4] рассматривает модель действий нарушителя в сфере информационной безопасности. В работе создана последовательность событий, представляющая собой

математическую модель Марковского случайного процесса, позволяющая описать поведение нарушителя в зависимости от состояния защищенности охраняемого объекта.

О.Т. Данилова [5] рассмотрела алгоритм разработки математической модели нарушителя в информационной системе. На начальном этапе создания алгоритма формируется несколько множеств. После чего строится платежная матрица, строками которой является стратегия охраны или защиты, а столбцами соответственно нарушителя. Далее О.Т. Данилова использует графовый метод, в частности модифицированный алгоритм Дейкстры для нахождения вероятности проникновения и определения кратчайшего маршрута нарушителя.

В.И. Белоножкиным [6] создана структура модели нарушителя безопасности информационно-аналитической системы, представлена типология нарушителей, построена описательная модель. На основе структурной и описательной моделей можно синтезировать наиболее вероятные типы злоумышленников, а так же построить его математическую модель.

Для создания нашей модели нарушителя будем использовать Постановление Правительства от 08.02.2018 № 127 [7].

В данном документе введены следующие сферы значимости объектов КИИ:

- 1) экономическая;
- 2) политическая;
- 3) социальная;
- 4) экологическая;
- 5) оборонная.

Возникла необходимость выделения нарушителей, которые посягают на данные сферы.

Таблица 1

Классы нарушителей на объектах КИИ

сфера нарушитель	Экономическая (X_1)	Политическая (X_2)	Социальная (X_3)	Экологическая (X_4)	Оборонная (X_5)
J_1 $(X_1, \bar{X}_2, X_3, \bar{X}_4, \bar{X}_5)$	1	0	1	0	0
J_2 $(\bar{X}_1, X_2, X_3, \bar{X}_4, \bar{X}_5)$	0	1	1	0	0
J_3 $(\bar{X}_1, \bar{X}_2, X_3, \bar{X}_4, \bar{X}_5)$	0	0	1	0	0
J_4 $(\bar{X}_1, \bar{X}_2, X_3, X_4, \bar{X}_5)$	0	0	1	1	0
J_5 $(\bar{X}_1, \bar{X}_2, \bar{X}_3, \bar{X}_4, X_5)$	0	0	0	0	1
J_6 $(X_1, \bar{X}_2, \bar{X}_3, \bar{X}_4, X_5)$	1	0	0	0	1
J_7 $(X_1, X_2, X_3, X_4, X_5)$	1	1	1	1	1

На следующей стадии классификации выделим отличительные количественные и качественные признаки нарушителя КИИ.

Отличительные признаки нарушителя в сфере информационной безопасности в своих статьях рассмотрели: А.Ю. Иванов и М.Ю. Синешук [8], Ю.А. Мерзлов [9], А.Л. Осипенко [10], Е.А. Маслакова [11].

В своей публикации А.Ю. Иванов и М.Ю. Синешук рассмотрели особенности внутреннего нарушителя, который, по их мнению, представляет собой легитимного сотрудника организации, обладающего определенными правами на доступ к информационным ресурсам. При умышленных или ошибочных действиях внутренний нарушитель может принести огромный ущерб.

Ю.А. Мерзлов определяет нарушителя информационной безопасности, как творческую личность, способную идти на технический вызов, риск. Данный нарушитель действует с целью получения несанкционированного доступа к чужой информации.

А.Л. Осипенко считает, что нарушителями информационной безопасности являются представители молодежи, которым присуща потребность в самоутверждении, стремление получить максимальное количество жизненных благ, при отсутствии реальной возможности. В нарушителях данной категории сочетаются мотивы корысти и убеждения, также имеются наклонности к вандализму в киберпространстве.

Их отличает хвастовство, презрительное отношение к людям. Это люди с низкой самооценкой, склонны к депрессии, тревожные, у них сложные отношения со сверстниками. В общении характерна холодность, конфликтность, пониженная эмоциональность. Потребность объединения в хакерские сообщества, безответственность, непонимание возможных последствий, гипертрофированная самооценка. Обладание высоким уровнем абстрактного мышления, высокая работоспособность, упорство, высокий интеллект и профессиональная подготовленность, стремление иметь в своем окружении положительную репутацию. Им присущ опыт работы с информационными системами, умение программировать, способность изучать языки программирования, участие в конференциях хакерской направленности, заявление о совершении правонарушения в сети.

Нарушитель в сфере информационной безопасности, как считает Е.А. Маслакова имеет замкнутый характер. Он склонен к депрессии, погружен в личные переживания. Нарушитель такой категории имеет достаточный уровень квалификации, знания в области информационных технологий. Поддерживает связи с хакерскими группами и использует специфический жаргон.

На основе проанализированных нами данных, мы смогли классифицировать правонарушения в различных сферах жизнедеятельности общества, используя следующие нормативные документы: Уголовный кодекс Российской Федерации [12], кодекс Российской Федерации об административных правонарушениях [13].

Таблица 2

Правонарушения в различных сферах жизнедеятельности общества,
за совершение которых наступает ответственность предусмотренная
санкциями статей уголовного кодекса РФ и кодекса
об административных правонарушениях РФ

Преступления террористической направленности	Правонарушения общекриминальной направленности	Правонарушения в сфере информационной безопасности
Преступления за совершение которых влечет уголовная ответственность, предусмотренная статьями (205, 206, 207, 208, 209, 211, 226, 239, 277, 278, 279, 360)	Преступления за совершение которых влечет уголовная ответственность, предусмотренная статьями (105, 139, 158, 161, 162, 165, 167)	Преступления за совершение которых влечет уголовная ответственность, предусмотренная статьями (138, 146, 159.6, 183, 187, 272, 273, 274, 276, 283)
Преступления за совершение которых влечет административная ответственность, предусмотренная статьями (13.37, 15.27)	Преступления за совершение которых влечет административная ответственность, предусмотренная статьями (7.17, 20.17)	Преступления за совершение которых влечет административная ответственность, предусмотренная статьями (13.11, 13.12, 13.13, 13.14, 13.18)

Правонарушения в различных сферах жизнедеятельности общества были квалифицированы по статьям уголовного и административного кодексов.

ЛИТЕРАТУРА

1. Стефаров А.П. Формирование типовой модели нарушителя правил разграничения доступа в автоматизированных системах / А.П. Стефаров, В.Г. Жуков // Известия ЮФУ. Технические науки. № 12 (137). – 2012. – С. 45-54.
2. Гришина Н.В. Модель потенциального нарушителя объекта информатизации / Н.В. Гришина // Известия ТРТУ. № 4(33). – 2003. – С. 356-358.
3. Богданов А.В. Неформальная модель нарушителя безопасности объектов культуры / А.В. Богданов, И.Г. Малыгин, Ю.И. Синещук // Научно-аналитический журнал вестник Санкт-Петербургского университета государственной противопожарной службы МЧС России. № 3. – 2013. – С. 109-113.
4. Гудов Г.Н. Математическая модель действий "нарушителя" информационной безопасности / Г.Н. Гудов, О.С. Купач // Технологии техносферной безопасности. № 4(56). – 2014. – С.24-31.
5. Данилова О.Т. Алгоритм построения модели нарушителя на примере системы физической защиты с применением теории игр и теории графов / О.Т. Данилова, С.О. Савченко, Н.В. Капчук // Омский научный вестник. № 4 (154). – 2017. – С. 115-119.
6. Белоножкин В.И. Модель нарушителя безопасности региональной антитеррористической ИАС / В.И. Белоножкин // Информация и безопасность. Т. 9. № 2. – 2006. – С. 155-157.
7. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства РФ от 08.02.2018 № 127 // СПС «КонсультантПлюс».

8. Иванов А.Ю. Классификация нарушителей и угроз безопасности автоматизированной информационной управляющей системы МЧС России [Электронный ресурс] /Иванов А.Ю., Синещук М.Ю. // Научно - аналитический журнал Вестник Санкт-Петербургского университета ГПС МЧС России. – 2013. – № 4 (12). С. 74 -79.

9. Мерзлов Ю.А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации /Ю.А. Мерзлов // Правопорядок: история, теория, практика. № 4 (7). – 2015. – С. 56-61.

10. Осипенко А.Л. Психологические особенности лиц, совершающих преступления в глобальных компьютерных сетях /А.Л. Осипенко // Психопедагогика в правоохранительных органах. № 2 (24). – 2005. – С. 50-52.

11. Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика /Е.А. Маслакова // Среднерусский вестник общественных наук. № 1 (31). – 2014. – С. 114-121.

12. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 3 августа 2018 г.) // СПС «Консультант Плюс».

13. Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ (ред. от 29.07.2018) // СПС «Консультант Плюс».

СВЕДЕНИЯ ОБ АВТОРАХ

Жилин Роман Андреевич. Командир взвода радиотехнического факультета.
Воронежский институт МВД России.
E-mail: zhilin99.zhilin@yandex. ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-52.

Шпак Александр Викторович. Преподаватель кафедры административного права.
Воронежский институт МВД России.
E-mail: zhilin99.zhilin@yandex. ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-47.

Zhilin Roman Andreevich. The platoon commander of the radio engineering faculty.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-52.

Shpak Alexander Viktorovich. Lecturer, Department of Administrative Law.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-47.

Ключевые слова: квалификация преступлений, объекты критической информационной инфраструктуры, классификация нарушителей, нормативно-правовые акты.

Key words: qualification of crimes, objects of critical information infrastructure, classification of violators, normative legal acts.

УДК 004.942

**АНАЛИЗ РЕЗУЛЬТАТОВ ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА
ПО ФОРМИРОВАНИЮ ОДНОРОДНЫХ ГРУПП НАРУШИТЕЛЕЙ ОХРАНЫ
ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

**ANALYSIS OF THE RESULTS OF THE COMPUTATIONAL EXPERIMENT FOR
THE FORMATION OF HOMOGENEOUS GROUPS OF VIOLATORS FOR THE
PROTECTION OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE**

Статья посвящена анализу результатов вычислительного эксперимента по формированию однородных групп нарушителей охраны объектов критической информационной инфраструктуры.

The article is devoted to the analysis of the results of a computational experiment on the formation of homogeneous groups of violators of the protection of critical information infrastructure objects.

Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» [1] в 2017 году введено понятие КИИ, после чего данный термин приобрел наибольшую актуальность.

КИИ включает в себя:

- 1) совокупность автоматизированных систем управления;
- 2) технологические процессы критически важных объектов Российской Федерации;
- 3) обеспечение взаимодействия информационно-телекоммуникационных сетей;
- 4) обеспечение обороноспособности, безопасности и правопорядка;
- 5) обеспечение взаимодействия информационных технологий и сетей связи.

Рассмотрев нормативные документы по обеспечению безопасности в сфере КИИ, были сформированы следующие однородные группы нарушителей и соответствующие им отличительные признаки.

Таблица 1

Пространство признаков нарушителей

корыстно-статусный мотив действий (H_1)	нарушитель экономической безопасности
последствия – материальный ущерб (H_2)	
цель – достижение высоких социальных позиций (H_3)	
политическая одержимость (H_4)	нарушитель политической безопасности
цель - стремление утвердить свою власть (H_5)	
цель – политическая карьера (H_6)	
национальная ненависть (H_7)	
антиобщественная мотивация (H_8)	нарушитель социальной безопасности
цель – нарушение стабильности социально-экономического развития (H_9)	
социальный паразитизм (H_{10})	
аморальное противоправное поведение (H_{11})	
халатность (H_{12})	нарушитель экологической
безответственность (H_{13})	

возможные последствия – нарушение функционирования объекта обеспечения жизнедеятельности (H_{14})	безопасности
хулиганские побуждения (H_{15})	нарушитель безопасности обороны страны
беснаказанность (H_{16})	
вседозволенность (H_{17})	
профессионализм в области компьютерной техники (H_{18})	нарушитель информационной безопасности
цель – самоутверждение (H_{19})	
возможные последствия – нарушение конфиденциальности (H_{20})	
протестное сознание и идейный абсолютизм (H_{21})	нарушитель антитеррористической безопасности
возможные последствия – массовая гибель людей (H_{22})	
возможные последствия – устрашение общества (H_{23})	

Сформируем алгоритм, который отражает последовательность сравнения однородных групп нарушителей охраны объектов КИИ.

Для реализации алгоритма выбран многофункциональный язык программирования Python, направленный на увеличение продуктивности и читабельности кода. Является интерпретируемым языком программирования высокого уровня, формирующим последовательный синтаксис с мощной элементарно-ориентированной семантикой.

Данный язык программирования используется для написания программ различной сложности и размерности, при этом он поддерживает значительную часть характеристик эргономичного программирования.

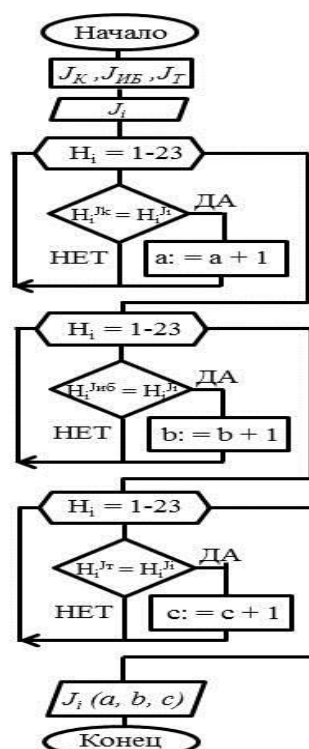


Рис 1. Алгоритм формирования однородных групп нарушителей

Составные компоненты Python представлены на рисунке 2.

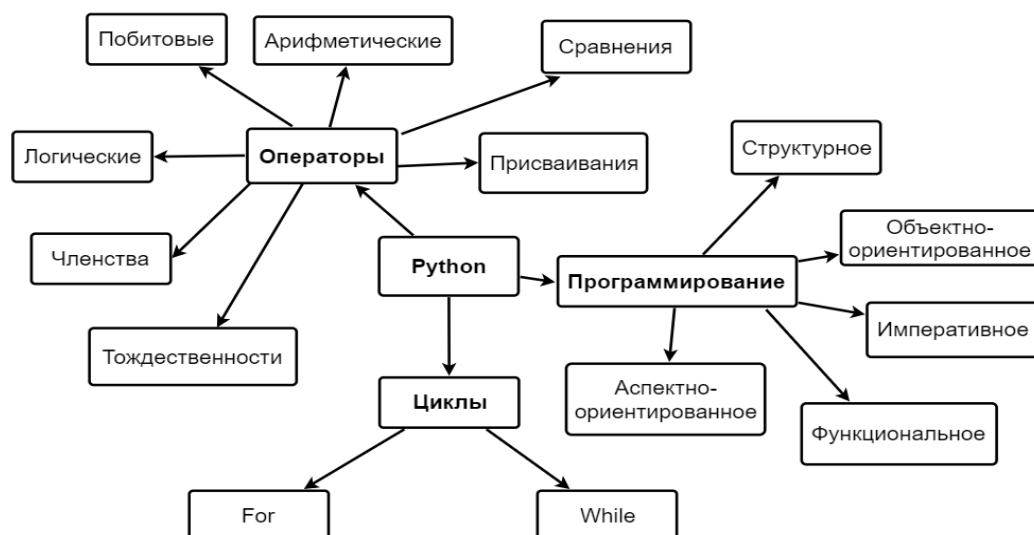


Рис 2. Составные компоненты языка программирования Python

Реализуя алгоритм, представленный на рис.1, через Python, получили следующий программный код. Данный код реализует классификацию нарушителей по различным категориям.

```

Python 3.7.2 Shell
File Edit Shell Debug Options Window Help
Python 3.7.2 (tags/v3.7.2:9a3ffc0492, Dec 23 2018, 22:20:52) [MSC v.1916 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: D:\Влад\Питон\Итог.py =====
['1', '1', '1', '0', '0', '0', '0', '0', '0', '0', '0', '0', '1', '0', '0', '0', '0', '0', '0', '0', '0', '0']
['1', '1', '1', '0', '0', '0', '0', '0', '0', '0', '0', '1', '1', '1', '0', '0', '0', '0', '0', '0', '0', '0']
['1', '1', '1', '0', '0', '0', '0', '0', '0', '0', '0', '0', '1', '1', '0', '0', '0', '0', '0', '0', '0', '0']
Верно, подходит J_6!
>>>
  
```

Рис 3. Результат алгоритма

Верифицируя показатели нарушителя при помощи алгоритма, определяется его категория.

Исследованное множество нарушителей (на основе данных г. Воронежа и Воронежской области) в различных сферах жизнедеятельности общества показало следующие результаты.

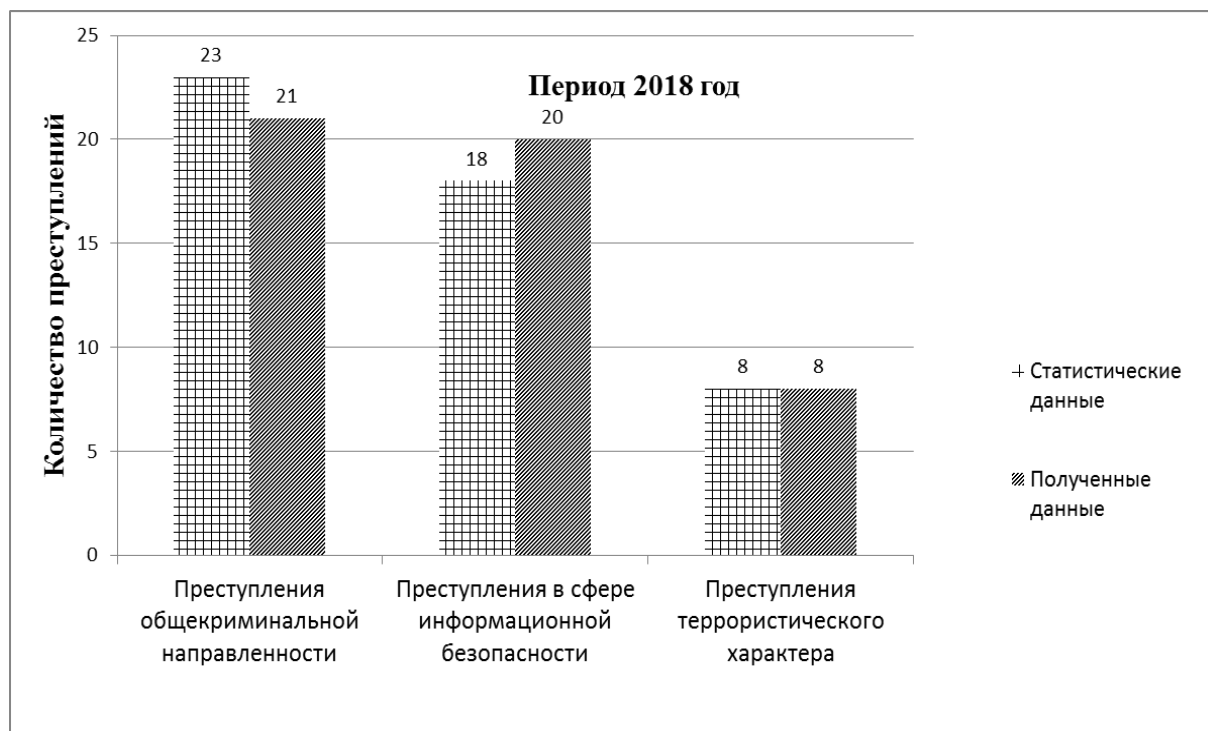


Рис 4. Гистограмма частот правонарушений при охране объектов КИИ

Результаты алгоритма в 97 % соответствуют статистическим данным. Разработанный алгоритм формирования однородных групп нарушителей позволит в дальнейшем реализовать наиболее адекватную модель нарушителя КИИ.

ЛИТЕРАТУРА

1. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г. № 187-ФЗ // СПС «Консультант Плюс».
2. Ахлюстин С.Б. Определение частного критерия интегрированной системы безопасности симметричным методом анализа иерархий / С.Б. Ахлюстин, А.В. Мельников // Вестник Воронежского института МВД России, 2018, № 2. – С. 37-44.
3. Ахлюстин С.Б. Нечетко-множественное моделирование обобщенных показателей опасности объектов топливно-энергетического комплекса / С.Б. Ахлюстин, А.В. Мельников, И.В. Щербакова // Вестник Воронежского института МВД России, 2018, № 3. – С. 44-55.
4. Жилин Р.А. К вопросу о модели нарушителя системы безопасности объекта охраны / Р.А. Жилин, А.В. Мельников, И.В. Щербакова // Вестник Воронежского института МВД России, 2019, № 2. – С. 57-69.

СВЕДЕНИЯ ОБ АВТОРАХ

Жилин Роман Андреевич. Командир взвода радиотехнического факультета.
Воронежский институт МВД России.
E-mail: zhilin99.zhilin@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-52.

Zhilin Roman Andreevich. The platoon commander of the radio engineering faculty.
Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: zhilin99.zhilin@yandex. ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-52.

Саркисов Владислав Геннадьевич. Курсант 1 курса радиотехнического факультета.
Воронежский институт МВД России.
E-mail: zhilin99.zhilin@yandex. ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-52.

Sarkisov Vladislav Gennadyevich. Cadet 1 course of the Faculty of Radio Engineering.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: zhilin99.zhilin@yandex. ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-52.

Ключевые слова: объекты критической информационной инфраструктуры, алгоритм формирования однородных групп нарушителей.

Key words: objects of critical information infrastructure, algorithm for forming homogeneous groups of violators.

УДК 004.942

Жилин Роман Андреевич

КАТЕГОРИАЛЬНАЯ ИЕРАРХИЯ НАРУШИТЕЛЕЙ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

CATEGORIAL HIERARCHY OF VIOLATORS OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Статья посвящена рассмотрению современных нормативно-правовых актов в области критической информационной инфраструктуры, а также созданию классификации нарушителей на их основе.

The article is devoted to the consideration of modern legal acts in the field of critical information infrastructure, and the creation of a classification of violators that is based on them.

Для регламентирования и стандартизации в области безопасности объектов критической информационной инфраструктуры (КИИ), разработаны нормативные правовые документы, в которых указываются особенности эксплуатации объектов КИИ.

В Постановлении Правительства от 08.02.2018 № 127 [1], утверждены критерии значимости объектов критической информационной инфраструктуры: социальная, политическая, экономическая, экологическая, обеспечение обороны страны.

Исходя из критериев значимости, можно сформулировать соответствующие цели предполагаемого нарушителя на объекте критической информационной инфраструктуры.

Особое место в обеспечении безопасности объектов КИИ занимают электроподстанции, так как их роль в обеспечении жизнедеятельности и функционирования объекта КИИ важна, но при этом зачастую не учитывается при категорировании охраняемого объекта.

В методических рекомендациях Р 063 — 2017 [2] представлена классификация охраняемых объектов, в которой обеспечение противокриминальной защищенности является неотъемлемой составляющей безопасности. Преступные посягательства на охраняемые объекты могут иметь широкий общественный резонанс и привести к особо крупному экономическому ущербу государству.

Существуют различные математические методы по оценке и выбору категории объекта [5, 6].

Разработка соответствующей методики по оценке и выбору категории объекта обуславливает формирование соответствующей классификации нарушителей охраны объектов критической информационной инфраструктуры. С учетом классификации и характеристик нарушителя определяются требования к комплексу ИТСО или к его составным частям.

Задачи кластеризации и классификации являются идентичными, поэтому используем метод «кластерного сита» предложенный в работе [3].

Процедура включает в себя совокупность методов теории экспертных систем и кластерного анализа, являясь единым исследовательским процессом.

Из множества категорий нарушителей, представленных в нормативно-правовых актах, выберем две наиболее предпочтительные. Затем осуществим разделение каждой из категорий на 4 класса признаков (наличие либо отсутствие этих признаков). Нарушители, объединенные в группы, позволят в дальнейшем выделить необходимые средства защиты, которые будут направлены на охрану именно этих классов.

Далее устанавливается однородность этих классов.

Однородные объекты – объекты, которые обладают схожими свойствами, только их можно и нужно сравнивать между собой.

Примером такой кластеризации является вычисление расстояния Хэмминга. Множество векторов равной длины образуют метрическое пространство, где для каждой пары элементов пространства определено число – расстояние Хэмминга удовлетворяющее аксиомам метрики.

$$\hat{a} = \frac{a}{n_a}; \hat{b} = \frac{b}{n_b}; \hat{c} = \frac{c}{n_c} \quad (1)$$

Выявлена следующая закономерность: большое количество совпадений признаков в той или иной группе говорит о том, что выделенный нарушитель будет относиться к данной группе.

Выделив нарушителя, сравнив и подсчитав, согласно расстоянию Хемминга определили категорию с наименьшим расстоянием, которая и будет присвоена данному злоумышленнику. Однако недостатком данного метода является однозначное отнесение к тому или иному классу нарушителей.

В завершении выделяются количественные и качественные признаки, признаки наличия. Важность этих групп признаков устанавливается с помощью метода, предложенного Т. Саати.

Классификация произведена на основании наличия признака R (нарушитель с высоким потенциалом) и другого признака P (внутренний нарушитель). Обозначим через $\bar{R}$ отсутствие первого признака, а через $\bar{P}$ – отсутствие второго. Такое условие представлено на рисунке 1. Тогда показатель взаимосвязи, применительно к обозначенным величинам будет иметь следующий вид:

$$\lambda = \frac{[q(RP) + q(R\bar{P})][q(\bar{R}P) + q(\bar{R}\bar{P})]}{q(RP)k} \quad (2)$$

Будем считать, что если $\lambda < 1$, величины R, P положительно связаны; если $\lambda = 1$ – не связаны; если $\lambda > 1$ – отрицательно связаны.

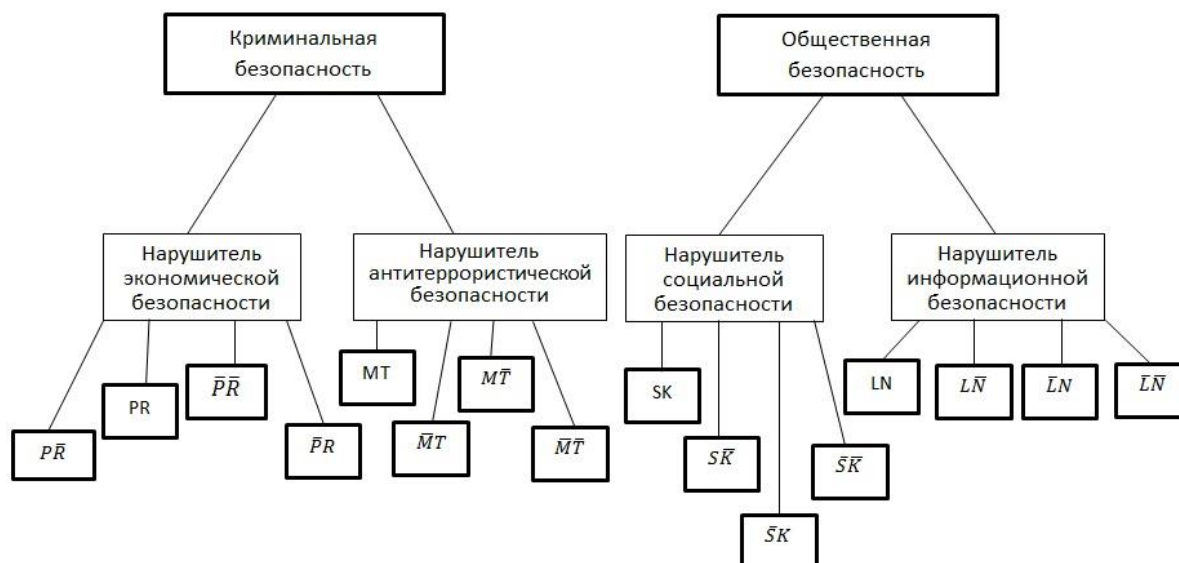


Рис. 1. Нечетко-множественная иерархия основных признаков нарушителя

- $P\bar{R}$ – внутренний нарушитель с низким потенциалом;
 PR – внутренний нарушитель с высоким потенциалом;
 $\bar{P}\bar{R}$ – внешний нарушитель с низким потенциалом;
 $\bar{P}R$ – внешний нарушитель с высоким потенциалом;
 MT – нарушитель с высокой оснащенностью, причиняющий значительный ущерб;
 $\bar{M}\bar{T}$ – нарушитель с низкой оснащенностью, причиняющий не значительный ущерб;
 $M\bar{T}$ – нарушитель с высокой оснащенностью, причиняющий не значительный ущерб;
 $\bar{M}T$ – нарушитель с низкой оснащенностью, причиняющий значительный ущерб;
 SK – намеренное проникновение, знания об объекте имеются;
 $\bar{S}\bar{K}$ – намеренное проникновение, знания об объекте не имеются;
 $\bar{S}K$ – не намеренное проникновение, знания об объекте имеются;
 $\bar{S}\bar{K}$ – не намеренное проникновение, знания об объекте не имеются;
 LN – осведомленность о ТСО высокая, степень технической оснащенности высокая;
 $\bar{L}\bar{N}$ – осведомленность о ТСО высокая, степень технической оснащенности низкая;
 $\bar{L}N$ – осведомленность о ТСО низкая, степень технической оснащенности высокая;
 $\bar{L}\bar{N}$ – осведомленность о ТСО низкая, степень технической оснащенности низкая.

Разработка адекватной модели нарушителя в соответствии с приведенной классификацией и государственными стандартами является весьма актуальной задачей и требует проведения дополнительных научных исследований.

ЛИТЕРАТУРА

1. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : Постановление Правительства РФ от 08.02.2018 № 127 // СПС «КонсультантПлюс».

2. Обследование объектов, принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации : методические рекомендации (Р 063 — 2017). — М. : ФКУ «НИЦ «Охрана» Росгвардии», 2017. — 50 с.

3. Мельников А.В. Кластерно-иерархические методы экспертизы технических и экономических объектов / А.В. Мельников: Дисс. ... докт. техн. наук. - Специальность 05.13.18. -Воронеж: Воронежский институт МВД России. -16.09.2014.

4. Бухарин С.В. Моделирование нейронных сетей в экспертизе технических объектов / С.В. Бухарин, А.В. Мельников. — Воронеж, 2016. — 179 с.

5. Мельников А.В. Расширение метода анализа иерархий для определения согласованности оценок экспертов / А.В. Мельников, А.В. Иванченко // Системы управления и информационные технологии. 2012. — Т. 47. № 1. — С. 75-78.

6. Бухарин С.В. Экспертная оценка и прогнозирование обобщенного показателя структуры капитала предприятий / С.В. Бухарин, А.В. Мельников, А.И. Хорев // ФЭС: Финансы. Экономика. — 2013. — № 5. — С. 9.

СВЕДЕНИЯ ОБ АВТОРАХ

Жилин Роман Андреевич. Командир взвода радиотехнического факультета.
Воронежский институт МВД России.
E-mail: zhilin99.zhilin@yandex. ru
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-52.

Zhilin Roman Andreevich. The platoon commander of the radio engineering faculty.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-52.

Ключевые слова: объекты критической информационной инфраструктуры, классификация нарушителей, категориальная иерархия.

Key words: objects of critical information infrastructure, classification of offenders, categorical hierarchy.

УДК 004.942

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ОПТИМИЗАЦИИ ПРОЦЕССОВ МОДЕРНИЗАЦИИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

RATIONALE OF OPTIMIZATION OF INFOCOMMUNICATION NETWORKS MODERNIZATION PROCESSES

В данной работе представлен анализ различных вариантов использования инфокоммуникационных сетей в органах внутренних дел, обоснование необходимости и рассмотрение возможных вариантов их модернизации.

This paper presents an analysis of various options for using infocommunication networks in the internal affairs bodies, substantiating the need and considering possible options for their modernization.

Инфокоммуникационные сети и системы нашли широкое применение практически во всех сферах человеческой деятельности и не перестают быть актуальными. В органах внутренних дел они так же нашли применение в качестве инструмента управленческой деятельности, доступа к необходимым ресурсам и связи [1].

В настоящее время важнейшей задачей повышения эффективности функционирования информационных систем МВД является интеграция различных видов связи, таких как: передача данных, телефония, телеграфия. Это достигается построением инфокоммуникационных сетей, обеспечивающих качественной связью подразделения ОВД [2].

Ключевую роль в информационном обеспечении ОВД играет интегрированная мультисервисная телекоммуникационная сеть МВД России (ИМТС МВД России). Целью создания ИМТС являлось обеспечение органов внутренних дел различными подсистемами связи (передача данных, видеоконференцсвязь, телефонная связь и др.) на базе единых схемотехнических решений и типовых программных и аппаратных средств [3].

ИМТС МВД России представляет собой универсальную телекоммуникационную транспортную среду, которая является главным компонентом Единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России [1,4].

Структура ИМТС МВД России представляет собой совокупность коммутационных и опорных узлов, узлов мультисервисной транспортной сети ОВД и каналов передачи данных.

В структуру входят следующие элементы:

- 1) главный коммутационный узел;
- 2) опорные коммутационные узлы ИМТС МВД России федеральных округов Российской Федерации;
- 3) региональные коммутационные узлы ИМТС МВД России территориальных органов МВД России на региональном уровне [1,4].

Взаимодействие указанных узлов осуществляется с использованием магистральных каналов передачи данных по радиальному принципу. В тех местах, где организация каналов связи невозможна по каким-то причинам, применяется сеть спутниковой связи ОВД. Данная сеть является составной частью ИМТС, построена на базе геостационарных спутников-ретрансляторов, состоит из центральной земной станции спутниковой связи и спутниковых терминалов, установленных по месту дислокации органов внутренних дел Российской Федерации [4].

ИСОД МВД использует в качестве среды передачи данных ИМТС. В основе структуры ИСОД МВД России лежит центр обработки данных, на базе которого созда-

ется единое информационное пространство, в котором размещаются сервисы ИСОД МВД России. С помощью ИМТС доступ к сервисам предоставляется сотрудникам по стационарной, спутниковой или мобильной связи [1,5].

Для повышения устойчивости и надежности сетей, а так же эффективности их функционирования выделяются приоритетные направления передачи информации [4]. Каждое из направлений может иметь свою оценку важности для функционирования системы.

Динамика изменения оценок важности невысокая и поддается прогнозированию. Например, заранее может быть известно о проведении массовых мероприятий, таких как международные соревнования, фестивали, праздники, концерты, для охраны общественного порядка которых привлекаются силы и средства ОВД. Таким образом, зная о планирующихся событиях можно заранее оценить важность направлений передачи информации в интересующий период времени.

Вопрос распределения ресурсов на замену оборудования в плановом режиме (замена оборудования в связи с его износом и устареванием, техническое обслуживание и тд.) хорошо изучен [6-12], поэтому в работе они не рассматриваются. Данная работа посвящена вопросам модернизации сетей для оптимизации функционирования и (или) повышения пропускной способности сети.

В ОВД применяются различные варианты использования инфокоммуникационных сетей [1,13-16]:

аренда каналов связи инфокоммуникационных сетей у провайдера, с возможностью изменения количества предоставляемого трафика;

эксплуатация инфокоммуникационных сетей, находящихся в собственности.

Увеличение количества служебных задач, решаемых с использованием инфокоммуникационных систем может потребовать перераспределения трафика и модернизации сетей.

Пропускная способность арендованных каналов связи может быть, как уменьшена, так и увеличена, в зависимости от решаемой задачи (повышение пропускной способности или уменьшение расходов), тогда как модернизацию целесообразно проводить в целях увеличения пропускных способностей.

Заклучение.

Таким образом, анализ различных вариантов использования инфокоммуникационных систем в ОВД, обоснование необходимости и рассмотрение возможных вариантов их модернизации позволили сделать вывод о необходимости оптимизации процессов модернизации инфокоммуникационных сетей ОВД.

ЛИТЕРАТУРА

1. Применение современных инфокоммуникационных технологий в управлении деятельностью подразделений органов внутренних дел: учеб.-практ. пособие / К. М. Бондарь [и др.]. – Москва: ДГСК МВД России, 2018. – 192 с.

2. Лукьянов, А. С. Основы применения систем связи: учебное пособие. – Воронеж: Воронежский институт МВД России, 2019. – 128 с.

3. Мачтаков, С. Г. Единая система информационно-аналитического обеспечения деятельности (ИСОД) МВД России / С. Г. Мачтаков, М. В. Питолин // Пожарная безопасность: проблемы и перспективы. - 2016. - №1(7). – С. 156-158.

4. Об утверждении структуры и системы адресации интегрированной мультисервисной телекоммуникационной сети Министерства внутренних дел Российской Федерации : приказ МВД Российской Федерации от 23 сентября 2015 г. № 926 [Электронный ресурс]. Доступ из СТРАС «Юрист» (дата обращения: 01.06.2019).

5. Защита ведомственных мобильных устройств на Android [Электронный ресурс]. – Режим доступа : https://www.anti-malware.ru/analytics/Technology_Analysis/Protection_departmental_mobile_devices_Android (дата обращения: 01.06.19).
6. Правила технического обслуживания и ремонта линий кабельных, воздушных и смешанных местных сетей связи : утв. Министерством связи Российской Федерации 07 октября 1996 г. [Электронный ресурс] Доступ из СТРАС «Юрист» (дата обращения: 01.06.2019).
7. Правила технического обслуживания и ремонта линейных сооружений и оконечных устройств абонентских пунктов местных сетей связи: утв. Министерством связи Российской Федерации 07 октября 1996 г. [Электронный ресурс] Доступ из СТРАС «Юрист» (дата обращения: 01.06.2019).
8. Пятибратов, А.П. Вычислительные системы, сети и телекоммуникации / А.П. Пятибратов, Л.П. Гудыно, А.А. Кириченко ; под ред. А.П. Пятибратова. – 4-е изд., перераб. и доп. – Москва : Финансы и статистика, 2014. – 735 с.
9. Будылдина, Н.В. Сетевые технологии высокоскоростной передачи данных / Н.В. Будылдина, В.П. Шувалов ; под ред. В.П. Шувалова. – Москва : Горячая линия-Телеком, 2016. – 343 с.
10. Портнов, Э.Л. Принципы построения первичных сетей и оптические кабельные линии связи / Э.Л. Портнов. – Москва : Горячая линия-Телеком, 2013. – 544 с.
11. Межгосударственный стандарт ГОСТ 18322-2016 «Система технического обслуживания и ремонта техники. Термины и определения» (введен в действие Приказом Росстандарта 28.03.2017 № 186-ст) [Электронный ресурс]. Доступ из СТРАС «Юрист» (дата обращения: 01.06.2019).
12. Национальный стандарт Российской Федерации ГОСТ Р 57329-2016 «Системы промышленной автоматизации и интеграция. Системы технического обслуживания и ремонта. Термины и определения» (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7 декабря 2016 г. № 1977-ст) [Электронный ресурс]. Доступ из СТРАС «Юрист» (дата обращения: 01.06.2019).
13. Zvereva, D. D. Optimization of processes of modernization and operating conditions of infocommunication networks / D. D. Zvereva, V. V. Menshikh, A. V. Seifer // 2018 Global Smart Industry Conference (Chelyabinsk, 13-15 Nov. 2018). – Chelyabinsk, 2018. – P. 1-6.
14. Menshikh, V. V. Models and algorithms of optimal structure synthesis of infocommunication network with specified parameters / V.V. Menshikh, D.D. Zvereva // IOP Conf. Series: Journal of Physics: Conf. Series 1203 (2019) 012067.
15. Меньших, В. В. Модели и алгоритмы синтеза оптимальной структуры инфокоммуникационной сети с заданными параметрами / В. В. Меньших, Д. Д. Зверева // Актуальные проблемы прикладной математики, информатики и механики : сборник трудов Международной научной конференции (Воронеж, 17-19 декабря 2018 г.). – Воронеж, 2019. – С. 860-867.
16. Меньших, В. В. Численный метод оптимизации выбора варианта модернизации инфокоммуникационной сети органов внутренних дел / В. В. Меньших, Д. Д. Зверева // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2018. – № 4-2 (4). – С. 71-77.

СВЕДЕНИЯ ОБ АВТОРЕ

Зверева Дарья Дмитриевна. Адъюнкт института.
Воронежский институт МВД России.
E-mail: zubzv@yandex.ru
Россия, 394065, г. Воронеж, пр-т Патриотов, 53. Тел. (473)2005-216.

Zvereva Daria Dmitrievna..
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: zubzv@yandex.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473)2005-216.

Ключевые слова: инфокоммуникационная сеть, приоритетные направления передачи информации, пропускная способность сети.

Key words: infocommunication network, priority data transmission directions, network channel capacity.

УДК 004.94

Калков Дмитрий Юрьевич,
кандидат технических наук;
Гудков Максим Андреевич,
кандидат технических наук

К ВОПРОСУ ПРОЕКТИРОВАНИЯ СИСТЕМ ОХРАННЫХ ТЕЛЕВИЗИОННЫХ С УЧЕТОМ ОБЕСПЕЧЕНИЯ ИХ СОБСТВЕННОЙ БЕЗОПАСНОСТИ

THE ISSUE OF DESIGNING SYSTEMS FOR TELEVISION WITH A VIEW TO ENSURING THEIR OWN SAFETY

В данной работе предложен подход к проектированию систем охранных телевизионных, при котором учитывается безопасность технических средств видеонаблюдения от противоправных посягательств.

In this paper we propose an approach to the design of security television systems, which takes into account the safety of technical means of video surveillance from illegal attacks.

Одной из важнейших задач, возложенных на органы внутренних дел, является обеспечение общественного порядка и общественной безопасности. В последние годы наблюдается нехватка личного состава в практических подразделениях правоохранительных органов, в связи с чем решение данной задачи усложняется. С учетом сложившейся ситуации для повышения эффективности деятельности органов правопорядка необходимо использовать современные технические средства, в частности системы видеонаблюдения.

В настоящее время системы видеонаблюдения активно развиваются и предназначены для обеспечения безопасности объектов, людей, материальных и интеллектуальных ценностей, путем визуального контроля и мониторинга событий в режиме реального времени и анализа архивных данных. Системы видеонаблюдения доказали

свою эффективность, в связи с чем используются в интересах правоохранительных органов для раскрытия правонарушений, поиска разыскиваемых лиц, автоматической фиксации нарушений правил дорожного движения, обнаружения признаков чрезвычайных ситуаций [1]. С 2014 года для обеспечения централизованного мониторинга и управления средствами видеофиксации на территории Российской Федерации был создан аппаратно-программный комплекс «Безопасный город» на основании распоряжения Правительства Российской Федерации от 3 декабря 2014 года № 2446-р «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» [2].

Средства видеонаблюдения обладают высокой материальной ценностью, а также эффективно применяются как сдерживающий фактор правонарушений, поэтому они сами становятся объектами преступных посягательств (кража, порча). При этом дежурный мониторингового центра не имеет достоверной информации о состоянии технического средства, так как потеря сигнала от него помимо кражи и порчи может быть вызвана различными причинами: отключение электропитания, обрыв линии связи, аппаратный или программный сбой системы. В связи с этим возникает задача в обеспечении сохранности средств видеонаблюдения.

Безопасность видеокамер может быть достигнута комплексом мер, среди которых стоит выделить: сложность доступа к видеокамере, применение антивандальных конструктивных решений, корректное проектирование системы видеонаблюдения. Из перечисленных мероприятий с научной точки зрения наибольший интерес вызывает последнее, идея которого заключается в таком выборе мест расположения средств видеонаблюдения, при котором будут контролироваться не только зоны охраны, но и места установки видеокамер. Так как обеспечить контроль всех мест установки видеокамер не представляется возможным, критерием оптимальности будет выступать суммарная стоимость контролируемых средств видеонаблюдения. Также при проектировании необходимо учитывать, что видеокамеры обладают различными техническими характеристиками, наиболее важными из которых будут являться:

- чувствительность;
- дальность обзора;
- угол обзора;
- наличие инфракрасной подсветки;
- наличие поворотного устройства;
- наличие термокожуха.

Рассмотрим описательную модель расположения технических средств видеонаблюдения с учетом их собственной безопасности.

Главной задачей систем видеонаблюдения является контроль наиболее важных участков территорий или объектов, являющихся охраняемыми зонами. Поэтому при проектировании систем охранных телевизионных необходимо выполнять обязательное условие, заключающееся в том, чтобы все охраняемые зоны, контролировались хотя бы одним средством видеонаблюдения.

Введем множество охраняемых зон:

$$O = \{o_1, \dots, o_i, \dots, o_n\}.$$

При выборе места установки средства видеонаблюдения важно учитывать возможность расположения в той или иной точке пространства. Каждое потенциальное место установки должно удовлетворять ряду требований, заключающихся в наличии в непосредственной близости источника электропитания, возможности организации канала связи с мониторинговым центром, надежной конструкции опоры. Также необходимо предусмотреть, чтобы к установленным видеокамерам был затруднен или невоз-

можен прямой доступ со стороны граждан, что позволит снизить риск совершения противоправных действий в их отношении.

Введем множество потенциальных мест установки технических средств видеонаблюдения:

$$M = \{m_1, \dots, m_j, \dots, m_k\}.$$

Как было сказано выше, различные типы средств видеонаблюдения обладают различными техническими характеристиками, функциональными возможностями и, соответственно, стоимостью, что также будет вносить определенные ограничения при проектировании систем охранных телевизионных.

Обозначим множество типов технических средств видеонаблюдения:

$$T = \{t_1, \dots, t_q, \dots, t_l\},$$

стоимость которых:

$$C = \{c_1, \dots, c_q, \dots, c_l\}.$$

Таким образом, задача оптимизации сводится к тому, чтобы найти такой способ расположения средств видеонаблюдения, при котором все множество охраняемых зон O будет находится под наблюдением и при этом имелась возможность контроля видеокамер с наибольшей суммарной стоимостью.

ЛИТЕРАТУРА

1) Бокадаров С.А. О перспективах использования систем видеонаблюдения в целях обеспечения пожарной безопасности / С.А. Бокадаров, Д.Ю. Калков, М.А. Гудков // Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций. – 2018. – Т. 1. – С. 85-88.

2) Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» [Электронный ресурс]: распоряжение Правительства Российской Федерации от 3 декабря 2014 года №2446-р. – URL: http://www.consultant.ru/document/cons_doc_LAW_172077/ (дата обращения: 23.06.2019).

СВЕДЕНИЯ ОБ АВТОРАХ

Калков Дмитрий Юрьевич, кандидат технических наук, старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: DmitreyRUS@mail.ru

Россия, 394065, г. Воронеж, Проспект Патриотов, 53.

Тел. (473) 200-52-08.

Гудков Максим Андреевич, кандидат технических наук, преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: gudokmaksim@yandex.ru

Россия, 394065, г. Воронеж, Проспект Патриотов, 53.

Тел. (473) 200-52-08.

Kalkov Dmitry Yurievich, candidate of technical Sciences, senior lecturer of the Department of radio systems and complexes of security monitoring.

Voronezh Institute of the Ministry of internal Affairs of Russia.

E-mail: DmitreyRUS@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-08.

Gudkov Maxim Andreevich, candidate of technical Sciences, lecturer of the Department of radio systems and security monitoring systems.

Voronezh Institute of the Ministry of internal Affairs of Russia.

E-mail: gudokmaksim@yandex.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-08.

Ключевые слова: общественная безопасность, система видеонаблюдения, безопасный город, проектирование.

Key words: public security, video surveillance system, safe city, design.

УДК 004.02

Конобеевских Владимир Валерьевич,
кандидат технических наук

ВИЗУАЛЬНО-АНАЛИТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ ПРИ РАБОТЕ С ДАННЫМИ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ

THE ANALYSIS OF QUALITY METRICS IN USE OF AUTOMATED INFORMATION SYSTEMS OF POLICE

В статье рассмотрены основные характеристики программных систем, которые позволяют осуществляющих визуально-аналитическую деятельность при работе с данными из социальных сетей.

The article describes the main characteristics of software systems that allow performing visual and analytical activities when working with data from social networks.

Развитие информационной среды в нашем обществе, характеризуется множеством различных параметров. Одним из наиболее актуальных на сегодняшний день является работа с массивами данных, в том числе и с большими. Следует заметить, что с физиологической точки зрения такая работа достаточно утомительная и требует значительных трудовых ресурсов. Поэтому во многих областях науки и техники для комплексного решения задач, связанных с обработкой больших объемов информации используются специализированные аппаратно-программные комплексы.

Данные аппаратно-программные комплексы позволяют осуществлять визуально-аналитическую деятельность, направленную на обработку больших объемов информации. Достаточно важно заметить, что социальные сети в последнее время достаточно плотно вошли в жизнь практически каждого современного человека. Значительную часть своего свободного времени сегодня люди проводят в виртуальной информационно-телекоммуникационной среде. При этом, необходимо отметить, что виртуальная среда в последнее время все чаще стала использоваться в противоправных целях, связанных с совершением различных преступлений.

Указанное выше обстоятельство, требует повышенного внимания и изучения виртуальной среды общения граждан со стороны правоохранительных органов, а также создание соответствующих мер защиты, пресечения и предупреждения противоправных действий, особенно в социальных сетях. Одной из самых популярных социальных сетей для молодого поколения является сеть «ВКонтакте». Поэтому для анализа данных

из рассматриваемой социальной сети целесообразно использовать программные средства, позволяющие осуществлять визуально-аналитическую деятельность.

Важным обстоятельством является тот факт, что без использования визуализации невозможен корректный анализ больших объемов данных.

Основным преимуществом рассматриваемых систем является их ориентированность на организацию сведений в базах данных (проектах), имеющих структуру графа. Помимо стандартного полнотекстового поиска, подобная сетевая структура данных в виде графа позволяет применять множество мощных подходов для решения сложных аналитических задач. В частности, к таким задачам следует отнести поиск косвенных и неявных связей и взаимодействий между сущностями различного характера: документами, событиями, местами, лицами, организациями, предметами.

Графический интерфейс рассматриваемых программных систем должен содержать набор мощных инструментариев, созданных специально для осуществления визуально-аналитической деятельности при работе с данными.

Для осуществления визуально-аналитической деятельности при работе с данными из социальных сетей необходимо обладать аппаратом подключения к различным внешним информационным ресурсам и позволяет осуществлять интеграцию в первую очередь с ведомственными справочно-учетными и фактографическими базами данных, а также с открытыми источниками сети интернет, в том числе с социальными сетями. Данный инструмент может быть применен как для выполнения поиска и загрузки сведений из этих ресурсов, так и для осуществления непрерывного мониторинга и синхронизации с ними. Визуально-аналитическая деятельность при работе с данными из социальных сетей предполагает:

- выполнение аналитических задач различного характера;
- накопление и мониторинг данных из различных источников в едином хранилище, как в режиме реального времени, так и по заданному расписанию;
- выявление скрытых связей между сущностями и выявление замкнутых групп;
- организацию и визуализацию информации в виде интерактивных графов;
- автоматизированное построение досье;
- фильтрацию массивов данных с помощью набора исчерпывающих классификаторов;
- загрузку и обработку структурированных и неструктурированных файлов.

Следует заметить, что одним из важных компонентов рассматриваемых систем являются расчетные модули или так называемые виджеты. Они представляют собой инструмент выполнения аналитического запроса в базу данных и отображения результата этого запроса. Подобные модули позволяют решать различные аналитические задачи, в том числе выполнять статистические расчеты. При этом результат выполнения запроса, как правило, представляется в виде таблицы, графика или карты.

Для повышения эффективности аналитической деятельности данных из соцсетей рассматриваемые системы оснащены соответствующим веб интерфейсом и возможностью визуальной работы с графом, которая заключается в выявлении прямых и косвенных связей между сущностями базы данных проекта. Например, работа осуществляется посредством формирования и анализа выборки из базы данных проекта, представляемой в виде диаграммы связей графа объектов.

Организация работы с графами в веб интерфейсе позволяет осуществлять следующие мероприятия:

- выполнение визуального и статистического анализа;
- поиск информации в базе данных;
- ручное и автоматическое построение диаграмм связей;
- получение связей объектов или цепочек связей между парой объектов;
- стилизацию и фильтрацию элементов;
- экспорт отчетных данных в файлы текстовых и графических форматов.

Необходимо также отметить, что удобство рассматриваемых программных систем также заключается в том, что интерфейс рабочей области представляет собой визуальное пространство, на котором размещаются прорабатываемые объекты. Данная область условно не имеет границы (по типу электронной карты), поэтому позволяет располагать большое количество элементов, а также выполнять масштабирование и панорамирование (по аналогии с картографическими инструментами). Размещение элементов в пространстве рабочей области происходит как вручную пользователем, так и автоматически при помощи инструментов построения.

Следующим компонентом систем, осуществляющих анализ данных из соцсетей является инструмент полнотекстового поиска по атрибутам объектов в базе данных проекта, а также подсветка (выделение) найденных элементов в рабочей области текущего документа. Поиск по заданному ключевому слову или фразе происходит по всем атрибутам указанного класса, в том числе по текстам файловых вложений. Найденные объекты могут быть добавлены пользователем в рабочую область документа.

При этом результаты поиска возвращаются сгруппированными по классам, с указанием количества найденных элементов. Кроме того, в панели поиска для каждого объекта отображается количество связей в базе данных проекта.

Системы реализующие визуально-аналитическую деятельность при работе с данными могут функционировать в режиме «задача», который позволяет загружать сведения из различных информационных ресурсов, в том числе из реляционных и nosql баз данных, rest сервисов, файлов, а так же из открытых источников сети «Интернет» таких как социальные сети или поисковые сервисы.

Таким образом, из представленного выше материала можно констатировать, что применение правоохранительными органами систем, осуществляющих визуально-аналитическую деятельность при работе с данными из социальных сетей позволит эффективно противостоять противоправным действиям в виртуальном пространстве.

ЛИТЕРАТУРА

1. Основные возможности использования программного средства «Ostorus» для анализа информации из открытых источников / В. В Конобеевских, Д. К. Печенина // Сборник материалов всероссийской научно-практической конференции Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. – 2018. – С. 317 – 318.

СВЕДЕНИЯ ОБ АВТОРЕ

Конобеевских Владимир Валерьевич. Доцент кафедры автоматизированных информационных систем ОВД. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: vkonobeevskikh@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53. Тел. (473) 2005-183.

Konobeevskikh Vladimir Valerevich. Associate professor of the automated information systems of interior units chair. Candidate of sciences (technical).

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-183.

Ключевые слова: социальная сеть, графический интерфейс, система, визуально-аналитическая деятельность.

Key words: social network, graphic interface, system, visual and analytical activities.

УДК 621.001

К ВОПРОСУ СПЕЦИФИКИ НАЧАЛЬНОГО ЭТАПА ПРОЕКТИРОВАНИЯ СИСТЕМ ОПОВЕЩЕНИЯ

TO THE QUESTION OF THE SPECIFICS OF THE INITIAL STAGE OF DESIGN OF WARNING SYSTEMS

В данной статье рассматриваются актуальные вопросы начального этапа проектирования систем речевого оповещения, основной задачей которых является обеспечение трансляции понятной информации, направленной на защиту людей.

This article discusses the current issues of the initial stage of the design of voice warning systems, the fundamental task of which is to ensure the transmission of clear information aimed at protecting people.

Для крупных городов сегодня остается актуальной, к сожалению, проблема решения непростых задач по обеспечению безопасности людей, которые находятся в офисах, многочисленных торговых центрах, в бассейнах, кинотеатрах, в спортивных сооружениях. В таких местах в любое время высок риск возникновения чрезвычайных ситуаций. Как правило, общество начинает задумываться об обеспечении безопасности в местах массового нахождения людей, когда происходит трагедия с человеческими жертвами.

В настоящее время существующие технические нормы в сфере безопасности обязательно содержат в себе требования по оборудованию зданий, сооружений и территорий с массовым пребыванием людей системами оповещения. Это так называемые системы оповещения и управления эвакуацией (СОУЭ) людей. Сейчас одной из важнейших является задача интеграции различных подобных систем. Под интеграцией подразумевается объединение СОУЭ как на верхнем уровне, где требуется применение современных цифровых технологий, так и на нижнем уровне, требующем надежных базовых решений. При решении любой из масштабных задач очень важно правильно выбрать так называемый базис, или точку опоры, с одной стороны, и материал для построения, с другой. К примеру, для проектирования и построения надежной интегральной системы оповещения с централизованным управлением необходимо обратиться к опыту построения систем оповещения и управления эвакуацией СОУЭ.

Системы управления оповещением и эвакуацией являются сравнительно новым направлением, как в области пожарной безопасности, так и в гражданской обороне, в энергетике, в сфере промышленности и транспорта. Есть различия организационные, предполагающие специфику в данных областях применения. Но общие требования к работе этих систем имеют одно направление – обеспечение максимальной безопасности людей, находящихся как на отдыхе, так и на работе [1].

Такие требования к вышеуказанным системам и их параметрам отражены в соответствующих нормах пожарной безопасности и других нормативных документах. Однако, вопросы как раз технической реализации, в частности, особенностей построения для различного уровня сложности и функционального назначения объектов не проработаны детально. Поразительно быстро развивающиеся цифровые технологии оказывают существенное влияние на многие сферы человеческой деятельности, в том числе, и сферу безопасности, выдвигают повышенные требования к профессионалам, работающим в этой сфере. Современный проектировщик обязательно должен осуществлять постоянную обратную связь с поставщиками и разработчиками. Применение той

или иной системы должно быть всесторонне обосновано и подкреплено расчетами, проведенными на основании актуальных, современных методик.

Основным документом, содержащим необходимые для проектирования систем оповещения и управления эвакуацией – СОУЭ технические нормы, является свод правил СП 3-13130-2009, разработанный в соответствии со статьей 84 федерального закона от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности». В указанном нормативном документе (НД) дается такое определение: СОУЭ – это комплекс организационных мероприятий и технических средств, предназначенный для своевременного обращения к людям с информацией о возникновении пожара и необходимых путях эвакуации [2].

К СОУЭ предъявляются следующие основные требования [3]:

- надежное функционирование;
- в случае поступления сигнала о пожаре минимальное время реакции;
- надежная защита доступа к органам управления;
- при необходимости возможность автоматической работы;
- присутствие системы контроля для входных и выходных шлейфов;
- протоколирование всех событий;
- организация резервного питания.

СОУЭ 3-5 типов оповещения являются системами речевого оповещения, у которых в основе является звуковой тракт. Звуковой тракт представляется элементом трех-этапной структуры, рис.1:

- создание;
- распространение;
- восприятие.

Таким образом, основной задачей данной структуры является передача звуковой информации от источника к получателю в максимально понятном, неискаженном виде и с необходимой громкостью.



Рис. 1. Распространение звукового сигнала

При разработке звуковых систем оповещения должна учитываться специфика всех трех этих составляющих. Этап создания. Здесь основное значение имеет звуковой тракт, включающий следующие этапы преобразования:

- звуковой источник (микрофон), как преобразователь акустической энергии на входе в электрический сигнал на выходе;
- система усиления звука;
- громкоговоритель, как преобразователь электрического сигнала на входе в слышимый акустический сигнал на выходе.

Важнейшим выступает такое понятие, как “нормирование” звукового тракта, то есть оптимально согласованное взаимодействие всех элементов системы, обеспечивающих эффективное прохождение звукового сигнала с входа на выход.

Согласование системы звукоусиления с нагрузкой корелирует с решением одной из таких важных задачи, как расчет потерь на проводах – задаче, предшествующей электроакустическому расчету. В СОУЭ усилитель сигнала соединяется с громкоговорителями линиями связи (шлейфами). Как и в любых линиях связи, в них возникают потери, что может являться причиной существенного снижения качества передаваемого. С учетом этого, СОУЭ, начиная со 2-го типа, разбиваются на зоны. В каждую из зон прокладывается, как минимум, одна линия (шлейф), нагруженная громкоговорителями. Величина суммарной нагрузки (Вт) в линии определяется результатами электроакустических расчетов, в процессе которых определяются необходимые уровни звукового давления для каждого громкоговорителя.

Расчет потерь на проводах связан с решением двух задач – расчетом потерь по напряжению (мощности) при условии, что проводник заранее выбран, и расчетом минимально необходимого сечения проводника при условии, что нужный кабель еще предстоит выбрать.

На этапе распространения звука в качестве среды распространения данного звука рассматривается воздушное пространство. Этот этап в полной мере учитывается в акустических расчетах, результаты которых являются основой для выбора технических средств.

Электроакустический расчет опирается на требования нормативных документов (НД) и определяется параметрами защищаемого помещения – его геометрическими размерами и уровнем шума.

В процессе электроакустического расчета рассчитываются уровни звукового давления в определенных расчетных точках (РТ). Данный расчет основывается на следующих постулатах:

1. При расчете необходимо учитывать параметры всего звукового тракта, оказывающие непосредственное влияние на характеристики громкоговорителей, которые являются, в свою очередь, входными для электроакустического расчета. Геометрическая лучевая теория – наиболее простая, эффективная и удобная для проведения элементарного электроакустического расчета. Физические принципы, разработанные в оптике, формируют основу геометрической лучевой теории. Простота данной теории вытекает из ее наглядности. Геометрическая лучевая теория акустического расчета основана на законах геометрической оптики, в которой:

- звуковую волну отождествляют со световым лучом;
- угол отражения звуковой волны равен углу ее падения;
- оба луча, падающий и отраженный, рассматриваются в одной плоскости, что для акустических волн вполне справедливо, если размеры отражающих поверхностей больше длины волны нижней границы частотного диапазона для 0,2кГц – 1,7м, а размеры неровностей отражающих поверхностей меньше длины волны верхней границы частотного диапазона для 5кГц – 0,068м.

2. Для упрощения расчета рассматривается изучение одного отражения звукового сигнала от пола или от стены (что вполне согласуется с понятием первичных отражений в акустике), что позволяет, с одной стороны, существенно упростить расчетную часть, а с другой – получить приемлемые результаты для основных типов озвучиваемых помещений (коридоры, фойе, аудитории). Для озвучивания объектов со сложной архитектурой (формой) – театров, концертных залов и т.п. имеется возможность использовать альтернативные методы расчета, такие как программные средства и измерительные приборы.

3. Отдельный интерес представляют реверберационные процессы, присутствующие в закрытых помещениях. Реверберация имеет два значения — процесс постепенного уменьшения интенсивности звука при его многократных отражениях или время, в течение которого звуковое давление уменьшится на 60дБ.

Стоит учесть такой важный момент, касающийся точности расчетов. Так, например, в ГОСТе по шуму 2005 г. предполагаемая точность расчетов составляет 0,1%. В расчетах электроакустических это приводит к необходимости определения уровня шума в защищаемых помещениях с указанной точностью, что не представляется возможным, так как в качестве параметра шума принимается не конкретное, а среднестатистическое усредненное значение. Кроме того, не представляется возможным расчет с точностью даже в 1%, так как значения т.н. “пространственного угла”, используемого при расчетах, даются (в табличном виде) уже с шагом в 3дБ. Для устойчивой разборчивости данная разница должна составлять минимум 6дБ. В нормативной же документации данный запас составляет 15дБ [4]. С учетом вышесказанного, очень важной представляется задача создания современных актуальных методик, учитывающих подобные моменты.

Этап восприятия. Восприятие обуславливается общими физиологическими особенностями человека вообще и индивидуальными особенностями отдельного человека в частности. Поэтому решения задач расчета акустического направления могут значительно отличаться, к примеру, для детских развлекательных центров, домов престарелых или бассейнов. Подход должен быть индивидуален, за верным решением таких задач стоят довольно сложные расчеты, от которых зависят жизни людей. Учет особенностей восприятия отражается, кроме того, в необходимости осуществлять электроакустический расчет в определенных единицах – децибелах – уровнях звукового давления. Важнейшую роль в системах оповещения играет так называемая речевая система оповещения. В международных стандартах указывается необходимость обеспечения населения понятной информацией, направленной на защиту людей. «Понятность» донесенной до человека информации имеет важнейшее значение в то короткое время, которое отведено для эвакуации напуганных людей, готовых в любой момент к паническому поведению. Учет специфики восприятия человека связан с разработкой такой важной темы, как расчет разборчивости. Область, в которой перспективны разработки в этом направлении, называется “психоакустикой”.

ЛИТЕРАТУРА

1. Информационно-коммуникационные технологии обеспечения безопасности жизнедеятельности: монография/ Под общ. ред. П.А. Попова, МЧС России. – М.: ФГУ ВНИИ ГОЧС (ФЦ), 2009. – 279 с.
2. Федеральный закон от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности».
3. Свод правил СП 3.13130-2009 «Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре».
4. Кочнов, О.В. Особенности проектирования систем оповещения: учебное пособие / О.В. Кочнов, Издательство «Стерх», ИП Коськин А.М., 2012.–154 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Кузнецова Наталья Николаевна. Преподаватель кафедры математики.
Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина.
E-mail: slavna.1@ya.ru
Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54 «А».
Тел. 8 (908) 137-26-73.

Kuznetsova Natalia Nikolaevna. Teacher of the Department of mathematics.
Air force Academy named after Professor N. E. Zhukovsky and Y. A. Gagarin.

E-mail: slavna.1@ya.ru
Russia, 394064, Voronezh, St. Old Bolsheviks, 54 "A".
Tel. 8 (908) 137-26-73.

Ключевые слова: системами речевого оповещения, передача информации, обеспечение безопасности, звуковой тракт.

Key words: voice warning systems, information transmission, security, sound path.

УДК 654.924/926

Лунёв Юрий Станиславович,
кандидат технических наук;
Амирханян Ваге Гагикович

ПРОГРАММНЫЙ КОМПЛЕКС СОПРЯЖЕНИЯ МИКРОКОНТРОЛЛЕРА С ЭВМ ДЛЯ КОНТРОЛЯ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

SOFTWARE COMPLEX OF MICROCONTROLLER PAIRING WITH COMPUTER FOR CONTROL OF SAFETY INFORMATIZATION OBJECT

В статье проанализирован рынок охранных устройств и выбран оптимальные состав для объекта информатизации. Разработана программа сопряжения технических устройств.

The article analyzes the market of security devices and selects the optimal composition for the object of information. A program for interfacing technical devices has been developed.

Различные типы помещений зачастую оснащаются охранной сигнализацией (ОС) с интерфейсом управления ею. Цель ОС – пресечение любой возможности несанкционированного проникновения в помещение или на территорию находящиеся под охраной. Датчики, входящие в состав ОС, являются ее основой, их основной задачей является передача информации на центральный пульт. ОС может эксплуатироваться как автономно, так и в комплексе с другими системами безопасности на охраняемом объекте. Автоматизированная система ОС позволяет 24 часа в сутки контролировать помещение или территорию находящиеся под охраной.

На текущий момент рынок охранных услуг предлагает много отечественного и импортного оборудования, с помощью которого можно построить систему безопасности любого объекта. Можно построить охранную систему с различным функционалом с наименьшей насыщенностью средствами охранно-пожарной сигнализации, до усложнённой, системы безопасности, соединяющей в себе системы видеонаблюдения, контроля доступа, учета рабочего времени, а также охранно-пожарную и тревожную сигнализации, систему оповещения о кризисных ситуациях [1, 2].

Предлагаемые варианты систем сигнализации имеют ряд недостатков. Те образцы, которые полностью удовлетворяют современным требованиям, имеют высокую стоимость. Более простые системы, как правило, не обеспечивают многорубежной охраны. Другим серьезным недостатком отсутствие возможности интеграции в единую охранно-пожарную систему сигнализации. Поэтому целью работы является обеспечение контролируемого доступа в охраняемое помещение с помощью разработанной системы охранной сигнализации на базе программируемого микроконтроллера рисунок 1, рисунок 2.

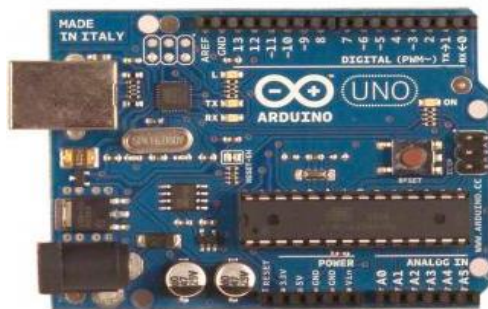


Рис.1. Плата Arduino Uno

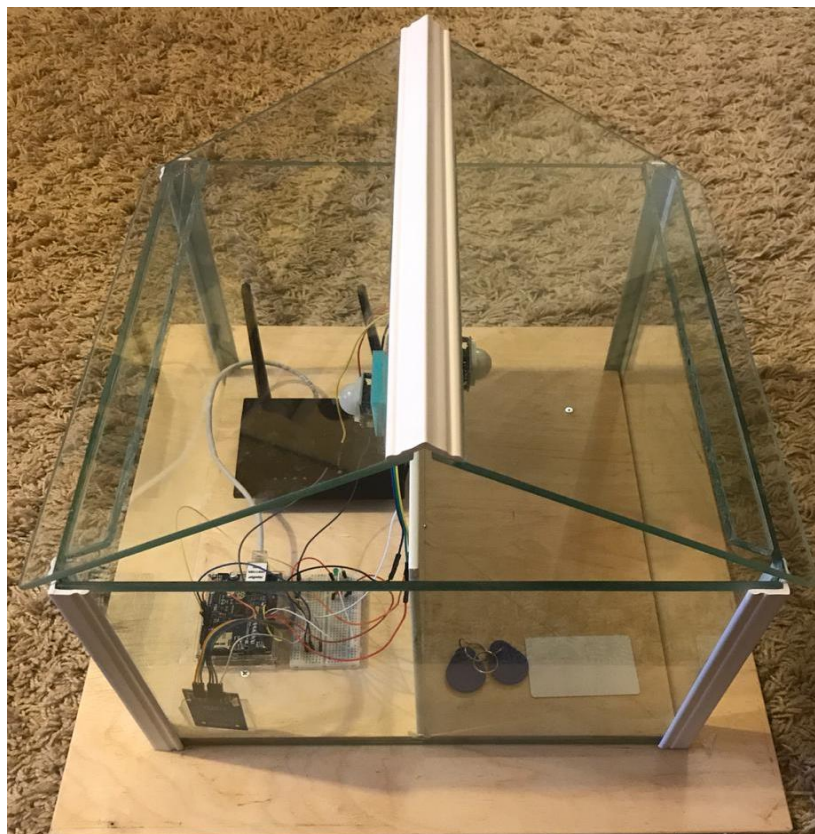


Рис. 2. Макет объекта информатизации

Для создание охранного комплекса системы охранной сигнализации было отдано предпочтение микроконтроллеру работающего на плате *Arduino Uno* с установленным микроконтроллером (МК) *Atmega*. Выбор был сделан с учетом стоимости самой платы, ее производительности и возможностей по подключению периферийных устройств. Одним из существенных преимуществ платформы *Arduino* является то, что ее среда разработки распространяется свободно. Управление сигнализацией осуществляется через интернет-браузер с помощью интерфейса *Ethernet* или *Fast Ethernet*. В будущем возможно совершенствование WEB-интерфейса для управления сигнализацией и сбора информации о ее состоянии, а также интеграция устройства в единую систему контроля и управления доступом.

Реализованное устройство позволяет обнаруживать факт несанкционированного доступа (НСД) и передавать информацию на компьютер через локальные и глобальные вычислительные сети. Используются извещатели, основанные на разных физических принципах, тем самым обеспечивается многорубежная охрана. В данном проекте предложена схема с двумя датчиками движения (*PIR*-сенсорами и *RFID* меткой). Управляется

сигнализация любым WEB-браузером благодаря использованию платы расширения Ethernet. Кроме того, код программы работы управляющего устройства легко модифицируется, что позволяет расширять возможности устройства посредством подключения дополнительных извещателей, в том числе основанных на других физических принципах, и посредством интегрирования сигнализации в единую систему контроля и управления доступом.

ЛИТЕРАТУРА

1. ГОСТ Р 50776-95: Системы тревожной сигнализации. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.

2. Соммер У. Программирование микроконтроллерных плат Arduino/Freeduino / У. Соммер. – СПб: Изд-во СПб – 2012. – 246 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Лунёв Юрий Станиславович. Старший преподаватель кафедры автоматизированных информационных систем органов внутренних дел. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: xalt@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-51-87.

Амирханян Ваге Гагикович. Преподаватель кафедры физической подготовки.

Воронежский институт МВД России.

E-mail: amirhanyan@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-54-01.

Lunev Yuri Stanislavovich. Senior lecturer of the chair of Computer-Based Information Systems of the law enforcement agencies. Candidate of the technical sciences.

Voronezh Institute of the Ministry of the Interior of the Russian Federation.

Work address: Russia, 394065, Voronezh, Patriotov Pr., 53.

Tel. (473) 200-51-81.

Amirkhanyan Vage Gagikovich. Lecturer of the chair of physical fitness. Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: fitness@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-54-01.

УДК 624

Мещерякова Татьяна Вячеславовна,
кандидат физико-математических наук;
Фирюлин Максим Евгеньевич,
кандидат технических наук;
Родионов Евгений Александрович

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ СЕРВИСА ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ДЕЖУРНЫХ ЧАСТЕЙ В ИСОД МВД РОССИИ

FUNCTIONAL MODEL OF THE SERVICE SUPPORT ACTIVITIES ACTIVE- DUTY UNITS IN ISAD OF THE MIA OF RUSSIA

В статье рассматривается построение функциональной модели сервиса обеспечения деятельности дежурных частей как один из этапов разработки учебного макета данного сервиса.

The article deals with the construction of a functional model of the service to ensure the activities of duty units as one of the stages of the development of the educational layout of the service.

В настоящее время каждый сотрудник ОВД имеет доступ к Единой системе информационно-аналитического обеспечения деятельности МВД России. Доступ к отдельным сервисам ИСОД МВД России предоставляется в соответствии с должностными обязанностями сотрудника. Преподаватели, курсанты и слушатели образовательных организаций не имеют доступ к сервисам оперативно-служебной деятельности, однако процесс обучения предполагает изучение этих сервисов, в соответствии с их специальностью и специализацией. В связи с этим необходимо обеспечение возможности работы с данными сервисами либо в тестовом режиме, либо с учебными макетами таких сервисов.

Воронежский институт МВД России проводит повышение квалификации сотрудников по направлениям, связанным с работой сервиса обеспечения деятельности дежурных частей (СОДЧ). Для формирования умений и навыков работы с СОДЧ преподавателями кафедры АИС ОВД Воронежского института МВД разрабатывается учебный макет СОДЧ ИСОД МВД России. Одним из этапов разработки такого макета является построение функциональной модели сервиса.

Наиболее распространенной формой представления функциональных моделей является представление их в виде графа. Графовое представление дает возможность отразить функциональную иерархию исследуемых процессов, получаемую в результате декомпозиции функций этих процессов [1,2,3]. В основе такой иерархии лежит графовое представление целевой функции исследуемого процесса в наиболее обобщенном виде, определяемое как обобщенная функциональная модель нулевого уровня. Детализация целевой функции, позволяющая выявить полный набор подфункций, образует первый уровень декомпозиции обобщенной функциональной модели исследуемого процесса.

В нашем случае функциональная модель первого уровня декомпозиции целевой функции содержит четыре функции:

$\phi_1^{(1)}$ - «Инициализация информационного процесса в СОДЧ»;

$\phi_2^{(1)}$ – «Сбор информации в СОДЧ».

$\phi_3^{(1)}$ – «Обработка информации в СОДЧ».

$\phi_4^{(1)}$ – «Анализ информации в СОДЧ».

Графовое представление данной функциональной модели иллюстрируется рис.1.

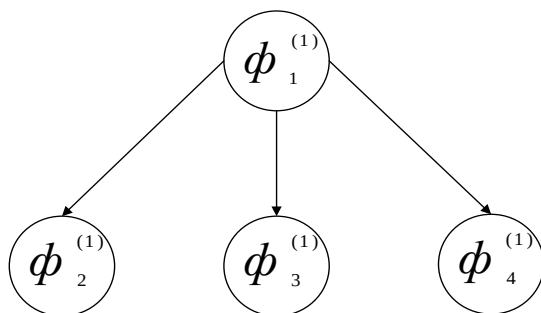


Рис. 1.

Функциональная модель «Сбор информации в СОДЧ» содержит 5 функций ($\phi_{2.1}^{(2)} - \phi_{2.5}^{(2)}$) (рис. 2.).

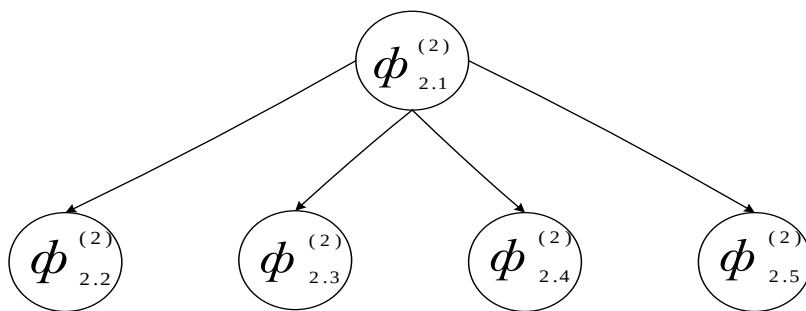


Рис. 2.

Представленные на рисунке 2 состояния графа идентифицируются следующим образом:

$\phi_{2.1}^{(2)}$ - «Инициализация сбора информации»;

$\phi_{2.2}^{(2)}$ – сервис «Книга учёта сообщений о происшествиях»;

$\phi_{2.3}^{(2)}$ – сервис «Журналы»;

$\phi_{2.4}^{(2)}$ – сервис «Оперативная ориентировка»;

$\phi_{2.5}^{(2)}$ – сервис «Доставленные».

Функциональная модель «Обработка информации в СОДЧ» содержит 3 функций ($\phi_{3.1}^{(2)} - \phi_{3.3}^{(2)}$) (рис. 3.).

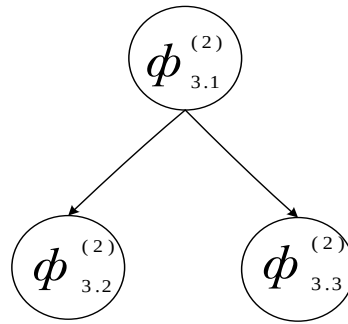


Рис. 3.

Представленные на рисунке 3 состояния графа идентифицируются следующим образом:

$\phi_{3.1}^{(2)}$ - «Инициализация обработки информации»;

$\phi_{3.2}^{(2)}$ – сервис «Управление силами и средствами»;

$\phi_{3.3}^{(2)}$ – сервис «ППС».

Функциональная модель «Анализ информации в СОДЧ» содержит 3 функций ($\phi_{4.1}^{(2)}$ – $\phi_{4.3}^{(2)}$) (рис. 3.).

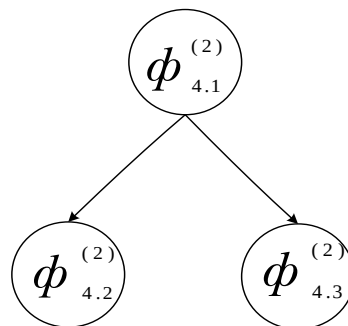


Рис. 4.

Представленные на рисунке 4 состояния графа идентифицируются следующим образом:

$\phi_{3.1}^{(2)}$ - «Инициализация обработки информации»;

$\phi_{3.2}^{(2)}$ – сервис «Сводка»;

$\phi_{3.3}^{(2)}$ – сервис «Аналитика».

Детализация любой функциональной модели второго уровня декомпозиции целевой функции «Инициализация информационного процесса в СОДЧ» позволяет перейти к функциональному описанию информационных процессов в СОДЧ на третьем уровне декомпозиции рассматриваемой целевой функции.

Рассмотрим графовое представление функциональной модели «Аналитика» (рис. 5).

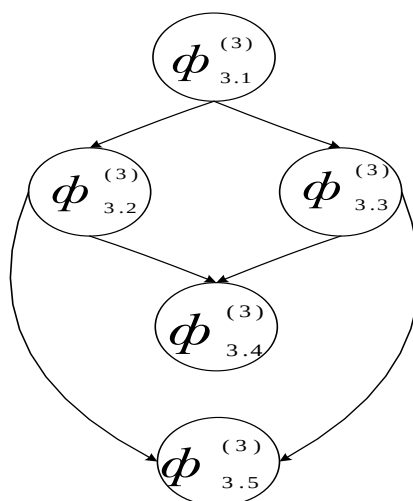


Рис. 5.

Представленные на рисунке 3 состояния графа идентифицируются следующим образом:

$\phi_{3.1}^{(3)}$ - Инициализация формирования отчета;

$\phi_{3.2}^{(3)}$ – Динамический отчет;

$\phi_{3.3}^{(3)}$ – Статистический отчет;

$\phi_{3.4}^{(3)}$ – Удаление отчета.

$\phi_{3.5}^{(3)}$ – Вывод отчета.

Как следует из результатов структуризации целевой функции на третьем уровне ее декомпозиции, согласно [4] возможно представление последовательностей выполняемых функций в терминах марковского процесса. Это свидетельствует о достаточной степени детализации целевой функции и возможности перехода к методам формализации полученного функционального описания для дальнейшего его математического представления.

ЛИТЕРАТУРА

1. Математическая модель автоматизированной информационной системы обработки информации по опознанию личности/ Т.В. Мещерякова, Е.А. Рогозин, Ю.С. Лунев// XI Всероссийская научно-практическая конференция "Математические методы и информационно-технические средства": сборник трудов конференции. Краснодар, 2015 г. С. 152-155.
2. Функциональная модель информационных процессов в территориальных сегментах единого информационного пространства органов внутренних дел / Т.В. Мещерякова, С.А. Баркалов // Системы управления и информационные технологии, Москва-Воронеж, «Научная книга», 2014, Т. 57. № 3.1. С. 112-116.
3. Татт У. Теория графов: пер. с англ. / У. Татт. — М.: Мир, 1988. — 424 с.
4. Тихонов В.И., Миронов М.А. Марковские процессы. —М.: «Сов. радио», 1977. — 488 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Мещерякова Татьяна Вячеславовна. Начальник кафедры автоматизированных информационных систем ОВД. Кандидат физико-математических наук.

Воронежский институт МВД России.

E-mail: mescher73@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-81.

Фирюлин Максим Евгеньевич. Преподаватель кафедры автоматизированных информационных систем органов внутренних дел. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: orugejnik68@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-56-46.

Родионов Евгений Александрович. Преподаватель кафедры тактико-специальной подготовки.

Воронежский институт МВД России.

E-mail: eugeny.svistunov2017@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-51-52.

Mescheryakova Tatiana Vyacheslavovna. Deputy head of the chair Department of Automated Information Systems of the Law Enforces Agencies. Candidate of Physical and Mathematical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Phone. (473) 200-51-81.

Firyulin Maxim Evgenievich. Lecturer of the chair of Automatic Informative Systems of the Law Enforces Agencies. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: orugejnik68@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Phone. (473) 200-56-46.

Rodionov Evgeny Aleksandrovich. Lecturer at the department of special tactics.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Phone. (473) 200-56-42

Ключевые слова: сервис обеспечения деятельности дежурных частей, функциональная модель, уровень декомпозиции, учебный макет.

Keywords: service support activities active-duty units, the functional model, the decomposition level, educational layout.

УДК 621.3

Мишин Сергей Александрович,
кандидат технических наук, доцент;
Солодуха Роман Александрович,
кандидат технических наук, доцент

**РАЗРАБОТКА КОНЦЕПТУАЛЬНОЙ МОДЕЛИ СИСТЕМЫ
АВТОМАТИЗИРОВАННОГО МОНИТОРИНГА СОСТОЯНИЯ СЛУЖЕБНОЙ
ДИСЦИПЛИНЫ И ЗАКОННОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ**

**THE DEVELOPMENT OF AUTOMATED MONITORING SYSTEM CONCEPTUAL
MODEL OF THE CONDITION OF THE SERVICE DISCIPLINE AND LEGALITY
IN THE INTERNAL AFFAIRS**

В статье предложена концептуальная модель системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел. Рассмотрены автоматизированные функции, которые должна исполнять данная система, и подход к их реализации.

The article proposes the automated monitoring system conceptual model of the condition of the service discipline and legality in the internal affairs. The automated functions that this system must perform and the approach to their implementation are considered.

Введение. В целях получения достоверной информации и своевременного реагирования на происшествия с участием сотрудников ОВД РФ, федеральных государственных гражданских служащих (ФГГС) и работников системы МВД России, осуществления контроля за принятием организационно-правовых мер, направленных на профилактику нарушений служебной дисциплины и законности, инспекцией по личному составу Управления организации морально-психологического обеспечения ДГСК МВД России осуществляется ежесуточный мониторинг сведений о происшествиях, представляемых органами, организациями и подразделениями МВД России [1].

В настоящее время в ДГСК МВД России отсутствуют программные средства, позволяющие автоматизировать процессы сбора поступающих сведений и систематизировать их в информационно-аналитические материалы в соответствии с требуемыми параметрами, что не позволяет оптимизировать систему анализа и учета информации о состоянии дисциплины и законности в ОВД. Использовать для этих целей введенный в эксплуатацию Сервис обеспечения кадровой деятельности ИСОД МВД России не представляется возможным, поскольку сведения о происшествиях, принятых по ним мерах реагирования, вынесенных судебных решениях не являются объектами учета указанного сервиса, а в его структуре отсутствует подсистема, предназначенная для организации сбора, учета, накопления и анализа подобного рода информации.

Актуальность темы исследования обуславливается наличием противоречия между существенным влиянием мониторинга сведений о происшествиях с участием сотрудников ОВД РФ, ФГГС и работников системы МВД России на осуществление контроля за принятием организационно-правовых мер, направленных на профилактику нарушений служебной дисциплины и законности в ОВД, с одной стороны и недостаточным развитием инструментальных средств, позволяющих автоматизировать процессы сбора, учета, накопления и анализа поступающих сведений о происшествиях с другой стороны. Разрешение данного противоречия возможно путем создания

соответствующей автоматизированной информационной системы. Присутствие единого центра хранения данных (БД) с одной стороны позволит упростить накопление необходимой информации, а с другой стороны повысит оперативность их анализа.

Организационная характеристика предметной области. В настоящее время порядок представления в ДГСК МВД России сведений о происшествиях с участием сотрудников ОВД РФ (далее – «сотрудники»), федеральных государственных гражданских служащих (далее – «гражданские служащие») и работников системы МВД России ходе (далее – «работники») определен приказом этой МВД России мест от 26.06.2018 № 400 [1]. Согласно данного приказа в ДГСК МВД России поступает информация о следующих происшествиях с участием сотрудников, гражданских служащих и работников, а также принятых по ним мерах:

- возбуждение уголовного дела в отношении сотрудника, гражданского служащего или работника;
- ДТП с участием сотрудника, гражданского служащего или работника, повлекшее вред здоровью или смерть человека или получившее общественный резонанс в связи с распространением сведений в СМИ и (или) информационно-телекоммуникационной сети Интернет;
- управление сотрудником, гражданским служащим или работником транспортным средством в состоянии алкогольного, наркотического или иного токсического опьянения, а равно отказ от прохождения медицинского освидетельствования на состояние опьянения при управлении транспортным средством;
- гибель сотрудника, гражданского служащего или работника либо причинение ему тяжкого вреда здоровью;
- самоубийство сотрудника, гражданского служащего или работника;
- происшествие с участием сотрудника, гражданского служащего или работника, ставшее причиной нарушения прав и свобод граждан и получившее общественный резонанс в связи с распространением сведений в СМИ и (или) информационно-телекоммуникационной сети Интернет;
- сведения о судебных решениях по уголовным делам, возбужденным в отношении сотрудников, гражданских служащих или работников, в том числе уволенных со службы (работы) в ОВД РФ, совершивших уголовно наказуемое деяние в период прохождения службы (работы) в ОВД РФ.

Информация и сведения, указанные выше, направляются в формате текстового процессора Microsoft Word посредством СЭП ИСОД МВД России на адрес инспекции по личному составу Управления организации морально-психологического обеспечения ДГСК МВД России, где по средствам ручной обработки формируется ежесуточный отчет и происходит накопление обобщенной информации в формате табличного процессора Microsoft Excel (рис. 1).

Концептуальная модель системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел. На наш взгляд, разрабатываемая система должна автоматизировать следующие функции:

- ввод данных (первичной и итоговой информации, сведений о судебных решениях) в единую отчетную форму о происшествиях с участием сотрудников, гражданских служащих и работников и формирования на ее основе xml-файла, представляемого в ДГСК МВД России с использованием СЭП ИСОД МВД России;

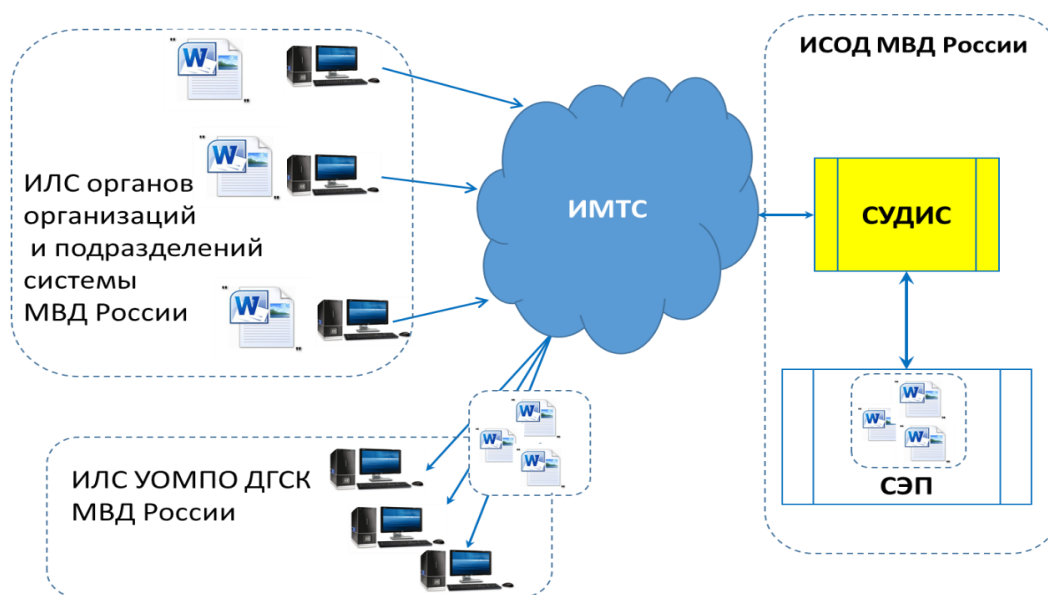


Рис. 1. Организационная характеристика предметной области

- сбор, учет и накопление сведений о происшествиях с участием сотрудников, гражданских служащих и работников в базе данных автоматизированной информационной системы мониторинга состояния служебной дисциплины и законности в ОВД;
- систематическое наблюдение за состоянием состояния служебной дисциплины и законности в ОВД;
- контроль за принятием мер реагирования по происшествиям с участием сотрудников, гражданских служащих и работников системы, сроками представления информации в ДГСК МВД России;
- поиск запрашиваемой информации о происшествии (его участниках и обстоятельствах) и формирование на основе заданных поисковых параметров информационно-аналитических материалов;
- экспорт формируемых на основе заданных поисковых параметров информационно-аналитических материалов в текстовый процессор Microsoft Word, табличный процессор Microsoft Excel для их последующего форматирования и анализа.

Входной информацией для автоматизированной информационной системы мониторинга состояния служебной дисциплины и законности в ОВД является [1]:

- наименование органа, организации или подразделения МВД России, представляемого сведения о происшествии в ДГСК МВД России,
- дата представления в ДГСК МВД России первичной и итоговой информации, сведений о судебных решениях;
- сведения об исполнителе разделов «Первичная информация», «Итоговая информация», «Сведения о судебном решении» отчетной формы о происшествиях;
- сведения об участнике(ах) происшествия;
- обстоятельства происшествия;
- сведения об общественном резонансе (публикации в СМИ);
- сведения о принятых организационно-правовых мерах по факту происшествия;
- сведения о судебных решениях.

При разработке автоматизированной информационной системы мониторинга состояния служебной дисциплины и законности в ОВД предлагается использовать двухзвенную архитектуру «клиент – сервер», подразумевающую присутствие определенного числа компьютеров, объединенных в сеть, один из которых выполняет особые управляющие функции (является сервером сети). Выбор архитектуры обоснован небольшим количеством пользова-

телей (сотрудники инспекции по личному составу (ИЛС) Управления организации морально-психологического обеспечения (УМПО) ДГСК МВД России), объема обрабатываемых данных и низкой активности SQL-запросов к таблицам БД. Подобная архитектура положительно зарекомендовала себя при построении системы автоматизированного мониторинга обучения иностранных граждан в образовательных организациях МВД России [2]. Концептуальная модель разрабатываемой системы представлена на рисунке 2.

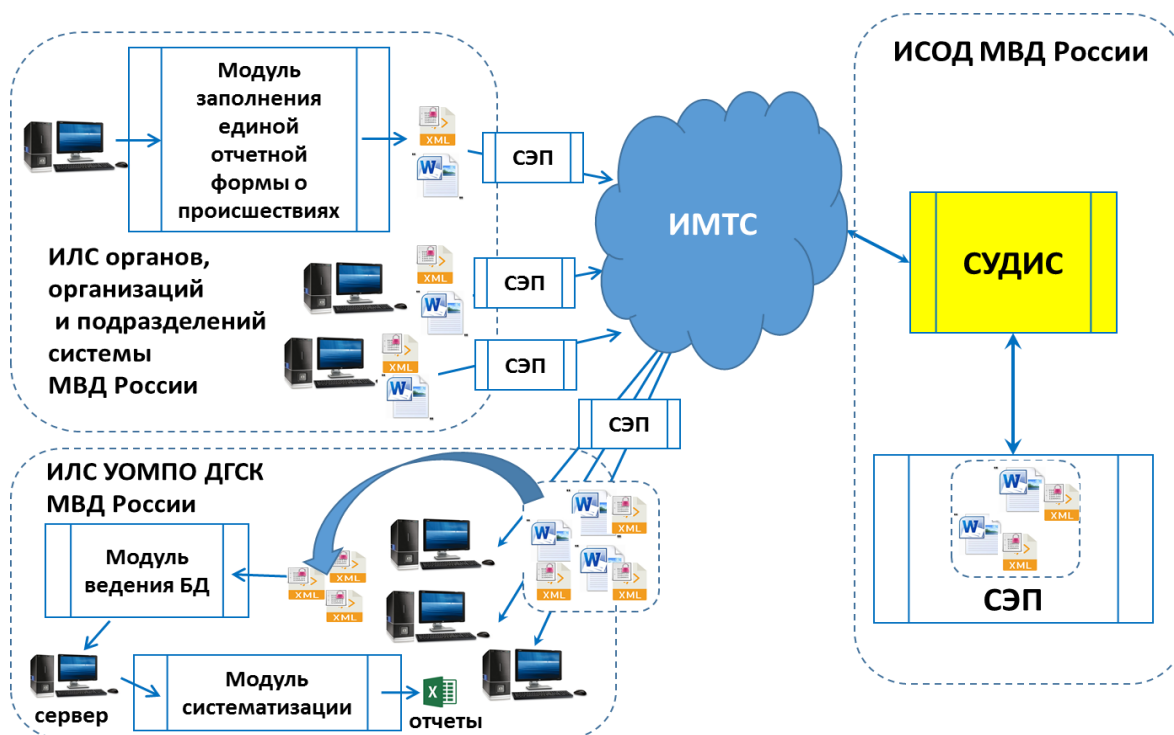


Рис. 2. Концептуальная модель системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел

Модель состава автоматизированной информационной системы мониторинга состояния служебной дисциплины и законности в ОВД предлагается представить в виде трех программных модулей (подсистем):

1) программный модуль заполнения единой отчетной формы о происшествиях с участием сотрудников, гражданских служащих и работников и принятых по ним мерах реагирования и формирования на ее основе xml-файла, представляемого в ДГСК МВД России с использованием сервиса электронной почты ИСОД МВД России, с целью автоматизации процессов сбора, актуализации и систематизации информации;

2) программный модуль ведения БД автоматизированной информационной системы мониторинга состояния служебной дисциплины и законности в ОВД на основе поступающих в ДГСК МВД России сведений о происшествиях в формате xml-файлов;

3) программный модуль систематизации в информационно-аналитические материалы сведений о происшествиях с участием сотрудников, гражданских служащих и работников.

Заключение. Проведенный анализ текущего состояния и перспектив автоматизации процессов сбора и систематизации в информационно-аналитические материалы сведений о происшествиях с участием сотрудников, гражданских служащих или работников позволил сделать следующие выводы:

- информация о происшествиях, представляемая органами, организациями и подразделениями МВД России ДГСК МВД России в формате текстового процессора Microsoft Word, слабо структурирована, что затрудняет ее автоматическую обработку;
- для автоматической обработки информации о происшествиях, представляемой органами, организациями и подразделениями МВД России ДГСК МВД России требуется разработка единого формата обмена сведениями о происшествии с участием сотрудников, гражданских служащих или работников;
- реализация предложенного в статье подхода к автоматизации процесса мониторинга состояния служебной дисциплины и законности в ОВД с единым центром хранения сведений о происшествиях позволит повысить эффективность контроля за принятием мер реагирования по происшествиям с участием сотрудников, гражданских служащих и работников, установления причин и условий, способствующих происшествиям, за счет оптимизации процессов сбора, учета, накопления и анализа поступающей в ДГСК МВД России информации.

ЛИТЕРАТУРА

1. Приказ МВД России от 26.06.2018 № 400 «О представлении информации о мерах реагирования по фактам происшествий с участием сотрудников органов внутренних дел Российской Федерации, федеральных государственных гражданских служащих и работников системы МВД России» - URL: https://мвд.пф/upload/site134/document_text/003/413/664/Prikaz_MVD_Rossii_ot_26.06.2018__400_O_predstavlenii_informatsii_o_merakh_reagirovaniya_po_faktam_proisshestiyy.doc (дата обращения: 04.03.2019).
2. Мишин С. А. Разработка концептуальной модели системы автоматизированного мониторинга обучения иностранных граждан в образовательных организациях МВД России [Текст] / С.А. Мишин, Р.А. Солодуха // Охрана, безопасность, связь. – 2018. – № 3(3). – С. 120- 125.

СВЕДЕНИЯ ОБ АВТОРАХ

Мишин Сергей Александрович. Заместитель начальника кафедры автоматизированных информационных систем ОВД. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: samishin@bk.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 2005-186.

Солодуха Роман Александрович. Доцент кафедры автоматизированных информационных систем ОВД. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: aisovd@vimvd.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 2005-184.

Mishin Sergey Alexandrovich. Deputy chief of the chair of automated information systems of interior units. Candidate of sciences (technical), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-186.

Solodukha Roman Alexandrovich. Assistant professor of the automated information systems of interior units chair. Candidate of sciences (technical), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-184.

Ключевые слова: автоматизированная информационная система; концептуальная модель; мониторинг состояния служебной дисциплины и законности в органах внутренних дел.

Key words: automated information system; conceptual model; monitoring of the condition of the service discipline and legality in the internal affairs.

УДК 004.9.

Мишин Александр Владимирович,
кандидат технических наук, доцент;

Мишин Сергей Александрович,
кандидат технических наук, доцент

ПРИНЦИПЫ ПРОВЕРКИ СОГЛАСОВАННОСТИ ЭКСПЕРТНЫХ МНЕНИЙ

PRINCIPLES OF THE CHECK TO CONSENSUS OF THE EXPERT OPINIONS

Рассматриваются правила проверки согласованности экспертных мнений, обеспечивающие их количественное оценивание, выявление причин расхождения мнений, исключение из рассмотрения аномальных оценок, решение вопроса о повторении экспертизы.

They are considered check-out procedures to consensus of the expert opinions, providing their quantitative оценивание, revealing the reasons of the divergence of the opinions, consideration exception anomalous estimation, decision of repetition of the expert operation.

Введение. Для решения слабоструктурированных задач в различных сферах деятельности [1-5] принято привлекать группы экспертов и, опираясь на их мнение, снять неопределённость данных об объектах экспертизы. Традиционно экспертное оценивание реализуется путём последовательной реализации пяти этапов, представленных на рис. 1.

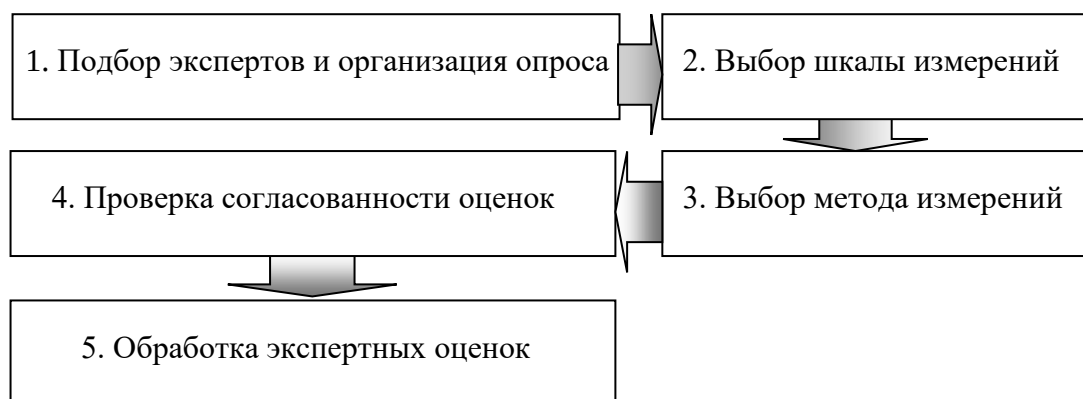


Рис. 1. Этапы экспертного оценивания

Цель работы – сформулировать правила реализации четвёртого этапа – проверки согласованности оценок, обеспечивающие их количественное оценивание, выявление причин расхождения мнений и исключение из рассмотрения аномальных оценок.

Проверка согласованности оценок экспертов. Схема проверки согласованности представлена на рис. 2. Получение количественной меры согласованности позволяет более обоснованно интерпретировать причины расхождения мнений.

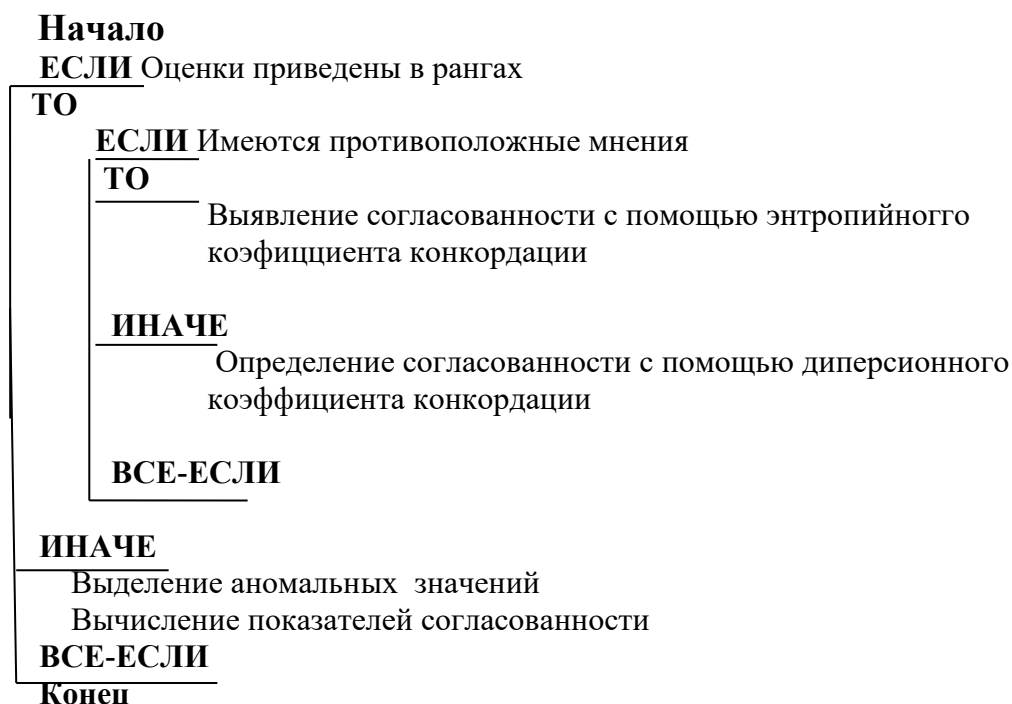


Рис. 2. Схема проверки согласованности оценок экспертов

Основную идею оценивания согласованности суждений экспертов можно интерпретировать геометрически: оценки экспертов – точки в m -мерном (по числу объектов экспертизы) пространстве. Чем компактнее они расположены, тем согласованность выше.

В настоящее время для проверки согласованности оценок проранжированных объектов, когда в качестве метода измерения было использовано ранжирование или парное сравнение, используются две меры согласованности: дисперсионный и энтропийный коэффициенты конкордации.

Вначале рассмотрим правила вычисления дисперсионного коэффициента конкордации. В этом случае исходные данные содержатся в матрице $\|r_{is}\|$ результатов ранжировки m объектов группой из d экспертов, элементы r_{is} которой указывают ранг, присвоенный s -м ($s = 1, \dots, d$) экспертом i -му ($i = 1, \dots, m$) объекту.

Просуммировав r_{is} по каждой строке матрицы получим обобщённые ранги объектов

$$r_i = \sum_{s=1}^d r_{is}, \quad i = 1, \dots, m.$$

Очевидно, что r_i являются случайными величинами. Следовательно, имеем оценку дисперсии

$$D = \frac{1}{m-1} \sum_{i=1}^m (r_i - \bar{r})^2, \quad (1)$$

где $\bar{r}$ – оценка математического ожидания (средняя арифметическая), равная

$$\bar{r} = \frac{1}{m} \sum_{i=1}^m r_i. \quad (2)$$

Дисперсионный коэффициент W_D конкордации определяется как отношение оценки дисперсии (1) к максимальному значению этой оценки ($W \in [0; 1]$):

$$W_D = \frac{D}{D_{\max}}, \quad (3)$$

где при отсутствии связанных рангов

$$D = \frac{\sum_{i=1}^m \left(\sum_{s=1}^d r_{is} - \bar{r} \right)^2}{m-1}, \quad (4)$$

$$D_{\max} = \frac{d^2(m^3 - m)}{12 \cdot (m-1)}. \quad (5)$$

Подставив выражения (4), (5) в формулу (3) и, сократив числитель и знаменатель на общий множитель $(m-1)$, окончательно имеем

$$W_D = \frac{12 \cdot \sum_{i=1}^m \left(\sum_{s=1}^d r_{is} - \bar{r} \right)^2}{d^2(m^3 - m)}. \quad (6)$$

В ряде источников вычисляемую часть числителя (6) обозначают как

$$S = \sum_{i=1}^m \left(\sum_{s=1}^d r_{is} - \bar{r} \right)^2, \quad (7)$$

что упрощает запись (но не вычисление) дисперсионного коэффициента конкордации:

$$W_D = \frac{12 \cdot S}{d^2(m^3 - m)}.$$

При наличии в ранжировках связанных рангов максимальное значение дисперсии уменьшается на величину

$$T = d \sum_{s=1}^d T_s, \quad (8)$$

где показатель T_s связанных рангов для s -той ранжировки вычисляется по формуле:

$$T_s = \sum_{k=1}^{H_s} h_k \cdot (h_k^2 - 1). \quad (8)$$

В выражении (8) число h_k определяется, исходя из количества совпадающих рангов k -той группе из H_s групп связанных рангов в s -той ранжировке. В простейшем случае, когда нет совпадающих рангов, H_s , h_k и, следовательно, T_s равны нулю.

Таким образом, при наличии в ранжировках связанных рангов коэффициент W вычисляется по следующей формуле:

$$W_D = \frac{12 \cdot S}{d^2(m^3 - m) - T}. \quad (9)$$

Коэффициент конкордации (КК) можно интерпретировать как вероятность полной согласованности экспертных оценок. Если все ранжировки экспертов совпадают, то $W_D = 1$. Если все ранжировки экспертов различаются между собой, $W_D = 0$. Решение о достаточной согласованности экспертных оценок по фактическому значению КК может быть принято на основе процедуры статистической проверки гипотез: величина $d \cdot (m - 1) \cdot W_D$ имеет χ^2 -распределение с $\nu = m - 1$ степенями свободы.

Энтропийный W_g КК вычисляется по формуле

$$W_g = 1 - \frac{H}{H_{\max}}, \quad (10)$$

где H – энтропия ранжировки объектов экспертизы;

$H_{\max}$ – максимальное значение энтропии.

Энтропия H определяется, исходя из значений оценок P_{is} вероятностей S -го ранга, присваиваемых i -му объекту:

$$H = - \sum_{i=1}^m \sum_{s=1}^d P_{is} \cdot \log P_{is}, \quad (11)$$

где оценки P_{is} вычисляются как отношение количества экспертов d_{is} , приписавших i -му объекту ранг S , к общему числу экспертов d :

$$P_{is} = \frac{d_{is}}{d}. \quad (12)$$

Максимальное значение энтропии достигается при $d_{is} = \frac{d}{m}$. Поэтому

$$H_{\max} = m \cdot \log m. \quad (13)$$

Если в результате опроса мнения экспертов разделяются на две компактные подгруппы с противоположными ранжировками, то энтропийный КК будет равен 0,7, а дисперсионный – нулю.

При непосредственной (количественной) оценке объектов в качестве меры согласованности экспертных мнений можно принять отношение суммы расстояний оценок от среднего значения к расстоянию этого среднего значения до начала координат.

Заключение. Во мнениях при оценивании объектов эксперты обычно расходятся. Важность согласованности оценок экспертов обусловлена тем обстоятельством, что в случае отсутствия таковой последующая групповая оценка не будет достаточно достоверной. Поэтому потребуются дополнительные организационные мероприятия, вплоть до проведения повторной экспертизы.

ЛИТЕРАТУРА

1. Афоничкин А.И. Управленческие решения в экономических системах [Текст]: учебник для вузов / А.И. Афоничкин, Д.Г. Михаленко. – СПб: Питер, 2009. – 480 с.
2. Демидов Б.А. Методы военно-научных исследований. Часть 3. Книга 1. [Текст]. – Харьков: ВИРТА ПВО, 1988. – 419 с.
3. Люгер Дж.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем [Текст] / Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 864 с.
4. Мистров Л.Е. Метод синтеза стратегий по урегулированию социально-экономических конфликтов [Текст] // Динамика сложных систем – XXI век. – 2016. – Т. 10. – № 4. – С. 41-65.
5. Саврасова Л.Н. Системный анализ познавательной деятельности субъекта на основе когнитивного подхода // Научный вестник ВГАСУ. Серия: Информационные технологии в строительных, социальных и экономических системах. – 2013. – № 2. – С. 82-87.

СВЕДЕНИЯ ОБ АВТОРАХ

Мишин Александр Владимирович, заведующий кафедрой правовой информатики, информационного права и естественно-научных дисциплин кандидат технических наук, доцент.

Центральный филиал ФГБОУВО «Российский государственный университет правосудия», г. Воронеж.

E-mail: odpvo@mail.ru

Россия, 394006, г. Воронеж, ул. 20-летия Октября, 95.

Тел. (473) 271-54-15.

Мишин Сергей Александрович. Заместитель начальника кафедры автоматизированных информационных систем ОВД. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: samishin@bk.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 2005-186.

Mishin Alexander Vladimirovich, chief of the chair of the legal informatics, information law and natural-science discipline, candidate of sciences (technics), assistant professor.

Central branch FGBOUVO «Russian State University of the Justice», Voronezh.

E-mail: odpvo@mail.ru;

Russia, 394006, Voronezh, 20 Years of October str., 95.

Tel. (473) 271-54-15.

Mishin Sergey Alexandrovich. Deputy chief of the chair of automated information systems of interior units. Candidate of sciences (technical), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-186.

Ключевые слова: эксперт; согласованность; коэффициент конкордации; ранжировка; ранг объекта; энтропия.

Key words: expert; consensus; the factor конкордации; ранжировка; the rank of the object; entropy.

УДК 654.924

Мишин Сергей Александрович,
кандидат технических наук, доцент;
Солодуха Роман Александрович,
кандидат технических наук, доцент

**ОРГАНИЗАЦИЯ И ВЕДЕНИЕ БАЗЫ ДАННЫХ СИСТЕМЫ
АВТОМАТИЗИРОВАННОГО МОНИТОРИНГА СОСТОЯНИЯ СЛУЖЕБНОЙ
ДИСЦИПЛИНЫ И ЗАКОННОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ**

**STRUCTURE AND MAINTENANCE OF DATABASE OF AUTOMATED
MONITORING SYSTEM CONCEPTUAL MODEL OF THE CONDITION OF THE
SERVICE DISCIPLINE AND LEGALITY IN THE INTERNAL AFFAIRS**

В статье описывается структура базы данных системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел. Приведено описание клиентского приложения для ведения базы данных.

The article proposes the database structure of automated monitoring system conceptual model of the condition of the service discipline and legality in the internal affairs. The client application for database maintenance is considered.

Введение. В рамках концептуальной модели системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел¹ предусмотрено наличие базы данных и модуля ведения базы данных. Для разработки данного сегмента системы использовалась связка MS SQL Server 2014 и MS Visual Studio 2015, язык C#, как оптимальная для построения 2-звенных информационных систем под управлением операционных систем семейства Windows. Специфика архитектуры системы, а именно, отсутствие централизованных классификаторов (не как в традиционном подходе [1, 2]), наложила отпечаток на структуру базы данных и приложение, что показано в данной статье. На рисунке 1 приведена обобщенная схема функционирования описываемого сегмента информационной системы.

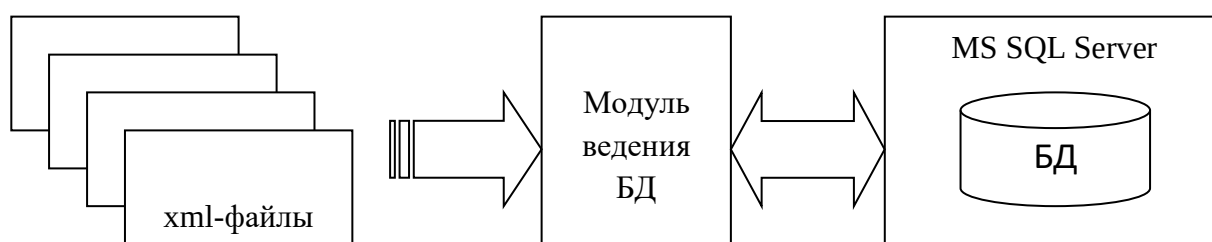


Рис. 1. Схема ведения базы данных

Организация базы данных. База состоит из следующих таблиц (Рисунок 2):

- Case – общая информация о происшествии;
- Person – информация об участнике происшествия;
- Crime_case – информация об уголовном деле;
- Crime_cod – информация о статьях по которым возбуждено уголовное дело;

¹ Мишин С.А., Солодуха Р.А. Разработка концептуальной модели системы автоматизированного мониторинга состояния служебной дисциплины и законности в органах внутренних дел / в данном сборнике.

- DTP – информация о ДТП;
- Drunk_driver – сведения о выявлении управлением транспортным средством в состоянии опьянения;
- Court_crime_cod – сведения о статьях уголовного кодекса в судебных решениях;
- Media – сведения о СМИ, где опубликована информация о происшествии;
- Media_comment – сведения о СМИ, где опубликованы комментарии представителей ОВД по происшествию;
- Case_DB – даты фиксации информации в базе данных;
- spr_FO – справочник федеральных округов;
- spr_CO – справочник территориальных органов.

Отдельно расположены таблицы с федеральными округами и территориальными органами, т.к. задача добавления данного сегмента была поставлена в процессе эксплуатации базы для получения отчетов с группировкой по федеральным округам. Поскольку наименования территориальных органов хранятся на клиентской стороне, и организовать соединение таблиц типу поля varchar(max) сервер не позволяет, пришлось в запросах использовать реляционную операцию cross join.

Особенностью базы является отсутствие централизованных справочников (классификаторов), что упрощает структуру базы и уменьшает количество таблиц, но способствует снижению производительности за счет соединений таблиц по текстовым полям в запросах.

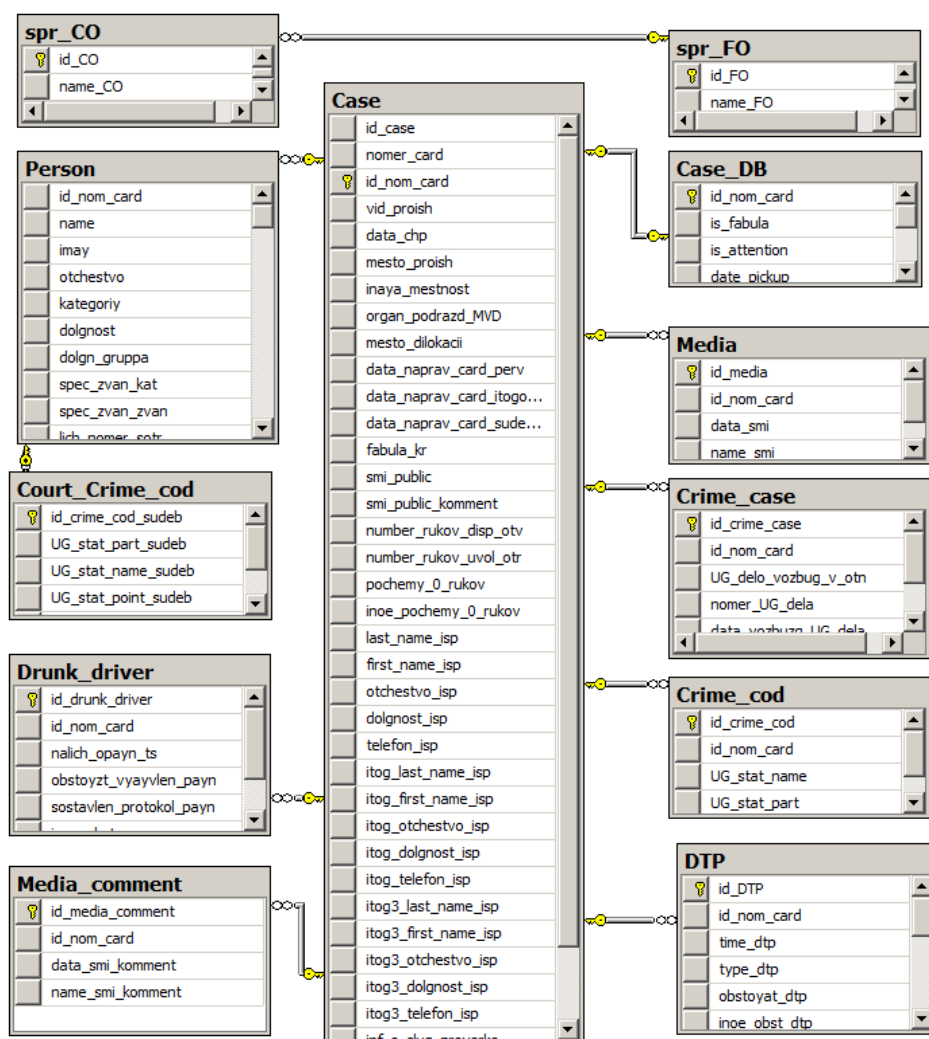


Рис. 2. Схема базы данных

Описание модуля ведения базы данных. Диалог пользователя с программным модулем происходит с помощью интерфейса, который служит для просмотра, ввода, обновления и удаления информации о происшествии с участием сотрудников ОВД, федеральных государственных гражданских служащих и работников МВД России и принятых по нему мерах реагирования, в рамках базы данных.

Программный модуль состоит из главной формы и двух вспомогательных форм сравнения. Главная форма содержит области для вывода в них информации из xml-файла и ее сравнения с информацией в базе данных, если такая карточка была загружена ранее. Также имеется возможность корректировки даты занесения информации в базу данных, постановки происшествия на контроль и на вывод фабулы в суточной сводке.

В центре формы приводится информация об этапах размещения информации в базе данных и кнопки управления. В нижней части формы находится поле для ввода текущей даты, кнопка «Удалить карточку», сведения о подразделении, типе карточки.

Главная форма программного модуля представлена на рисунке 3.

Рис. 3. Главная форма программного модуля

Описание областей для вывода информации:

- сведения и происшествия;
- сведения об участниках;
- сведения о ДТП;
- сведения о возбужденном уголовном деле;
- сведения о выявлении управлением транспортным средством в состоянии опьянения;
- сведения о публикациях в СМИ;
- сведения о комментариях в СМИ;
- сведения о статьях УК РФ по уголовному делу;
- сведения о статьях УК РФ в судебных решениях;
- фабула;
- даты фиксации информации в базе данных.

Для открытия карточки необходимо нажать на кнопку «Открыть» и выбрать нужную карточку. Если происшествие с таким номером еще не внесено в базу, то форма примет вид показанный на рисунке 2. Верхние части всех таблиц для отображения останутся пустыми.

Если происшествие уже было занесено в базу, то форма примет вид показанный на рисунке 4. В верхней части будет отображаться информация из базы, в нижней из открытой карточки.

При этом зеленым цветом заливается ячейки, которые в базе данных пусты, а в карточке заполнены. Красным цветом заливается ячейки, которые уже заполнены в базе данных, но в карточке иное значение.

The screenshot shows a web-based application for managing incidents. The main area contains three tables:

- Top Table (Incident Overview):** Columns include номер (number), ID, дата (date), место (place), место происшествия (place of incident), орган (organ), дата 1 (date 1), дата 2 (date 2), дата 3 (date 3), СМН (SMN), СМН комментарий (SMN comment), наложено лиц (imposed on persons), наложено руководителей (imposed on managers), почему не наложено (why not imposed), иная причина (other reason), Исполнитель 1 (Executor 1), иная 1 (other 1).
- Middle Table (Detailed Incident Data):** Columns include фамилия (surname), имя (name), отчество (patronymic), место регистрации (place of registration), почему не приняты (why not accepted), категория (category), должность (position), должностная группа (official group), вид взыскания (type of punishment), статус (status), дата рождения (date of birth), стаж СМН (SMN tenure), в должности (in position), наложено взысканий (imposed punishments), действует взысканий (active punishments), семейное (family), иная 1 (other 1).
- Bottom Table (Related Documents):** Columns include дата (date), тип ДТП (type of accident), обстоятельства (circumstances), иные обстоятельства (other circumstances), жертв всего (total victims), погибших сотрудников (deceased employees), погибших граждан (deceased citizens), погибших детей (deceased children), травмировано сотрудников (injured employees), травмировано граждан (injured citizens), травмировано детей (injured children), возбуждено УД (initiated investigation).

The right sidebar contains a section for 'ДТП-фабула' (Accident scenario) with a date and a note about management. Below it are buttons for 'Открыть' (Open), 'Учтено' (Acknowledged), 'Досудка' (Dismissal), 'Итоги' (Results), 'Суд' (Court), 'Зачесть' (Accept), and 'Выход' (Exit).

Рис. 4. Создание новой карточки о происшествии

Заключение. В настоящее время разработанное программное обеспечение находится в стадии опытной эксплуатации. Появляются новые задачи, исправляются старые ошибки. Архитектура информационной системы предопределяет изменение и перекомпиляцию модуля ведения базы данных когда меняется структура или поля таблиц базы данных. При этом рассылка обновленного модуля заполнения карточек происходит каждый раз, когда требуется простая коррекция классификаторов. Это происходит при изменении бизнес-логики работы системы или законодательства.

ЛИТЕРАТУРА

1. Мишин С. А. Разработка концептуальной модели системы автоматизированного мониторинга обучения иностранных граждан в образовательных организациях МВД России / С.А. Мишин, Р.А. Солодуха // Охрана, безопасность, связь. – 2018. – № 3. – С. 120 – 125.
2. Валеев Е. В. Миграция АИС "Мониторинг обучения иностранных граждан в высших образовательных учреждениях МВД России" на 3-х звенную архитектуру / Е.В. Валеев, Р.А. Солодуха // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. – 2018. – С. 283 – 284.

СВЕДЕНИЯ ОБ АВТОРАХ

Мишин Сергей Александрович. Заместитель начальника кафедры автоматизированных информационных систем МВД. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: samishin@bk.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 2005-186.

Солодуха Роман Александрович. Доцент кафедры автоматизированных информационных систем МВД. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: standartal@list.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 2005-184.

Mishin Sergey Alexandrovich. Deputy chief of the chair of automated information systems of interior units. Candidate of sciences (technical), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-186.

Solodukha Roman Alexandrovich. Assistant professor of the automated information systems of interior units chair. Candidate of sciences (technical), assistant professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-184.

Ключевые слова: автоматизированная информационная система; база данных; мониторинг состояния служебной дисциплины и законности в органах внутренних дел.

Key words: automated information system; database; monitoring of the condition of the service discipline and legality in the internal affairs.

УДК 004.9.

Никулина Екатерина Юрьевна,
кандидат технических наук, доцент

ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ ЗАДАЧИ ПЕРЕХОДА НА ИСПОЛЬЗОВАНИЕ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

CHALLENGES AND SOLUTIONS FOR THE TRANSITION TO DOMESTIC SOFTWARE

Рассматриваются особенности работы с операционной системой отечественной разработки Astra Linux, предназначенной для обеспечения повседневной деятельности подразделений МВД России. Проведена сравнительная характеристика рассматриваемой системы с точки зрения графического интерфейса пользователя, наличия встроенных программных продуктов и технических требований к ее эксплуатации.

The peculiarities of working with the operating system of the domestic development Astra Linux, designed to ensure the daily activities of the departments of the Ministry of Internal Affairs of the Russian Federation, are considered. The system was compared in terms of graphical user interface, availability of built-in software products and technical requirements for its operation.

В соответствии с программой импортозамещения в Российской Федерации и Постановлением правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» в настоящее время актуально решение проблемы перехода на отечественное программное обеспечение (далее ПО) [1]. Согласно приказу МВД России от 10 мая 2018 г. № 284 «Об утверждении плана-графика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года» переход на отечественное ПО планируется выполнить на 80% к 2020 году.

При выполнении этого перехода должно быть установлено ПО, работающее под управлением операционной системы отечественной разработки.

В качестве такой операционной системы была выбрана разработка научно-производственного объединения «РусБИТех» (открытое акционерное общество «Научно-производственное объединение «Русские базовые информационные технологии»)) – операционная система (далее ОС) с ядром Linux, получившая название Astra Linux. Данная ОС была представлена в двух вариантах – Common Edition (ОС общего назначения) и Special Edition (ОС специального назначения), созданных на основе свободного программного обеспечения. Различные версии ОС Astra Linux были названы в честь городов-героев России, это так называемые «релизы» ОС. Релиз «Орел» для Common Edition и релиз «Смоленск» для Special Edition устанавливаются на персональные компьютеры с процессорами x86-64. Релизы «Тула», «Нововосийск», «Мурманск» разработаны и предназначены для работы на различных технических устройствах, таких как серверы, мобильные и портативные устройства, коммутационное оборудование и др.

Проведем анализ возможностей ОС Astra Linux Common Edition на примере релиза «Орел» версии 2.12.

Для установки ОС Astra Linux Common Edition на персональный компьютер (далее ПК) потребуется установочный файл, желательно с последней версией системы;

установка системы возможна как с оптических носителей (CD, DVD диск и т.п.), так и с флэш-накопителей.

Для установки и оптимального функционирования системы рекомендуется наличие определенных параметров аппаратной составляющей персонального компьютера, которые представлены в табл. 1.

Таблица 1

Системные требования к ПК при установке Astra Linux Common Edition

Параметры	Минимальные требования (подразумевается работа без рабочего стола Fly и графических приложений)	Рекомендованные значения (подразумевается работа с рабочим столом Fly, графическими и высоконагруженными приложениями)
Аппаратная платформа	Процессор с архитектурой x86-64 (AMD, Intel)	
Оперативная память	Не менее 1 Гб	4 Гб
Объем свободного дискового пространства	Не менее 4 Гб	16 Гб
Монитор	Допускается работа без монитора	Стандартный монитор SVGA

В ходе тестирования ОС Astra Linux Релиз «Орел» было выявлено, что минимальные требования действительно являются минимальными и система «подтормаживает» и «подвисает». Для более эффективной работы на ПК, когда не требуется использовать большие потоки информации и обрабатывать графику высокого уровня качества, вполне достаточно выделить 2 Гб оперативной памяти и 50 Гб постоянной памяти, что вполне реализуемо для современных ПК, используемых в образовательных организациях МВД России, в том числе в Воронежском институте МВД России.

Стоит отметить дружеский графический интерфейс ОС Astra Linux Common Edition, чем-то напоминающий интерфейс ОС MS Windows. Данный интерфейс носит название Fly и является собственной разработкой НПО «РусБИТех».

Отличительной особенностью данной ОС является наличие четырех рабочих столов, отображаемых на панели быстрого доступа (рис. 1).



Рис. 1. Панель быстрого доступа ОС Astra Linux Common Edition

На панели быстрого доступа располагается переключатель рабочих столов, с помощью которого пользователь может изменить их общее количество и геометрию конфигурации. По умолчанию менеджер поддерживает в конфигурации два рабочих стола по вертикали и два по горизонтали. Стоит отметить, что менеджер рабочих столов позволяет размещать окна приложений в пространстве, превышающем размер видимой области экрана.

С левой стороны панели быстрого доступа расположена кнопка меню в виде пятиконечной звезды (см. рис. 1). С помощью меню можно запустить на выполнение приложения, которые в ОС Windows не содержались в списке приложений меню, и для их открытия необходимо было выполнять ряд пользовательских действий – переход из

одного пункта в другой, выбор в нем вкладки и т.д. В качестве примера можно привести запуск утилиты «Информация о системе», которая позволяет в разделе «Системные» отслеживать полную информацию об операционной системе и о всех выполняющихся в ней процессах.

Однако, несмотря на дружелюбный интуитивно понятный графический интерфейс системы, при первом опыте работы с ней возникали проблемы, для решения которых приходилось либо обращаться за помощью к разработчикам системы (наличие интерактивной помощи на официальном сайте разработчиков), либо убеждаться в том, что данная проблема не решена для ОС Astra Linux, и ее решение возможно лишь с выходом последующих версий ОС. В качестве примера можно привести неотображение в файловом менеджере (аналог программы «проводник» в ОС Windows) подключений к локальной сети. Другой проблемой явилась невозможность подключения принтера с общим доступом к ПК. Можно предположить, что в системе существуют и другие проблемы, которые пользователям ОС придется решать самостоятельно или убеждаться в том, что для данной версии ОС решений проблемы не существует.

В результате проведенного исследования можно сделать следующие выводы об основных преимуществах и недостатках работы ОС Astra Linux Common Edition Релиз «Орел» версии 2.12:

1. Система полностью работоспособна, критичных ошибок и недостатков обнаружено не было.

2. Относительно невысокие системные требования обеспечивают работоспособность ПК даже с минимальными техническими характеристиками (оперативная память, объем свободного дискового пространства).

3. Процесс установки ОС на ПК сопровождается интуитивно понятным и доступным графическим интерфейсом, что обеспечивает простоту и удобство ее использования.

4. Интерфейс данной системы схож с интерфейсом ОС Windows, поэтому работать в ОС Astra Linux легко и понятно.

5. В системе имеется встроенное программное обеспечение, необходимое для повседневной работы: офисный пакет LibreOffice, являющийся аналогом пакета Microsoft Office, графические редакторы, редакторы аудио- и видео-файлов и др.

В целом ОС Astra Linux Common Edition выглядит как неплохая замена привычной версии ОС Windows в рамках программы импортозамещения и перехода на свободное программное обеспечение органов государственной власти и организаций.

ЛИТЕРАТУРА

1. Постановлением правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд». — <http://https://www.garant.ru/products/ipo/prime/doc/71152170/>.

СВЕДЕНИЯ ОБ АВТОРАХ

Никулина Екатерина Юрьевна. Доцент кафедры автоматизированных информационных систем органов внутренних дел, кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: nikeu@mail.ru

Россия, 394065, г.Воронеж, проспект Патриотов, 53.
Тел. (473) 200-51-85.

Nikulina Ekaterina Urevna. Assistant professor of the chair of the automated information systems of interior unit chair, candidate of sciences (technical), assistant professor.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: nikeu@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-85.

Ключевые слова: отечественное программное обеспечение, персональный компьютер, операционная система, графический интерфейс пользователя.

Key words: domestic software, personal computer, operating system, graphical user interface.

УДК 681.3

Обухова Людмила Александровна,
кандидат технических наук

**ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ
В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
НА ТЕРРИТОРИИ РОССИИ**

**CYBER CRIME DEVELOPMENT TRENDS
IN THE FIELD OF INFORMATION TECHNOLOGIES
ON RUSSIAN TERRITORY**

В статье рассмотрены проблемы, возникающие при расследовании киберпреступлений, приведены статистические показатели по преступлениям данного вида, совершенным на территории России за последние 4 года, выявлены тенденции развития киберпреступности в сфере информационных технологий на территории России.

The article discusses the problems that arise in the investigation of cybercrime, provides statistical indicators for crimes of this type committed in Russia over the past 4 years, identifies trends in the development of cybercrime in the field of information technology in Russia.

Введение. Сегодня киберпреступность – одна из острейших проблем, с которой столкнулось международное сообщество на протяжении последних лет в связи с его информатизацией. Сеть Интернет практически безнаказанно используется преступниками как место и основное средство совершения различных посягательств, как традиционных (мошенничеств, краж), так и иных – похищений и продажи конфиденциальной информации, вымогательств, «геймерских» мошенничеств, и распространения предметов и услуг, исключенных из легального оборота. Особую опасность представляют киберэкстремизм и крайняя его форма – кибертерроризм. Все перечисленное образует феномен киберпреступлений. Это понятие нередко употребляется наряду с тер-

минами «компьютерная преступность», «кибербандитизм», «преступность в информационном пространстве».

Целью работы – определение статистических показателей по преступлениям данного вида, анализ текущего состояния киберпреступлений в сфере информационных технологий в России.

Текущее состояние киберпреступности на территории России. Под киберпреступностью понимают совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

На сегодняшний день киберпреступления составляют почти каждое двадцатое среди всех преступлений, зарегистрированных в России (4,4% среди всех преступлений). Самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации (статья 272 УК РФ), и создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ). Распространение получили мошеннические действия, совершенные с использованием электронных средств платежа (статья 159.3 УК РФ).



Рис. 1. Статистические данные по неправомерному доступу к компьютерной информации на территории России.



Рис. 2. Статистические данные о случаях создания, использования и распространения вредоносных компьютерных программ на территории России.



Рис. 3. Статистические данные о случаях мошенничества с использованием электронных средств платежа на территории России

По данным Генпрокуратуры РФ в 2018 году на 19,6% уменьшилось количество расследованных преступлений по этим статьям, связанным с преступлениями в сфере инфокоммуникационных технологий (с 903 до 726), выросло на 30,5% (с 790 до 1031) число нераскрытых преступлений. Раскрываемость данных преступлений составила 41,3%.

Вышеперечисленные статистические данные за 2015 – 2018 годы представлены на рисунках 1 – 3.

В-третьих, компьютерные преступления вынуждены расследовать люди с юридическим образованием, тогда как во многих странах мира следователи по cybercrime – это прежде всего технические эксперты с дополнительным юридическим образованием.

Следует понимать, сегодня мы наблюдаем опасную концентрацию проблем практически во всех сферах инфокоммуникационных технологий. Главную опасность представляет эксплуатация процессорных уязвимостей. Началом может стать утечка готового инструментария спецслужб, как было в случае с EternalBlue. Теряет актуальность тема криптовалют, но защита торговых терминалов на биржах ценных бумаг оказывается не лучше, чем у криптокошельков, что чревато атаками на курсы валют и акций. Переход нефтегазовой отрасли на интеллектуальные месторождения, работающие по сути на автопилоте, оказывается столь быстрым, что сценарий, при котором злоумышленники останавливают нефтедобычу по всему миру, при таком количестве уязвимостей в автоматизированных системах управления топливной переработки, уже не кажется фантастическим. В телекоме уязвимы 78% сетей, но SMS-сообщения – все еще безальтернативный способ двухфакторной аутентификации. При этом широко внедряются новые, «недообследованные» технологии, такие как удаленная биометрическая идентификация, а уровень осведомленности населения о проблемах информационной безопасности, по-прежнему, остается невысоким. Поэтому основная задача для специалистов в области информационной безопасности, разработчиков программного обеспечения и государства – сделать так, чтобы негативные сценарии никогда не воплотились в жизнь.

Заключение. В заключении хотелось бы процитировать выступление Министра внутренних дел Российской Федерации генерала полиции В.А. Колокольцева на расширенном заседании коллегии МВД России 28.02.2018. «Серьёзные вызовы и угрозы безопасности страны представляет неконтролируемое функционирование и развитие компьютерных и телекоммуникационных технологий, которые сопровождаются активизацией противоправных проявлений. Однако надо понимать, что проблему не решить без адекватного правового регулирования интернет-среды; повышения ответственности за размещение в сети запрещённого контента; формирования правовых и организационно-технических механизмов реагирования на противоправную деятельность в данной сфере. Только так мы сможем обеспечить безопасность наших граждан в киберпространстве».

ЛИТЕРАТУРА

1. Масалков А.С. Особенности киберпреступлений. Инструменты нападения и защита информации / А.А. Масалков. – М.: ДМК-Пресс, 2018, – С. 226.
2. Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации // Российский следователь, 2016. – № 10. – С. 25.
3. Шевченко Е.С. Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист, 2015. – № 3. – С. 89.

4. Александров А.А. Организационно-правовое обеспечение информационной безопасности / А.А. Александров, М.П. Сычев. – М.: МГТУ им. Н.Э. Баумана, 2018 – Формат : PDF.

5. Руденков Н.А. Технологии защиты информации в компьютерных сетях / Руденков Н.А., Пролетарский А.В., Смирнова Е.В. – М.: Интуит, 2016 – Формат : PDF.

СВЕДЕНИЯ ОБ АВТОРЕ

Обухова Людмила Александровна. Доцент кафедры автоматизированных информационных систем МВД. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: obuhova.lyudmila@bk.ru.

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 2005-189.

Obuhova Lyudmila Aleksandrovna. Docent of the chair of Computer-Based Information Systems of the law enforcement agencies. Candidate of the technical sciences.

Voronezh Institute of the Ministry of the Interior of the Russian Federation.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 2005-189.

Ключевые слова: киберпреступление, статистические показатели киберпреступности в России, тенденции развития киберпреступности.

Key words: cybercrime, statistical indicators of cybercrime in Russia, trends in the development of cybercrime.

УДК 004.75

**ИСПОЛЬЗОВАНИЕ ПРОГРАММНОЙ СРЕДЫ ИМИТАЦИОННОГО
МОДЕЛИРОВАНИЯ С ЦЕЛЬЮ РАЗРАБОТКИ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ
ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОВД**

**USING THE SOFTWARE ENVIRONMENT OF IMITATION MODELING TO
DEVELOP A MODEL OF INFORMATION PROTECTION SYSTEM FROM
UNAUTHORIZED ACCESS IN AUTOMATED SYSTEMS OF THE LAW
ENFORCEMENT AGENCIES**

В статье представлены перспективы разработки имитационной модели системы защиты информации от несанкционированного доступа в автоматизированных системах ОВД.

The article presents the prospects for the development of a simulation model of the system for protecting information from unauthorized access in automated systems of the law enforcement agencies.

Современный этап жизнедеятельности человека характеризуется глубокой информатизацией, который связан с разработкой, эксплуатацией автоматизированных систем различного назначения. В связи с этим злоумышленниками постоянно совершенствуются способы получения конфиденциальной информации. Для предотвращения попыток несанкционированного доступа в автоматизированные системы внедряются системы защиты информации от несанкционированного доступа (СЗИ от НСД). Зачастую штатные пользователи таких систем пренебрегают своими должностными полномочиями и нарушают правила работы с автоматизированной системой. Пользовательские ошибки в защищенных системах являются самыми распространенными, поэтому в работе мы допускаем что он допустил ошибку и вредоносная программа проникла в автоматизированную систему. Рассмотрим именно этот случай для съёмного носителя информации CD/DVD/HD/Flesh и т.д.

Вредоносная программа может быть реализована в виде отдельного программного продукта с функцией автозапуска при подключении к автоматизированному рабочему месту (АРМ). В случае, когда пользователь сам отключает антивирусное программное обеспечение (ПО), т.к. зачастую они сильно загружают оперативную память и, следовательно, работать за становится неудобно, а зачастую невозможно из-за загрузки системы.

В связи с вышесказанным данные аспекты необходимо учитывать при разработке и эксплуатации СЗИ от НСД для определения ее вероятностно-временных, качественных и количественных характеристик, а также взаимосвязи ее подсистем и компонентов, а также построению её логичной структуры в целом. Данная задача может быть решена при помощи построения имитационной модели СЗИ от НСД, которая и будет предопределять вышеперечисленные характеристики.

В качестве программной среды построения имитационной моделей в данной статье используем программу, разработанную в университете Орхуса (Дания) – CPN Tools. Отличительной особенностью CPN Tools, от других сред, является наличие обширного инструментария, позволяющего анализировать различные аспекты функционирования моделей на базе сетей Петри (безопасность и ограниченность позиций, уровень активности переходов, наличие тупиковых маркировок и т.д.). CPN Tools исполь-

зуются во множестве реальных проектов в области телекоммуникации, при моделировании сетей и сетевых устройств, а также при верификации протоколов связи и т.д. В данном программном продукте для построения моделей используются иерархические, временные, раскрашенные сети Петри, которые представляют собой универсальную алгоритмическую систему. CPN Tools поддерживает язык Meta language (ML), который используется для описания операций, условий и функций. Благодаря применению ML программа позволяет упростить процесс построения и анализа моделей на ранней стадии проектирования системы. В данный момент язык ML представляет большие перспективы. Это в свою очередь обусловлено его простотой как в изучении, так и в синтаксисе. Во многих институтах и университетах язык ML является одним из первых, для изучения, языков программирования наравне с JavaScript, C++, C#, Java, PHP, Python.

Имитационное моделирование в CPN Tools является дискретно-событийным, что предполагает мгновенную смену состояния сети Петри в определенные моменты времени, которые называют шагами. Наличие временных меток позволяет моделировать процессы с учетом времени их выполнения. Также CPN Tools предоставляет различного вида отчёты, которые позволяют проанализировать построенную систему и сделать соответствующие выводы в зависимости от целей исследования. Интерфейс программы CPN Tools является интуитивно понятным и достаточно прост в изучении, он предусматривает проверку работоспособности модели и выявление различных ошибок как в синтаксисе встроенного языка ML, так и в маркировке сети, что заметно облегчает работу с данной программой.

Перспектива разработки имитационной модели СЗИ от НСД заключается в проведении системного анализа функциональных компонентов СЗИ от НСД которые позволят выделить ее ключевые подсистемы. При помощи программного пакета CPN Tools в частности инструмента «Hierarchy» установить взаимосвязи между подсистемами СЗИ от НСД. Установить взаимосвязи между компонентами СЗИ от НСД с использованием пространства состояний, что позволит провести ее функциональный анализ. В перспективе разработки получить отчеты о работе имитационной модели, которые содержат в себе основную информацию о ее характеристиках рисунок 1.

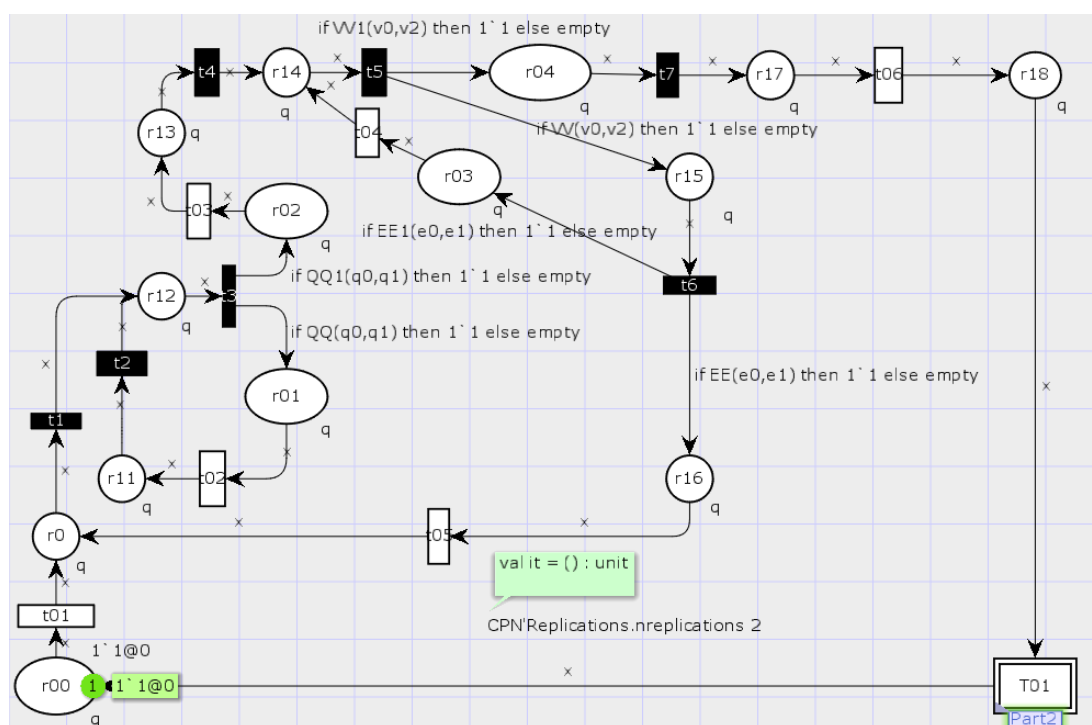


Рис.1. «Включение АРМ и идентификация пользователя»

ЛИТЕРАТУРА

1. K. Jensen and L.M. Kristensen. Coloured Petri Nets — Modeling and Validation of Concurrent Systems. Springer-Verlag Berlin, 2009.
2. . Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book. – Odessa: ONAT, 2006. – 60 p.

СВЕДЕНИЯ ОБ АВТОРАХ

Попов Антон Дмитриевич. Преподаватель кафедры автоматизированных информационных систем ОВД. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: anton.holmes@mail.ru

Россия, 394065, г. Воронеж, пр. Патриотов, 53. Тел. (473) 200-51-87.

Popov Anton Dmitrievich. Lecturer of the chair of Automatic Informative Systems of the Law Enforces Agencies. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: anton.holmes@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-51-87.

Ключевые слова: информационная безопасность, автоматизированная система, информационный ресурс, объект информатизации, несанкционированный доступ.

Keywords: information security, automated system, information resource, informatization object, unauthorized access.

УДК 621.3

Рогозин Евгений Алексеевич,
доктор технических наук, профессор;
Каднова Айжана Михайловна

**К ВОПРОСУ О РЕШЕНИИ НАУЧНОЙ ЗАДАЧИ КОЛИЧЕСТВЕННОЙ
ОЦЕНКИ ЭРГАТОТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК СИСТЕМ ЗАЩИТЫ
ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В
АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОВД**

**TO THE QUESTION OF THE SOLUTION OF THE SCIENTIFIC OBJECTIVE OF
THE QUANTITATIVE EVALUATION OF ERGATOTECHNICAL
CHARACTERISTICS OF INFORMATION PROTECTION SYSTEMS FROM
UNAUTHORIZED ACCESS TO AUTOMATED SYSTEMS OF THE LAW
ENFORCEMENT AGENCIES**

Статья посвящена решению научной задачи формирования системы эргатотехнических показателей качества функционирования систем защиты информации от несанкционированного доступа в автоматизированные системы ОВД и разработки моделей и алгоритмов их оценки.

The article is devoted to solving the scientific problem of creating a system of ergatotechnical indicators of the quality of functioning of information protection systems against unauthorized access to automated systems of the law enforcement agencies and developing models and algorithms for their assessment.

Анализ нормативных документов, посвященных качеству программных продуктов [1–3] и информационной безопасности АС [4–6], показал, что на сегодняшний день отсутствуют показатели оценки эргатотехнических характеристик систем защиты информации (СЗИ) от несанкционированного доступа (НСД) в автоматизированных системах (АС) ОВД и методики их оценки.

В результате невозможности их оценки на начальных этапах проектирования СЗИ от НСД встречаются следующие проблемы:

- 1) не полностью обеспечивается реализация целей и требований заказчиков к функционалу и потребительскому качеству СЗИ от НСД;
- 2) достоверность первичной оценки бюджета, срока и требуемых ресурсов для разработки СЗИ от НСД при разработке технического задания (заданий по безопасности) низкая, вследствие чего могут не выполняться требования заказчика;
- 3) недостаточно контролируется ход выполнения проекта, в связи, с чем повышается риск отсутствия у конечного программного продукта требуемого качества, срыва директивных планов, несоответствия функциональным и экономическим разделам технического задания (заданий по безопасности) на разработку СЗИ от НСД;
- 4) отсутствие эргатотехнических показателей затрудняет сравнение и оценку сертифицированных СЗИ от НСД при их выборе.

В этой связи возникает практически значимая задача разработки и оценки показателя качества СЗИ от НСД «удобство использования».

Для решения практической задачи необходимо решение научной задачи формирования системы эргатотехнических показателей качества функционирования СЗИ от НСД и разработки моделей и алгоритмов их оценки.

Для решения научной задачи необходимо:

1. Проанализировать принципы, методы и особенности функционирования администратора СЗИ от НСД при выполнении своих функций, исследовать применяемые им пользовательские интерфейсы основных программных модулей.

2. Разработать систему эрготехнических показателей качества СЗИ от НСД, с учетом существующих требований отечественных и международных стандартов в области качества программных систем, особенностей архитектуры технологического цикла выполнения типовых задач администратором.

3. Разработать методики экспериментальной оценки эрготехнических показателей и аналитические модели и алгоритмы для расчетов предложенных показателей «удобства использования».

4. Апробировать экспериментальные методы и аналитические методики при проведении оценки «удобства использования» типовых СЗИ от НСД.

Структурная схема проведения научных исследований по решению научной задачи разработки системы эрготехнических показателей качества функционирования СЗИ от НСД в АС ОВД представлена на рисунке 1.

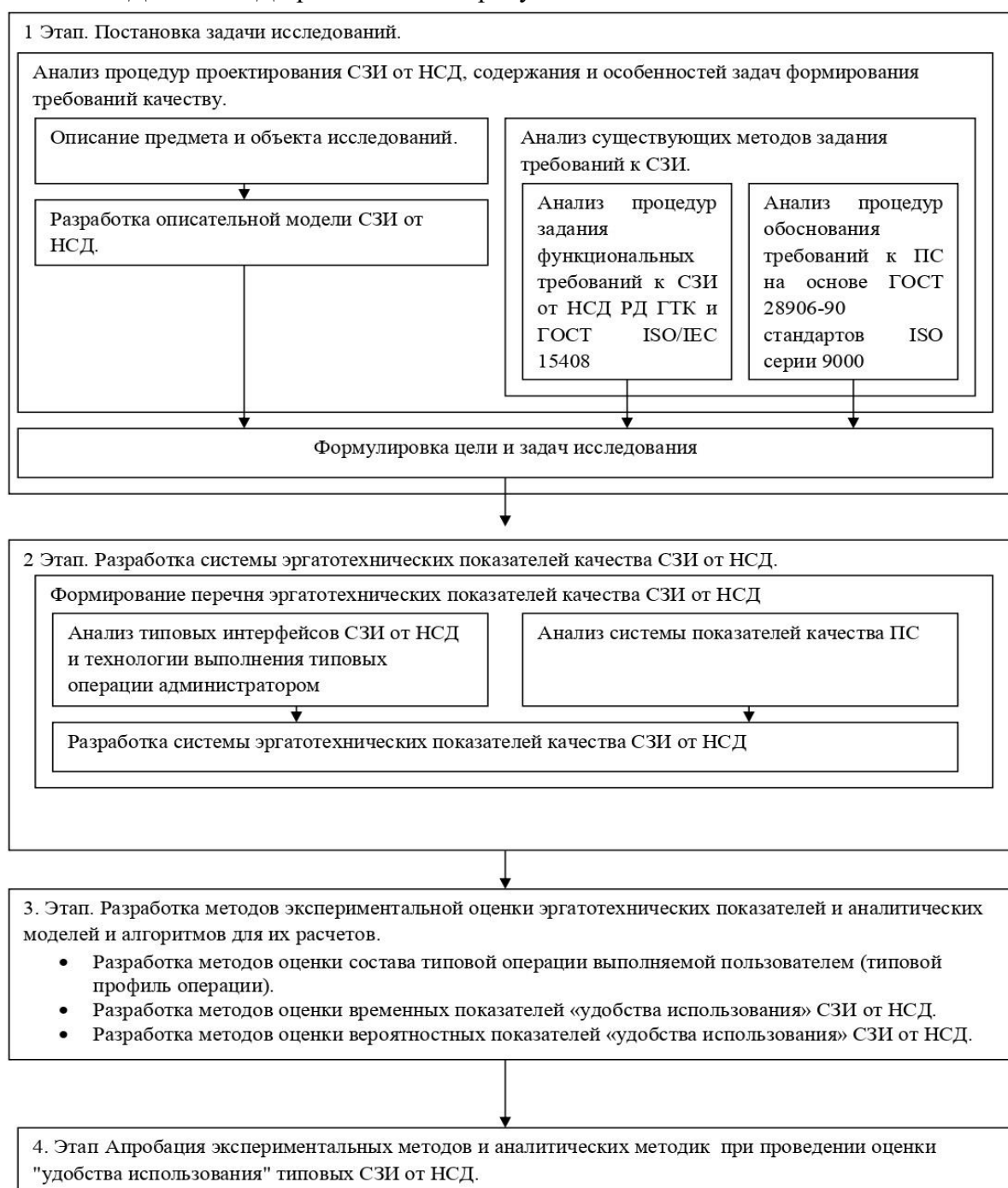


Рис. 1. Схема проведения научных исследований

Вывод: научные исследования, связанные с оценкой операционных характеристик СЗИ от НСД в АС ОВД являются весьма актуальными и требуют дальнейшей проработки с целью оценки и анализа защищенности АС на объектах информатизации ОВД.

ЛИТЕРАТУРА

1. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 19.12.2016) // СПС «Консультант Плюс».
2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 01.11.2012 N 1119 // СПС «КонсультантПлюс».
3. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18.02.2013 № 21 // СПС «КонсультантПлюс».
4. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2 : Функциональные компоненты безопасности. – Введ. 2013-11-08. – [Электронный ресурс]. – URL: <https://files.stroyinf.ru/Data2/1/4293774/4293774728.pdf>.
5. ISO/IEC 17000:2004. Оценка соответствия. Словарь и общие принципы. – Введ. 2001-11-01. – [Электронный ресурс]. – URL: https://pqm-online.com/assets/files/lib/std/iso_17000-2004.pdf.
6. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. – Введ. 1989-07-28. – Москва : Госстандарт СССР. 1990 г. – 15 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Рогозин Евгений Алексеевич. Профессор кафедры автоматизированных информационных систем органов внутренних дел. Доктор технических наук, профессор. Воронежский институт МВД России.
E-mail: evgenirogozin@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.
Тел. (473) 200-51-82.

Каднова Айжана Михайловна. Адъюнкт кафедры автоматизированных информационных систем органов внутренних дел. Воронежский институт МВД России.
E-mail: aizhana_kadnova@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.
Тел. (473) 200-51-89.

Rogozin Evgeniy Alekseevich. Professor of the chair of Automatic Informative Systems of the Law Enforces Agencies. Doctor of Technical Sciences, Professor. Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: evgenirogozin@yandex.ru
Work address: Russia, 394065, Voronezh, Revolution Avenue, 53.
Phone. (473) 200-51-82.

Kadnova Aizhana Mikhailovna. Adjunct of the chair of Automatic Informative Systems of the law enforces agencies.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: aizhana_kadnova@mail.ru

Work address: Russia, 394065, Voronezh, Revolution Avenue, 53.

Phone. (473) 200-51-89.

Ключевые слова: система защиты информации, информационная безопасность, автоматизированная система, объект информатизации, несанкционированный доступ.

Keywords: information security system, information security, automated system, informatization object, unauthorized access.

УДК 621.3

Рогозин Евгений Алексеевич,
доктор технических наук, профессор;
Каднова Айжана Михайловна,
Фирюлин Максим Евгеньевич,
кандидат технических наук

**КЛАССИФИКАЦИЯ И АНАЛИЗ СУЩЕСТВУЮЩИХ УГРОЗ
НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОВД**

**CLASSIFICATION AND ANALYSIS OF EXISTING THREATS OF
UNAUTHORIZED ACCESS IN AUTOMATED SYSTEMS OF THE LAW
ENFORCEMENT AGENCIES**

В статье разработана классификационная схема и проанализирована возможная реализация угроз информационному ресурсу АС ОВД.

The article developed a classification scheme and analyzed the possible implementation of threats to the information resource of automated systems of the law enforcement agencies.

Угроза информационному ресурсу — это потенциальная возможность реализации дестабилизирующего действия (воздействия) или события (критической ситуации), наносящих ущерб информационной безопасности автоматизированных систем (АС) ОВД, выраженный в копировании, несанкционированном распространении, искажении, уничтожении, блокировании доступа штатных пользователей АС ОВД к информационному ресурсу, а также оказывающих воздействие на составные компоненты АС ОВД, последствиями которого могут стать утрата, уничтожение или сбой функционирования носителей информационного ресурса, средств взаимодействия с носителями или средств управления этими носителями. В настоящее время перечень угроз информационному ресурсу насчитывает более сотни пунктов и позиций [1]. Анализ вышеуказанного перечня угроз информационной безопасности [2] показал, что угрозы информационной безопасности в АС ОВД по природе возникновения можно разделить на две категории: естественные (объективные) и искусственные (субъективные). Естественные угрозы — угрозы, источником которых являются объективные физические процессы или стихийные природные явления, не зависящие от человека и его деятельности. Недопущение возникновения данного вида угроз достигается исключительно путем принятия элементарных мер безопасности (например, объективный выбор места располо-

жения АС ОВД в здании, оборудование здания противопожарными и иными датчиками, экранирование кабелей, назначение ответственных). Искусственные угрозы — угрозы, источником которых является человек и его деятельность. Учитывая мотивацию действий человека, данный вид угроз подразделяется на непреднамеренные (случайные) и преднамеренные (умышленные). Непреднамеренные угрозы — угрозы, связанные с некомпетентностью, незнанием, небрежностью, неосторожностью, невнимательностью или любопытством пользователей (установка программных продуктов, не входящих в список необходимых, ошибки при разработке и проектировании АС ОВД и ее элементов, ошибки в программном обеспечении и т.п.). Механизмы реализации данных угроз, а также методы их предотвращения, изучены достаточно хорошо. Преднамеренные угрозы — угрозы, связанные с корыстным умыслом преднамеренного воздействия на АС ОВД (несанкционированный доступ к структурам АС ОВД, распространение вирусных программ и т.д.). Данная категория угроз изучена недостаточно, она динамична и постоянно пополняется новыми видами угроз.

Компании, разрабатывающие методы и способы защиты от внутренних и внешних угроз информационному ресурсу, информационных атак, обеспечения промышленной безопасности предприятий, как правило, имеют в своем составе аналитические центры, которые регулярно проводят исследования по утечкам информации и результаты таких исследований публикуют на их официальных сайтах. К таким компаниям относится InfoWatch. Приведем некоторую статистику из ежегодного аналитического отчета данной компании за I полугодие 2018 года [3]. Согласно отчету, за I полугодие 2018 года зарегистрировано 1039 случаев утечки информации. Это на 85% больше, чем за аналогичный период 2006 года (157 утечек). На рисунке 1 представлено число зарегистрированных утечек информации в период с I полугодия 2006 г. по I полугодие 2018 г.



Рис. 1. Число зарегистрированных утечек информации в период с I полугодия 2006 г. по I полугодие 2018 г.

Согласно отчету [3], в таблице 1 представлены распределения преднамеренных и непреднамеренных утечек информации по каналам, которые принципиально отличны друг от друга

Таблица 1

Распределение утечек по каналам за I полугодие 2018 г.	
Умышленные	Случайные
Кража/потеря оборудования	
0,6 %	6,6 %
Съемные носители	
1,3 %	3,2 %
Электронная почта	
1,7 %	18,2 %
ИМ (текст, голос, видео)	
4,0 %	4,5 %
Бумажные документы	
4,8 %	15,5 %
Сеть (браузер, Cloud)	
87,2 %	51,8 %

Таким образом, на основании анализа утечек в разрезе каналов, можно сделать вывод о том, что природа умышленных и случайных утечек различна, а, следовательно, методы защиты информации, обрабатываемой в АС ОВД, будут различны.

На основе анализа нормативной документации ФСТЭК России в области обеспечения информационной безопасности и ведомственной документации МВД России [4], регламентирующей требования по защите информации от несанкционированного доступа (НСД) на объекте информатизации (ОИ) ОВД, разработана классификационная схема угроз информационному ресурсу АС ОВД на ОИ ОВД, представленная на рисунке 2.

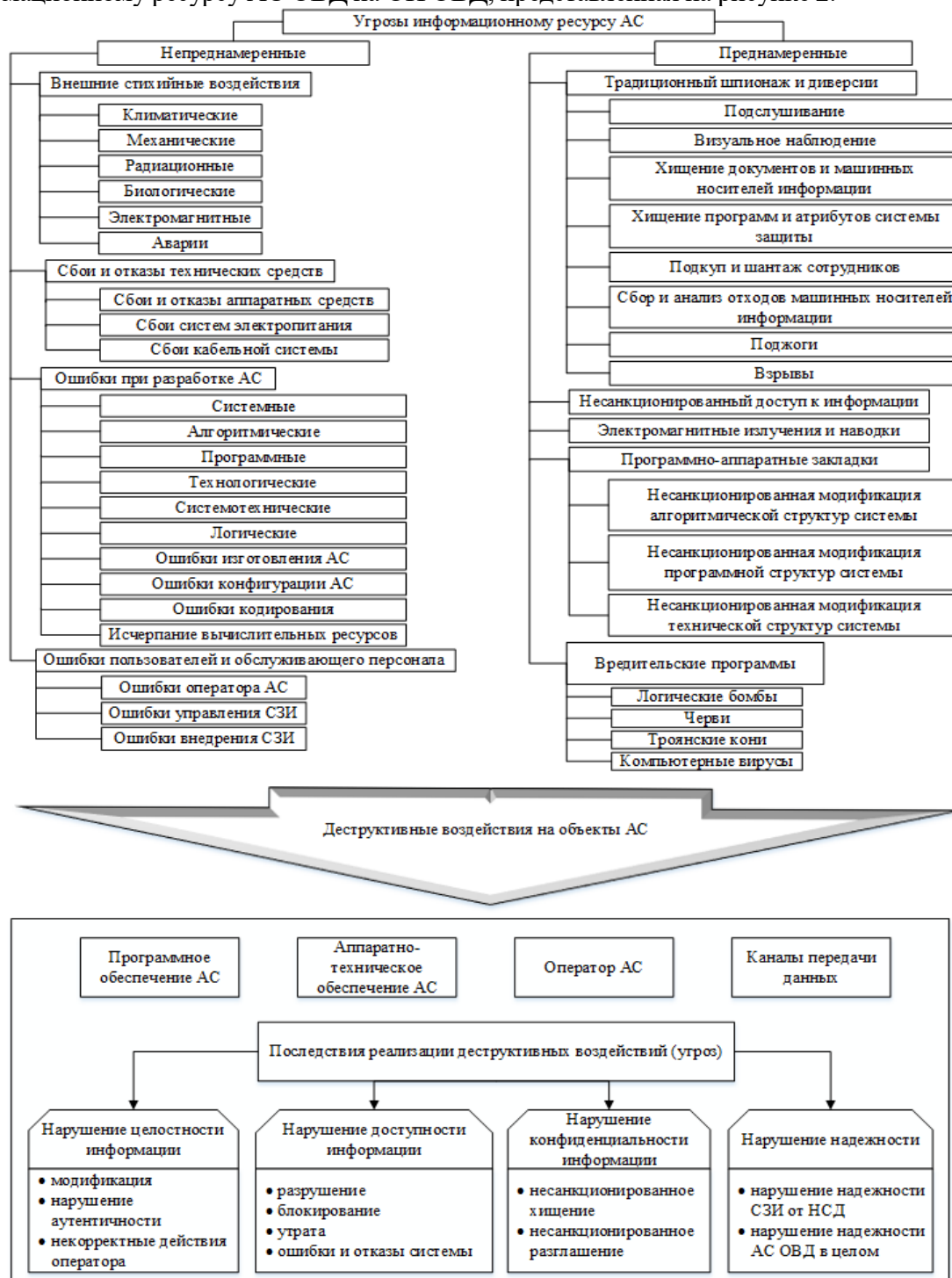


Рис. 2. Классификационная схема угроз информационному ресурсу АС ОВД

Таким образом, в статье разработана, классификационная схема угроз НСД к информационному ресурсу АС ОВД на ОИ ОВД. Полученные результаты в дальнейшем могут использоваться при проектировании и эксплуатации защищенных АС ОВД.

ЛИТЕРАТУРА

1. ФСТЭК РФ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god>.

2. Проектирование систем защиты информации от несанкционированного доступа автоматизированных систем ОВД / Е.А. Рогозин, А.Д. Попов, Т.В. Шагиров // Вестник ВИ МВД России, Выпуск 2, 2016 г., стр. 174-183.

3. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года [Электронный ресурс]. — URL: https://www.infowatch.ru/report2018_half.

4. Система показателей качества функционирования при создании системы информационной безопасности на объекте информатизации ОВД / О.И. Бокова, А.М. Каднова, Е.А. Рогозин, А.С. Серпилин // Приборы и системы, управление, контроль, диагностика. 2019. № 1, С. 26-33.

СВЕДЕНИЯ ОБ АВТОРАХ

Рогозин Евгений Алексеевич. Профессор кафедры автоматизированных информационных систем органов внутренних дел. Доктор технических наук, профессор.

Воронежский институт МВД России.

E-mail: evgenirogozin@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-51-82.

Каднова Айжана Михайловна. Адъюнкт кафедры автоматизированных информационных систем органов внутренних дел.

Воронежский институт МВД России.

E-mail: aizhana_kadnova@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-51-89.

Фирюлин Максим Евгеньевич. Преподаватель кафедры автоматизированных информационных систем органов внутренних дел. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: orugejnik68@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-56-46.

Rogozin Evgeniy Alekseevich. Professor of the chair of Automatic Informative Systems of the Law Enforces Agencies. Doctor of Technical Sciences, Professor.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: evgenirogozin@yandex.ru

Work address: Russia, 394065, Voronezh, Revolution Avenue, 53.

Phone. (473) 200-51-82.

Kadnova Aizhana Mikhailovna. Adjunct of the chair of Automatic Informative Systems of the law enforces agencies.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: aizhana_kadnova@mail.ru

Work address: Russia, 394065, Voronezh, Revolution Avenue, 53.

Phone. (473) 200-51-89.

Firyulin Maxim Evgenievich. Lecturer of the chair of Automatic Informative Systems of the Law Enforces Agencies. Candidate of Technical Sciences.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: orugejnik68@mail.ru

Work address: Russia, 394065, Voronezh, Revolution Avenue, 53.

Phone. (473) 200-56-46.

Ключевые слова: информационная безопасность, автоматизированная система, информационный ресурс, объект информатизации, несанкционированный доступ.

Keywords: information security, automated system, information resource, informatization object, unauthorized access.

УДК 621.3

Самороковский Андрей Федорович,
кандидат технических наук, доцент;

Горлов Виталий Викторович,
кандидат технических наук

МОДЕЛЬ УПРАВЛЕНИЯ ТЕРРИТОРИАЛЬНЫМИ ОРГАНАМИ МВД РОССИИ НА НАЧАЛЬНОМ ЭТАПЕ МАССОВЫХ БЕСПОРЯДКОВ

MODEL OF MANAGEMENT OF TERRITORIAL BODIES OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA AT THE INITIAL STAGE OF RIOTS

В статье рассматривается дискретно-стохастическая модель управления территориальными органами МВД России на начальном этапе массовых беспорядков.

The article discusses the discrete-stochastic model of management of territorial bodies of the ministry of internal affairs of Russia at the initial stage of riots.

В последние годы увеличивается количество групповых нарушений общественного порядка и массовых беспорядков которые возникают на фоне возросшей протестной активности населения, происходящих в стране социально-экономических и политических преобразований.

Массовые беспорядки относятся к числу наиболее опасных чрезвычайных происшествий, посягающих на общественную безопасность. Это правонарушение, совершаемое группой лиц и подлежащее уголовной ответственности в соответствии со ст. 212 УК РФ.

Процессы возникновения и развития массовых беспорядков можно разделить на три этапа:

Начальный этап – формирование причин и поводов для возникновения массовых беспорядков, формирование толпы.

Активный этап – период, когда сформировавшаяся толпа переходит к противоправным действиям, включая акты насилия и разрушения.

Заключительный этап – период активного участия территориальных органов МВД России (ТО) в пресечении массовых беспорядков или их самостоятельное затухание [1].

Представим модель управления ТО на начальном этапе массовых беспорядков. В данном случае целесообразно использовать дискретно-стохастические модели.

Начальный этап массовых беспорядков характеризуется:

- резким увеличением групповых нарушений общественного порядка;
- увеличением количества случаев неповиновения требованиям представителей власти;
- распространение провокационной и недостоверной информации;
- увеличением количества участников массовых беспорядков;
- увеличением количества жалоб населения на злоупотребления властью со стороны сотрудников ТО и т.д.

Основными задачами ТО по предупреждению массовых беспорядков являются:

Z_1 – сбор, обобщение и оценка данных об оперативной обстановке;

Z_2 – подготовка и организация профилактических мероприятий по предупреждения массовых беспорядков;

Z_3 – информирование органов государственной власти и управления социальной напряженности, оказание содействия в реализации предложений, относящихся к компетенции ТО;

Z_4 – постановка задач по пресечению массовых беспорядков.

Необходимо определить момент перехода от решения задачи Z_1 к решению задач Z_2 и Z_3 , Z_4 .

В данном случае число возможных состояний решения задач является конечным и равно 4 [2].

Для случайного процесса с дискретным состоянием характерен скачкообразный переход из одного состояния в другое (рис. 1).

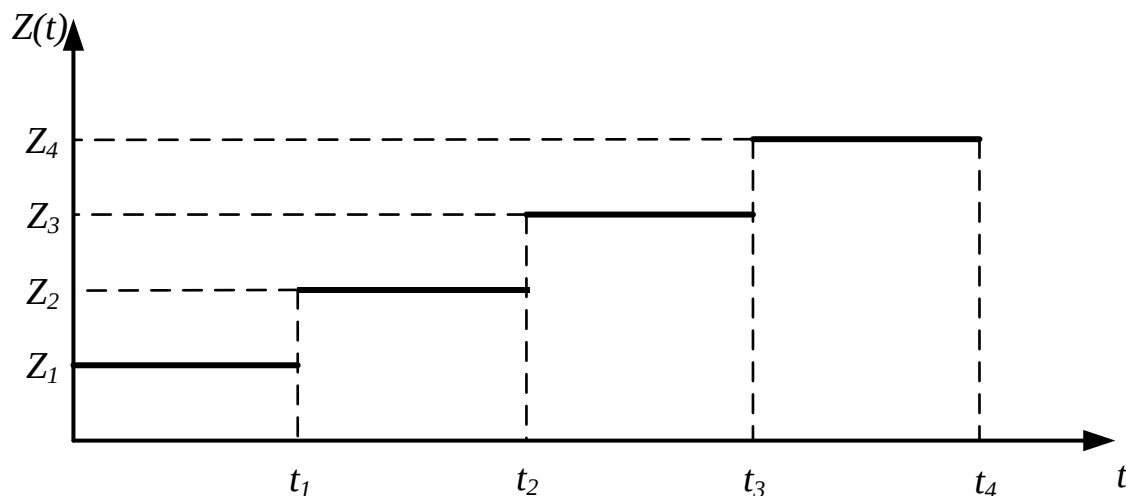


Рис. 1. График процесса решения задач

Тогда случайный процесс, протекающий в простейшей системе массового обслуживания (СМО) с однородным потоком заявок, может быть представлен количеством заявок, находящихся в произвольный момент времени. Тогда состояние Z_k процесса возникновения и развития массовых беспорядков будет означать, что в данной СМО находится k заявок, где $k = 0, 1, 2 \dots$ [3].

При описании дискретных систем одним из основных этапов является этап кодирования состояний, заключающийся в определении состава переменных и их значений, используемых для описания состояний.

Наша система может находиться в одном из четырех состояний Z_1, Z_2, Z_3, Z_4 в определенные моменты времени t . Причем переход из одного состояния в другое является случайным. Случайный процесс Z_t является случайным процессом с дискретным временем, так как переходы из состояния в состояние возможны только в строго определенные моменты времени $t_1, t_2, \dots, t_n$. Данный процесс является случайным процессом с непрерывным временем, так как переход из одного состояния в другое состояние возможен в любой заранее неизвестный момент времени.

Процесс предупреждения массовых беспорядков можно изобразить в виде графа переходов, в котором вершины соответствуют состояниям, а ориентированные дуги – переходам из одного состояния в другое. Указанный график является размеченным, так как на дугах графа указаны условия перехода в виде вероятностей переходов (рис. 2), где p_1, p_2, p_3 – вероятности переходов.

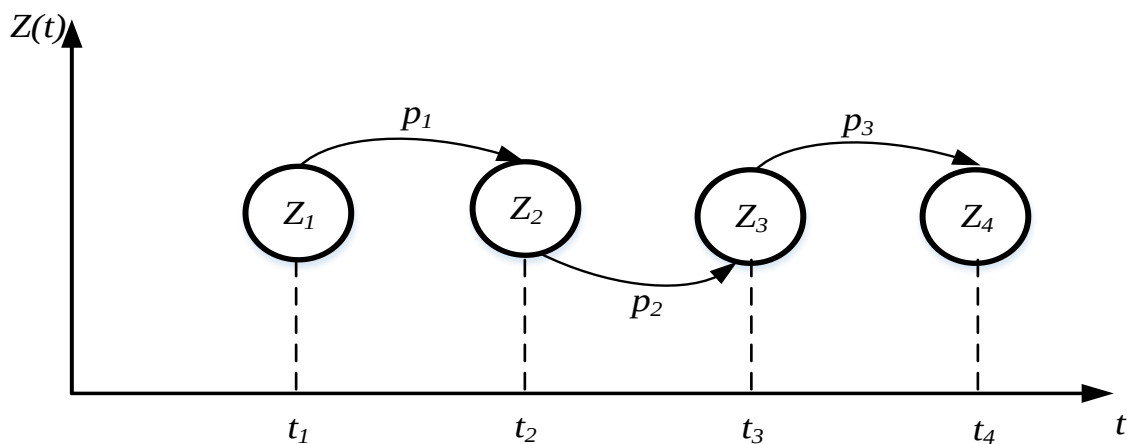


Рис. 2. Граф переходов

Для описания параметров данной системы целесообразно использовать марковские случайные процессы, где применяются следующие параметры:

$Z_1, Z_2, \dots, Z_n$ – перечень состояний;

Q – матрица вероятностей переходов;

$p_1(0), p_2(0), \dots, p_n(0)$ – начальные вероятности.

Изменения состояний данной системы происходят только в определенные моменты времени $t_1, t_2, \dots, t_n$. Переходы между состояниями описываются вероятностями переходов p_{ij} .

Вероятности переходов задаются в виде квадратной матрицы вероятности переходов

$Q = [p_{ij} | i, j = \overline{1, n}]$, при выполнении следующих условий:

$$0 \leq p_{ij} \leq 1; \sum_{j=1}^n p_{ij} = 1 \quad (i_{ij} = \overline{1, n}). \quad (1)$$

Начальные вероятности $p_{1(0)}, p_{2(0)}, \dots, p_{n(0)}$ задают состояние системы в начальный момент времени $t = 0$. Данные вероятности необходимы при изучении переходных процессов, так как данная система работает в нестационарном режиме.

Рассматриваемая система имеет конечное число состояний: $Z_1, Z_2, \dots, Z_n$. Вероятность $p_{i(t)}$ того, что система будет находиться в состоянии Z_i равна $p_{i(t)} = P_r \{Z(t) = E_i\}$.

В любой момент времени t система может находиться в одном из n возможных состояний при котором выполняется условие:

$$\sum_{j=1}^n p_j(t) = 1. \quad (2)$$

Данное условие называется нормировочным.

Совокупность вероятностей $p_i(t)$ может быть представлена вектором:

$p(t) = \{p_1(t), \dots, p_n(t)\}$, где

$$0 \leq p_i(t) \leq 1; \sum_{i=1}^n p_i(t) = 1. \quad (3)$$

Использование дискретно-стохастических моделей, в основу которых положен вектор состояний $p(t)$, позволяет рассматривать вопросы управления ТО на начальном этапе возникновения массовых беспорядков [4, 5].

ЛИТЕРАТУРА

1. Меньших В.В. Сетевая модель действий органов внутренних дел при чрезвычайных обстоятельствах криминального характера на примере массовых беспорядков / В.В. Меньших, А.Ф. Самороковский, В.В. Горлов // Труды Академии управления МВД России. – 2013. – № 4 (24). – С. 54–59.
2. Меньших В.В. Математическое моделирование действий органов внутренних дел в чрезвычайных обстоятельствах : монография / В.В. Меньших [и др.]. – Воронеж : Воронежский институт МВД России, 2016. – 187 с.
3. Алиев Т.И. Основы моделирования дискретных систем. – СПб: СПбГУ ИТМО, 2009. – 363 с.
4. Меньших В.В. Моделирование коллективных действий сотрудников органов внутренних дел : монография / В.В. Меньших [и др.]. – Воронеж : Воронежский институт МВД России, 2017. – 236 с.
5. Самороковский А.Ф. Системный подход к описанию процессов управления подразделениями ОВД при возникновении чрезвычайных обстоятельств / А.Ф. Самороковский // Вестник Воронежского института МВД России. – 2015. – № 1. – С. 76–85.

СВЕДЕНИЯ ОБ АВТОРАХ

Самороковский Андрей Федорович. Начальник кафедры тактико-специальной подготовки. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: samorokovskii_an@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. 8-905-656-16-34.

Горлов Виталий Викторович. Заместитель начальника кафедры тактико-специальной подготовки. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: gorlovvv@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-53-95.

Samorokovskiy Andrey Fedorovich. Head of the department of tactical and special preparation. Candidate of technical sciences, associate professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: samorokovskii_an@mail.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. 8-905-656-16-34.

Gorlov Vitaly Viktorovich. Deputy head of the department of tactical and special preparation. Candidate of technical sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-53-95.

Ключевые слова: чрезвычайные обстоятельства, математическое моделирование.

Key words: extraordinary circumstances, mathematical modeling.

УДК 519.8

Самороковский Андрей Федорович,
кандидат технических наук, доцент;
Толстых Андрей Андреевич

АНАЛИЗ ПРИМЕНИМОСТИ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ К ЗАДАЧЕ ВЫДЕЛЕНИЯ ТОПОГРАФИЧЕСКОЙ ИНФОРМАЦИИ С ПЕЧАТНЫХ НОСИТЕЛЕЙ

ANALYSIS OF THE APPLICATION OF ARTIFICIAL NEURAL NETWORKS TO THE TASK OF EXTRACTING TOPOGRAPHIC INFORMATION FROM PRINT MEDIA

В работе рассматриваются подходы к выделению топографической информации с печатных носителей, на основе применения сверточных нейронных сетей. Проведен сравнительный анализ архитектур, даны рекомендации.

The paper presents approaches to the extracting of topographic information with print media, based on the use of convolutional neural networks. A comparative analysis of architectures, recommendations were made.

Проблема планирования специальных операций (СО) и информационной поддержки руководителей имеет большое значение в деятельности органов внутренних дел. В предыдущей работе была предложена концепция системы поддержки принятия решений, первый блок которой представляет собой подсистему обработки топографической информации. Так как, в настоящее время, графические документы представлены в печатном виде, задача автоматической обработки приобретает высокую сложность. Одним из перспективных решений в области анализа изображений является аппарат искусственных нейронных сетей.

На основе концепции системы обработки топографической информации, возможно разработать функциональную схему системы сбора топографической информации. Данная схема представлена на рис. 1.

В настоящее время ведутся активные работы в области детектирования объектов на телевизионных изображениях. Основной частью практически любого детектора является распознающая сверточная нейронная сеть, однако различаются методы пред- и постобработки. Эффективность сверточных нейронных сетей подробнее рассмотрена в [1]. Рассмотрим подробнее наиболее успешные подходы в данной области.

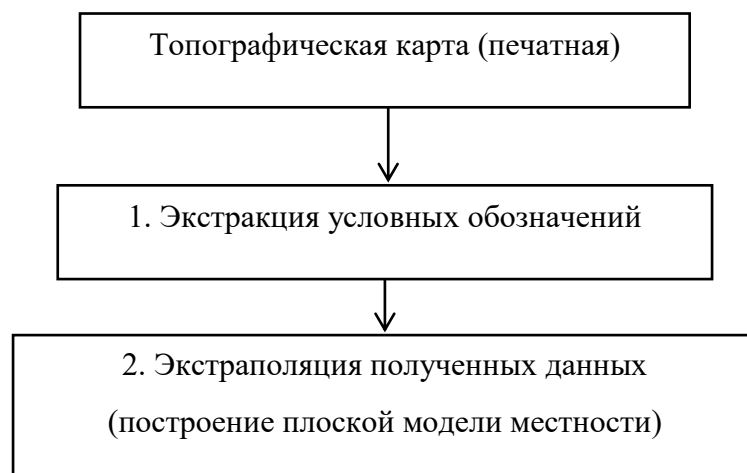


Рис. 1. Функциональная схема системы сбора топографической информации

Faster R-CNN расшифровывается как *Faster Region-based Convolutional Neural Networks* – быстрее сверточная нейронная сеть, основанная на областях интереса (БНСО). Является развитием метода сверточной нейронной сети, основанной на областях интереса (НСО). Под областью интереса понимается область, в которой с наибольшей вероятностью присутствует искомым объект [1].

В модели НСО следует выделить два основных шага: первый – выделение на входном изображении областей интереса; второй – применение к выделенным областям сверточной нейронной сети для классификации объекта в данной области [2].

Из всех методов выделения областей интереса наиболее эффективным признан метод селективного поиска [2]. Данный метод основан на иерархичном группировании [3]. На вход подается цветное изображение, результатом работы являются набор областей L , гипотетически содержащих объекты. На первом шаге работы алгоритма формируется набор начальных областей и множество подобия:

$$R = \{r_1, \dots, r_n\}, \quad S = \emptyset \quad (1)$$

где R – множество начальных областей; r – одна из начальных областей; n – количество начальных областей, определяемое до начала алгоритма; S – множество подобия. Далее, для каждой пары соседних начальных областей вычисляется подобие, полученный результат объединяется с множеством подобия:

$$S = S \cup s(r_i, r_j), \quad (2)$$

где $s(\square)$ – вычисление меры подобия. В работе [3] применяется следующая форма данной меры:

$$\begin{aligned} s_c(r_i, r_j) &= \sum_{k=1}^p \min(c_i^k, c_j^k), \quad C_i = \{c_i^1, \dots, c_i^p\}; \\ s_t(r_i, r_j) &= \sum_{k=1}^l \min(t_i^k, t_j^k), \quad T_i = \{t_i^1, \dots, t_i^l\}; \\ s_s(r_i, r_j) &= 1 - \frac{v(r_i) + v(r_j)}{v(I)}; \\ s_f(r_i, r_j) &= 1 - \frac{v(B_{ij}) - v(r_i) - v(r_j)}{v(I)}; \end{aligned} \quad (3)$$

$$s(r_i, r_j) = \alpha_1 s_c(r_i, r_j) + \alpha_2 s_t(r_i, r_j) + \alpha_3 s_s(r_i, r_j) + \alpha_4 s_f(r_i, r_j),$$

где C_i – гистограмма для i начальной области; c_i^p – значение p столбца гистограммы i начальной области; p – количество столбцов гистограммы; T_i – множество характеристик текстуры i области; t_i^l – значение l характеристики текстуры i начальной области; l – количество вычисляемых характеристик текстуры; $v(\square)$ – количество пикселей рассматриваемой области; I – входное изображение; BB_{ij} – прямоугольная рамка, описанная вокруг областей i и j . Следует отметить, что к гистограммам применяется операция L -нормировки.

После вычисления подобия всех соседних начальных областей выполняются следующие действия:

$$s(r_i, r_j) = \max(S); \quad (4)$$

$$r_z = r_i \cup r_j; \quad (5)$$

$$r_i : S = S \setminus s(r_i, r_*); \quad r_j : S = S \setminus s(r_*, r_j); \quad (6)$$

$$S = S \cup S_z; \quad R \cup r_i; \quad (7)$$

$$S \neq \emptyset, \quad (8)$$

где R – набор областей, прошедших отбор; (8) – условие остановки. На последнем шаге вычисляется положение областей, входящих в R .

Наиболее эффективными являются следующие параметры: $p=75$; $l=240$. Подобный подход к детектированию объектов на телевизионных изображениях требует большого объема вычислений.

Вторым этапом метода на основе СНСО является применение ко всем областям интереса, вычисленным на первом этапе, сверточной нейронной сети (СНС). Оптимизация данной СНС полностью повторяет оптимизацию СНС для решения задач классификации.

Модель БСНСО позволяет увеличить скорость детектирования объектов путем изменения последовательности этапов СНСО, однако, данный подход приводит к увеличению слоев СНС. Логика метода БСНСО состоит в следующем:

1. Тренируется глубокая СНС для классификации изображений.
2. Сохраняются карты признаков с последнего сверточного слоя для каждого изображения в тренировочной выборке.
3. Тренируется нейронная сеть, определяющая начальные области интереса по полученным картам признаков.
4. Производится разделение областей интереса (для многообъектного детектирования)
5. Производится классификация объекта внутри области интереса на карте признаков с помощью полносвязной нейронной сети.

В таблице 2 приведены результаты измерения скорости СНСО и БСНСО а также их достоинства и недостатки.

Таблица 1

Скорость СНСО и БСНСО

Наименование сети	Скорость прямого прохода	Достоинства	Недостатки
СНСО	50 с/изобр.	Относительно небольшая архитектура нейронной сети, подлежащая тренировке.	Крайне низкая скорость работы, обуславливаемая большим количеством вычислений при прямом проходе.
БСНСО	0.2 с/изобр.	Высокая скорость работы (однако не достаточная для потокового видео)	Большой размер нейронной сети, значительно увеличивающий время обучения.

В настоящее время способы детектирования развиваются на основании подхода, предлагаемого БСНСО. Данный факт обусловлен тем, что обучение сети можно производить на высокоскоростных графических ускорителях, собранных в кластер, а непосредственное применение может быть реализовано практически на любых платформах (ПК, смартфоны, одноплатные компьютеры. Последние две платформы – только при использовании python) [4].

Анализ подходов к детектированию информации с топографических карт демонстрирует преимущества архитектур искусственных нейронных сетей типа БСНСО. Таким образом, блок реализующий преобразование информации с бумажного носителя в электронный вид наиболее рационально выполнить на базе алгоритмов БСНСО. Подобная реализация обеспечит системе поддержки принятия решений точное и быстрое получение актуальных топографических данных с карт района проведения СО.

ЛИТЕРАТУРА

1. Толстых А.А., Голубинский А.Н. Распознавание объектов на телевизионных изображениях с использованием аппарата сверточных нейронных сетей // Вестник Воронежского института МВД России, – 2017. – №1. – С. 7–17.
2. Udupa J.K., Samarasekera L.W., Miki Y. Sclerosis Lesion Quantification Using Fuzzy-Connectedness Principles // Transactions on Medical Imaging. – 1997. – № 5. – С. 598–609.
3. Girshick R., Donahue J., Darrell T., Malik J. Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation // CVPR '14 Proceedings of the 2014 IEEE Conference on Computer Vision and Pattern Recognition Pages. – 2014. – С. 580–587.
4. Uijlings J.R., van de Sande K.E., Gevers T., Smeulders A.W. Selective Search for Object Recognition // International Journal of Computer Vision. – 2013. – Т. 104. – №. 2. – С. 154–171.

СВЕДЕНИЯ ОБ АВТОРАХ

Самороковский Андрей Федорович. Начальник кафедры тактико-специальной подготовки. Кандидат технических наук, доцент.

Воронежский институт МВД России

E-mail: samorokovskii_an@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-53-90.

Толстых Андрей Андреевич. Преподаватель кафедры тактико-специальной подготовки.

Воронежский институт МВД России.

E-mail: tolstykh.aa@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-56-47.

Samorokovsky Andrey Fedorovich. Head of the Department of special tactics. Candidate of Technical Sciences, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-53-90.

Tolstykh Andrey Andreevich. Lecturer of the department of special tactics.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-56-47.

Ключевые слова: обработка топографической информации, машинное зрение.

Key words: topographic information processing, computer vision.

УДК 004.932: 519.7.

АНАЛИЗ РАЗРАБОТКИ МОДЕЛЕЙ НАДЕЖНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В АВИАЦИИ

ANALYSIS OF DEVELOPMENT MODELS OF RELIABILITY OF AVIATION SOFTWARE IN AVIATION

В статье описаны проблемы оценки показателей безотказности комплекса аппаратно-программных средств в авиации, рассмотрены подходы к решению данных задач.

The article describes the evaluation of indicators of reliability of the complex hardware and software, the approaches to solving these problems.

В настоящее время в связи с повышением конструктивной сложности проектируемых современных образцов вооружения и военной техники все более остро встает проблема обеспечения безотказности. Особенно это характерно для систем ответственного целевого назначения.

Обеспечение заданного уровня надежности является решением проблемы синтеза для аппаратного и программного обеспечения системы. Он предназначен для обеспечения заданного уровня надежности программного обеспечения (ПО) на этапе его разработки. Вторая составная часть проблемы относится к надежности ранее имеющегося программного обеспечения, представленного на реально действующем комплексе. Эта задача возникает, когда необходимо оценить надежность комплекса в целом, подчеркнув вклад аппаратных и программных компонентов в общие характеристики.

Чтобы решить эту проблему, необходимо проанализировать данные, полученные в реальной системе за определенный период ее работы, чтобы оценить существующие параметры надежности и предсказать поведение системы в будущем.

Программные сбои в результате ошибок имеют совершенно иную физическую природу, чем технологические сбои. Это связано с тем, что аппаратные сбои вызваны физическими характеристиками реализации конкретного модуля, тогда как основным источником программных сбоев являются ошибки проектирования, которые проявляются в каждом экземпляре программы. Программное обеспечение с точки зрения теории надежности являются восстанавливаемыми продуктами.

Расчет показателей надежности сложных систем следует проводить комплексно, с учетом всех факторов. Их можно разделить на две основные группы: факторы, связанные с надежностью программного обеспечения, установленного на них, и традиционные факторы, которые учитывают надежность самого оборудования.

Рассматривать надежность программного обеспечения очень сложно из-за того, что регистрация времени и причин сбоев программного обеспечения на этапе его эксплуатации, а тем более на этапе тестирования и отладки, как правило, недостаточны. Кроме того, следует учитывать обстоятельства, при которых в отличие от аппаратных модулей любые характеристики надежности используемых программных модулей не предоставляются при их доставке. Также нет подробной информации о структуре программы.

Среди структурных схем обеспечения надежности аппаратных средств выделяются два способа: методы, основанные на избыточности их компонентов, и методы, включающие реконфигурацию системы в случае сбоя.

Методы резервного копирования системы предполагают, что базовая рабочая конфигурация системы остается неизменной во время ее работы. В случае сбоев частей конструкции происходит элементарная замена неисправных модулей на исправные дополни-

тельные блоки. Подобная замена способна осуществляться либо как часть переключения рабочего оборудования (в этом случае время простоя системы считается незначительным), либо как часть процесса восстановления вышедших из строя блоков (в этом случае время окончательного восстановления учитывается, когда анализ надежности системы). Методы реконфигурации систем подразумевают изменение рабочей конфигурации системы в процессе ее эксплуатации. В то же время отдельные показатели производительности меняются, например, размер памяти, скорость или параметры отказоустойчивости.

При разработке моделей надежности программного обеспечения для оружия следует учитывать тот факт, что в системе параллельно функционируют три категории программ, любая из которых приносит свои вложения в показатели прочности: операционная система, системы управления базами данных и прикладные программы. Ключевыми отличительными чертами функционирования программно-аппаратных комплексов считаются высокие запросы к их надежности и потребность учета абсолютно всех условий, которые его характеризуют.

Учитывание прочности системных программ весьма сложная процедура, так как у них нет достоверных характеристик надежности. Кроме того отсутствует детальная информация о структуре проектов подобного вида. По этой причине следует применять оценочные характеристики, сопряженные с продолжительностью программы.

Для систем, которые были протестированы, согласно различным анализам, существует от пяти до ста ошибок на 1000 строк исполняемого программного кода. По мере развития программного обеспечения в каждой новой версии появляется все больше и больше кода, и часто новая версия менее надежна, чем предыдущая. Количество ошибок на тысячу строк кода имеет тенденцию стабилизироваться с увеличением количества выпущенных версий, но асимптотически этот показатель отличается от нуля. Для критически важных приложений, включающих операционные системы и другое системное программное обеспечение, к моменту доставки системы клиенту она может содержать 0,04 ... 0,15 ошибок на 1000 строк программного кода.

Однако незначительность этой величины не дает оснований полностью отказаться от влияния ошибок в этих программных средствах из-за большого объема таких программ.

Например, ядро Windows XP содержит более 5 миллионов строк кода. Это означает, что даже при самых оптимистичных оценках к моменту начала поставки системы клиентам, ядро Windows XP содержит более 200 ошибок.

Нужно кроме того выделить, что приблизительно 70% кода операционной системы забрано под код драйвера. Драйверы устройств как правило разрабатываются программистами, которые работают с производителями дополнительных и вспомогательных устройств, и контроль свойств их продуктов, как правило, ниже, чем у поставщиков операционных систем. Для того чтобы дать оценку вклада системных программ в единую безопасность программного обеспечения, следует знать не только лишь число ошибок в нем, однако и законы распределения времени их выявления. Подобные сведения могут быть получены на основании рассмотрения протоколов испытания программного обеспечения. Анализ вида и характеристик таких законов может быть проведен посредством рассмотрения в базе данных периода подготовки к выпуску новейшей версии программного обеспечения. Как правило, считается, что для системных программ более новая версия включает приблизительно 30% кода по сравнению с предшествующей версией. Для приложений это значение будет 50%.

Согласно словам создателей Windows 8, размер программного кода данной системы - 339 105 291 байт. Средняя длина машинной команды составляет 8 байт. Предполагая, что любая строка начального кода переведена в 10 машинных команд, мы получаем, что исходный код был примерно $4,2 \cdot 10^6$ строк.

Количество ошибок в тексте системных программ будет взято как минимум из расчетных значений, непосредственно 5 ошибок на 1000 строк начального программного кода и 0,04 ошибки на 1000 строк кода уже после испытаний. Значения данных характеристик для драйверов, введенных в операционную систему, приняты в 3 раза выше, чем для кода ядра.

Период подготовки к выпуску новой версии программного продукта и, следовательно, продолжительность этапа тестирования T , установим равным 3 годам.

В таблице 1 представлены исходные данные для расчета надежности программного обеспечения на примере Windows XP (данные взяты из открытых источников). Подсчет знаменателя, применяемого с целью установления времени отказов на разных стадиях тестирования, был вычислен с использованием пакета Mathcad.

Таблица 1

Исходные данные для расчета надежности программного обеспечения

Вид ПО	Исходный код				Этап тестирования		
	Объем	Объем нового кода	Количество ошибок на 1000 строк кода	Общее количество ошибок	Знаменатель при заполнении исходных данных	Количество строк на 1000 строк кода	Количество ошибок к окончанию тестирования
ОС без учета вклада драйверов	$5 \cdot 10^6$	$1,5 \cdot 10^6$	5	7500	1,00026	0,04	60
Ядро ОС	$1,5 \cdot 10^6$	$0,45 \cdot 10^6$	5	2250		0,04	18
Драйверы	$3,5 \cdot 10^6$	$1,05 \cdot 10^6$	15	15750		0,12	126
ОС с учетом драйверов	$5 \cdot 10^6$	$1,5 \cdot 10^6$		18000	1,00004		144
Oracle Content Server	$4,2 \cdot 10^6$	$1,3 \cdot 10^6$	5	6500	1,00037	0,04	52
Прочие программы	$1 \cdot 10^5$	$0,5 \cdot 10^5$	10	500	1,0116	0,08	4

При расчете надежности операционной системы (с учетом драйверов и без) используется формула Стерджеса, которая демонстрирует наилучшую величину интервала, что дает возможность раскрыть отличительные закономерности рассматриваемого явления при наименьшем числе промежутков:

$$H = R / (1 + 3,32 \cdot \lg n),$$

где n – количество наблюдаемых значений;

$$R = X_{\max} - X_{\min}.$$

Левая граница первого интервала определяется как:

$$a_1 = X_{\min} - H/2,$$

Правая граница i -го интервала совпадает с левой границей $(i+1)$ -го интервала

$$b_i = a_{i+1},$$

Правая граница конечного промежутка обязана удовлетворять следующему условию:

$$b_i \geq X_{\max}.$$

Интервалы, для которых частота попадания менее 5, необходимо совместить с соседними интервалами. Вычисление характеристик прочности на основании полученных данных представлены в таблице 2.

Таблица 2

Результаты расчета надежности операционной системы

a_i	b_i	Частота	Объединенные интервалы			Расчет показателей надежности			
			a_i	b_i	Частота	Относит. частота	λ_i , 1/ч	λ_{cp} , 1/ч	$T_{отк}$, ч
12	92	2	12	172	13	0,325	0,00203	0,00240	417,21
92	172	11	172	253	12	0,300	0,0037		
172	253	12	253	333	11	0,275	0,00344		
253	333	11	333	574	4	0,100	0,00041		
333	413	0							

Особенностью надежности программного обеспечения по сравнению с надежностью аппаратного обеспечения является то, что одно и то же программное обеспечение работает одновременно на большом количестве компьютеров. Число выявленных ошибок соразмерно с количеством компьютеров. При этом ошибка, обнаруженная на одном компьютере, сразу поправляется на всех иных компьютерах. Отталкиваясь от этого, полученные результаты являются неотъемлемой частью потока сбоев программного обеспечения для всех компьютеров, на которых оно установлено.

Приобретенные величины среднего времени выработки на отказ хорошо согласуются с данными о том, что за период выпуска для реализации Windows XP компанией Microsoft было официально выпущено 16 патчей. Если учесть, что каждый патч в среднем содержит исправления для трех ошибок, то интенсивность отказов составит $0,0018 \text{ ч}^{-1}$.

Путь выполнения программы для каждого конкретного приложения уникален. Ввиду почти безграничного числа подобных следов для абсолютно всех вероятных применений интенсивность выявления погрешностей программного обеспечения на определенном компьютере обратно пропорциональна количеству компьютеров, где применяется данная программа.

Таким образом, задача построения интегрированной модели надежности системы с учетом ее аппаратного и программного обеспечения является актуальной.

ЛИТЕРАТУРА

1. Шубинский И.Б. Функциональная надежность информационных систем (Методы анализа).- М.: ООО «Журнал «Надежность», 2012, - 296 с.
2. ГОСТ Р 51904-2002 Программное обеспечение встроенных систем. Общие требования к разработке и документированию.

СВЕДЕНИЯ ОБ АВТОРЕ

Сафонова Надежда Леонидовна. Преподаватель.
ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина».
E-mail: nadin_qu@mail.ru
Россия, 394064, г. Воронеж, ул. Старых Большевиков, 54 «А».
Тел. 8-951-540-84-34.

Safonova Nadezhda Leonidovna. Teacher.
Voronezh Air Force Military Academy named after N. Zhukovskiy and J.Gaganin.
Work address: Russia, 394064, Voronezh, Old Bolsheviks Str., 54 «A».
Tel. 8-951-540-84-34.

Ключевые слова: надежность программного обеспечения, методы обеспечения надежности, интегрированная модель надежности системы.

Key words: software reliability, reliability assurance methods, integrated system reliability model.

УДК 004.45

Сидоров Александр Викторович,

кандидат технических наук;

Гречаный Сергей Анатольевич,

кандидат технических наук;

Романов Михаил Сергеевич,

кандидат технических наук

ПЕРСПЕКТИВНЫЕ ИНСТРУМЕНТЫ ДЛЯ СЕРВЕРНОЙ ЧАСТИ WEB-ПРИЛОЖЕНИЙ ПРИ РАЗРАБОТКЕ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

PERSPECTIVE TOOLS FOR THE SERVER PART OF WEB APPLICATIONS IN THE DEVELOPMENT OF AUTOMATED INFORMATION SYSTEMS

Настоящая статья посвящена вопросам выбора оптимальных инструментов для серверной части web-приложений при разработке автоматизированных информационных систем.

This article is devoted to the selection of optimal tools for the server part web-applications in the development of automated information systems.

В настоящей статье речь пойдёт о перспективных инструментах для разработки Web-приложений при создании автоматизированных информационных систем (АИС), в частности о backend фреймворк Laravel и интегрированной среде разработки IDE. С выбором языка программирования, фреймворка серверной и клиентской части приложения, структуры базы данных, системы управления базой данных (СУБД) и других вопросов сталкиваются большинство разработчиков. Хотелось бы отметить, что в статье не рассматривается выбор типа приложения, СУБД, языка программирования, хотя данные вопросы первичны при создании компьютерных программ.

Одним из важных составляющих Web-приложений является Framework (фреймворк), его можно дословно перевести с английского как «каркас», «структура», «конструкция». Backend фреймворки – это программные продукты, которые упрощают создание и поддержку технически сложных или нагруженных проектов. Backend фреймворк, как правило, содержит только базовые программные модули, а все специфичные для проекта компоненты реализуются разработчиком на их основе [1].

Одним из главных преимуществ при использовании фреймворков является то, что Web-приложения часто используют стандартизированную структуру организации компонентов. Создание структуры при разработке на фреймворках очень упрощается. По сути, backend фреймворк – это множество конкретных и абстрактных классов, а также определений способов их взаимоотношения. Конкретные классы обычно реализуют взаимные отношения между классами, а абстрактные классы представляют собой точки расширения, в которых каркасы могут быть использованы или адаптированы. Для обеспечения расширения возможностей обычно используются техники объектно-

ориентированного программирования (например, части приложения могут наследоваться от базовых классов фреймворка).

Разработка на backend фреймворке (в отличие от «самописных» решений) позволяет добиться простоты сопровождаемого проекта. Возможна (и относительно проста) реализация любых процессов, а не только тех, которые изначально заложены в систему. Также проекты на базе фреймворков легко масштабируемы и модернизируемы.

Решения на backend фреймворках, как правило, работают значительно быстрее и выдерживают большую нагрузку. По уровню безопасности решения на backend фреймворках значительно превосходят «самописные» системы.

Для разработки Web-приложений АИС наиболее перспективным является фреймворк Laravel. На сегодняшний день этот фреймворк является лучшим выбором для создания проекта отвечающего всем современным требованиям разработки на языке программирования PHP. Фреймворк позволит упростить решение основных рутинных задач, таких как аутентификация, маршрутизация, сессии и кэширование. Laravel объединяет и использует в своей работе самые лучшие модули, существующие в других PHP фреймворках.

Основные преимущества Laravel [2, 3]:

- большая экосистема с мгновенным разворачиванием своей платформы. Официальный сайт предоставляет множество документации и информации для ознакомления;
- подробная и хорошо структурированная документация;
- современные тенденции и подходы в Web-разработке;
- собственный «движок» для шаблонов «Blade», синтаксис языка которого, способствует решению всех необходимых задач при создании пользовательского интерфейса.

Первый релиз Laravel вышел в 2011 году. Согласно статистике запросов, которую предоставляет Google Trends (сайт – trends.google.com), он занимает первое место по популярности среди разработчиков PHP в мире.

График статистики запросов фреймворка Laravel за последние 5 лет представлен на рисунке 1.

Как видно из графиков Google Trends, фреймворк Laravel занимает уверенное первое место (синий цвет на графике).

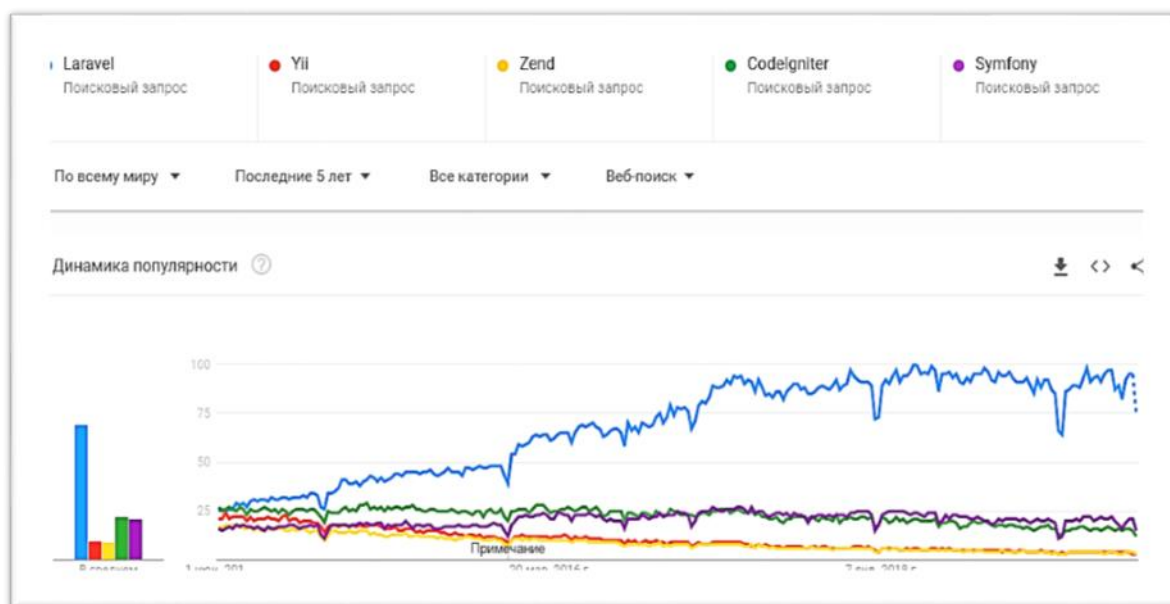


Рис. 1. График популярности фреймворка Laravel

Если взять статистику запросов в Google Trends по России, то ситуация по популярности фреймворка Laravel практически не изменится, график статистики представлен на рисунке 2.

Разработка приложений в Laravel основана на шаблоне проектирования MVC [3]. Шаблон проектирования MVC предполагает разделение данных приложения, пользовательского интерфейса и управляющей логики на три отдельных компонента: модель, представление и контроллер, причём модификация каждого компонента может осуществляться независимо.

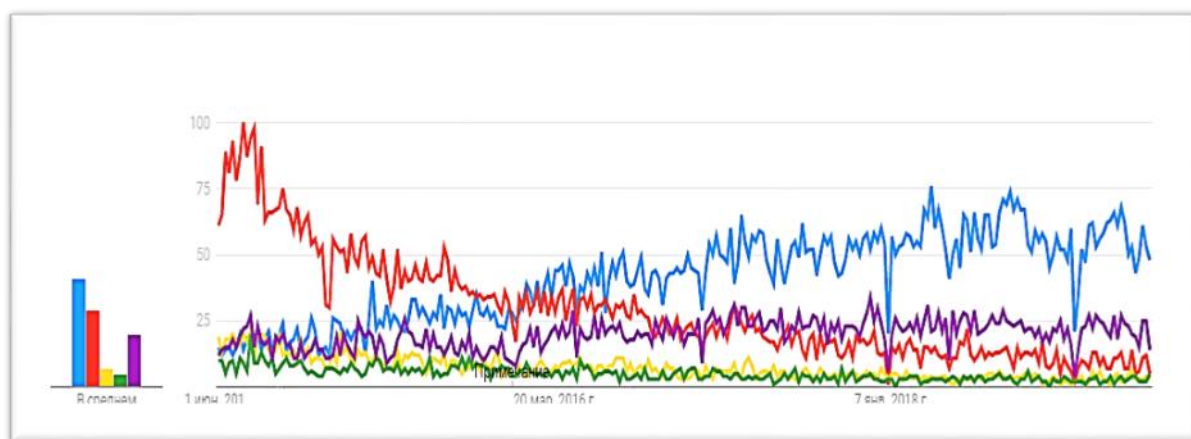


Рис. 2. Статистика запросов в Google Trends по России

На рисунке 3 представлена схема работы приложения, основанная на шаблоне проектирования MVC.

Модель (Model) – предоставляет собой объектную модель определённой предметной области, включает в себя данные и методы работы с этими данными, реагирует на запросы из контроллера, возвращая данные и (или) изменяя своё состояние, при этом модель не содержит в себе информации, как данные можно визуализировать, а также не «общается» с пользователем напрямую.

Контроллер (Controller) – обеспечивает связь между пользователем и системой, использует модель и представление для реализации необходимой реакции на действия пользователя, как правило, на уровне контроллера осуществляется фильтрация полученных данных и авторизация (проверяются права пользователя на выполнение действий или получение информации).

Представление (View) – отвечает за отображение информации (визуализацию), одни и те же данные могут представляться различными способами, например, коллекцию объектов при помощи разных «View» можно представить как в табличном виде, так и списком.

Контроллер, который получает все запросы и вызывает другие контроллеры для выполнения действий в зависимости от ситуации, обычно называется «роутинг» (англ. routing – процесс определения маршрута данных.).

После выбора фреймворка необходимо определиться с интегрированной средой разработки, хотя её выбор во многом определяет язык программирования

Интегрированная среда разработки (IDE, от англ. – Integrated Development Environment) – система программных средств, используемая программистами для разработки программного обеспечения.

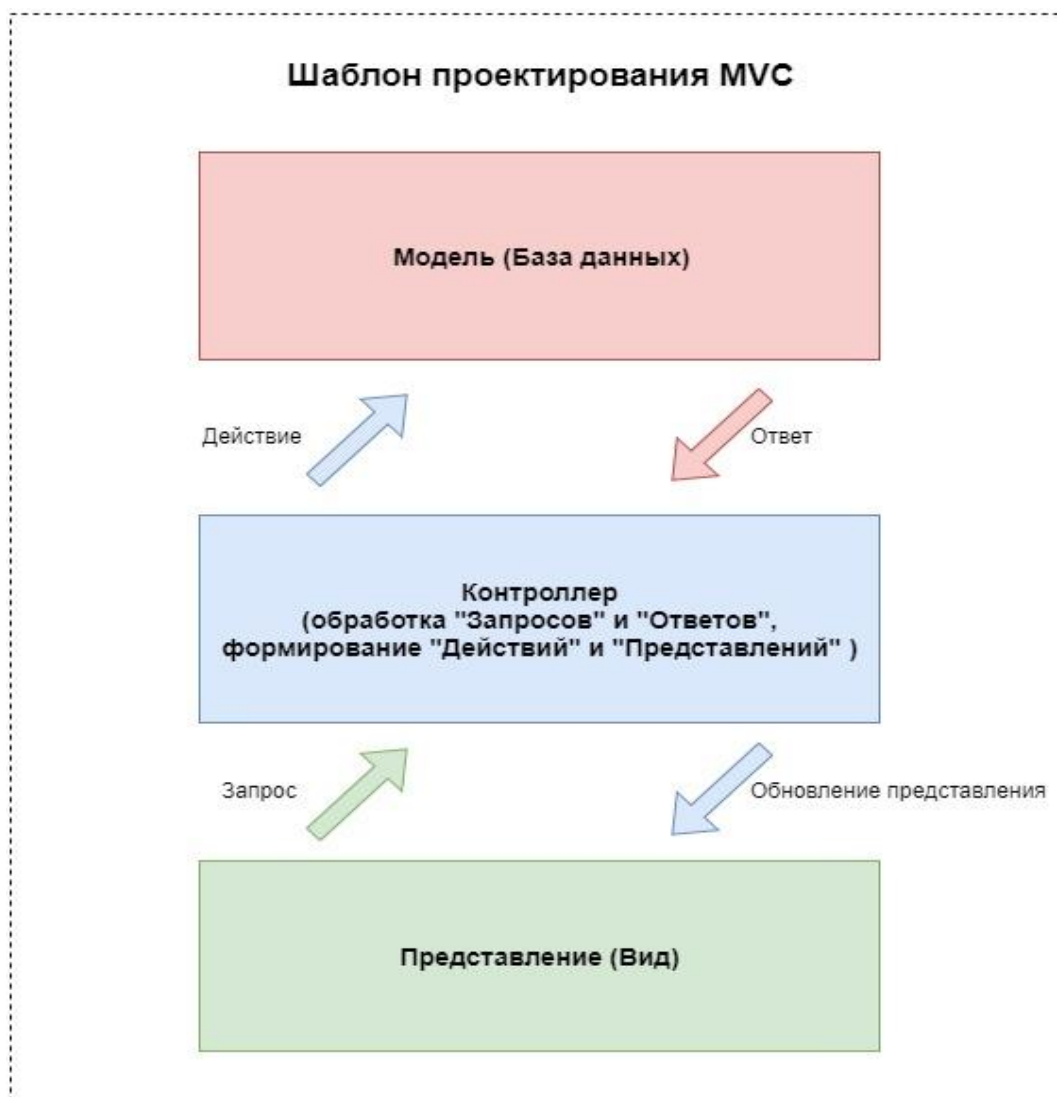


Рис. 3. Шаблон проектирования MVC

IDE – это не просто текстовый редактор. В то время как текстовые редакторы для кода, такие как Sublime или Atom, предлагают множество удобных функций, таких как подсветка синтаксиса, настраиваемый интерфейс и расширенные средства навигации, они позволяют только писать код. Для создания функционирующих приложений как минимум нужен компилятор и отладчик.

Правильно выбранная среда IDE максимально важна для создания и поддержания высокого качества кода. Интегрированная среда разработки дает возможность записывать, транслировать программы, отлаживать код, при этом не потребуется использование дополнительных программ.

IDE включает в себя эти компоненты, как и ряд других. Некоторые из них поставляются с дополнительными инструментами для автоматизации, тестирования и визуализации процесса разработки. Термин «интегрированная среда разработки» означает, что предоставляется все необходимое для превращения кода в функционирующие приложение [4]. Хорошая IDE для PHP упростит и облегчит процесс разработки. Чтобы выбрать интегрированную среду разработки, необходимо провести сравнительный анализ самых популярных предлагаемых решений.

NetBeans среда разработки для PHP, которая открывает список самых популярных. Важно отметить, что среда разработки бесплатная и поддерживает русский и английский языки. Создание данной среды было начато еще в 1996 году, но с того времени разработчики проделали огромную работу по оптимизации проекта. NetBeans IDE динамично развивается и постоянно совершенствуется.

Проект не был бы столь успешен, если бы корпорация Oracle не спонсировала его, но в 2016 году курирование было передано фонду Apache. Разработчиками на данный момент являются NetBeans Community и NetBeans Org.

В список функций среды редактирования входят: редактор автоматического завершения php кода с заложенной подсветкой синтаксиса, ошибок, вхождений; отладка кода, также есть удобный интерфейс и система навигации. Одним из дополнительных плюсов возможность просмотреть историю работы с файлом, в случае ошибки всегда есть возможность вернуться назад и восстановить нужный элемент. Расширить возможности среды можно установив дополнительные плагины.

IDE PHPStorm интеллектуальный редактор для PHP с подсветкой кода, который обладает возможностью анализировать код, устраняя ошибки и даже предотвращая их появление [4, 5]. Среда допускает установку плагинов, которые могут увеличить функционал и модифицировать продукт под свои потребности.

Интеграция этой среды с системами управления версиями, позволяет сравнивать несколько файлов, находить между ними разницу, совмещать данные не покидая PHPStorm. Осуществляется отслеживание всех изменений в коде, а также есть поддержка Phing.

Еще одной функцией, которая существенно облегчает работу с кодом: автодополнение. Достаточно ввести часть текста или кода, а программа ее дополнит, допишет. Функция финализирует имена переменных, ключевые слова PHP, классы и методы.

Простая и легкая IDE – PHP Designer. Звание самой простой среды разработки было дано из-за небольшого набора функций, который значительно уступает в количестве другим продуктам. По сути данная IDE больше чем просто редактор кода, но и полноценным IDE назвать ее не получится. Набор расширений, дополнений и плагинов делает ее более функциональной позволяет больше работать с кодом и во многом упрощает работу и повышает производительность.

Среда PHP Designer отлично подойдет новичкам, она позволит легко разобраться с набором инструментов и при этом удовлетворит всем требованиям и качественно выполнит все поставленные перед ней задачи. Интеллектуальная подсветка синтаксиса один из главных плюсов, он сразу указывает на ошибки в коде, что помогает избежать дальнейших сложностей. Но тут же можно отметить минус данной среды, работает только в системе Windows.

Еще одна перспективная IDE – Codelobster. Она работает со многими языками программирования, в том числе PHP. Удобная система навигации, набор горячих клавиш и инструменты, которые облегчат работу, ускорят ее и увеличат производительность. IDE поддерживает установку дополнительных плагинов, которыми можно расширить и модифицировать интегрированную среду разработки для комфортной работы.

Список IDE намного больше представленного выше, выбирая подходящую интегрированную среду разработки в первую очередь нужно определиться, какие функции в приоритете, что планируется делать и какие инструменты понадобятся в первую очередь. Язык программирования, который используется в работе, также играет большую роль при выборе.

По моему мнению, IDE PHPStorm, по сравнению с другими решениями обладает наиболее мощным функционалом профессиональной разработки; фреймворк Laravel представляет собой набор хорошо отлаженных и прекрасно зарекомендовавших себя

независимых компонентов, которые в связке с шаблоном проектирования MVC образуют самый популярный и быстроразвивающийся фреймворк. Тем самым, при использовании данных инструментов, достигается не только высокая скорость разработки Web-приложений при создании АИС, но и большая производительность и надёжность решений.

ЛИТЕРАТУРА

1. Мезенцев К. Н. Автоматизированные информационные системы : учебник / К.Н. Мезенцев. – М. : Академия, 2012. – 176 с.
2. Laravel – материал из Википедии – свободной энциклопедии [Электронный ресурс] – URL : <https://ru.wikipedia.org/wiki/Laravel>.
3. Документация Laravel [Электронный ресурс] – URL : <https://laravel.com/docs/5.7>.
4. Котеров Д. В. PHP 7 : отдельное издание / Д. В Котеров, Симдянов И. В. – СПб. : БХВ-Петербург, 2016. – 1088 с.
5. Никсон Робин Создаем динамические Web-сайты с помощью PHP, MySQL, JavaScript и CSS / Робин Никсон – М. : Питер, 2016. – 204 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Сидоров Александр Викторович. Доцент кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: fisherman.16.10.1980@gmail.com

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-84.

Sidorov Aleksandr Viktorovich. Associate Professor of radio engineering systems and security monitoring systems Department. Candidate of Engineering Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: fisherman.16.10.1980@gmail.com.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-84.

Гречаный Сергей Анатольевич. Начальник кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: grechan7777@mail.ru.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-02.

Grechanyj Sergej Anatol'evich. Chief of department of radio engineering systems and complexes of security monitoring. Candidate of Engineering Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: grechan7777@mail.ru.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-02.

Романов Михаил Сергеевич. Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: m.romanov90@mail.ru.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-81.

Romanov Mikhail Sergeyevich. Teacher of the department of radio engineering systems and complexes of security monitoring. Candidate of Engineering Sciences

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: m.romanov90@mail.ru.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-81.

Ключевые слова: Web-приложение, автоматизированная информационная система, фреймворк, Laravel, интегрированная среда разработки.

Key words: Web application, automated information system, framework, Laravel, integrated development environment.

УДК 004.4

Синегубова Светлана Владимировна,
кандидат технических наук, доцент;

Синегубов Сергей Владимирович,
кандидат технических наук, доцент

МОДЕЛЬ СЕГМЕНТА МОБИЛЬНОЙ СВЯЗИ

MODEL OF SEGMENT OF MOBILE COMMUNICATION

В работе рассматриваются вопросы размещения оборудования сегмента мобильной связи для повышения живучести данной системы. Сформулирована модель организации мобильной связи для выявления оптимального соединения между абонентами телекоммуникационной сети. Представлена имитационная модель, реализующая связь между абонентами телекоммуникационной сети.

The paper deals with the placement of equipment in the mobile communication segment to increase the survivability of this system. A model of the organization of mobile communication is formulated to identify the optimal connection between subscribers of a telecommunications network. A simulation model that implements communication between subscribers of a telecommunications network is presented.

Введение. Вопросы повышения эффективности, живучести и информационной безопасности систем управления и связи органов внутренних дел занимают первоочередное место в деятельности органов внутренних дел для решения оперативно-служебных задач подразделений полиции. Решение проблем выявления и расследования преступлений в сфере информационных технологий затруднительно без создания соответствующих математических моделей, позволяющих моделировать ситуацию без

привлечения значительных людских и материальных ресурсов. Решение данного вопроса возможно лишь в плоскости системного подхода.

Математическая модель сегмента мобильной связи. Построим сегмент мобильной связи.

Конкретизируем постановку задачи. Каждый абонент «прикрепляется» к ближайшей башне (если их несколько, то к любой из них). Необходимо разместить N вышек так, чтобы после «прикрепления» абонентов к вышкам разница между максимальным и минимальным числом абонентов, «закрепленных» за вышками, была минимальной.

Введем обозначения:

$I = \{1, \dots, m\}$ — множество всех клиентов;

$J = \{1, \dots, n\}$ — множество мест размещения вышек.

Введем переменные:

$x_{ij} = \begin{cases} 1, & \text{если } i\text{-й абонент обслуживается вышкой в } j\text{-м месте размещения;} \\ 0, & \text{иначе.} \end{cases}$

$y_j = \begin{cases} 1, & \text{если в } j\text{-м месте размещена вышка;} \\ 0, & \text{иначе.} \end{cases}$

c_{ij} — расстояние от абонента до вышки;

u — максимальное число абонентов, обслуживаемых одной вышкой;

v — минимальное число абонентов, обслуживаемых одной вышкой.

Задача организации связи будет решаться при следующих ограничениях:

на использование только «активных» вышек

$$x_{ij} \leq y_j, \quad i \in \{1, 2, \dots, m\}, \quad j \in \{1, 2, \dots, n\};$$

на максимально возможное число вышек

$$\sum_{j=1}^n y_j = N;$$

на обслуживание одного абонента только одной вышкой

$$\sum_{j=1}^n x_{ij} = 1, \quad i \in \{1, 2, \dots, m\};$$

на максимальное число абонентов

$$\sum_{i=1}^m x_{ij} \leq u, \quad j \in \{1, 2, \dots, n\};$$

на минимальное число абонентов

$$v \leq \sum_{i=1}^m x_{ij} + m \cdot (1 - y_j), \quad j \in \{1, 2, \dots, n\};$$

на соединение абонента с ближайшей вышкой

$$\sum_{k=1}^n c_{ik} \cdot x_{ik} + (M_i - c_{ij}) \cdot y_j \leq M_i, \quad i \in \{1, 2, \dots, m\}, \quad j \in \{1, 2, \dots, n\},$$

$$M_i = \max_{j \in \{1, 2, \dots, n\}} c_{ij};$$

на значения переменных

$$x_{ij} \in \{0, 1\}, \quad y_j \in \{0, 1\}, \quad i \in \{1, 2, \dots, m\}, \quad j \in \{1, 2, \dots, n\},$$

$$u, v \in Z^+.$$

Оптимизационная задача по организации связи имеет вид:
Найти

$$C^* = \text{Arg} \min_{i,j} (u - v).$$

Имитационная модель. Рассмотрим пример. Пусть основное устройство опрашивает рабочую станцию каждые 1500 ед. времени по радиоканалу, ответ от которой поступает по выделенной проводной линии связи. Резерв сообщений от рабочей станции составляет 500 штук. Задержка запроса по радиоканалу составляет 10..20 ед. времени, задержка в проводной линии составляет 20..30 ед. времени. Ответы от рабочей станции записываются на жесткий диск в течение 30..40 ед. времени. При передаче сообщения по радиоканалу теряется до 30 % информации. Ответы от рабочей станции представляют интерес для злоумышленников, которые перехватывают до 30 % отчетов. Опишем работу системы с позиции временных сетей Петри.

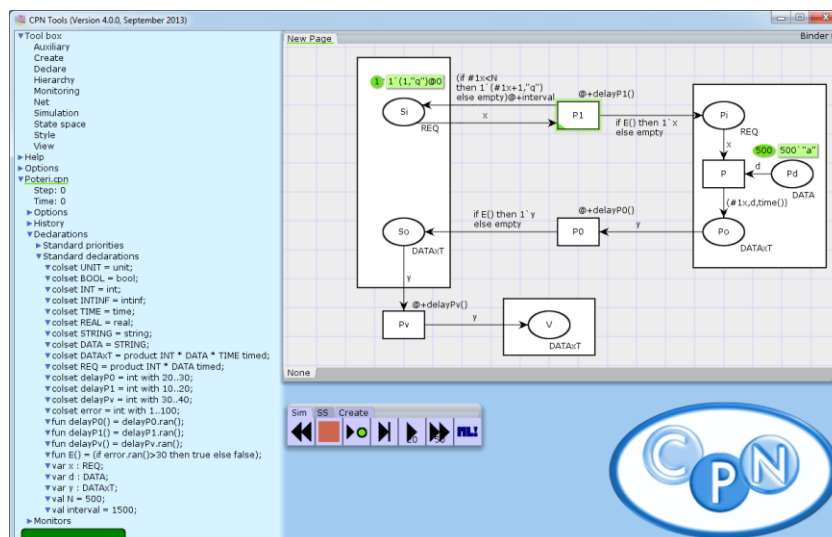
При описании изучаемого вопроса с позиций временных сетей Петри в пакете CPN Tools используются следующие множества и:

- colset REQ = product INT*DATA timed; — пакет, состоящий из данных запроса и порядкового номера, временное множество;
- colset DATA = STRING; — данные запроса;
- colset DATAxT = product INT*DATA*TIME timed; — пакет отчета, состоящий из порядкового номера, данных и временной метки, временное множество;
- colset delayP_i = int with 10..20;
- colset error = int with 10..20;
- fun delayP_i() = delayP_i().ran();
- fun E() = (if error.ran() > 30 then true else false); — функция, возвращающая вероятность события;

Также использованы условия переходов:

- (if #1x < N then 1`(#1x+1,"q") else empty)@+interval — новый запрос со смещением на interval при условии, что количество посланных запросов меньше N;
- if E() then 1`y else empty — данные передаются, в случае если пакет не перехвачен.

Вывод. Представленные математическая и имитационная модели позволяют рассматривать вопросы, связанные с обеспечением безопасности телекоммуникационной сети, регулировать вопросы предупреждения, раскрытия и расследования преступлений в указанной сфере. Используя данные модели как основу, можно получать различные варианты моделей под конкретную ситуацию, что говорит о гибкости и адекватности рассмотренных способов описания изучаемого вопроса.



ЛИТЕРАТУРА

1. Спиридонова Н. Е. Моделирование несанкционированного доступа к информационным системам органов внутренних дел с использованием методов теории автоматов // Актуальные вопросы эксплуатации систем охраны и защищенные телекоммуникационных систем. — 2018. — С. 218—219.
2. Меньших В. В., Спиридонова Н. Е. Оценки возможности несанкционированного доступа в информационную систему с помощью метода анализа иерархий // Техника и безопасность объектов уголовно-исполнительной системы. — 2018. — № 5-1 — С. 241—244.
3. Меньших В. В., Спиридонова Н. Е. Структурно-параметрическая модель несанкционированных действий нарушителя информационной безопасности // Некоторые вопросы анализа, алгебры, геометрии и математического образования. — 2018. — № 8 — С. 216—217.
4. Меньших В. В., Спиридонова Н. Е. Моделирование несанкционированного доступа к защищаемой информации с учетом возможностей нарушителей. // Вестник Воронежского института МВД России. — 2018. — №4. — С. 26—32.
5. Спиридонова Н. Е., Меньших В. В. Подходы к описанию динамики компьютерных преступлений // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-практической конференции. Под ред. Д.Н. Борисова. — 2019. — С. 1242—1246.

СВЕДЕНИЯ ОБ АВТОРАХ

Синегубова Светлана Владимировна. Доцент кафедры технических комплексов охраны и связи. Кандидат технических наук, доцент.

Воронежский институт ФСИН России.

E-mail: swp13@yandex.ru

Россия, 394072, г. Воронеж, ул. Иркутская, 1а. Тел. (473) 260-68-27.

Синегубов Сергей Владимирович. Доцент кафедры математики и моделирования систем. Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: sinusdvm@vimvd.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-11.

Sinegubova Svetlana Vladimirovna. Lecturer of the chair of technical systems of protection and communication. Candidate of Sciences (Radio Engineering), assistant professor. Voronezh Institute of the Russian Federal Penitentiary Service.
Work address: Russia, 394072, Voronezh, Irkutskaya str., 1a.
Tel. (473) 260-68-27.

Sinegubov Sergey Vladimirovich. Assistant professor of the chair of Mathematics and Systems Modelling. Candidate of Sciences (Radio Engineering), assistant professor. Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-52-11.

Ключевые слова: имитационная модель, телекоммуникационная система, сетевой трафик, защита информации.

Key words: simulation model, telecommunications system, network traffic, protection of information.

УДК 519.7

Сошнева Дарья Алексеевна,
кандидат технических наук;
Ахлюстин Сергей Борисович

**ОСОБЕННОСТИ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ ВОЙСК
НАЦИОНАЛЬНОЙ ГВАРДИИ С МИНИСТЕРСТВОМ ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ВЫПОЛНЕНИИ ЗАДАЧ
ПО ОХРАНЕ ОБЩЕСТВЕННОГО ПОРЯДКА И ОБЕСПЕЧЕНИЯ
ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ**

**PECULIARITIES OF ORGANIZING THE INTERACTION OF NATIONAL GUARD
TROOPS WITH THE MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN
FEDERATION IN THE PROTECTION OF PUBLIC ORDER AND PUBLIC
SECURITY TERMINATION**

В статье рассмотрены актуальные для практической деятельности вопросы организации взаимодействия Федеральной службы войск национальной гвардии Российской Федерации с органами внутренних дел МВД России при выполнении задач по охране общественного порядка и обеспечения общественной безопасности.

The article deals with the actual for practical activities of the organization of interaction of the Federal Service of the National Guard of the Russian Federation with the internal affairs bodies of the Ministry of Internal Affairs of Russia in carrying out tasks of protecting public order and ensuring public safety.

Взаимодействие войск национальной гвардии и МВД России представляет собой согласованную деятельность, в пределах полномочий каждого из органов, по проведению совместных мероприятий в ходе выполнения различных задач, в том числе по охране общественного порядка и общественной безопасности.

Общественный порядок обеспечивается при непосредственном взаимодействии войск национальной гвардии с МВД России. Результатом такого взаимодействия является решение следующих задач:

- охрана общественного порядка в общественных местах;
- охрана общественного порядка и обеспечение безопасности лиц, находящихся на транспортных магистралях, поездах дальнего следования и пригородного сообщения, самолетах, а также обеспечение безопасности речных портов и акваторий водных объектов;
- охрана общественного порядка и обеспечение общественной безопасности при проведении митингов, шествий, собраний, демонстраций, а также различных культурных, спортивно-массовых и иных мероприятий;
- обеспечение общественной безопасности в период подготовки и проведения международных спортивных и иных официальных мероприятий;
- проведение комплексных оперативно-профилактических операций, оперативно-профилактических мероприятий и специальных мероприятий;
- личная охрана лиц, в отношении которых избрана мера безопасности «личная охрана, охрана жилища и имущества»;
- обеспечение повышенных мер безопасности при конвоировании и содержании подозреваемых и обвиняемых в совершении преступлений, совершенных организованной группой, преступным сообществом, террористической или иной экстремистской организацией, действия которых могут иметь большой общественный и политический резонанс, а также предупреждения массовых беспорядков, покушений на свидетелей, а также побегов в местах их содержания, при проведении судебного заседания и иных процессуальных действий;
- обследование различных объектов объектов, а также мест массового пребывания людей, на предмет выявления и обезвреживания взрывных устройств. Применение специальных взрывчатых веществ, необходимых при проведении специальных мероприятий, а также обнаружение, изъятие, обезвреживание, транспортировка и уничтожение взрывных веществ, устройств и средств взрывания. Обеспечение безопасности граждан при проведении указанных мероприятий.
- выполнение задач при возникновении чрезвычайных обстоятельств.

Взаимодействие войск национальной гвардии с МВД России, его территориальными органами при выполнении задач по охране общественного порядка и обеспечения общественной безопасности в общественных местах осуществляется путем патрулирования населенных пунктов и общественных мест, выставления постов и заслонов, использования иных форм охраны общественного порядка, также усиления нарядов полиции, выполняющих задачи по охране общественного порядка и обеспечению общественной безопасности общественных мест, транспортных магистралей, речных портов, акваторий водных объектов.

Из состава войск национальной гвардии к участию в охране общественного порядка и обеспечения общественной безопасности в общественных местах в пределах их полномочий выделяются:

1. Патрульные подразделения территориальных органов Росгвардии, воинских частей войск национальной гвардии, в районах дислокации – решением начальника территориального органа Росгвардии, командира воинской части войск национальной гвардии согласно плану единой дислокации и (или) обращениям руководителей территориальных органов МВД России, направленным в соответствии с их полномочиями, с учетом следующих особенностей:

- личный состав войск национальной гвардии для патрулирования населенных пунктов и общественных мест привлекается не более 4 дней в неделю. Служебная

нагрузка военнослужащих (сотрудников) патрульных подразделений с учетом подготовки к несению службы, выдвижения и прибытия в места выполнения задач, непосредственного несения службы на маршруте патрулирования (посту) и возвращения в пункт дислокации не должна превышать 7 часов в сутки;

- численность личного состава, задействованного для патрулирования на улицах и в иных общественных местах, не должна превышать 70 процентов от численности личного состава патрульного подразделения, в том числе 10 процентов для содержания резерва в пункте дислокации.

2. Подразделения оперативного назначения воинских частей войск национальной гвардии, подразделения Центра специального назначения сил оперативного реагирования и авиации Федеральной службы войск национальной гвардии Российской Федерации, подразделения ОМОН войск национальной гвардии в районах дислокации – решением командиров войск национальной гвардии, начальников территориальных органов Росгвардии на основании обращения руководителей территориальных органов МВД России, направленных в соответствии с их полномочиями;

3. Морские подразделения территориальных органов Росгвардии, воинских частей (подразделений) войск национальной гвардии в районах дислокации – решением начальника территориального органа Росгвардии (командира воинской части войск национальной гвардии) согласно плану единой дислокации и обращением руководителей территориальных органов МВД России, направленным в соответствии с их полномочиями;

4. Личный состав военных образовательных организаций высшего образования войск национальной гвардии для выполнения задач по охране общественного порядка и обеспечения общественной безопасности в районах дислокации – решением главкомандующего войсками национальной гвардии.

Организационной основой совместных действий МВД России, его территориальных органов и войск национальной гвардии при выполнении задач по охране общественного порядка и обеспечения общественной безопасности на улицах и иных общественных местах является план единой дислокации.

Проанализировав вышеизложенное, можно сделать вывод о том, что взаимодействие войск национальной гвардии и МВД России по обеспечению общественной безопасности и общественного порядка представляет собой взаимовыгодное сотрудничество, которое должно быть обязательно согласовано по целям, месту, времени, методам. Такое сотрудничество, проводимое каждым органом в пределах своих полномочий, позволяет решить поставленные задачи на более высоком уровне

ЛИТЕРАТУРА

1. О полиции [Электронный ресурс] : федер. закон от 7 февраля 2011 г. № 3-ФЗ. - URL : <http://base.consultant.ru/>.

2. О войсках национальной гвардии Российской Федерации : федеральный закон от 3 июля 2016 г. № 226-ФЗ [Электронный ресурс]. – СПС «Консультант плюс». – URL : [http // www.base.consultant. ru](http://www.base.consultant.ru).

3. Федеральный закон Российской Федерации от 23 июля 2013 г. № 208-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам антитеррористической защищенности объектов».

4. Приказ Росгвардии от 21.09.2018 № 420 «Об утверждении Наставления по организации службы строевых подразделений вневедомственной охраны войск национальной гвардии Российской Федерации».

5. Постановление Правительства Российской Федерации от 7 октября 2017 года № 1235 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации».

6. Постановление Правительства РФ от 19 января 2005 г. № 30 «О типовом регламенте взаимодействия федеральных органов исполнительной власти». // СЗ РФ. 2005. №4. Ст. 305.

7. Сошнева Д.А., Меркулова Н.И. Разработка комплексной системы безопасности объекта, подлежащего обязательной охране войсками национальной гвардии РФ / Д.А. Сошнева, Н.И. Меркулова // Сборник научных статей 7-й международной научно-практической конференции. – 2017. С. 362-367.

СВЕДЕНИЯ ОБ АВТОРАХ

Сошнева Дарья Алексеевна. Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Кандидат технических наук.

Воронежский институт МВД России.

E-mail: dasha48rus@mail.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-07.

Ахлюстин Сергей Борисович. Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: cerg7676@yandex.ru

Россия, 394065, г. Воронеж, пр. Патриотов, 53. Тел. (473) 200-52-04.

Soshneva Daria Alekseevna. Senior lecturer of the Department of radio engineering systems and security monitoring systems. Candidate of Engineering Sciences

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-04.

Akhlyustin Sergey Borisovich. Senior lecturer of the chair of electronic systems and complexes of security monitoring.

Voronezh Institute of the Ministry of the Interior of Russia.

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-04.

Ключевые слова: Министерство внутренних дел Российской Федерации, Федеральная служба войск национальной гвардии, охрана общественного порядка, обеспечение общественной безопасности.

Key words: Ministry of Internal Affairs of the Russian Federation, Federal Service of the National Guard, public safety, public safety.

УДК 351.74

АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К КОЛИЧЕСТВЕННОЙ ОЦЕНКЕ ИНТЕРОПЕРАбельНОСТИ СИСТЕМ

ANALYSIS OF EXISTING APPROACHES TO QUANTITATIVE ASSESSMENT OF SYSTEM INTEROPERABILITY

В статье рассматриваются различные подходы к оценке интероперабельности систем, проводится сравнительный анализ существующих моделей оценки.

The article discusses various approaches to assessing the interoperability of systems, a comparative analysis of existing assessment models.

В современных условиях количество разнообразных инфокоммуникационных технологий неуклонно возрастает. Вместе с тем особую популярность приобретают и системы, имеющие в своей структуре гетерогенные компоненты [1]. В связи с этим одним из ключевых вопросов при разработке таких систем является обеспечение интероперабельности. Под интероперабельностью понимается способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена [2].

В общем случае модель интероперабельности можно представить как совокупность различных уровней совместимости систем или их компонентов (рис.1). На техническом уровне совместимость устройств рассматривается с точки зрения стандартизации протоколов связи. Семантический уровень подразумевает возможность систем или компонентов обмена данными в общем формате. Организационный уровень включает в себя аспекты взаимодействия на уровне администрирования.



Рис.1. Модель интероперабельности

На сегодняшний день не существует универсального метода, позволяющего дать количественную оценку интероперабельности любых систем. Данной проблеме посвящено большое количество зарубежных и отечественных исследований [3,4,5].

Так, работа Батоврина В.К., Королева А.С. [6] посвящена разработке способа количественной оценки интероперабельности на основе нечеткой логики. Авторы предлагают находить численные значения показателей, присущих каждому уровню интероперабельности, с помощью экспертного оценивания. Петров А.Б., Стариковская Н.А. в своей работе [7] используют метод интервальной и экспертной взвешенной оценки, при этом рассматривая интероперабельность через совокупность свойств, присущих той или иной системе в зависимости от ее архитектуры.

Однако для расчета количественной оценки интероперабельности недостаточно рассмотрения конкретных характеристик и свойств системы, необходимо также учитывать возможные барьеры при обеспечении интероперабельности. Согласно определению, данному в ГОСТ Р 55062-2012 под барьером понимается несовместимость сущностей, которая препятствует обмену информацией с другими сущностями, использованию сервисов или общему пониманию обмененных элементов. В ГОСТ Р ИСО 11354-1-2012 [8] определяются следующие категории барьеров на пути реализации интероперабельности системы:

- концептуальные (включают в себя семантические, синтаксические и семиотические несовместимости компонентов системы);
- технологические (несовместимости технических средств взаимодействия между компонентами системы);
- организационные (несовместимости на уровне организационных структур, связанные с методами управления).

Таким образом, обеспечение интероперабельности сегодня является одной из ключевых проблем при проектировании систем, так как с появлением новых технологий степень гетерогенности таких систем постоянно увеличивается. Необходима разработка универсального метода количественной оценки интероперабельности, с помощью которого будет возможно реорганизовать имеющуюся систему с целью повышения ее эффективности.

ЛИТЕРАТУРА

1. Меньших В.В., Спиридонова Н.Е. Структурно-параметрическое моделирование гетерогенных систем в интересах обеспечения их безопасности // Труды XXI Международной конференции «Проблемы управления и моделирования в сложных системах», САМГТУ – Самара, 2019. С. 289-292.
2. Национальный стандарт Российской Федерации ГОСТ Р 55062-2012 «Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения.» – М.: Стандартинформ, 2018.
3. Бойченко А., Корнеев Д.Г., Лукинова О.В. Интероперабельность информационных систем на основе стека eif и модели ose/rm // Материалы международной научно-практической конференции (ТАС-2014), ИПУ РАН – Москва, 2014. С. 230-233.
4. Райкин Л.И., Субботина М.Н. Об интероперабельности информационных технологий создания, эксплуатации и управления промышленными объектами // Труды XVIII Международной молодежной конференции «Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта», ИПУ РАН – Москва, 2018. С. 354-358.
5. Аникин Д.В. Критерии оценки применения интероперабельности, заданные условиями принятия решения // Вестник МГСУ. –2013. – №10. – С. 249-257.
6. Батоврин В.К., Королев А.С. Способ количественной оценки интероперабельности // Информационные технологии и вычислительные системы. –2009. –№5. – С. 91-96.
7. Петров А.Б., Стариковская Н.А. Методика сравнительной оценки интероперабельности информационных систем // Информационные технологии и вычислительные системы. –2009. – №5. – С. 82-90.
8. Национальный стандарт Российской Федерации ГОСТ Р ИСО 11354-1-2012 «Усовершенствованные автоматизированные технологии и их применение. Требования к установлению интероперабельности процессов промышленных предприятий. Часть 1. Основа интероперабельности предприятий.» – М.: Стандартинформ, 2014.

СВЕДЕНИЯ ОБ АВТОРЕ

Спиридонова Наталья Евгеньевна. Адъюнкт.
Воронежский институт МВД России.
E-mail: spiridonova_n@icloud.com
Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-52-14.

Spiridonova Natalia Evgenevna.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: spiridonova_n@icloud.com
Russia, 394065, Voronezh, Prospect Patriotov, 53. Tel. (473) 200-52-14.

Ключевые слова: информационная система, интероперабельность, методика количественной оценки, модель интероперабельности.

Key words: information system, interoperability, quantification method, model of interoperability.

УДК 519.87

Таравков Михаил Владимирович

ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

QUESTIONS OF LEGAL REGULATION OF APPLICATION OF VIDEO SURVEILLANCE SYSTEMS

В статье рассмотрены назначение и задачи систем охранного телевидения как инструмента информационного обеспечения и повышения эффективности оперативной деятельности правоохранительных органов. Изложены положения некоторых нормативных правовых актов, регламентирующих применение систем охранного телевидения в различных целях.

The article discusses the purpose and tasks of security television systems as a tool for information support and improving the efficiency of the operational activities of law enforcement agencies. The provisions of some regulatory legal acts regulating the use of security television systems for various purposes are stated.

Государство как форма политической организации общества на определенной территории предназначено для обеспечения нормального функционирования и развития населения. Данная цель достигается посредством решения ряда задач, среди которых содействие социальному, культурному, экономическому и технологическому развитию общества, обеспечения его безопасности, защита жизни и здоровья, прав и свобод человека от преступных посягательств. Среди перечисленных задач следует отметить обеспечение безопасности как состояния защищенности личности, общества и государства в целом от внутренних и внешних угроз естественного и искусственного характера. К естественным угрозам относятся различные природные явления: пожары, наводнения, ураганы, удары молний и другие стихийные бедствия. К искусственным

относят угрозы криминального, террористического и технологического характера. Здесь следует отметить первые две как наиболее часто проявляющиеся и оказывающие сильное влияние на население. Очевидно, что нормальное развитие и процветание населения возможно только при отсутствии подобного рода угроз.

С целью реализации государственной функции по защите жизни и здоровья, прав и свобод человека, обеспечения общественной безопасности и правопорядка созданы и функционируют правоохранительные органы. Для эффективного решения возложенных на них задач используются современные достижения науки и техники. Технические средства обеспечения безопасности объединяются в системы безопасности, которые могут быть комплексными и интегрированными. В состав таких систем входят подсистемы охранно-тревожной и пожарной сигнализации, контроля и управления доступом, охранного телевидения (СОТ), оповещения и управления эвакуацией, управления аппаратурой жизнеобеспечения (вентиляция, отопление, кондиционирование, водоснабжение и т.д.) и ряд других. Среди перечисленных подсистем следует выделить подсистему СОТ, являющуюся мощным инструментом информационного обеспечения оперативной работы правоохранительных органов.

Правоохранительные органы и частный сектор активно используют СОТ для различных условиях и для различных целей. Такие системы используются в местах массового пребывания людей (парки, скверы, площади, набережные и т.п.), на объектах транспортной инфраструктуры (авто- и железнодорожные вокзалы, речные и морские порты), объектах здравоохранения (больницы, поликлиники, госпитали), объектах образования (детские сады, школы, институты и т.д.), объектах жилого сектора (многоквартирные и частные дома, коттеджные поселки), объектах культуры (театры, кинотеатры, концертные залы и т.д.), производственных объектах (заводы, фабрики, склады) для охраны периметров и самих объектов, контроля посетителей и персонала, наблюдения за производственными процессами. Одним словом, перечень объектов достаточно обширен и для каждого из них система разрабатывается с учетом особенностей его функционирования.

В литературе, посвященной СОТ можно встретить такие термины как «система видеоконтроля», «система видеонаблюдения», «система телевизионного наблюдения» и им подобные. На первый взгляд может показаться, что эти понятия родственные и имеют одно и то же толкование. Однако в нормативно-технических документах этим понятиям даны разные определения [1]. Согласно данному документу система видеонаблюдения представляет собой совокупность видеоканалов, программных и технических средств записи и хранения видеоданных и управления. То есть таковой система будет называться тогда, когда в ней будут присутствовать все перечисленные компоненты. По сути, данное определение является общим и не затрагивает цели использования системы. Поэтому системой видеонаблюдения можно назвать любую систему для получения на расстоянии изображений объектов, например, видеоняню. Тот же документ содержит и определение СОТ. Ей является телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях противокриминальной и антитеррористической защиты. Сходство данных определений в том, что обе системы предназначены для получения изображений объектов. Первое отличие заключается в замкнутости второй системы и использовании ее именно для защиты объектов от криминальных и террористических угроз. Замкнутость означает, что данная система не предназначена для широкой аудитории в отличие от систем вещательного телевидения и защищена от утечки видеоизображений во внешнюю среду. Второе отличие заключается в назначении системы – она используется для оперативного реагирования на угрозы конкретного вида.

Несмотря на отличия в определениях, обе системы могут с успехом применяться в обоих случаях, так как физические принципы их функционирования одинаковые. Система видеонаблюдения при решении задач охраны автоматически превращается в СОТ.

К СОТ, как и к любой технической системе предъявляются определенные требования и накладываются ограничения. На первый взгляд может показаться, что применение СОТ ничем не ограничено, так как она физически не контактирует с объектом наблюдения и не влияет на него. Однако существует ряд запретов и ограничений, продиктованных различными нормативными документами. Рассмотрим их более подробно.

Попадание СОТ под действие того или иного нормативного документа зависит от места, цели использования, функциональных характеристик и возможностей системы, качества изображения, возможности хранения и доступа к видеозаписям, необходимости регулярного контроля ее работы. СОТ может применяться в общественных местах, на объектах частной собственности, в местах индивидуального пользования. Общественным местом является любое место возможного появления в любой момент посторонних лиц. К таким местам относятся парки, скверы, улицы, кафе рестораны и т.д. По цели использования системы могут применяться в административной, уголовно-процессуальной, оперативно-розыскной и частной деятельности, например, наблюдения за подчиненными с целью повышения трудовой дисциплины (приход и уход с работы, поведение на рабочем месте). К функциональным возможностям, определяющим применение СОТ, можно отнести возможность обнаружения, различения и идентификации объекта (лица на фоне толпы, государственного регистрационного номера транспортного средства в потоке и т.д.). Качество изображения может в некоторых случаях оказаться ключевым критерием применения видеоизображения в судебном процессе. Могут предъявляться требования к периоду хранения видеозаписей и разграничению к ним доступа. В некоторых случаях нормативные документы предписывают регулярные проверки работоспособности СОТ [2].

Основным нормативным документом, затрагивающим применение СОТ является Конституция РФ. В ч.1 ст. 23 сказано, что каждый гражданин обладает правом на неприкосновенность частной жизни. Ст. 24 запрещает проведение каких-либо операций (сбор, хранение, использование и распространение) с информацией о частной жизни лица без его согласия. Существуют и исключения из этого правила. При проведении следственных действий, дознания, оперативно-розыскной деятельности не требуется согласия лица [3].

Ст. 81, 84 Уголовно-процессуального кодекса относят видеозаписи к вещественным доказательствам, которые могут быть использованы при расследовании уголовного дела [4].

Ст. 55 ч. 2 Гражданского процессуального кодекса также определяет возможность использования видеозаписей в качестве доказательной базы в судебном разбирательстве. Известны случаи подачи гражданских исков к гостиницам, торговым центрам. Напротив, в свою очередь они также могут быть инициаторами судебного разбирательства, например, при причинении вреда имуществу [5].

Ст. 26.7 ч. 2 Кодекса об административных правонарушениях РФ также предусматривает возможность использования видеозаписей в качестве доказательств. Следовательно, видеозаписи могут быть использованы в административном производстве по делам о мелком хулиганстве, порче имущества на незначительную сумму и т. п. [6].

Не исключает использования видеоизображений в качестве доказательств и Ст. 64 ч. 2 Арбитражного процессуального кодекса [7].

В соответствии со ст. 21 Трудового кодекса РФ работник имеет право на полную информацию об условиях и охране труда на рабочем месте. По мнению суда, негласно полученная видеозапись не может являться основанием для наложения дисциплинар-

ной ответственности на работника в виде увольнения (ст. 192, 193 ТК РФ) в тех случаях, когда работодатель не предоставил иных доказательств совершения дисциплинарного проступка [8].

Закон «О персональных данных» в ч. 1 статьи 22 обязывает операторов, осуществляющих обработку персональных данных граждан, полученных посредством СОР, уведомлять уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении производить обработку за исключением некоторых случаев, например, обработки персональных данных в рамках трудового договора [9].

Таким образом, применение систем видеонаблюдения на различных объектах в зависимости от конкретных условий может подпадать под действие сразу нескольких нормативных документов. Неукоснительное их соблюдение является гарантом дальнейшего правомерного использования видеоматериалов.

ЛИТЕРАТУРА

1. ГОСТ Р 52551-2016. Системы охраны и безопасности. Термины и определения. – Введ. 2017-07-01. – Москва : Стандартинформ, 2016. – 58 с.

2. Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса: пост. Правительства РФ от 5 мая 2012 г. № 458.

3. Конституция Российской Федерации : принята всенар. голосованием 12.12.1993 г. / Российская Федерация. Конституция (1993). – Москва : Юридическая литература, 2009. – 65 с.

4. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (с изм. и доп.) // Консультант Плюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_34481 (дата обращения: 25.06.2019).

5. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (с изм. и доп.) // Консультант Плюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_39570 (дата обращения: 25.06.2019).

6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. и доп.) // Консультант Плюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_34661 (дата обращения: 25.06.2019).

7. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ (с изм. и доп.) // Консультант Плюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_37800/ (дата обращения: 25.06.2019).

8. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (с изм. и доп.) // Консультант Плюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 25.06.2019).

9. О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.06.2019).

СВЕДЕНИЯ ОБ АВТОРЕ

Таравков Михаил Владимирович. Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга. Воронежский институт МВД России.

E-mail: berloga_@rambler.ru

Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Тел. (473) 200-52-81.

Taravkov Mikhail Vladimirovich. Lecturer of the department of radio engineering systems and complexes of security monitoring.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: berloga_@rambler.ru

Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Tel. (473) 200-52-81.

Ключевые слова: безопасность, угроза безопасности, система видеонаблюдения, система охранного телевидения, видеоизображение.

Key words: security, security threat, video surveillance system, CCTV, video image.

УДК 621.397

**Толстых Андрей Андреевич;
Ступников Дмитрий Сергеевич,**
кандидат технических наук

ОБУЧЕНИЕ С ПОДКРЕПЛЕНИЕМ В ЗАДАЧАХ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

REINFORCEMENT LEARNING IN THE PROBLEMS OF CONTROL OF ROBOT- ENGINEERING SYSTEMS

В работе проведен анализ подходов к решению задач машинного обучения с подкреплением. Даны рекомендации по применению методов обучения с подкреплением для управления робототехнических систем.

The paper analyzes the approaches to solving machine learning problems with reinforcement. Recommendations on the use of reinforced learning methods for the control of robotic systems are given.

Робототехнические системы все более широко используются как в повседневной жизни, так и в различных сферах профессиональной деятельности человека. Спектр различных робототехнических систем достаточно разнообразен: от простейшего контроллера положения гражданского беспилотного летательного аппарата (БПЛА) в полете до сложнейших систем прецизионной обработки микросхем. Подобное разнообразие предполагает разработку алгоритмов действия робототехнических систем для каждого конкретного случая их применения. Однако, в настоящее время, появляется иная концепция разработки алгоритмов – обучение действия робототехнических систем на синтетических примерах. Целью данной работы является рассмотрение современных подходов к обучению с подкреплением.

Рассмотрим математическую постановку задачи обучения с подкреплением. В литературе [1] используются термины «агент» и «среда» – для обозначения робототехнической системы и внешних факторов соответственно. Вся концепция подхода строится на утверждении, что существует функция стоимости [2], зависящая от предыдущих действий агента и состояния среды, которая может быть рассчитана в каждый момент времени и ее максимизация влечет за собой выполнение поставленной перед робототехнической системой задачи. На рис. 1 приведена схема процесса обучения с подкреплением.

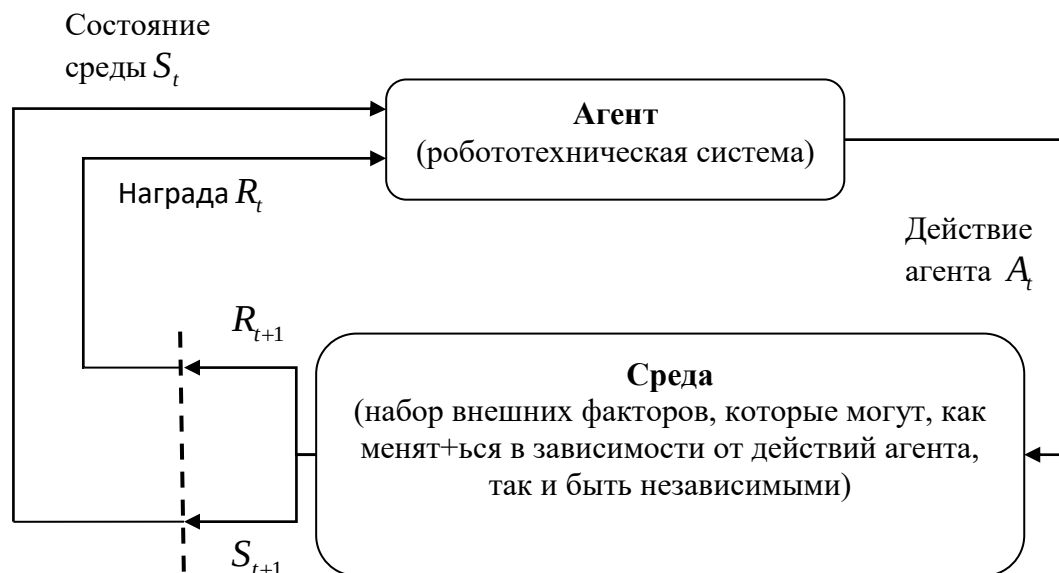


Рис. 1. Схема обучения с подкреплением

Технически наиболее сложным является математическое описание функции стоимости, в то время как задача её оптимизации может быть решена с помощью численных методов оптимизации. Рассмотрим подробнее механизм определения функции стоимости. Введем к уже используемым обозначениям переменную V_t , определяющую взвешенную сумму ранее полученных наград к шагу t [1]:. Она определяется как

$$V_t = \sum_{i=0}^t \gamma^i R(S_t), \quad (1)$$

где γ – коэффициент, обеспечивающий снижение значения последних действий. Подобная формулировка необходима для увеличения количества действий, приводящих к положительному результату. Выражение (1) справедливо для случая, когда действия последовательны, то есть у агента нет выбора. Для случая выбора из K действий на каждом шаге:

$$V_t|_{S_1} = \sum_{k=2}^K P(s_k|s_1) (R_k + \gamma V|_{S_k}), \quad (2)$$

где $V_t|_S$ – ранее полученные награды к шагу t , при текущем состоянии среды S ; $P(s_k|s_1)$ – вероятность перехода среды в состояние S_k , при выборе действия k . Заключительным изменением данной формулировки является введение «политики» [3]. Под политикой (π) понимается стратегия принятия решения выбора конкретного действия в текущем состоянии среды:

$$V_{\pi}|_S = \sum_a \pi(a|s) \sum_{s' \in S} \sum_{r \in R} p(s', r|s, a) (r + \gamma V_{\pi}|_{s'}), \quad (3)$$

где a – все доступные для агента действия; π – текущая политика.

Одним из наиболее перспективных подходов к оптимизации функции стоимости является глубокое обучение с использованием искусственных нейронных сетей [1]. Его широкое применение обусловлено возможностью генерации множества примеров для обучения алгоритма.

В ходе исследования был проведен эксперимент с обучением упрощенной динамической системы двух мерная модель роботизированной руки с двумя сочленениями. На рис. 2 приведена геометрия эксперимента.

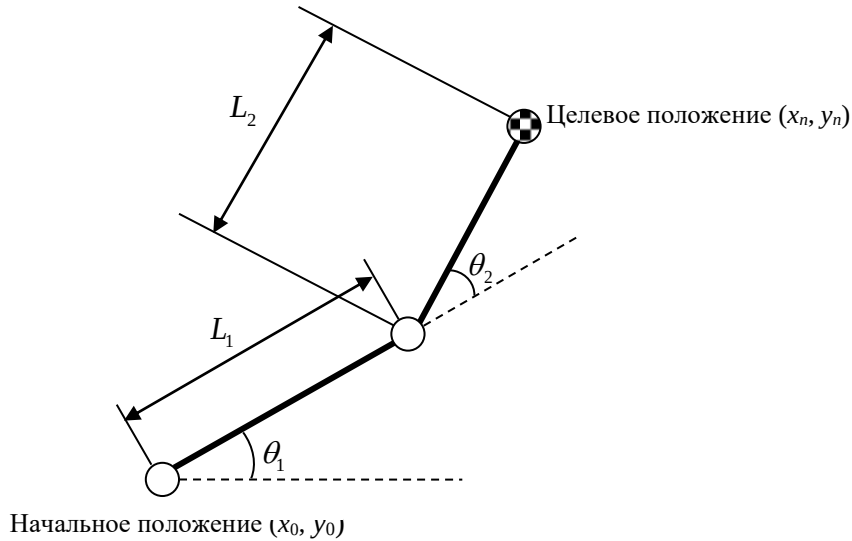


Рис. 2. Геометрия среды и действий агента

Приведенная задача является задачей обратной кинематики. Для данного простейшего примера существует аналитический способ решения, однако сложность задач данного класса экспоненциально растет при введении новых параметров (дополнительного измерения, увеличения числа сочленений и т.д.). Цель данной робототехнической системы является помещение края плеча L_2 в точку целевого положения. Перемещение плеч происходит путем вращения сочленений.

В работе реализован алгоритм глубокого обучения с подкреплением. Робототехническая система достигла стабильного выполнения задачи, в среднем, за 120 эпох. Следует отметить, что в некоторых случаях система может действовать не единственным способом. Данное поведение продемонстрировано на рис. 3.

Моделирование производилось в поле со стороной 400 пикселей. Для более простой технической реализации функция стоимости определялась как модуль разности между положением края плеча L_2 и целевой точки умноженный на -1. Вследствие этого функция стоимости везде была отрицательная за исключением точного совпадения координат.

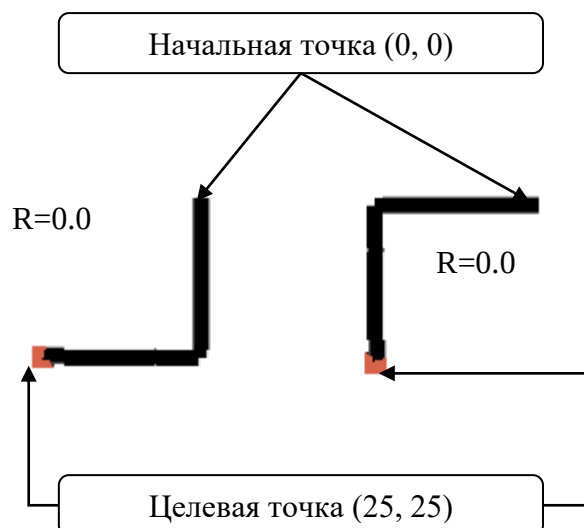


Рис. 3. Два варианта решения с одинаковой функцией стоимости

Таким образом, можно сделать вывод о применимости рассмотренного подхода к управлению роботизированными системами. Следует отметить, что преимуществами данного подхода являются: универсальность, алгоритмическая простота и менее быстрое возрастание вычислительной сложности с ростом параметров по сравнению с классическими аналитическими подходами. В последующих работах предполагается проведение исследований эффективности данных систем управления базе реальных робототехнических систем.

ЛИТЕРАТУРА

1. Обучение с подкреплением / Р.С. Саттон, Э.Г. Барто – М.:Бином. Лаборатория знаний, 2017. – 399 с.
2. Dueling Network Architectures for Deep Reinforcement Learning / Z. Wang, T. Schaul, M. Hessel, N. van Hasselt, M. Lanctot, N. de Freitas // CoRR. – abs/1511.06581. – 2016. – С. 1–15.
3. Policy Gradient Methods for Reinforcement Learning with Function Approximation / R.S. Sutton, D.A. McAllester, S.P. Singh, M. Yishay // Advances in Neural Information Processing Systems 12. – 2000. – 1057–1063.

СВЕДЕНИЯ ОБ АВТОРАХ

Толстых Андрей Андреевич. Преподаватель кафедры тактико-специальной подготовки.

Воронежский институт МВД России.

E-mail: tolstykh.aa@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53. Тел. (473) 200-56-47.

Ступников Дмитрий Сергеевич. Преподаватель кафедры механизации лесного хозяйства и проектирования машин. Кандидат технических наук.

Воронежский государственный лесотехнический университет.

E-mail: Neiti1992@mail.ru

Россия, 394087, г. Воронеж, ул. Тимирязева, 8. Тел (473) 253-78-47.

Tolstykh Andrey Andreevich. Lecturer of the department of special tactics.
Voronezh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-56-47.

Stupnikov Dmitriy Sergeevich Lecturer of the department of. Lecturer at the Department
of Forestry Mechanization and Machine Design. Candidate of Technical Sciences.
Voronezh State Forestry University.
Work address: Russia, 394006, Voronezh, Timiryazeva Str., 8.
Tel. (473) 253-78-47.

Ключевые слова: обучение с подкреплением, искусственные нейронные сети, оптимизация.

Key words: reinforcement learning, artificial neural networks, optimization.

УДК 004.94

Коллектив авторов

**Общественная безопасность, законность
и правопорядок в III тысячелетии**

Сборник статей

Выпуск 5

Часть 2

В авторской редакции

Оригинал-макет Г.И. Чибисова, Е.А. Швецов

Подписано в печать 14.11.2019. Формат 60х84 1/16

Усл. печ. л. 20,09.

Гарнитура Таймс Новая. Печать офсетная. Бумага типографская

Тираж 80 экз. Заказ № 193.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53

