

ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

**НАУЧНЫЙ БЮЛЛЕТЕНЬ
ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ**

*Сборник материалов
научно-представительских мероприятий*

Выпуск 4

**Воронеж
2024**

Редакционная коллегия:

Председатель: С. В. Родин, кандидат технических наук, доцент;

Заместитель председателя: Р. В. Бузин, кандидат экономических наук;

Ответственный секретарь: Н. В. Крючкова.

Члены редакционной коллегии:

Н. В. Гвоздева, кандидат филологических наук;

С. Б. Ахлюстин, кандидат технических наук;

А. И. Ляпин, кандидат педагогических наук, доцент;

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

Т. В. Мещерякова, доктор технических наук, доцент;

М. М. Жуков, кандидат технических наук, доцент;

С. В. Железный, кандидат технических наук, доцент;

С. А. Гречаный, кандидат технических наук, доцент;

А. В. Пучнин, кандидат юридических наук, доцент;

И. В. Сычев, кандидат физико-математических наук, доцент;

Е. А. Буданова, кандидат юридических наук, доцент;

О. В. Пьянков, доктор технических наук, профессор;

О. С. Авсентьев, доктор технических наук, доцент;

К. К. Панько, доктор юридических наук, доцент;

И. А. Сабирова, доктор педагогических наук, доцент;

П. П. Фомин, кандидат юридических наук, доцент;

Д. А. Шашков.

Научный бюллетень Воронежского института МВД России : сборник материалов научно-представительских мероприятий. Вып. 4. [Электронный ресурс]. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2024. – 2 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

ISBN 978-5-00229-160-1

Сборник содержит материалы Международного семинара «Правовое обеспечение противодействия правонарушениям несовершеннолетних» (26 марта 2024 года), Всероссийского семинара «Проблемы формирования доказательств по уголовным делам в сфере информационных технологий» (27 июня 2024 года), Всероссийского круглого стола «Проблемы адаптации сотрудников подразделений по делам несовершеннолетних на первоначальном этапе профессиональной деятельности и пути их решения» (23 октября 2024 года), Всероссийских семинаров: «Актуальные проблемы обеспечения информационной безопасности в деятельности органов внутренних дел» (24 октября 2024 года), «Организационно-техническое обеспечение безопасности охраняемых территорий и объектов органов внутренних дел» (30 октября 2024 года), «Уголовно-правовые и криминологические аспекты противодействия преступности среди несовершеннолетних» (30 октября 2024 года), «Использование перспективных технологий в создании технических устройств и подготовке специалистов для органов внутренних дел» (31 октября 2024 года), «Математическое моделирование информационных систем органов внутренних дел» (25 ноября 2024 года).

Издание представляет интерес для профессорско-преподавательского состава, адъюнктов, курсантов и слушателей образовательных организаций МВД России и сотрудников правоохранительных органов.

© Воронежский институт МВД России, 2024

СОДЕРЖАНИЕ

МЕЖДУНАРОДНЫЙ СЕМИНАР

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ ПРАВОНАРУШЕНИЯМ НЕСОВЕРШЕННОЛЕТНИХ

М. А. Горностаева

Особенности применения меры воспитательного воздействия в виде ограничения досуга в отношении несовершеннолетних, освобожденных от административной ответственности 9

А. А. Деминская

Исследование причин совершения правонарушений несовершеннолетними 15

С. В. Кончатова

Сравнительно-правовой анализ привлечения к административной ответственности несовершеннолетних в Республике Беларусь и в Российской Федерации 19

ВСЕРОССИЙСКИЙ СЕМИНАР

ПРОБЛЕМЫ ФОРМИРОВАНИЯ ДОКАЗАТЕЛЬСТВ ПО УГОЛОВНЫМ ДЕЛАМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В. В. Батоев

О некоторых вопросах информационного обеспечения оперативно-розыскной деятельности по делам экстремистской направленности 25

А. И. Гайдин, А. Л. Стефанский

Проблемы и пути их решения при получении информации о соединении абонентов и абонентских устройств в России и Республике Беларусь 30

А. В. Головчанский

Sim-боксы как средство реализации современных схем дистанционных мошенничеств 36

О. О. Гуменчук

К вопросу об использовании специальных знаний при расследовании преступлений в сфере информационных технологий . 44

И. С. Звягин

Особенности идентификации лиц по биометрическим параметрам в ходе расследования преступлений 49

С. С. Паутов

Характеристика личности преступника и потерпевшего в рамках дистанционного мошенничества, совершаемого с использованием Интернет-сервисов размещения объявлений 54

Е. А. Пидусов	
Цифровые следы в расследовании телефонного мошенничества ...	58
Е. И. Пырьева, А. Е. Беляева	
Механизм следообразования при совершении мошенничества с использованием мобильных средств сотовой связи	63

ВСЕРОССИЙСКИЙ КРУГЛЫЙ СТОЛ

ПРОБЛЕМЫ АДАПТАЦИИ СОТРУДНИКОВ ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И ПУТИ ИХ РЕШЕНИЯ

А. И. Алимова	
Некоторые вопросы взаимодействия органов профилактики с сотрудниками подразделений по делам несовершеннолетних	68
А. С. Короткова	
Сущность и особенности профессиональной позиции курсантов образовательных организаций МВД России на современных этапах	73
Н. В. Полякова	
Актуальные вопросы реализации приоритетного профиля подготовки «Деятельность подразделений по делам несовершеннолетних»	77
Т. Н. Семенихина	
О некоторых особенностях социально-психологической и профессиональной адаптации инспекторов по делам несовершеннолетних на первоначальном этапе служебной деятельности	81
А. С. Ситникова	
Профессионально-правовая культура сотрудников подразделений по делам несовершеннолетних	86
И. Н. Соломатина	
О формировании административно-организационной компетентности у сотрудников подразделений по делам несовершеннолетних в органах внутренних дел	90
Н. А. Швецова	
Особенности социально-психологической и профессиональной адаптации молодых сотрудников подразделений по делам несовершеннолетних к службе в органах внутренних дел	94

ВСЕРОССИЙСКИЙ СЕМИНАР

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

И. С. Ивануха

Использование информационных технологий для фиксации и документирования правонарушений и преступлений экстремистской направленности	98

Н. С. Кобяков

Возможный подход к классификация АССН ОВД для моделирования оценки опасности деструктивных программных воздействий	103

К. А. Цыганов

Сценарии реализации угроз безопасности информации внешним нарушителем с использованием скрытых стеганографических каналов	107

ВСЕРОССИЙСКИЙ СЕМИНАР

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОХРАНЯЕМЫХ ТЕРРИТОРИЙ И ОБЪЕКТОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Е. М. Абросимова

Использование системы видеонаблюдения и аналитики данных для повышения безопасности объектов органов внутренних дел	115

О. В. Багринцева

Особенности внедрения мониторинговых систем в деятельность подразделений правоохранительных органов	118

Е. С. Бондаренко

К вопросу о методах и средствах организации обеспечения антитеррористической защищенности объектов органов внутренних дел Российской Федерации	122

В. Г. Волкова, Н. В. Зубова

К вопросу о применении «умных замков» в качестве технических средств охраны	127

С. А. Гречаный

Особенности организации охраны объекта при угрозе применения беспилотных воздушных судов в террористических целях ..	132

М. А. Гудков, А. А. Гапеев, Д. Ю. Калков, И. С. Никитин

К вопросу методики оценки безопасной зоны по действию воздушной ударной волны	135

П. М. Дуплякин

Угрозы периметральной защиты территорий и объектов ОВД .	140

И. С. Ивануха, Д. Ю. Калков

Проблемные вопросы при проведении обследования собственных объектов МВД России на предмет антитеррористической защищенности	143

Д. Ю. Калков, М. А. Гудков, И. С. Ивануха	
К вопросу охраны общественного порядка и обеспечению общественной безопасности при проведении массовых мероприятий	148
Н. И. Меркулова	
Аспекты формирования у персонала ПЦО знаний, умений и навыков по конфигурированию устройств оконечных объектов	154
А. А. Миллер	
Деятельность сотрудников полиции по пресечению функционирования робототехнических комплексов и беспилотных воздушных судов (дронов) в воздушном пространстве над объектами транспортной инфраструктуры: правовая регламентация и проблемные аспекты	157
А. В. Сидоров	
Совершенствование антитеррористической защищенности охраняемых объектов в условиях противодействия беспилотным воздушным судам	162
О. В. Толстых	
Правовое регулирование вопросов противодействия беспилотным воздушным судам на объектах охраны	167
А. И. Янгиров, И. М. Янгиров, С. Б. Ахлюстин, Н. А. Садчикова	
Организация охраны объектов с применением спутникового канала связи	169

ВСЕРОССИЙСКИЙ СЕМИНАР

УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ СРЕДИ НЕСОВЕРШЕННОЛЕТНИХ

А. И. Бадретдинов	
Особенности предупреждения вовлечения несовершеннолетних в систематическое употребление алкогольной продукции в сельской местности	178
Р. В. Колесников, А. В. Польшиков	
Некоторые криминологические особенности предупреждения преступлений, совершаемых несовершеннолетними	184
А. А. Кулешов	
Вовлечение несовершеннолетнего в совершение преступления: проблемы квалификации	190
А. В. Максименко, А. С. Лимарь	
Предупреждение вовлечения несовершеннолетних в диверсионную деятельность	194
А. Р. Нугуманов	
Буллинг: уголовно-правовые средства противодействия	200

А. В. Польшиков, А. В. Кушнарёва	
Современное состояние и тенденции изменения преступности в России, связанной со склонением подростков к употреблению наркотиков	204
В. С. Прохонов, О. В. Демидова	
Факторы, способствующие совершению преступлений, связанных со склонением подростков к употреблению наркотиков ...	210
М. Ю. Пучнина	
Тенденции вовлечения несовершеннолетних в совершение преступлений террористического характера и экстремистской направленности	215
М. Ю. Пучнина, Д. Ю. Кузнецов	
Криминологический анализ вовлечения несовершеннолетних в скулшутинг	219
Д. Н. Соловьев	
Некоторые уголовно-правовые меры борьбы с преступностью среди несовершеннолетних	224
С. А. Солодина	
К вопросу о необходимости криминализации вовлечения несовершеннолетних в азартные игры	228

ВСЕРОССИЙСКИЙ СЕМИНАР

ИСПОЛЬЗОВАНИЕ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ В СОЗДАНИИ ТЕХНИЧЕСКИХ УСТРОЙСТВ И ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

С. Л. Анисимов	
Прогнозирование преступлений, совершаемых с использованием информационно-телекоммуникационных технологий	234
А. О. Авсентьев	
Технические аспекты модели защиты компьютерной системы от несанкционированного доступа	236
И. В. Гилев, Р. В. Ртищев	
Программный модуль «Вражеский БПЛА» в процессе подготовки сотрудников, несущих службу в особых условиях	241
В. И. Кудряш	
Перспективы совершенствования средств электропитания систем безопасности и связи	244
А. Н. Лукьянова	
Пороговые значения для вейвлет-фильтрации исследуемого сигнала	247
А. С. Лукьянов	
Возможности цифровой системы радиосвязи на базе многофункциональной привязной высотной платформы	252

Р. М. Ляшко, В. А. Николаев, Н. В. Талышев	
Перспективные направления применения технологий искусственного интеллекта в деятельности правоохранительных органов	257
Е. В. Прокофьева, П. С. Порываева	
Виртуальные технологии и технологии дополненной реальности при подготовке специалистов МВД России	266
И. В. Сычев	
Прикладные аспекты преподавания курсов физики и математических дисциплин	270

ВСЕРОССИЙСКИЙ СЕМИНАР

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

М. А. Алексюк	
Анализ результатов численного эксперимента с использованием нейронной сети прямой передачи сигнала, решения обратной задачи экспертизы	274
С. В. Зарубин	
Специфика реализации суперсервиса «Правосудие онлайн» для повышения эффективности деятельности судебной системы Российской Федерации	279
А. В. Мельников	
К вопросу об обеспечении целостности информации электронного документооборота органов государственной власти	283
В. В. Меньших, А. В. Подольских	
Теоретико-графовая модель обучения гетерогенной группы специалистов действиям в кризисных ситуациях	288
А. Н. Никитенко	
Подходы к классификации условий функционирования мультиагентных систем	293
А. Д. Попова, И. Г. Дровникова	
К вопросу об исследовании временных характеристик уязвимостей при подготовке к их эксплуатации в программном обеспечении объектов информатизации органов внутренних дел	299
В. Р. Романова	
Влияние системы «человек-машина-среда» на надежность автоматизированных систем органов внутренних дел Российской Федерации	305

МЕЖДУНАРОДНЫЙ СЕМИНАР
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ
ПРАВОНАРУШЕНИЯМ НЕСОВЕРШЕННОЛЕТНИХ

М. А. Горностаева

ОСОБЕННОСТИ ПРИМЕНЕНИЯ
МЕРЫ ВОСПИТАТЕЛЬНОГО ВОЗДЕЙСТВИЯ
В ВИДЕ ОГРАНИЧЕНИЯ ДОСУГА
В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ, ОСВОБОЖДЕННЫХ
ОТ АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ

FEATURES OF APPLICATION OF EDUCATIONAL INFLUENCE
MEASURES IN THE FORM OF LIMITATION OF LEISURE
IN RELATION TO MINORS RELEASED
FROM ADMINISTRATIVE RESPONSIBILITY

В статье рассматривается одна из мер воспитательного воздействия, применяемых к несовершеннолетним, освобожденным от административной ответственности, – ограничение досуга. В статье также анализируются особенности и проблемные вопросы применения воспитательного воздействия меры в виде ограничения досуга.

The article examines one of the educational measures applied to minors exempted from administrative responsibility – restriction of leisure time. The article also analyzes the features and problematic issues of applying the educational impact of measures in the form of restricting leisure time.

Одним из основных национальных интересов в социальной сфере в Республике Беларусь является обеспечение общественной безопасности и безопасности жизнедеятельности населения, снижение уровня преступности и криминализации общества [1].

В частности, одним из путей достижения должного уровня правопорядка в государстве является профилактика правонарушений, совершаемых несовершеннолетними.

Основными законодательными актами, регулирующими общественные отношения в области профилактики правонарушений несовершеннолетних, являются Кодекс Республики Беларусь об административных правонарушениях (далее – КоАП) и Закон Республики Беларусь от 31 мая 2003 года № 200-З «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» (далее – Закон).

Ограниченная правоспособность и дееспособность, личностные особенности несовершеннолетнего обуславливают его особый правовой статус. В этой связи КоАП предусматривает не только особенности привлечения и освобождения несовершеннолетних от административной ответственности, но и закрепляет общие и специальные профилактические меры воздействия, применяемые к несовершеннолетним в случае совершения ими административных правонарушений.

Часть 1 статьи 5.1 КоАП содержит исчерпывающий перечень профилактических мер воздействия, применяемых к лицам, совершившим административные правонарушения, а именно:

- 1) устное замечание;
- 2) предупреждение;
- 3) меры воспитательного воздействия (в отношении несовершеннолетних) [2].

Исходя из толкования статьи 5.1 КоАП следует сделать вывод, что такие профилактические меры воздействия, как устное замечание и предупреждение, могут быть применены к правонарушителю независимо от его возраста, в то время как меры воспитательного воздействия могут быть применены только в отношении несовершеннолетних.

При этом КоАП устанавливает единственное основание, при котором профилактические меры воздействия могут быть применены к лицу, совершившему административное правонарушение, – в случае его освобождения от административной ответственности [2].

Меры воспитательного воздействия, применяемые к несовершеннолетним, закреплены в статье 9.4 КоАП. Перечень указанных мер также является исчерпывающим и расширению не подлежит. В соответствии с частью 1 статьи 9.4 КоАП к несовершеннолетнему, совершившему административное правонарушение, в целях его воспитания могут применяться следующие меры воспитательного воздействия:

- 1) разъяснение законодательства;
- 2) возложение обязанности принести извинения потерпевшему;
- 3) возложение обязанности загладить причиненный вред;
- 4) ограничение досуга [2].

Согласно части 2 статьи 9.4 КоАП к несовершеннолетнему могут быть применены как одна, так и несколько мер воспитательного воздействия [2].

Согласно части 4 статьи 9.5 КоАП ограничение досуга заключается в возложении на несовершеннолетнего обязанности соблюдения на срок до тридцати суток определенного порядка использования свободного от учебы и (или) работы времени [2].

При применении данной меры воспитательного воздействия орган, ведущий административный процесс, может предусмотреть:

1) запрет посещения несовершеннолетним определенных мест пребывания, использования отдельных форм досуга, в том числе связанных с управлением транспортным средством;

2) ограничения пребывания несовершеннолетнего вне места жительства или места пребывания в определенное время суток;

3) возложение обязанности являться для регистрации в орган, осуществляющий контроль за поведением несовершеннолетнего [2].

В то же время законодатель не конкретизирует условия, при наличии которых целесообразно применение указанных выше запретов или ограничений.

По нашему мнению, при выборе того либо иного запрета или ограничения следует учитывать личность несовершеннолетнего, характер и категорию совершенного им административного правонарушения, в том числе время и место его совершения.

Например, запрет на посещение определенных мест пребывания может быть связан с совершением несовершеннолетним правонарушения, связанного с употреблением алкогольных напитков, при этом в качестве таких мест могут выступать кафе, бары, рестораны, дискотеки.

За правонарушения, совершенные с использованием компьютерной техники, возможно наложение запрета на использование отдельных форм досуга (например, посещение компьютерных кружков и секций) и т. д.

Ограничение пребывания вне места жительства или места пребывания в определенное время суток может применяться, в частности, при совершении несовершеннолетним правонарушения в вечернее либо ночное время.

При возложении обязанности являться для регистрации в орган, осуществляющий контроль за поведением несовершеннолетнего, следует учитывать характеристику последнего по месту жительства и учебы (работы), склонность несовершеннолетнего к самовольному уходу из учреждения образования либо из семьи.

Стоит отметить, что из всех мер воспитательного воздействия, закрепленных в части 1 статьи 9.5 КоАП, ограничение досуга носит наиболее строгий характер, так как на несовершеннолетнего правонарушителя возлагается обязанность выполнения и соблюдения определенных законодателем запретов и ограничений, что частично ограничивает его права и свободы. Данное обстоятельство влечет за собой особый контроль со стороны заинтересованных государственных органов.

Однако, как показывает анализ меры воспитательного воздействия в виде ограничения досуга, в настоящее время ряд аспектов применения и выполнения данной меры законодателем не урегулирован.

Во-первых, КоАП не устанавливает определенный вид и конкретное количество ограничений, запретов и обязанностей, которые могут быть применены по отношению к несовершеннолетнему за совершенное им административное правонарушение. Как было указано выше, при выборе то-

го или иного запрета либо ограничения следует учитывать личность несовершеннолетнего, причины и условия совершения правонарушения, характер и категорию совершенного административного правонарушения, повторность совершения правонарушения. На наш взгляд, вид и количество применяемых ограничений и запретов следует определять исходя из оценки всех обстоятельств совершения правонарушения и в целях достижения наилучшего профилактического эффекта.

Во-вторых, законодателем не урегулирован порядок выполнения несовершеннолетним ограничений, запретов и обязанностей, возложенных на него в рамках меры воспитательного воздействия в виде ограничения досуга.

Например, при наложении на несовершеннолетнего ограничения пребывания вне места жительства или места пребывания в определенное время суток КоАП не закрепляет перечень государственных органов, осуществляющих контроль за соблюдением несовершеннолетним данного ограничения. По нашему мнению, контроль за нахождением несовершеннолетнего по месту жительства в определенное ему время суток следует возложить на органы внутренних дел (далее – ОВД). Практика применения меры воспитательного воздействия в виде ограничения досуга показывает, что, как правило, для несовершеннолетнего устанавливаются ограничительные рамки в вечерний и ночной периоды времени. В силу возложенных на ОВД функций и задач последние обладают определенной спецификой работы, в частности, временем выхода на службу и продолжительностью рабочего дня.

Также в законодательстве не установлены периодичность соблюдения данного ограничения, формы контроля за его исполнением.

На наш взгляд, периодичность соблюдения несовершеннолетним ограничения в виде пребывания вне места жительства (места пребывания) в определенное время суток должна быть ежесуточной.

Формами контроля за соблюдением несовершеннолетним данного ограничения могут являться, например, посещение сотрудниками ОВД несовершеннолетнего по месту жительства (месту пребывания), а также осуществление телефонной связи с несовершеннолетним посредством стационарного телефона, установленного по его месту жительства (месту пребывания), либо через средства видеосвязи.

Также одной из обязанностей несовершеннолетнего является его явка для регистрации в орган, осуществляющий контроль за его поведением. При этом в КоАП отсутствует понятие «органа, осуществляющего контроль за поведением несовершеннолетних». По нашему мнению, к органам, осуществляющим контроль за поведением несовершеннолетних, следует отнести органы, которые в рамках своей компетенции осуществляют профилактику правонарушений несовершеннолетних.

Статьей 4 Закона закреплён перечень органов, учреждений и иных организаций, осуществляющих профилактику безнадзорности и правонарушений несовершеннолетних. К ним относят:

- комиссии по делам несовершеннолетних;
- органы опеки и попечительства;
- Министерство образования, структурные подразделения областных (Минского городского) исполнительных комитетов, городских, районных исполнительных комитетов, местных администраций районов в городах, осуществляющие государственно-властные полномочия в сфере образования;
- Министерство здравоохранения, структурные подразделения областных (Минского городского) исполнительных комитетов, осуществляющие государственно-властные полномочия в сфере здравоохранения, органы управления здравоохранением других республиканских органов государственного управления;
- Министерство труда и социальной защиты, структурные подразделения областных (Минского городского) исполнительных комитетов, городских, районных исполнительных комитетов, осуществляющие государственно-властные полномочия в сфере труда, занятости и социальной защиты;
- Министерство внутренних дел, территориальные органы внутренних дел;
- иные органы, учреждения и организации в пределах своей компетенции осуществляют деятельность по профилактике безнадзорности и правонарушений несовершеннолетних в порядке, установленном Законом и иными актами законодательства [3].

Также при возложении на несовершеннолетнего обязанности являться для регистрации в орган, осуществляющий контроль за его поведением, следует закрепить механизм явки на регистрацию. Например, в постановлении органа, рассматривающего дело об административном правонарушении, должно найти отражение:

- периодичность явки (например, два раза в неделю);
- дни явки (например, каждая среда);
- время явки (например, в свободное от учебы (работы) время в рамках рабочего времени органа, осуществляющего контроль за поведением несовершеннолетних);
- место явки (наименования и адрес органа, в который следует явиться несовершеннолетнему, номер кабинета).

В-третьих, законодателем не предусмотрены меры ответственности за невыполнение несовершеннолетним меры воспитательного воздействия в виде ограничения досуга. По нашему мнению, в случае выявления государственными органами, осуществляющими контроль за поведением несовершеннолетних, умышленных фактов уклонения от выполнения, невыполнения, а равно отказу от выполнения несовершеннолетним меры воспитательного воздействия в виде ограничения досуга данные органы обя-

заны уведомить ОВД и орган, рассматривающий дело об административном правонарушении. ОВД, в свою очередь, инициирует вопрос о начале административного процесса в отношении несовершеннолетнего по ст.24.3 КоАП («Неповиновение законному распоряжению или требованию должностного лица при исполнении им служебных полномочий»).

Таким образом, мера воспитательного воздействия в виде ограничения досуга позволяет принять к несовершеннолетнему определенные запреты и ограничения, но без наступления для него каких-либо правовых последствий.

В то же время в целях эффективного применения ограничения досуга в КоАП требуется внесение ряда дополнений и изменений. Полагаем, что ст. 9.5 целесообразно дополнить примечаниями следующего содержания

«1. При наложении меры воспитательного воздействия в виде ограничения досуга правом выбора вида и количества применяемых к несовершеннолетнему запретов и ограничений наделен орган, рассматривающий дело об административном правонарушении, с учетом всех обстоятельств совершения правонарушения и в целях выполнения задач, предусмотренных настоящим Кодексом.

2. Установить, что периодичность соблюдения несовершеннолетним ограничения в виде пребывания вне места жительства (места пребывания) в определенное время суток должна быть ежесуточной.

3. Определить, что органом, осуществляющим контроль за поведением несовершеннолетних, являются органы, осуществляющие профилактику безнадзорности и правонарушений несовершеннолетних. Правом выбора органа, осуществляющим контроль за поведением несовершеннолетних, наделен орган, рассматривающий дело об административном правонарушении».

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ През. Респ. Беларусь, 09 ноября 2010 г., № 575 : в ред. Указа През. Респ. Беларусь от 24.01.2014 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс] : 6 янв. 2021 г., №91-3: принят Палатой представителей 18 дек. 2020 г. : одобр. Советом Респ. 18 дек. 2020 г.: в ред. Закона Респ. Беларусь от 09.12.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

3. Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних [Электронный ресурс] : Закон Респ. Беларусь, 31 мая 2003 г., № 200-3 : в ред. Закона Респ. Беларусь от 18.05.2022 г. //

ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информ. Респ. Беларусь. – Минск, 2024.

СВЕДЕНИЯ ОБ АВТОРЕ

Горностаева Мария Александровна.
Преподаватель кафедры административной деятельности факультета милиции.

Могилёвский институт МВД Республики Беларусь.

E-mail: masha.gornostaeva.98@mail.ru

Республика Беларусь, 212001, г. Могилёв, ул. Крупской, д. 67.

Gornostaeva Mariya Alexandrovna.

Lecturer at the Department of administrative activities faculty of police
Mogilev Institute of the Ministry of Internal Affairs of the Republic of Belarus

Republic of Belarus, 212001, Mogilev, Krupskoy str., 67.

Ключевые слова: несовершеннолетний; меры воздействия; ограничение досуга.

Keywords: minor; measures of influence; restriction of leisure.

УДК 342.92

А. А. Деминская

ИССЛЕДОВАНИЕ ПРИЧИН СОВЕРШЕНИЯ ПРАВОНАРУШЕНИЙ НЕСОВЕРШЕННОЛЕТНИМИ

RESEARCH OF THE REASONS FOR COMPLETING OFFENSES BY MINORS

Статья представляет собой исследование причин, способствующих совершению несовершеннолетними правонарушений. В статье проведен анализ факторов, которые могут оказывать влияние на поведение несовершеннолетних, таких как семейная остановка, окружение, социальный аспект.

The article is a study of the reasons contributing to the commission of offenses by minors. The article analyzes factors that may influence the behavior of minors, such as family stop, environment, and social aspect.

Проблема совершения несовершеннолетними правонарушений является одной из наиболее актуальных. Исследование причин, которые спо-

способствуют совершению несовершеннолетними правонарушений, позволит построить эффективную модель профилактической работы.

Проведенный анализ специальной литературы по данной проблематике позволяет выделить причины, способствующие совершению правонарушений и преступлений несовершеннолетними, а именно:

1. Семейное неблагополучие. Семья является важным институтом социализации подрастающего поколения. Она создает индивидуальную среду жизни и развития детей. Ни одно общественное или государственное учреждение не может сыграть, как бы ни было оно совершенно, решающую роль в развитии личности на том или ином возрастном этапе. Семейное неблагополучие почти всегда создает реальные сложности в формировании детей и подростков.

2. Неблагоприятное бытовое окружение. Является одной из основных причин противоправного поведения подростков. Рост числа одиноких и неполных семей, дезорганизация семьи способствуют тому, что дети начинают искать общения вне дома, чтобы компенсировать дефицит эмоциональных контактов с родителями.

3. Подстрекательство со стороны взрослых. Как правило, около 1/3 противоправных деяний совершаются подростками под воздействием взрослых. Подстрекательство – это не только склонение, но и вовлечение в противоправное поведение. Любыми способами подстрекатели манипулируют несовершеннолетними и стремятся сделать их зависимыми.

4. Низкая правовая грамотность. Одной из причин правонарушений и преступлений несовершеннолетних является правовая безграмотность.

Несовершеннолетние не всегда понимают и знают, что некоторые моральные запреты могут быть санкционированы на законодательном уровне, а некоторые поступки, с точки зрения нравственности, не только не допустимы, но и влекут за собой ответственность.

Правовая воспитательная работа с несовершеннолетними направлена на развитие правовой культуры детей через усвоение ими основных правовых ценностей, знаний об основных правах и свободах человека, способах их реализации, об основных отраслях права и прежде всего, о тех нормах права, с которыми приходится постоянно сталкиваться в повседневной жизни.

5. Средства массовой коммуникации. Рассматривая вопрос влияния на несовершеннолетних средств массовой коммуникации, необходимо отметить прежде всего их информационное воздействие.

В настоящее время мощными источниками формирования навыков агрессивного поведения являются интернет и телевидение. Несовершеннолетние посредством телевидения и интернета получают многочисленные возможности обучения различным формам агрессии, находясь дома. Проведенные исследования показали, что демонстрация по телевидению и ин-

тернету насилия способствует: а) агрессивному стилю поведения; б) искажению представления об окружающей реальности.

На поведение несовершеннолетних большое влияние оказывает то, что у них недостаточный жизненный опыт, их эмоционально-волевая сфера ограничена, в том числе следует учитывать неуравновешенность, неспособность контролировать свои поступки, необъективность самооценки, склонность к подражанию, и тот факт, что они легко внушаемы. Характеризуя трудных подростков, важно отметить, что все внешние воздействия воспринимаются ими враждебно. Такие подростки в большей степени через показное проявление демонстрируют свою взрослость, а именно употребляют спиртные напитки, используют утилитарные способы развлечений, говорят на особом «взрослом» лексиконе, курят, необдуманно подражают моде и т.п. Как правило, такая «взрослость» формируется в неформальном общении, некритическом подражании взрослым и старшим ребятам. Например, грубо отвечают старшим либо родителям, не слушают их советы, сомневаются в их справедливости и доброжелательности. Только незначительное количество трудновоспитуемых подростков имеют ярко выраженную антиобщественную направленность действий. Отрицательное поведение большинство этих подростков проявляют, как правило, в зависимости от ситуации.

Без выявления причин совершения правонарушений и преступлений несовершеннолетними невозможно создание эффективной системы профилактики. Учитывая эти причины, можно определить круг ответственных и заинтересованных лиц, которых следует вовлекать для создания эффективной системы социального контроля и предупреждения противоправного поведения несовершеннолетних.

Проведение ранней профилактики является приоритетным направлением в работе по предупреждению правонарушений и преступлений. И именно в школе, создавая условия, способствующие нормальному развитию детей. Например, выявлять учащихся, имеющих склонности нарушать морально-правовые нормы, изучать индивидуальные особенности таких школьников и причины нравственной деформации личности, своевременно выявлять типичные кризисные ситуации, возникающие у несовершеннолетних определенного возраста.

На наш взгляд, устранение причин противоправного поведения несовершеннолетних возможно путем проведения индивидуальной профилактической работы. Под индивидуальной профилактической работой понимается деятельность по своевременному выявлению несовершеннолетних и семей, находящихся в социально опасном положении, а также по их социально-психолого-педагогической реабилитации или предупреждению совершения несовершеннолетними правонарушений [1].

Органами, осуществляющими профилактику безнадзорности и правонарушений несовершеннолетних, являются:

- комиссии по делам несовершеннолетних;
- органы опеки и попечительства;
- Министерство образования Республики Беларусь, структурные подразделения областных (Минского городского) исполнительных комитетов, городских, районных исполнительных комитетов, местных администраций районов в городах, осуществляющие государственно-властные полномочия в сфере образования (далее, если не установлено иное, – органы управления образованием);

- Министерство здравоохранения Республики Беларусь, структурные подразделения областных (Минского городского) исполнительных комитетов, осуществляющие государственно-властные полномочия в сфере здравоохранения, органы управления здравоохранением других республиканских органов государственного управления (далее, если не установлено иное, – органы управления здравоохранением);

- Министерство труда и социальной защиты Республики Беларусь, структурные подразделения областных (Минского городского) исполнительных комитетов, городских, районных исполнительных комитетов, осуществляющие государственно-властные полномочия в сфере труда, занятости и социальной защиты (далее – органы по труду, занятости и социальной защите);

- Министерство внутренних дел Республики Беларусь, территориальные органы внутренних дел Республики Беларусь (далее, если не установлено иное, – органы внутренних дел).

- иные органы, учреждения и организации в пределах своей компетенции осуществляют деятельность по профилактике безнадзорности и правонарушений несовершеннолетних в порядке, установленном настоящим Законом и иными актами законодательства [1].

В общении, в разнообразной трудовой и творческой деятельности воспитываются нравственные начала личности, формируются интересы и потребности, что является основой организации работы с несовершеннолетними всеми субъектами профилактики.

Подводя итог, хотелось бы отметить, что не все причины и условия совершения правонарушений возможно устранить, в отношении некоторых причин и условий можно говорить лишь о минимизации, но не полного устранения.

СПИСОК ЛИТЕРАТУРЫ

1. Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних [Электронный ресурс] : Закон Республики Беларусь от 31 мая 2003 г. № 200-3: принят Палатой представителей 22 апреля 2003 г. : одобрен Советом Респ. 15 мая 2003 г. : в ред. Закона Респ. Бе-

ларусь от 04.06.2006 г. // ЭТАЛОН. Законодательство Республики Беларусь/ Нац. Центр правовой информ. Респ. Беларусь. – Минск.

СВЕДЕНИЯ ОБ АВТОРЕ

Деминская Анна Александровна.

Преподаватель кафедры административной деятельности факультета милиции.

Магистр юридических наук.

Могилевский институт МВД Республики Беларусь

E-mail: deminscaya.anya@mail.ru

Республика Беларусь, 212000, Могилев, улица Крупской, 67.

Dziaminskaya Hanna Alexandrovna.

Lecturer at the Department of Administrative Activities of the Faculty of Police.

Master of Law.

Mogilev Institute of the Ministry of Internal Affairs of the Republic of Belarus

E-mail: deminscaya.anya@mail.ru

Republic of Belarus, 212000, Mogilev, Krupskaya street, 67.

Ключевые слова: правонарушение; несовершеннолетний; индивидуальная профилактическая работа; субъекты профилактики.

Keywords: offense; minor; individual preventive work; subjects of prevention.

С. В. Кончатова

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ПРИВЛЕЧЕНИЯ К АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТИ НЕСОВЕРШЕННОЛЕТНИХ В РЕСПУБЛИКЕ БЕЛАРУСЬ И В РОССИЙСКОЙ ФЕДЕРАЦИИ

COMPARATIVE LEGAL ANALYSIS OF BRINGING MINORS TO ADMINISTRATIVE LIABILITY IN THE REPUBLIC OF BELARUS AND IN THE RUSSIAN FEDERATION

В статье представлен сравнительно-правовой анализ привлечения к административной ответственности несовершеннолетних в Республике Беларусь и в Российской Федерации. Обозначено профилактическое воздействие и индивидуальный подход к правонарушениям, совершенным подростками.

The article presents a comparative legal analysis of bringing minors to administrative responsibility in the Republic of Belarus and the Russian Federation. The preventive impact and individual approach to offenses committed by adolescents are indicated.

1 марта 2021 года в Республике Беларусь вступили в силу новые Кодекс Республики Беларусь об административных правонарушениях и Процессуально-исполнительный кодекс Республики Беларусь об административных правонарушениях.

Кодексы начали разрабатываться по распоряжению Президента Республики Беларусь А. Г. Лукашенко после того, как, проведя анализ административной практики, увидели: достаточно много граждан привлекаются к административной ответственности. При этом есть правонарушения, которые можно вывести в разряд так называемых проступков, чтобы, с одной стороны, уменьшить количество фактов подобных привлечений, с другой – усилить профилактическую функцию [1, с. 6].

Особое внимание хотелось бы обратить на главу 9 Кодекса Республики Беларусь об административных правонарушениях «Административная ответственность несовершеннолетних». Законодатель, учитывая возраст этих лиц, подробнейшим образом изложил механизм и особенности привлечения их к ответственности.

Анализ данной главы позволяет сделать вывод о том, что установлен в целом более гуманный по сравнению с предусмотренным для взрослых режим административной ответственности, расширен спектр профилактических мер воздействия.

В соответствии со ст. 4.2 Кодекса Республики Беларусь об административных правонарушениях административной ответственности подлежит физическое лицо, достигшее ко времени совершения правонарушения шестнадцатилетнего возраста.

Установление возраста наступления административной деликтоспособности основано на презумпции того, что физическое лицо в этом возрасте способно в полной мере руководить своими действиями (или бездействием), осознавая их фактический характер, противоправность и общественную опасность, и может без ущерба для своего психофизиологического здоровья претерпеть физические и моральные лишения, связанные с административным взысканием [2, с. 47].

Вместе с тем в ст. 4.2 Кодекса Республики Беларусь об административных правонарушениях перечислены правонарушения, за которые физическое лицо подлежит административной ответственности с 14 лет.

К ним относятся 6 административных правонарушений:

- ст. 10.1 «Умышленное причинение телесного повреждения и иные насильственные действия либо нарушение защитного предписания»;
- ст. 10.2 «Оскорбление»;

- ст. 11.1 «Мелкое хищение»;
- ст. 11.3 «Умышленное уничтожение либо повреждение чужого имущества»;
- ст. 16.29 «Жестокое обращение с животными или избиение животного»;
- ст. 19.1 «Мелкое хулиганство» [3].

Установив, что за эти правонарушения административная ответственность наступает с четырнадцати лет, законодатель учел, что с достижением такого возраста несовершеннолетний в полной мере способен оценивать свое поведение в отношении своих деяний.

В соответствии со статьей 9.2 Кодекса Республики Беларусь об административных правонарушениях «Особенности наложения административного взыскания на несовершеннолетнего» к лицу, совершившему административное правонарушение, в возрасте от четырнадцати до восемнадцати лет административные взыскания применяются на общих основаниях с учетом следующих особенностей:

1) в отношении него не могут применяться общественные работы, административный арест;

2) размер налагаемого на него штрафа не может превышать двух базовых величин. В случае, если санкция предусматривает административное взыскание только в виде штрафа, а у несовершеннолетнего отсутствуют заработок, стипендия или иной доход, к нему применяются меры воспитательного воздействия;

3) лишение права заниматься определенной деятельностью может налагаться на срок не более одного года [3].

Обращает на себя тот факт, что в соответствии с частью 2 статьи 9.2 Кодекса Республики Беларусь об административном правонарушении при наложении административного взыскания на лицо, совершившее административное правонарушение, в возрасте от четырнадцати до восемнадцати лет учитываются следующие факторы:

- 1) условия его жизни и воспитания;
- 2) уровень его интеллектуального, волевого и психического развития, иные особенности личности несовершеннолетнего;
- 3) влияние на его поведение родителей или лиц, их заменяющих, а также близких родственников, членов семьи и иных старших по возрасту лиц;
- 4) характеристика по месту его учебы и (или) работы (при ее наличии) [3].

К условиям его жизни и воспитания в данном случае относятся материально-бытовые условия, характеризующие состав семьи, уровень дохода и жилищные условия.

Не следует недооценивать и негативной роли безразличного, пассивного отношения к воспитанию детей в некоторых семьях. Признаки

пассивной воспитательной позиции семьи свидетельствуют о возможном противоправном поведении детей из этих семей.

Исследуя причины и условия, способствующие совершению правонарушений несовершеннолетними, криминологи на достоверном материале доказали, что наиболее криминогенным фактором, провоцирующим противоправное поведение детей и подростков, является кризисная неблагополучная семья. Именно она наиболее интенсивно формирует личность, способную совершать правонарушения [4, с. 175].

При этом нахождение подростка в неблагополучной семье само по себе еще не влечет становление его на путь правонарушений. Семейное воспитание – сложный и ответственный процесс. Вместе с тем всестороннее выявление и оценка условий жизни семьи позволяют определять ошибки в семейном воспитании, дают возможность субъектам профилактики осуществлять раннюю профилактику в отношении поведения подростков.

Следует отметить, что при решении вопроса о привлечении к ответственности несовершеннолетнего закон предусматривает возможность освобождения его от ответственности с применением к нему предупреждения или мер воспитательного воздействия.

В соответствии со ст. 9.3 Кодекса Республики Беларусь об административных правонарушениях «Особенности освобождения несовершеннолетних от административной ответственности» лицо, совершившее административное правонарушение, в возрасте от четырнадцати до восемнадцати лет вне зависимости от категории административного правонарушения может быть освобождено от административной ответственности с применением к нему предупреждения [3].

Особого внимания в связи с изложенным выше, заслуживает статья 9.4 Кодекса Республики Беларусь об административном правонарушении «Меры воспитательного воздействия», в которой перечислены меры воспитательного воздействия, при освобождении от административной ответственности несовершеннолетнего.

К таким мерам относятся:

- разъяснение действующего законодательства;
- возложение обязанности принести извинения потерпевшему;
- возложение обязанности загладить причиненный вред;
- ограничение досуга.

К несовершеннолетнему могут быть применены как одна, так и несколько мер воспитательного воздействия [3].

Данные меры позволяют, исходя из условий жизни и воспитания подростка, уровня его интеллектуального, волевого и психического развития, ограничиться мерами воспитательного воздействия с целью дальнейшего недопущения им в своей жизни противоправного поведения, уважения действующего законодательства и формирования правовой культуры.

Обратимся к административной ответственности несовершеннолетних в Российской Федерации.

В соответствии со ст. 2.3 Кодекса об административных правонарушениях Российской Федерации административной ответственности подлежит лицо, достигшее к моменту совершения административного правонарушения возраста шестнадцати лет.

Ответственность за административное правонарушение, совершенное несовершеннолетними в возрасте от 14 до 16 лет, несут родители или иные законные представители (опекуны, попечители) [5].

При этом из десяти видов административных наказаний к несовершеннолетним чаще всего применяются только два – это предупреждение и административный штраф.

Закон не позволяет применять к лицам, не достигшим 18-летнего возраста, административный арест.

С учетом конкретных обстоятельств дела, данных о лице, совершившем административное правонарушение в возрасте от 16 до 18 лет, закон позволяет решать вопрос об освобождении его от административной ответственности с применением к нему меры воздействия, предусмотренной федеральным законодательством о защите прав несовершеннолетних.

Таковыми являются:

- обязанность принесения публичного извинения потерпевшему;
- предупреждение;
- объявления выговора или строгого выговора;
- возложение на несовершеннолетнего, достигшего 15 лет, обязанности возместить причиненный материальный ущерб;
- передача несовершеннолетнего под надзор родителей или лиц их заменяющих, или общественных воспитателей, а также под наблюдение трудового коллектива или общественной организации.

Как показывает правоприменительная практика, зачастую несовершеннолетние совершают административные правонарушения из-за низкого уровня знаний об особенностях административной ответственности.

Правовая культура должна лежать в основе становления жизнедеятельности подростков, так как это позволит соблюдать действующее законодательство.

Необходимо также отметить, что здоровая, благополучная семья, в которой любят и заботятся о детях, является нравственной основой законопослушного поведения подростков. В семье, где присутствуют крепкие духовные связи между членами семьи, хорошая психологическая атмосфера, дети будут уважать и соблюдать действующее законодательство.

Таким образом, главным критерием административного законодательства является не количество выявленных нарушений, совершенных несовершеннолетними, и привлечение к административной ответственности, а профилактическое воздействие и индивидуальный подход к каждой

конкретной ситуации. Подростку дается возможность осознать противоправный проступок и не допускать нарушений закона в будущем.

СПИСОК ЛИТЕРАТУРЫ

1. Ипатов. В. Главный критерий – не количество проступков, а успешность их профилирования / В. Ипатов // На страже. – 2020. – № 20. – С.10.
2. Круглов В. А. Комментарии к Кодексу Республики Беларусь об административных правонарушениях / В. А. Круглов. – Минск : Амалфея, 2014. – 1072 с.
3. Кодекс Республики Беларусь об административных правонарушениях: принят Палатой представителей 6 дек. 2020 г. : одобрен Советом Республики 18 дека. 2020 г. № 91-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. Центр правовой информации. Респ. Беларусь. – Минск, 2024.
4. Шиханцов, Г. Г. Криминология : учебник / Г. Г. Шиханцов. – Минск : Изд-во Гревцова, 2009. – 296 с.
5. Кодекс об административных правонарушениях Российской Федерации [Электронный ресурс]: 30 дек. 2001 г., № 195-ФЗ: принят Государственной Думой 20 декабря 2001 г.: одобрен Советом Федерации 26 декабря 2001 г.: в ред. Закона Российской Федерации от 11.03.2024 г. // Консультант Плюс. Российская Федерация / Нац. Центр правовой информ. Российской Федерации. – Москва, 2024.

СВЕДЕНИЯ ОБ АВТОРЕ

Кончатова Светлана Валерьевна.

Преподаватель кафедры административной деятельности факультета милиции.

Могилевский институт МВД Республики Беларусь.

E-mail: light.ratosh@mail.ru

Республика Беларусь, 212000, Могилев, улица Крупской, 67.

Konchatova Svetlana Valerievna.

Lecturer at the Department of Administrative Activities of the Faculty of Police.

Mogilev Institute of the Ministry of Internal Affairs of the Republic of Belarus.

Republic of Belarus, 212000, Mogilev, Krupskaya street, 67.

Ключевые слова: административная ответственность несовершеннолетних; освобождение несовершеннолетних от административной ответственности; меры воспитательного воздействия.

Keywords: administrative liability of minors; release of minors from administrative liability; educational measures.

УДК 342.9

ВСЕРОССИЙСКИЙ СЕМИНАР

ПРОБЛЕМЫ ФОРМИРОВАНИЯ ДОКАЗАТЕЛЬСТВ ПО УГОЛОВНЫМ ДЕЛАМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В. В. Батоев

О НЕКОТОРЫХ ВОПРОСАХ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПО ДЕЛАМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

ON SOME ISSUES OF INFORMATION SUPPORT FOR OPERATIONAL INVESTIGATIVE ACTIVITIES IN CASES OF EXTREMIST ORIENTATION

В статье рассматриваются вопросы совершенствования информационного обеспечения оперативно-розыскной деятельности по делам экстремистской направленности посредством использования современных информационных технологий, к числу которых следует отнести метод дистанционного зондирования земной поверхности. Автором обозначается ряд проблемных вопросов, устранение которых предлагается рассматривать в качестве направлений совершенствования деятельности оперативно-розыскных органов в деле добывания оперативно значимой, доказательственной и иной ориентирующей информации.

The article discusses the issues of improving information support for operational investigative activities in cases of extremist orientation through the use of modern information technologies, which include the method of remote sensing of the Earth's surface. The author identifies a number of problematic issues, the elimination of which is proposed to be considered as areas for improving the activities of operational investigative bodies in obtaining operationally significant, evidentiary and other orienting information.

Ситуация в сфере борьбы с экстремизмом продолжает оставаться напряженной. По официальным данным Главного информационно-аналитического центра МВД России на территории Российской Федерации в 2023 году было зарегистрировано 1340 преступлений экстремистской направленности.

Сложившуюся ситуацию усугубляют наличие нерешенных проблемных вопросов правового, организационного, финансового и иного характера, нашедших отражение в юридической литературе.

В подобной непростой ситуации перед субъектами противодействия экстремизму стоит задача совершенствования имеющегося инструментария [1, с. 7-9], в том числе посредством применения современных информационно-телекоммуникационных технологий при осуществлении поиска оперативно значимой и доказательственной информации [4, 5, 6 и др.]. В дополнение напомним, что немаловажным фактором, подлежащим учету в деле противодействия экстремистским проявлениям является и использование и иных источников информации в их совокупности [3, 7 и др.].

Цифровизация оперативно-розыскной деятельности по линии противодействия экстремизму приобретает особое значение в части применения современных технических средств и методов добывания «ценной» информации [2, с. 6-7]. В данном случае субъектам оперативно-розыскной деятельности предлагается обратить внимание на использование возможностей метода дистанционного зондирования земной поверхности из космоса (далее – ДЗЗ) при решении оперативно-розыскных задач в целом, и по делам экстремистской направленности в частности. Спектр задач по борьбе с экстремизмом, при решении которых возможно использование указанного метода достаточно широк. Практика показывает о наличии положительных примеров эффективного использования ДЗЗ при решении задач борьбы с преступностью.

Метод дистанционного зондирования земной поверхности из космоса подразумевает применение средств космической съемки поверхности Земли. В настоящее время ДЗЗ широко используется в различных отраслях экономики, сельского и лесного хозяйства, обеспечении безопасности государства, кадастре и картографии и др.

Организацией, ответственной по вопросам использования ДЗЗ является Госкорпорация «Роскосмос» (далее – РКС), а оператором космических средств ДЗЗ выступает научный центр оперативного мониторинга земной поверхности. Основная задача данного центра заключается в осуществлении деятельности по планированию съемки, приема и обработки данных ДЗЗ, а также предоставлению произведенной продукции конечным потребителям.

Поступающая информация со спутников концентрируется в Единой территориально-распределенной информационной системе ДЗЗ (далее – ЕТРИС ДЗЗ). Предоставлением космических снимков из ЕТРИС ДЗЗ занимается коммерческий оператор услуг ДЗЗ и геоинформационных сервисов на их основе АО «Терра Тех» (дочернее предприятие РКС). Данная организация осуществляет на коммерческой основе разработки геоинформационных решений, поиск и анализ информации с геопространственной и временной привязкой.

В настоящее время АО «Терра Тех» осуществляет комплекс мероприятий в рамках реализации национальной программы «Цифровая экономика».

В данном случае определенный интерес для субъектов правоохранительной деятельности представляют реализуемые в рамках национальной программы проекты, такие как:

1. «Цифровая Земля», в рамках которого осуществляется разработка инструментов получения объективных сведений о природных активах и хозяйственной деятельности с помощью космических снимков, в том числе с использованием технологий искусственного интеллекта. В данном случае получаемая информация с космических спутников предоставляется потребителю для использования в различных целях в виде аналитических отчетов о состоянии и развитии того или иного объекта, участка местности, природных ресурсов и др.

В данное время указанный проект подразумевает возможность использования следующих геоинформационных сервисов:

- эко-мониторинг (незаконные свалки, стоки, нарушенные и загрязненные земли и др.);
- карьеры (соблюдение правил недропользования и незаконные карьеры и др.);
- строй-контроль (объекты строительства на территории; активность, стадия строительства конкретных объектов и др.);
- чрезвычайные ситуации (ретроспективный мониторинг половодий, паводков, наводнений и др.);
- нарушенные земли;
- сельхоз-мониторинг (инвентаризация земель сельскохозяйственного назначения, развитие посевов, прогнозирование урожайности и др.);
- лес-контроль (естественные и хозяйственные изменения лесного фонда; незаконная деятельность в лесном фонде и др.).

2. Сервис «Pixel.AI», способный классифицировать сельхозугодия на такие категории как: распахивается, засеивается, зарастает и т.д.

3. «Докажи.рф» – сервис, предоставляющий доступ к архивной и реальной спутниковой информации и аналитическим отчетам в целях ее использования в суде¹.

4. Сервис «Геопространственная аналитика» со сведениями о чрезвычайных ситуациях, изменениях в природе и др.

5. «TerraCloud» – сервис онлайн-покупки снимков из космоса с отечественных и зарубежных спутников в круглосуточном режиме.

Таким образом, можно заключить, что указанные сервисы с их возможностями представляют определенный интерес в рамках осуществления противодействия экстремизму. Положительный потенциал данных серви-

¹ В соответствии с положениями статей 64, АПК РФ, статьи 55 ГПК РФ данные космической съемки могут рассматриваться как доказательства в судебной и досудебной практике при решении земельных, имущественных и хозяйственных споров (определение дат, нарушение границ, незаконная деятельность, подтверждение ущерба, соблюдение сроков, экомониторинг).

сов обусловлен масштабами космической съемки, оперативностью их получения, возможностью осуществления мониторингового контроля и др.

В деле решения вопросов организации доступа правоохранительных органов к данной информации подразумевает реализацию комплекса мероприятий правового, организационного, финансового и иного характера. Одновременно с этим потребуются принятие мер по устранению проблемных вопросов в части получения геокосмической информации со спутников.

К их числу следует отнести:

- недостатки правового регулирования порядка взаимодействия между правоохранительными органами и организациями, осуществляющими ДЗЗ;
- проблемы в финансировании вопросов получения геокосмической информации, вопросы интеграционного характера программного обеспечения;
- отсутствие соответствующего кадрового обеспечения высококвалифицированными специалистами, способными обрабатывать и анализировать поступающую со спутников информацию.

Важно отметить, что в данное время разработан проект Федерального закона «О дистанционном зондировании Земли из космоса», в котором отмечено, что правоохранительным органам для выполнения возложенных на них функций и реализации полномочий будет предоставлены данные на безвозмездной основе.

Таким образом, параллельно с законодательными положительными для правоохранительных органов сдвигами важно организовать работу по научно-методическому, финансовому, кадровому обеспечению данного направления деятельности, оснащению необходимым техническим оборудованием и др., что в дальнейшем позволит качественно усовершенствовать информационное обеспечение процесса противодействия экстремизму в частности и преступности в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов О. С. Роль оперативно-розыскной деятельности в раскрытии преступлений экстремистской направленности // В сборнике : Противодействие радикализации российской молодежи: вопросы теории и практики. сборник : в 2 частях. автор вступительной статьи Е. Г. Ичитовкина ; под общей редакцией доктора юридических наук, доц. С. Н. Мешалкина; составитель Ф. М. Жовтовский, Н. А. Горюнкова. – Домодедово, 2020. – С. 7–12.

2. Алехин Е. В. Проведение технических мероприятий при раскрытии и расследовании преступлений экстремистской направленности // В сборнике : Правовая культура России: современное состояние и тенденции развития. Сборник материалов Всероссийской научно-практической кон-

ференции. Под общей редакцией С. Е. Туркулец, Е. В. Листопадовой. – 2019. – С. 6–9.

3. Бессонов В. А. Взаимодействие оперативных подразделений ОВД с отдельными институтами гражданского общества при выявлении и раскрытии преступлений экстремистской направленности / А. В. Бессонов, Д. В. Намёткин // В сборнике : Государство и право в изменяющемся мире: правовая система в условиях информатизации общества. Материалы IV научно-практической конференции с международным участием. – 2019. – С. 130–134.

4. Бычков В. В. Искусственный интеллект в сфере раскрытия и расследования преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей / В. В. Бычков // Российский следователь. – 2022. – № 1. – С. 3–6.

5. Клянчина Е. В. Некоторые особенности использования информационных технологий при информационно-аналитическом обеспечении раскрытия преступлений экстремистской направленности // В сборнике : Информационные технологии в правоохранительной деятельности. Сборник научных трудов XV научно-практической конференции. – 2017. – С. 111–117.

6. Соляков В. Е. Использование искусственного интеллекта в ходе раскрытия и расследования преступлений экстремистской направленности // В сборнике : Безопасность личности, общества и государства: теоретико-правовые аспекты. Сборник научных статей международной научно-теоретической конференции курсантов, слушателей и студентов, проводимой в рамках I Санкт-Петербургского международного молодежного научного форума «Северная Пальмира: территория возможностей». Сост.: Е.А. Маркова, Т.В. Колпакова. – Санкт-Петербург. – 2022. – С. 1220–1226.

7. Трубкина О. В. К вопросу о комплексности применения специальных знаний в раскрытии и расследовании преступлений экстремистской направленности / О. В. Трубкина // Криминалистика: вчера, сегодня, завтра. – 2023. – № 2 (26). – С. 247–262.

СВЕДЕНИЯ ОБ АВТОРЕ

Батоев Владимир Батоевич.

Кандидат юридических наук, доцент.

ФКУ НПО «Специальная техника и связь» МВД России.

E-mail: vbatoev@mail.ru

111024, г. Москва, ул. Пруд Ключики, д. 2.

Batoev Vladimir Batoevich.

Candidate of Legal Sciences, associate professor.

Special Equipment and Communications of the Ministry of Internal Affairs of the Russian Federation.

E-mail: vbatoev@mail.ru

2, Prud Klyuchiki str., Moscow, 111024. Tel. 89149154701

Ключевые слова: преступления экстремистской направленности, информационное обеспечение, оперативно-розыскная деятельность, метод, дистанционное зондирование земной поверхности.

Keywords: extremist crimes, information support, operational investigative activities, method, remote sensing of the Earth's surface.

УДК 343.9

А. И. Гайдин

кандидат юридических наук, доцент;

А. Л. Стефанский

**ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ
ПРИ ПОЛУЧЕНИИ ИНФОРМАЦИИ О СОЕДИНЕНИИ АБОНЕНТОВ
И АБОНЕНТСКИХ УСТРОЙСТВ
В РОССИИ И РЕСПУБЛИКЕ БЕЛАРУСЬ**

**PROBLEMS AND WAYS TO SOLVE THEM
WHEN RECEIVING INFORMATION ABOUT THE CONNECTION
OF SUBSCRIBERS AND SUBSCRIBER DEVICES
IN RUSSIA AND THE REPUBLIC OF BELARUS**

В статье рассматриваются проблемы применения норм уголовно-процессуального законодательства при получении криминалистически значимой информации, характеризующей обстоятельства соединения абонентского оборудования сетей связи. Обоснована позиция необходимости совершенствования правовых норм. Рассмотрен опыт регулирования уголовно-процессуальной деятельности в Республике Беларусь. Определены возможные пути развития законодательства.

The article examines the problems of applying the norms of criminal procedure legislation when receiving forensically significant information characterizing the circumstances of the connection of subscriber equipment of communication networks. The position of the need to improve legal norms is substantiated. The experience of regulating criminal procedure activity in the Republic of Belarus is considered. Possible ways of developing legislation are determined.

В действующем отечественном законодательстве тайна переписки и телефонных переговоров является неотъемлемым правом каждого человека. Ограничение данного права допускается только на основании судебного ре-

шения, которое, в свою очередь, носит обязательный характер. Соответствующее решение суд выносит в результате рассмотрения ходатайства лица, осуществляющего производство по уголовному делу, о получении информации о соединениях между абонентами и (или) абонентскими устройствами.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами – следственное действие, представляющее собой процесс получения данных о взаимодействии между абонентами (пользователями) и/или их устройствами в рамках телефонных звонков, сообщений, интернет-сессий и других видов связи. Могут включать в себя информацию о времени и дате соединения, продолжительности разговоров, номерах телефонов или IP-адресах, а также другие метаданные, которые имеют значение для выявления фактов и установления связей между лицами или событиями [1]. Следственное действие было закреплено в уголовно-процессуальном законодательстве России в 2010 году для упорядочения процедуры получения технических данных, характеризующих соединение абонентского оборудования телекоммуникационной среде и укрепления механизма охраны конституционных прав на тайну телефонных переговоров, электронных и иных сообщений, передающихся по каналам связи.

Говоря о криминалистической значимости информации о соединениях между абонентами и абонентскими устройствами, следует отметить увеличение объемов использования данной информации, что в первую очередь связано, на наш взгляд, с ростом числа преступлений, в ходе которых происходят соединения абонентов и абонентских устройств, последовавшими за повсеместным распространением устройств связи. Криминалистическое значение указанная информация имеет в различных ситуациях расследования: при установлении местоположения предполагаемого преступника или лица, пропавшего без вести, анализе коммуникаций и выявлении связей между различными лицами для определения причастных к преступлению лиц и в иных случаях.

Формирование представления сущности следственного действия, предусмотренного ст. 186.1 УПК России [2], до настоящего времени является предметом научной дискуссии. В. Ю. Стельмах определяет его следующим образом: «...это самостоятельное следственное действие, которое проводится по судебному решению и заключается в получении от оператора связи на материальном носителе сведений о фактах соединений между абонентами и (или) абонентскими устройствами, осмотре следователем данного носителя и сведений, и решении вопроса о признании носителя с представленными сведениями вещественным доказательством и приобщении его к уголовному делу» [3]. На наш взгляд определение, которое предлагает В. Ю. Стельмах достаточно объемное, оно позволяет в полной мере охарактеризовать рассматриваемое средство доказывания, однако в нем не отражается сама цель следственного действия, хотя она находит свое содержание в ст. 186.1 УПК РФ.

Никак нельзя оставить без внимания определение получения информации о соединениях между абонентами и (или) абонентскими устройствами Н. А. Архиповой, которая определяет его как «комплекс взаимосвязанных действий следователя по получению судебного решения для истребования от осуществляющей услуги связи организации информации на любом материальном носителе о соединениях абонентов и поручения ей отслеживания поступающей искомой информации в базу данных мобильной связи, а также осмотру и анализу документов, содержащих указанную информацию, приобщению их к материалам дела в целях установления всех обстоятельств, имеющих значение для раскрытия и расследования преступлений» [4].

Достижение указанной цели осуществляется посредством решения следующих задач:

- определение конкретного оператора сотовой связи услугами которого пользуется проверяемый абонент;
- определение принадлежности индивидуального абонентского номера и (или) абонентского устройства конкретному физическому или юридическому лицу;
- установление определённого промежутка времени, за который необходимо получить детализацию соединений между абонентами и (или) абонентскими устройствами;
- оформление постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами;
- обращение к компании оператору связи для выполнения технических мероприятий, способствующих получению информации о соединениях между абонентами и (или) абонентскими устройствами;
- осмотр и оценка доказательственного значения полученной информации.

Не все ученые соглашались с обоснованностью закрепления в законодательстве следственного действия в существующем виде. Например, Ю. Н. Соколов предлагал ввести следственное действие, именуемое «электронное наблюдение», в рамках которого абсолютно все случаи получения сведений об абонентах и абонентских соединениях предусматривалось объединить в одно следственное действие [5].

В практике применения норм ст. 186.1 УПК РФ наибольшую сложность представляет решение вопроса о конкретном перечне данных, которые могут быть получены у оператора связи в рамках рассматриваемой процедуры. Это обусловлено конкуренцией норм уголовно-процессуального законодательства. В частности, ч. 4 ст. 21 УПК РФ обязывает все учреждения, предприятия, организации, должностных лиц и граждан исполнять требования, поручения и запросы прокурора, руководителя следственного органа, следователя, органа дознания и дознавателя, предъявленные в пределах их полномочий. Хотя использованная законодателем формулировка статьи с позиции юридической

техники требует более конкретного отражения в законе права следователя истребовать документы, предметы, направлять запросы о предоставлении сведений, имеющих значение для установления обстоятельств расследуемого события, норма активно применяется на стадии предварительного расследования. Запросы на предоставление информации в соответствии с данной нормой направляются органами предварительного расследования операторам связи и иным субъектам.

Закрепленное в ч. 1 ст. 144 УПК РФ право дознавателя, органа дознания, следователя, руководителя следственного органа при проверке сообщения о преступлении истребовать документы, тоже не вносит ясности в решение вопроса о содержании сведений, характеризующих обстоятельства соединения абонентов и (или) абонентских устройств, которые могут быть получены в рамках предварительной проверки сообщений о преступлении. Такие сведения предоставляются в форме документа, так как формируются оператором связи на основе технических данных, регистрируемых оборудованием в соответствии с алгоритмом управляющей программы и удостоверяются им. Соответственно при предварительной проверке сообщения о преступлении, должностное лицо вправе с согласия суда такие сведения истребовать у оператора связи. Однако изложенные рассуждения не согласуются с положением о недопустимости производства следственных действий на стадии возбуждения уголовного дела, если это прямо не предусмотрено в законе. Получение информации о соединениях между абонентами и (или) абонентскими устройствами не указано в ч.1. ст. 144 УПК России и соответственно можно сделать вывод, что истребование соответствующих сведений у оператора связи субъектом, осуществляющим предварительную проверку сообщения о преступлении, недопустимо.

Решение выявленных проблем реализации норм уголовно-процессуального законодательства традиционно может осуществляться по двум направлениям. Первое, связано с приспособлением юридической практики к деятельности в условиях противоречивости норм права. В частности, в стадии возбуждения уголовного дела оправданным является механизм получения сведений о соединении абонентов и (или) абонентских устройств путем проведения органом дознания оперативно-розыскного мероприятия наведение справок по поручению следователя или дознавателя.

На стадии предварительного расследования путем инициирования производства следственного действия, предусмотренного ст. 186.1 истребуется весь объем необходимых сведений, связанных с работой абонентского оборудования том числе и в случаях, когда сведения о соединении устройств сложно отнести к охраняемой законом тайне. Например, для установления данных о соединении объектов, относящихся к системе «интернета вещей».

Второй путь разрешения правоприменительных проблем – изменение законодательства, совершенствование норм, заимствование успешного опыта правового регулирования правоотношений, накопленного в других государствах. В данном случае разумно рассмотреть подход к регулированию аналогичных правоотношений в уголовно-процессуальном законодательстве Республики Беларусь.

Процессуальное законодательство Беларуси не предусматривает самостоятельного следственного действия, направленного на получении сведений о соединении абонентского оборудования. При этом в ст. 103 УПК Республики Беларусь [6] содержится норма, закрепляющая право органа уголовного преследования по находящимся в его производстве материалам и уголовному делу требовать от организаций, должностных лиц и граждан, а также органов, уполномоченных законом осуществлять оперативно-розыскную деятельность, представления информации, предметов и документов, имеющих значение для уголовного дела. Требование о представлении информации, документов, содержащих охраняемую законом тайну, в предусмотренных законодательными актами случаях, а также о представлении информации, документов, содержащих государственные секреты, санкционируется прокурором. Тем самым законодатель не стал перегружать уголовный процесс Республики Беларусь дополнительными самостоятельными следственными действиями, а пошел по пути детальной регламентации процессуального действия, производство которого обеспечивает возможность собирания широкого круга доказательств, не относящихся к числу формируемых субъектом доказывания.

Таким образом, в период действия ст. 186.1 УПК России, регламентирующей основания и порядок получения информации о соединениях между абонентами и (или) абонентскими устройствами, накопилось ряд проблем в правоприменительной деятельности, разрешение которых не может быть осуществлено без совершенствования действующих норм. Одним из направлений развития законодательства может стать заимствование опыта Республики Беларусь, суть которого заключается в снижении степени детализации нормативного регулирования процессуальных действий, в рамках которых получают сведения об обстоятельствах, подлежащих установлению и доказыванию.

СПИСОК ЛИТЕРАТУРЫ

1. Вазюлин С. А. Получение информации о соединениях между абонентами: специфика процедуры // Уголовный процесс. – 2014. – № 1. – С. 16.
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 02.10.2024) // СЗ РФ. – 2001. – № 52 (ч. I). – Ст. 4921.

3. Стельмах В. Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие : монография. – Екатеринбург : Уральский юридический институт МВД России, 2014. – С. 60.

4. Архипова Н. А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи : автореф. дис. ... канд. юрид. наук. – Санкт-Петербург : Санкт-Петербургский университет МВД России, 2011. – С. 11.

5. Соколов Ю. Н. Электронное наблюдение в уголовном судопроизводстве и оперативно-розыскной деятельности. – Екатеринбург, 2006. – С. 122.

6. Уголовно-процессуальный кодекс Республики Беларусь от 16 июля 1999 года № 455-Z (с изменениями и дополнениями). – URL: <https://pravo.by/document/?guid=3871&p0=НК9900295> (дата обращения: 22.10.24)

СВЕДЕНИЯ ОБ АВТОРАХ

Гайдин Александр Иванович.

Начальник кафедры уголовного процесса.

Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: gaidin78@mail.ru

Россия, 394065, Воронежская обл., г. Воронеж, пр-т Патриотов, 53.

Стефанский Альберт Леонидович.

Помощник начальника института по международному сотрудничеству.

Воронежский институт МВД России.

E-mail: aliks23@yandex.ru

Россия, 394065, Воронежская обл., г. Воронеж, пр-т Патриотов, 53.

Gaidin Alexander Ivanovich.

Head of the Criminal Procedure Department.

Candidate of Law, Associate Professor.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: gaidin78@mail.ru

Russia, 394065, Voronezh Region, Voronezh, Prospect Patriotov, 53.

Stefansky Albert Leonidovich.

Assistant to the Head of the Institute for International Cooperation.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: aliks23@yandex.ru

Russia, 394065, Voronezh Region, Voronezh, Prospect Patriotov, 53.

Ключевые слова: Получение информации о соединениях абонентов и (или) абонентских устройств; криминалистически значимая информация; уголовно-процессуальное законодательство; оператор связи.

Keywords: Obtaining information about subscriber connections and (or) subscriber devices; forensically significant information; criminal procedure legislation; communications operator.

УДК 343.1

А. В. Головчанский

SIM-БОКСЫ КАК СРЕДСТВО РЕАЛИЗАЦИИ СОВРЕМЕННЫХ СХЕМ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ

SIM BOXES AS A MEANS OF IMPLEMENTING MODERN REMOTE FRAUD SCHEMES

В статье рассмотрен механизм совершения дистанционных мошенничеств, проанализированы особенности использования при их совершении sim-боксов и иного сетевого оборудования.

The article examines the mechanism of committing remote fraud, analyzes the features of using sim-boxes and other network equipment when committing them.

Если проанализировать сведения официальной статистики, одним из наиболее сложных направлений деятельности МВД России в последние годы, является противодействие IT-преступлениям. Не смотря на принимаемые меры, за последние четыре года, доля указанных преступлений увеличилась более чем на треть и составляет практически 40% в общем массиве. Наибольшее количество среди таких преступлений составляет дистанционное мошенничество. Только за 2023 год от такого рода деяний пострадало более полмиллиона человек, из которых практически каждый четвертый – пенсионер [1]. Обеспокоенность данной проблемой проявляется на всех уровнях нашего гражданского общества и систематически отмечается в выступлениях Президента [2] представителей правоохранительных ведомств Российской Федерации [3,4,5]. Оценивая масштабы роста данных преступлений, многие рассматривают их в качестве угрозы национальной безопасности [6]. Подчеркивая значимость данного вопроса, создание системы эффективного противодействия преступлению, совершаемому с использованием информационно-телекоммуникационных технологий, и снижения ущерба от их соверше-

ния, Президентом РФ обозначено одной из национальных целей Развития Российской Федерации [7].

Как заметил на очередном заседании коллегии МВД, посвященном противодействию IT-преступности В. А. Колокольников, структура IT-преступлений постоянно меняется, непрерывно появляются новые способы совершения таких посягательств. В ответ на принятые меры противодействия коммуникациям посредством «подменной» телефонии преступники задействуют новые схемы и средства, позволяющие обходить принятые меры. [1]

В настоящее время большинство схем дистанционного мошенничества реализуется посредством использования так называемых сим-боксов, GSM шлюзов, виртуальных автоматических телефонных станций.

Особенности использования указанных средств в механизме совершения современных мошенничеств представляют значительный интерес с криминалистической точки зрения.

Механизм совершения преступления многими криминалистами справедливо рассматривается как важнейший элемент криминалистической характеристики преступления [8], так как представляет наиболее общую модель, учитывающую всё многообразие взаимосвязей материальных объектов и процессов, определяющих возникновение и формирование источников уголовно-правовой, уголовно-процессуальной и криминалистически значимой информации, необходимой для осуществления процесса доказывания [9].

Как показывает анализ практики, большинство фишинговых звонков исходит из специально подготовленной инфраструктуры располагающейся за пределами России. Наиболее распространенная схема реализации мошеннических действий в обобщенном виде может быть охарактеризована следующим образом.

Во-первых, это практически всегда хорошо организованная группа, с четкой структурой и распределением ролей между отдельными её подразделениями и конкретными участниками. Внешне схема построения такой преступной группы имеет явное сходство с легальной организацией офисного типа, с наличием руководителя, кадровых подразделений (рекрутов), занимающихся подбором и подготовкой персонала, структур обеспечения безопасности.

Одним из структурных элементов данной схемы является так называемый колл-центр. Это, как правило, офисное помещение или группа помещений, иногда организуемая в цельную, единую сеть, оборудованная специализированным компьютерным и сетевым оборудованием, имеющим доступ в сеть Интернет. Такие инфраструктурные объекты в основном располагаются за пределами Российской Федерации, и, как отмечается во множестве материалов, опубликованных по результатам журналистских расследований, а также обзорах, подготовленных специалистами ведущих

банковских организаций, преимущественно концентрируются на территории Украины [10, 11].

Данный криминальный «бизнес» функционирует по модели франчайзинга. Данная модель заключается в том, что организаторы предлагают приобрести колл-центр «под ключ», включая разработанные структуру центра, алгоритмизацию процесса его работы, готовые сценарии диалога с жертвой, а также наличием актуальных баз данных, содержащих персональные данные предполагаемых жертв, техническим и программным обеспечением, включая инструменты IP-телефонии, подмены номера и прочее.

Роли операторов таких колл-центров различны и зависят от имеющихся навыков и опыта работы в данной сфере. Наиболее распространена схема работы двумя группами, в первую из которых входят так называемые «звонари», то есть операторы, осуществляющие обзвон абонентов по заданному шаблону с целью выявления потенциальных жертв, наиболее подверженных воздействию. Это, как правило, наименее квалифицированные сотрудники. При установлении контакта с жертвой звонок переводится на параллельную линию операторам второй группы, которые, осуществляя второй этап реализации задействованного в обмане сценария, финализируют преступный замысел. Это уже более квалифицированные субъекты, задачей которых является оказание психологического давления с целью принуждения жертвы к осуществлению определенных действий, охватываемых преступным замыслом. В зависимости от исходной ситуации и реализуемой схемы, жертву убеждают передать имеющиеся у него денежные средства через курьера, либо посредством денежных переводов, либо предварительно получить эти денежные средства путем оформления кредита или продажи недвижимости. По аналогии с сотрудниками коммерческих организаций, осуществляющих закрытие деловых сделок, их называют «клоузерами».

Техническое обслуживание колл-центра, настройку оборудования, программного обеспечения, SIP-телефонии на персональных рабочих местах сотрудников, подготовку и распределение между ними баз данных, обеспечивает «группа технической поддержки». В работе операторов активно используются CRM-системы, упрощающие адресную работу с конкретной жертвой.

Однако после введения отечественными операторами связи средств блокировки звонков, осуществляемых с подменной номеров или обезличенных абонентов, реализуемых в рамках противодействия дистанционным мошенничествам, прямая коммуникация расположенных за рубежом колл-центров с абонентами российских операторов стала проблематична. В связи с этим схема работы подобных колл-центров получила своё развитие и цепочка связи между колл-центром и абонентом (жертвой) дополнена промежуточным элементом – узлом связи (АТС) размещаемым на территории Российской Федерации. Этот промежуточный хаб выполняет в первую очередь функции перевода маршрутизации трафика, с каналов IP-

телефонии (SIP, VoIP) на местную сеть сотовой связи [12]. С помощью таких «серых» АТС, создаваемых и обсуживающихся сообщниками мошенников, преступники обходят антифрод-системы, блокировки, устанавливаемые операторами связи в отношении подозрительного входящего зарубежного трафика и трафика, исходящего от дискредитированных абонентов. При этом в местной сети связи данный звонок идентифицируется как коммуникация, исходящая от абонента местной сети, тарифицируется согласно местным тарифам и абонентским устройством жертвы определяется как входящая коммуникация (звонок/сообщение) от абонента местной сети. Создание и организация таких серых АТС как правило осуществляется субъектами, не являющимися прямыми участниками преступной группы, организующей работу расположенного за рубежом мошеннического колл-центра и осуществляют представление услуг маршрутизации трафика через эксплуатируемые ими АТС на условиях аренды указанных мощностей. В то же время преступный характер реализуемого трафика, как и преступный характер функционирования таких узлов связи очевиден и вполне понятен данным субъектам. Помимо использования возможностей маршрутизации трафика в обход легальных каналов, указанные АТС используются преступниками для создания и администрирования аккаунтов электронных платежных систем, профилей в социальных сетях и мессенджерах, используемых в преступных схемах как непосредственно для осуществления преступных действий, так и для подбора и вовлечения соучастников и перемещения полученных преступных доходов.

В основе работы указанных нелегальных АТС лежит использования функционала VoIP GSM-шлюзов и сим-боксов. Первые используются для перекодировки пакета данных, передаваемых по протоколу, используемому в интернет-соединении в протоколы GSM-сети. Вторые позволяют осуществлять агрегацию большого количества сим-карт в одном месте с возможностью осуществления централизованного управления ими, автоматического перераспределения сим-карт между различными шлюзами по временному графику или иному запрограммированному сценарию. Связь между VoIP GSM-шлюзом и сим-боксом осуществляется через IP-сеть, поэтому территориально они могут находиться совершенно в разных местах, обособленно друг от друга. При этом оператором связи место расположения абонентского устройства, использующего сим-карту будет определяться по месту расположения GSM-шлюза.

Таким образом, при использовании запрограммированного сценария смены сим-картой используемого для передачи данных шлюза, оборудованием оператора связи фиксируется соединение сим-карты из разных локаций и создаётся иллюзия перемещения абонентского устройства, в котором используется данная сим-карта [13]. Использование вышеуказанных нелегальных узлов связи (хабов) не только позволяет преодолевать меры противодействия, применяемые в отношении мошеннических коммуникаций,

но и значительно усложняют установление причастных к преступлению лиц и организаций.

В одном сим-боксе может быть аккумуляровано до 128 сим-карт. В одном помещении, используемом преступниками для организации нелегальной АТС, может одновременно использоваться десятки таких устройств. Несложно предположить, какой объём преступного трафика проходит через такие хабы и какое количество преступлений совершается посредством их использования. Например, в ходе реализации комплекса совместных мероприятий, проведенных ФСБ России и МВД России в апреле текущего года, в 42 регионах России обнаружены 937 сим-боксов, 11 серверных станций, обеспечивающих работу устройств связи для теневого трафика. В ходе данных мероприятий изъято более 277 тысяч сим-карт различных операторов. По подсчетам специалистов, мощности изъятого оборудования позволяли совершать более 40 миллионов мошеннических звонков в сутки [14].

В то же время, стоит отметить, что оборот вышеуказанного оборудования, в том числе сим-боксов, никаким образом не регламентирован и не ограничен. Данные устройства находятся в свободной продаже – их может приобрести и использовать каждый. Единственное средство, используемое преступниками в приведённом примере, на оборот которых распространяется хоть какие-то ограничения, – это сим-карты, для приобретения которых требуется заключение договора и удостоверения личности приобретателя. Однако, как показывает приведенный пример, приобретение сим-карт не составляет особых затруднений для преступников.

Одновременно с этим следует отметить, что в последнее время подобные нелегальные узлы связи, представляющие услуги маршрутизации трафика в обход установленного порядка с сотнями сим-боксов, серверов, виртуальными АТС и иным оборудованием, использование которого в конечном итоге позволяет обезличить абонентское устройство исходящего трафика, возникают на территории нашей страны лавинообразно.

И причины такого роста очевидны. Доход таких криминальных АТС достаточно существенен. За их создание и эксплуатацию предусмотрена административная ответственность, наказание в рамках которой в процентном соотношении с получаемой от прибыли просто ничтожно. С учетом сложностей выявления подобных хабов, не велики и риски привлечения к ответственности. Большинство таких АТС функционируют по принципу сдачи в аренду эксплуатируемых мощностей, поэтому даже в случае установления факта их использования для совершения преступлений привлечь субъектов, организовавших работу такой АТС, к уголовной ответственности за соучастие в совершении преступлений достаточно проблематично. Поэтому в условиях отсутствия неотвратимости соразмерного наказания рост противоправных деяний, приносящих высокий доход, видится достаточно закономерным.

На основе анализа типового механизма совершения дистанционных мошенничеств следует выделить характеристику следовой картины данных преступных деяний, представленную следовой информацией, отражающей маршрутизацию коммуникации от исходного абонентского устройства до промежуточного узла связи (серых АТС), маршрутизацию сигнала, обработанного оборудованием данных АТС в сеть местных операторов связи, и последующую маршрутизацию сигнала до абонентского устройства жертвы. Одновременно с этим значимая следовая информация образуется при осуществлении коммуникации соучастников с организаторами и кураторами данной преступной деятельности, а также при перемещении похищенных денежных средств. Соответственно значимыми источниками значимой поисковой, доказательственной информации рассматриваемых преступлений помимо самой жертвы и его абонентского устройства выступают: технологическое оборудование операторов сотовой связи, интернет-провайдеров, а также нелегальных узлов связи, через которые проходит международный трафик; оборудование банковских организаций, электронных платежных систем, иных субъектов, представляющих услуги по осуществлению операций с криптовалютами; иностранные операторы связи и интернет-провайдеры. Очевидно, что в качестве наиболее значимого источника доказательственной информации выступает технологическое оборудование и документация колл-центра. Однако следует учитывать, что последние из приведенного перечня потенциальные источники криминалистически значимой информации, как правило, находятся вне юрисдикции Российской Федерации, чем с удовольствием пользуются преступники.

На основании изложенного следует заключить, что давно назрела необходимость принятия ряда правовых мер, направленных на упорядочение использования сим-боксов, GSM-шлюзов, иного сложного сетевого оборудования, используемого для организации связи на территории нашей страны, и ужесточение ответственности за нарушения установленного порядка предоставления услуг связи, вплоть до введения уголовной ответственности за нелегальное представление таких услуг. В том числе, видится необходимым введение требований об обязательной регистрации сим-боксов и шлюзов, используемых в организации сооружений и инфраструктуры связи.

С другой стороны, поддерживаем уже не раз звучавшее мнение об ужесточении наказания за участие в рассматриваемых мошенничествах для всех участников данной преступной схемы [15].

СПИСОК ЛИТЕРАТУРЫ

1. Владимир Колокольцев провел заседание коллегии МВД России, посвященное противодействию IT-преступности. // Сетевое издание «МВД МЕДИА». Новости. Официально. 4 июня 2024 года. – URL: <http://https://mvdmedia.ru/news/official/vladimir-kolokoltsev-provel-zasedanie-kollegii-mvd-rossii-posvyashchennoe-protivodeystviyu-it-prestu> (дата обращения: 12.06.2024).
2. Расширенное заседание коллегии МВД // Официальный сайт Президента Российской Федерации. События. 20 марта 2023 года. – URL: <http://kremlin.ru/events/president/news/70744> (дата обращения: 12.06.2024)
3. В. А. Колокольцев. Рост тяжкой преступности в России обусловлен увеличением числа киберпреступлений // Официальный сайт МВД РФ. Прямая речь. В. А. Колокольцев. 12.01.2021, 16:15. – URL: <https://mvd.rf/speech/item/22548863/?ysclid=lpvan23zig107885843> (дата обращения: 10.06.2024).
4. Генпрокурор рассказал о росте числа киберпреступлений в России в 25 раз // Интернет-портал «Российской газеты» 17.07.2020. – URL: <https://rg.ru/2020/07/17/genprokuror-rasskazal-o-roste-chisla-kiberprestuplenij-v-rossii> (дата обращения: 10.06.2024).
5. Состоялось совещание по вопросам национальной безопасности в регионах ЦФО // Официальный сайт Полномочный представитель Президента России в Центральном федеральном округе. 27.10.2021 – URL: <http://cfo.gov.ru/news/50999> (дата обращения: 10.06.2024).
6. В Генпрокуратуре заявили, что киберпреступность стала представлять угрозу нацбезопасности // Федеральное государственное унитарное предприятие «Информационное телеграфное агентство России (ИТАР-ТАСС) – 24 мая 2021. – URL: <https://tass.ru/obschestvo/11451173> (дата обращения: 12.06.2024).
7. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года. Указ Президента РФ от 07.05.2024 № 309 // Официальный сайт президента российской Федерации. – URL: <http://www.kremlin.ru/events/president/news/73986> (дата обращения: 12.06.2024).
8. Гавло В. К. О понятии криминалистического механизма преступления и его значении в расследовании криминальных событий / В. К. Гавло // Алгоритмы и организация решений следственных задач : Сб. науч. трудов. – Иркутск, 1982. – С. 76.
9. Новик В. В. Способ совершения преступления. Уголовно-правовой и криминалистический аспекты / В. В. Новик. – Санкт-Петербург, 2002. – С. 99.
10. Трудоустройство в мошеннический колл-центр // Официальный сайт Сбербанка России. Кибрарий. Расследования. – URL: <https://www.sberbank.ru/ru/person/kibrary/investigations/trudoustrojstvo-v-moshennicheskij-call-centr> (дата обращения: 12.06.2024).

11. Журналист устроился в киевский колл-центр, откуда «разводят» россиян под видом «службы безопасности банка». – URL: <http://www.kp.ru/daily/28343/4489034> (дата обращения: 12.06.2024).

12. Гайдин А. И. Механизм хищений денежных средств, совершаемых с использованием технологий ip-телефонии и программ подмены номеров / А. И. Гайдин, И. С. Звягин, И. С. Садырин // Вестник ВИ МВД России. – 2022. – № 3. – С. 204-205.

13. Что такое SIM-банк и как он работает. Веб-сайт Хабр. – URL: <https://habr.com/ru/companies/artel/articles/369963> (дата обращения: 12.06.2024).

14. Ирина Волк: МВД России проводит мероприятия, направленные на противодействие преступлениям в сфере информационно-телекоммуникационных технологий // Сетевое издание «МВД МЕДИА». Новости. Официальный представитель. 18 апреля 2024 года. – URL: <https://mvdmedia.ru/news/ofitsialnyy-predstavitel/irina-volk-mvd-rossii-provodit-meropriyatiya-napravlennye-na-protivodeystvie-prestupleniyam-v-sfere/> (дата обращения: 12.06.2024).

15. Володин предложил ужесточить ответственность за телефонное мошенничество // Парламентская газета. – 23.07.2021. – URL: <https://www.pnp.ru/politics/volodin-predlozhil-uzhestochit-otvetstvennost-za-telefonnoe-moshennichestvo.html> (дата обращения: 12.06.2024)

СВЕДЕНИЯ ОБ АВТОРЕ

Головчанский Алексей Владимирович.
Старший преподаватель кафедры криминалистики.
Воронежский институт МВД России.
E-mail: alexey.golovchanskiy@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Golovchanskiy Alexey Vladimirovich.
Senior lecturer at the Department of Criminology.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: alexey.golovchanskiy@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53

Ключевые слова: IT-преступления; дистанционные мошенничества; sim-боксы; иное сетевое оборудование.

Keywords: IT-crimes; remote scams; sim boxes; other network equipment.biometrics.

УДК 67.99

**К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ СПЕЦИАЛЬНЫХ ЗНАНИЙ
ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ
В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**ON THE QUESTION OF USING SPECIAL KNOWLEDGE
IN INVESTIGATION OF CRIMES
IN THE SPHERE OF INFORMATION TECHNOLOGY**

В статье рассматриваются возможности использования специальных знаний при расследовании преступлений в сфере информационных технологий. Проанализированы особенности привлечения субъектов, обладающих специальными знаниями к производству наиболее типичных следственных действий при расследовании преступлений указанной группы. Обоснована необходимость комплексного подхода в использовании специальных знаний для целей расследования преступлений, совершенных в сфере информационных технологий.

The article examines the possibilities of using special knowledge in investigating crimes in the field of information technology. The features of involving subjects with special knowledge in the production of the most typical investigative actions in investigating crimes of this group are analyzed. The need for an integrated approach to using special knowledge for the purposes of investigating crimes committed in the field of information technology is substantiated.

Успешное и качественное раскрытие и расследование преступлений, совершаемых в современных условиях, требует квалифицированного применения широкого арсенала специальных знаний, а также достижений науки и техники для обеспечения эффективного технико-криминалистического сопровождения деятельности правоохранительных органов.

Данные статистики свидетельствуют о неуклонном росте числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Так, за период времени с января по июнь 2024 года зарегистрировано 368,8 тыс. преступлений, совершенных в сфере информационных технологий, что составляет 38,5% от общего числа зарегистрированных преступлений. Относительно аналогичного периода прошлого года произошел рост числа преступлений на 15,8%. Более 98% таких преступлений выявляются органами внутренних дел. Из числа выявленных преступлений 47,1% относится к категориям тяжких и особо тяжких, при этом 82,4% совершаются с использованием сети Интернет, 46,4% – средств мобильной связи [1].

Следует отметить, что помимо составов преступлений, предусмотренных статьями главы 28 Уголовного кодекса Российской Федерации в число преступлений в сфере информационных технологий на сегодняшний день включены преступные деяния, предусмотренные иными статьями (например, ст. 158, 159, 159.3, 159.6, 171.2, 205.2, 228.1, 242, 242.1, 242.2, 280) [2].

Происходящая на сегодняшний день компьютеризация преступлений вполне закономерна. Развитие технологий, внедрений компьютерной и иной техники в повседневную деятельность каждого современного человека влекут за собой и перепрофилирование лиц, совершающих преступления. Компьютерная техника, сеть Интернет, мобильные средства связи становятся доступны и широко распространены, благодаря ним человек может оперативно выполнить стоящие перед ним профессиональные и иные задачи, а также мгновенно оформить покупку, подготовить документы, получить услуги или осуществить перевод по реквизитам без посещения отделения банка. В свою очередь, преступники используют вышеназванные средства – компьютерную технику, сеть Интернет, а также средства мобильной связи для целей совершения противоправных деяний. И вот уже местом совершения мошеннических действий выступают благоустроенные квартиры и офисные помещения, таким образом, формат мошеннических действий переходит в дистанционный, появляются новые виды и методы преступной деятельности – вишинг, скам, фишинг, социальная инженерия и иные.

Безусловно, в условиях компьютеризации преступлений происходит и трансформация имеющейся следовой картины. Криминалистически значимая информация из так называемой классической переходит в разряд цифровой. Электронно-цифровые следы могут быть образованы на стадиях подготовки, совершения и сокрытия преступлений, однако механизм их формирования обуславливает некоторые особенности их обнаружения и закрепления.

Все вышеперечисленное позволяет сделать вывод о том, что расследование преступлений в сфере информационных технологий требует наличия определенного вида знаний и умений у лиц, принимающих участие в этом процессе. Знания и практические навыки в раскрытии и расследовании данной группы преступлений требуются и следователям, и оперативным уполномоченным, задействованным в расследовании уголовного дела. При этом, по мнению автора, участие специалистов и экспертов становится обязательным на всех этапах и стадиях раскрытия и расследования данного вида преступлений. Следует отметить, что выбор формы использования специальных знаний, а также определение вида необходимой отрасли знаний осуществляет субъект расследования или же сотрудник, которому поручена проверка сообщения о преступлении.

По мнению большинства ученых, к наиболее типичным следственным действиям, производимым при расследовании преступлений в сфере информационных технологий, следует отнести: следственный осмотр,

осмотр предметов и документов, обыск, выемку, допрос и назначение экспертов. В случае привлечения к производству вышеназванных следственных действий лиц, обладающих специальными знаниями, речь будет идти о процессуальной форме их использования.

Рассмотрим некоторые особенности процессуальной формы использования специальных знаний при расследовании преступлений в сфере информационных технологий.

Прежде всего, выразим согласие с С. В. Зуевыми и В. Б. Веховым в том, что к числу особенностей производства типичных следственных действий по делам о преступлениях в сфере компьютерной информации относятся обязательное участие специалистов по профилю осматриваемых (изымаемых) компьютерных устройств и находящейся в их памяти компьютерной информации, а также подготовка необходимых программно-технических и технико-криминалистических средств для осмотра и изъятия компьютерной информации и ее электронных носителей [3, с. 39].

Производство следственного осмотра, а также его виды – осмотр места происшествия, а также осмотр предметов и документов возможны до возбуждения уголовного дела, на этапе проверки сообщения о преступлении. Значимость данных следственных действий не подлежит сомнению, в результате их производства может быть установлена первоначальная и наиболее значимая информация. Так, в ходе осмотра места происшествия, может быть получена информация о характере и механизме произошедшего события, а также обнаружена и зафиксирована криминалистически значимая информация, в том числе имеющиеся следы подготовки, совершения и сокрытия преступления.

Случаи непривлечения специалистов, обладающих специальными знаниями требуемой области с учетом специфики рассматриваемой группы преступлений, имеют своим следствием низкое качество и результативность такого следственного осмотра. Работа по обнаружению и фиксации электронно-цифровых следов происходит с обязательным применением программно-аппаратных средств, зачастую связана с предварительным получением копии выявленной информации.

Следует отметить важность комплексного подхода в выборе специалистов, помимо лиц, обладающих знаниями в области компьютерной информации, необходимо участие сведущих лиц, обладающих специальными криминалистическими знаниями, для содействия в обнаружении и изъятии так называемых традиционных следов. Помимо необходимости изъятия следовой информации следует помнить и о необходимости осуществления процесса видеофиксации хода и результатов производимого следственного действия.

Следственными действиями, требующими тщательной предварительной подготовки при расследовании преступлений, совершенных в сфере информационных технологий, являются обыск и выемка. Здесь должны быть учтены следующие обстоятельства: необходимость произ-

водства одновременного обыска по разным адресам в пределах одного или нескольких населенных пунктов, а также понимание вида, характера и перечня подлежащих обнаружению и изъятию предметов (компьютерной техники, носителей информации, сетевого и серверного оборудования, а также иных устройств содержащих потенциально значимую для целей расследования информацию).

Все вышесказанное обуславливает необходимость активного взаимодействия субъекта расследования с лицами, обладающими специальными знаниями, в рамках консультаций и обсуждений, исходя из сложившейся следственной ситуации и с учетом полученной к этому времени информации о произошедшем событии, способе и механизме осуществления преступного деяния.

Допросы различных участников уголовного судопроизводства по данной категории дел также имеют немаловажное значение. Специалисты, обладающие специальными знаниями в области компьютерной информации, на этапе подготовки к производству допроса могут помочь в составлении перечня вопросов для последующего допроса как потерпевшего, так и подозреваемого. Грамотно и верно сформулированные вопросы позволят осуществить данное следственное действие качественно, что безусловно приведет к уяснению следователем механизма преступного деяния, а также поможет выяснить степень участия каждого из подозреваемых в совершении преступления в случае совершения его в составе группы.

Производство судебных экспертиз является не менее важным источником получения доказательственной информации в процессе раскрытия и расследования преступлений в сфере информационных технологий. С учетом специфики рассматриваемой группы преступлений, наиболее часто назначаются судебные компьютерные экспертизы. К основным задачам данного вида экспертизы относятся поиск, обнаружение и анализ компьютерной информации. Помимо названного вида экспертизы могут быть назначены и традиционные криминалистические экспертизы, такие как дактилоскопические, трасологические, автороведческие и почерковедческие, а также некоторые специальные виды экспертиз.

На сегодняшний день становится возможным выполнение задачи идентификации интернет-пользователя в результате разработки методики идентификации интернет-пользователя на основе стилистических и лингвистических характеристик коротких электронных сообщений. Совершенствуется и методика производства лингвистических экспертиз, на предмет выработки подходов к лингвистическому исследованию материалов, размещаемых в сети Интернет.

Анализ практики расследования преступлений, совершенных с использованием информационных технологий, свидетельствует о том, что зачастую требуется комплекс экспертиз для полного и всестороннего анализа имеющейся компьютерной информации. В связи с чем к процессу расследования данной группы преступлений привлекаются лица, облада-

ющие не только специальными знаниями в области компьютерной информации, но также и эксперты судебно-психологической и комплексной судебно-психолого-психиатрической экспертиз.

В качестве вывода отметим, что расследование преступлений в сфере информационных технологий, совершаемых с учетом современного уровня развития технологий, практически невозможно без активного использования специальных знаний в различных отраслях науки и техники. Комплексный подход в использовании специальных знаний позволит качественно и в полном объеме установить механизм совершения преступления данной группы, изучить личность преступника, а также выяснить наличие причинно-следственной связи между действиями подозреваемых и наступившими последствиями по каждому конкретному преступлению.

СПИСОК ЛИТЕРАТУРЫ

1. Состояние преступности в России за январь-июнь 2024 г. URL: <https://мвд.рф/reports/item/53218362/> (дата обращения 26.07.2024).
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 12.06.2024) // СЗ РФ. – № 25. – 1996. – Ст. 2954.
3. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. – Москва : ЮРАЙТ, 2023. – 243 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Гуменчук Оксана Олеговна.
Преподаватель кафедры криминалистики.
Воронежский институт МВД России.
E-mail: gumenchuk_oksana@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Gumenchuk Oksana Olegovna.
Lecturer of the Department of Criminalistics.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: gumenchuk_oksana@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: специальные знания; экспертиза; расследование; преступление; информационные технологии.

Keywords: biometrics; biometric identity identification; fingerprinting methods; methods of habitoscopy; forensic identification.

УДК 343.985.7

**ОСОБЕННОСТИ ИДЕНТИФИКАЦИИ ЛИЦ
ПО БИОМЕТРИЧЕСКИМ ПАРАМЕТРАМ
В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ**

**FEATURES OF IDENTIFICATION
OF PERSONS BY BIOMETRIC PARAMETERS DURING
THE INVESTIGATION OF CRIMES**

В статье рассматривается система биометрических данных, составляющих основу криминалистических методов, приемов и средств, обеспечивающих идентификацию лиц в ходе раскрытия и расследования преступлений. Проанализированы современные возможности и перспективные направления развития методов биометрии для выполнения задач по выявлению и идентификации лиц, совершивших преступление.

The article examines the system of biometric data that form the basis of forensic methods, techniques and tools that ensure the identification of persons during the disclosure and investigation of crimes. The modern possibilities and promising directions of the development of biometrics methods for the tasks of identifying and identifying persons who have committed a crime are analyzed.

Рассмотрим распространенные в научном сообществе понятия биометрии и биометрической идентификации. А. И. Иванов трактует биометрию как науку, изучающую способы измерения различных параметров человека с целью установления сходства (различий) между людьми и выделения одного конкретного человека из множества других людей [1, с. 80]. Е. Г. Барковская определила биометрию как область научного знания, изучающего методы идентификации и аутентификации человека на основе измерения его биометрических параметров [2, с. 27]. Традиционно биометрические параметры человека делятся на две группы: статические и динамические. К статическим относятся уникальные параметры, заложенные в человеке при рождении:

- геометрия руки;
 - строение папиллярного узора;
 - строение радужной оболочки глаз;
 - строение сетчатки глаз;
 - структура дезоксирибонуклеиновой кислоты (далее – ДНК) и др.
- Систему динамических параметров составляют особенности:
- элементов внешнего облика;

- голоса;
- почерка;
- походки и т.д.

Под биометрической криминалистической идентификацией личности Л. Югай понимает автоматизированное распознавание лица по его анатомическим, физиологическим и биологическим признакам путем его идентификации или верификации в целях раскрытия или расследования преступлений [3, с. 244]. Основной задачей криминалистической биометрии выступает идентификация и верификация личности. Под идентификацией личности понимается нахождение тождества между конкретным человеком и отдельным лицом из имеющейся группы лиц, а под верификацией – сопоставление конкретного лица с имеющимся в базе данных другим лицом.

Наиболее известный и распространенный биометрический параметр человека, используемый для криминалистической идентификации – строение папиллярного узора. Изучением строения папиллярного узора, механизмом образования потожировых следов папиллярного узора и разработкой криминалистических средств, приемов и методов собирания и исследования данных следов занимается подотрасль криминалистики – дактилоскопия.

Долгое время задача по отождествлению преступников успешно решалась создаваемыми дактилоскопическими картотеками лиц, представляющими оперативный интерес, однако по мере накопления всё большего числа дактилокарт наметилась проблема обработки и использования дактилоскопической базы. Первоначальным решением данной проблемы явилось внедрение дактилоскопической формулы – классификационной системы папиллярных узоров, предназначенной для систематизации и упрощения работы с дактилоскопическим массивом. Однако по мере накопления дактилокарт применение дактилоскопической формулы не позволяло оперативно и эффективно использовать криминалистические учеты, что привело к постепенному отказу от ее использования к концу XX века.

Важной вехой в развитии дактилоскопии явилась разработка и внедрение в деятельность правоохранительных органов автоматизированных информационно-поисковых систем, пришедших на смену картотекам и натурным коллекциям, позволяющих накапливать, обрабатывать и использовать большой объем криминалистически значимой информации.

В настоящее время основной автоматизированной дактилоскопической информационной системой на вооружении органов внутренних дел, предназначенной для решения задач по идентификации лиц по отпечаткам на дактилокартах и следах рук, изъятых с мест нераскрытых преступлений, является «Папилон». Начиная с 2020 года в экспертных подразделениях МВД России осуществляется модернизация дактилоскопических систем «Папилон» за счёт внедрения нового алгоритма кодирования «Папилон-

Автокодер» и нейросети «Папилон-Нейро», значительно улучшающих качество кодировки поступающих дактилоскопических объектов и оптимизирующих автоматическую идентификацию следов рук и отпечатков на дактилокартах.

Несмотря на общеизвестность возможностей дактилоскопических методов не только среди специалистов, но и в криминальных кругах, следы рук по-прежнему являются важными криминалистическими объектами, обеспечивающими успешное раскрытие и расследование различных категорий преступлений, а автоматизированные дактилоскопические системы – идентификацию лиц, совершивших преступление, и неопознанных трупов. Эффективность применяемых автоматизированных технологий идентификации дактилоскопических объектов подтверждается и широкой географией применения АДИС «Папилон», успешно эксплуатируемой не только органами внутренних дел России, но и таких стран, как Турция, Индия, Узбекистан, Казахстан и др.

Еще одним важным биометрическим параметром, эффективно используемым при раскрытии и расследовании преступлений, является внешний облик человека. Начиная с середины XIX века методы габитоскопии активно используются для отождествления личности преступников. Более 50 лет для оперативной идентификации личности органами внутренних дел используются субъективные портреты – средство материализации мысленных образов в виде графического изображения, выступающих эффективным инструментом для розыска преступников и идентификации неопознанных трупов. Субъективные портреты в настоящее время активно составляются и используются в ходе расследования преступлений в тех случаях, когда очевидцы запомнили внешний вид преступника. Однако, как показывает практика, существует проблема достоверности отображаемой в субъективных портретах информации, зависящей от профессиональных навыков составителя и имеющихся у него в наличии технических средств. Повысить эффективность применения фотороботов, как отмечает А. М. Зинин, можно за счет привлечения к их составлению профессиональных художников и разработки системы их подготовки, применяемой в ряде стран [4, с. 87–88].

Перспективным вектором развития габитоскопии выступает разработка и внедрение автоматизированных систем идентификации лиц по внешнему облику, интегрированных в системы видеонаблюдения. Последние годы многие развитые страны активно развивают системы видеонаблюдения и распознавания лиц в целях предупреждения, раскрытия и расследования преступлений.

В настоящее время комплексы видеонаблюдения и идентификационные системы по внешнему облику эффективны в основном на общественном транспорте, где есть возможность установки камер в благоприятных местах для качественной фиксации изображения лиц. Так биометрическая

система распознавания лиц «Сфера», оборудованная в столичном метрополитене с 2019 года, за период с сентября 2020 года по декабрь 2022 год позволила идентифицировать около 5 тысяч человек, находящихся в розыске [5].

Эффективному повсеместному использованию систем автоматической идентификации лиц по внешнему облику в России препятствует ряд факторов. Во-первых, разрешение большинства распространенных камер видеонаблюдения накладывает определенные требования на места их установки. Для успешной работы идентификационной системы необходимы определенные ракурсы и расстояние от камеры до объекта фиксации. Как показывает практика, отечественные системы распознавания лиц успешно работают в общественном транспорте, где есть возможность установки камер в благоприятных местах для качественной фиксации изображения лиц. Во-вторых, сложная эпидемиологическая обстановка в стране и мире обусловила активное использование медицинских масок, закрывающих большую часть лица, и, соответственно, затрудняющих эффективное распознавание лиц имеющимися средствами и методами идентификации. Аналогичные трудности вызывают и климатические особенности нашей страны, предопределяющие длительное сезонное использование элементов одежды, закрывающих часть лица и головы. Стоит отметить и современные тенденции на ношение объемной растительности на лице (усы, борода) среди мужчин, также препятствующих распознаванию.

Важное место в системе биометрических параметров, используемых в раскрытии и расследовании преступлений, занимает структура ДНК. Биологические следы традиционно выступали источником криминалистически значимой информации, однако до определенного момента использовались лишь для диагностических целей и установления групповой принадлежности объекта, от которого они произошли

В нашей стране инструментом автоматизированной идентификации личности на основе геномной информации выступает автоматизированная информационная система «Ксенон-2», состоящая на вооружении экспертно-криминалистических подразделений МВД России. Источником геномной информации, содержащейся в базе данной системы, является биологический материал, изъятый с мест происшествий по нераскрытым преступлениям, и образцы биологического происхождения лиц, поставленных на учет геномной информации.

АИС «Ксенон-2» предназначена для решения задач по установлению личности лиц, оставивших биологические следы на месте происшествия; установлению факта оставления биологических следов на разных местах происшествия одним лицом; идентификации личности неопознанных трупов. В настоящее время активно ведется работа по увеличению количества лабораторий, оснащенных данной системой, и формированию баз данных.

Таким образом, отмечаем, что в Российской Федерации ведется динамичная системная работа по повышению эффективности использования биометрических методов идентификации личности в деятельность правоохранительных органов по раскрытию и расследованию преступлений. Активно внедряются передовые зарубежные и отечественные разработки технических средств и методов биометрической идентификации. Вышесказанное предопределяет необходимость разработки и совершенствования правовых, организационных и методических аспектов применения биометрических методов в предупреждении, раскрытии и расследовании преступлений в рамках обособленного учения о криминалистической биометрии.

СПИСОК ЛИТЕРАТУРЫ

1. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений : монография / А. И. Иванов. – Пенза, 2000. – 186 с.
2. Барковская Е. Г. Криминалистика и биометрия: проблемы интеграции научного знания / Е. Г. Барковская // Философия права. – 2011. – №. 3. – С. 27–31.
3. Югай Л. Биометрическая идентификация как инновация в криминалистике / Л. Югай // Жамият ва инновациялар – Общество и инновации – Society and innovations Special Issue. – 2022. – № 7. – С. 238–248.
4. Зинин А. М. Габитоскопия: научные и практические проблемы / А. М. Зинин // Актуальные проблемы современной криминалистики : материалы Международной научно-практической конференции. Москва, 15 апреля 2016 г. – Москва : РУДН, 2016. – 272 с.
5. Около 5 тыс. человек задержали благодаря системе распознавания лиц в метро Москвы // Официальный сайт сетевого издания «Интерфакс.ру». – URL:<https://www.interfax.ru/moscow/878994> (дата обращения: 18.09.2024).

СВЕДЕНИЯ ОБ АВТОРЕ

Звягин Иван Сергеевич.
Доцент кафедры криминалистики.
Кандидат юридических наук.
Воронежский институт МВД России.
E-mail: patronzv@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Zvyagin Ivan Sergeevich.
Docent of the Department of Criminalistics.
PhD in Law.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: patronzv@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: биометрия; биометрическая идентификация личности; дактилоскопические методы; методы габитоскопии; криминалистическая идентификация.

Keywords: biometrics; biometric identity identification; fingerprinting methods; methods of habitoscopy; forensic identification.

УДК 343.98.065

С. С. Паутов

**ХАРАКТЕРИСТИКА ЛИЧНОСТИ ПРЕСТУПНИКА И ПОТЕРПЕВШЕГО
В РАМКАХ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА,
СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ
ИНТЕРНЕТ-СЕРВИСОВ РАЗМЕЩЕНИЯ ОБЪЯВЛЕНИЙ**

**CHARACTERISTICS OF THE PERSONALITY
OF THE CRIMINAL AND THE VICTIM
IN THE FRAMEWORK OF REMOTE FRAUD COMMITTED
USING INTERNET ADVERTISEMENT SERVICES**

В статье рассматривается криминалистическая характеристика преступника и потерпевшего в рамках дистанционного мошенничества, совершаемого с использованием интернет-сервисов размещения объявлений. Автор анализирует ключевые черты поведения и мотивации участников преступления, а также акцентирует внимание на возможностях использования этих данных для повышения эффективности раскрытия и расследования подобного рода преступлений.

The article examines the forensic characteristics of the criminal and the victim in the context of remote fraud committed using online services for posting advertisements. The author analyzes the key behavioral features and motivations of the participants in the crime, and also focuses on the possibilities of using this data to improve the efficiency of solving and investigating such crimes.

Современный мир характеризуется стремительным развитием и внедрением информационно-коммуникационных технологий (далее – ИКТ) во все сферы жизни общества. Электронные средства платежа, цифровые платформы и онлайн-сервисы становятся неотъемлемой частью повседневных операций, существенно упрощая процессы обмена товарами и услугами. Однако наряду с позитивными изменениями, этот процесс создает благоприятные условия для совершения преступлений, совершаемых с использованием ИКТ.

Так, количество зарегистрированных в 2023 году органами внутренних дел преступлений, совершаемых с использованием ИКТ возросло на 29,8% (с 515 021 до 668 719), на 26% (с 268 450 до 338 270) – тяжких и особо тяжких составов данных преступлений. Одной из основных проблем, во многом определяющих формирование криминогенной ситуации в стране, продолжает оставаться являющиеся наиболее многочисленными дистанционные мошенничества и кражи (69,8%), которые демонстрируют устойчивый рост (+41,3% и +5%) [1].

Актуальность изучения личности преступника и потерпевшего в контексте дистанционного мошенничества, совершаемого с использованием интернет-сервисов размещения объявлений, обусловлена наглядным увеличением числа таких преступлений, а также высокой степенью анонимности и сложности их раскрытия.

Рассматривая личность преступника, необходимо понимать, что дистанционное мошенничество с использованием интернет-сервисов размещения объявлений имеет довольно разнообразный состав лиц, совершающих данные преступления, при этом они имеют разный уровень образования, социальный, служебный и материальный статусы. Так, например, мошенничество под предлогом продажи (покупки) товаров на таких интернет-ресурсах, как «Авито», «Юла» и т.п. в большинстве своем не требует определенных технических навыков. В свою очередь, злоумышленники, специализирующиеся на размещении объявлений на предварительно созданных «фишинговых» сайтах, нуждаются хотя бы в базовых профессиональных знаниях в области ИКТ или же должны иметь техническое образование [2].

Кроме того, большинство подобных преступников умеют оказывать сильное психологическое воздействие на жертв, применяя методы социальной инженерии в комбинации со знаниями в области ИКТ, воздействуют на эмоции, чувства и подсознание жертвы, впоследствии манипулируя их поведением.

Несомненно, как и все преступники, совершающие имущественные преступления, они имеют корыстный мотив, однако их мотивы могут заключаться в желании противопоставив себя окружающим, тем самым самоутвердиться и повысить свою самооценку, но ненасильственным способом, а за счёт своих умственных способностей.

Так, в рабочей книге пенитенциарного психолога под редакцией А. И. Мокрецовой авторы говорят о том, что некоторые мошенники, которые чувствуют себя внутренне бедными, сколько бы денег не заработали преступным путём, им всегда будет мало. Мотивы корысти скорее являются второстепенными, поскольку их значимость состоит в материальной выгоде или же является своеобразным «выигрышем» (имеется в виду успешное совершение преступления) [3].

Так В. Б. Вехов справедливо систематизировал интернет-мошенников на три группы, выделяя в них:

- лиц, которые отличаются профессиональными навыками в сфере компьютерной техники и являются в какой-то степени фанатиками собственной изобретательности;

- лиц, которые имеют психические отклонения из-за компьютерных фобий или же информационных болезней;

- профессиональных мошенников в сети Интернет, деятельность и мотивы которых направлены на извлечение прибыли, то есть это является их основным источником дохода [4, с. 162].

Анализ практики расследования, изучение уголовных дел о мошенничествах, совершаемых с использованием интернет-сервисов размещения объявлений, а также опрос сотрудников Главного следственного управления Главного управления МВД России по Воронежской области показал основные характеристики личности преступника и потерпевшего в рамках дистанционного мошенничества, совершаемого с использованием интернет-сервисов размещения объявлений.

Так, наиболее многочисленной возрастной группой среди обвиняемых в совершении данной категории преступлений являются лица в возрасте от 18 до 35 лет, обладающие высокими знаниями в области ИКТ, а также способами и приемами методов социальной инженерии, что позволяет им с легкостью вводить жертву в заблуждение, скрывать следы своей преступной деятельности и постоянно совершенствовать свои преступные схемы, в зависимости от конкретных ситуаций.

Что касается основных личностных характеристик потерпевших по данной категории преступлений, можно выделить – доверчивость, честность, добросовестность и открытость. При этом, в большинстве случаев явно прослеживается желание получить выгоду, неосведомленность о действующем законодательстве и рисках, связанных с совершением сделок через Интернет, недостаток опыта и информации о современных схемах и способах обмана, а также пренебрежение мерами безопасности в кибернетическом пространстве.

Изучая личности жертв дистанционного мошенничества, особое внимание следует обратить на такие факторы, как пол, возраст, уровень образования и род занятий. Анализ следственной практики свидетельствует о том, что подавляющее большинство жертв мошенничества – женщины, возраст которых в среднем варьируется от 25 до 44. Данный факт можно объяснить тем, что женщины более эмоциональны, часто полагаются на свои чувства и ощущения, тогда как мужчины больше обращают внимание на рациональную сторону дела. Однако необходимо учитывать, что не каждый мужчина готов признать себя пострадавшим от дистанционного мошенничества и обратиться в правоохранительные органы с заявлением.

Безусловно, характеристика личности потерпевшего может варьироваться в зависимости от конкретной ситуации и мошеннической схемы, используемой мошенниками [5, с. 65–70].

В заключение можно сделать вывод о том, что анализ характеристик личности преступника и потерпевшего в рамках дистанционного мошен-

ничества, совершаемого с использованием интернет-сервисов размещения объявлений, понимание их психологии и мотивации позволит органу расследования не только выявить некоторые закономерности преступного поведения мошенников, но и определить типичные уязвимости потерпевших, тем самым способствуя эффективному противодействию такого рода преступлениям.

СПИСОК ЛИТЕРАТУРЫ

1. Сборник ФКУ «Главный информационно-аналитический центр МВД России» «О состоянии преступности в Российской Федерации за январь-декабрь 2023 года. – URL: <https://мвд.рф/reports/item/47055751/> (дата обращения 21.06.2024).
2. Аксенов В. А. Особенности личности современного интернет-мошенника в механизме индивидуального преступного поведения / В. А. Аксенов, Т. В. Молчанова // Криминологический журнал, 2020. – № 4. – С. 82.
3. Мокрецова А. И Рабочая книга пенитенциарного психолога / под ред. А. И. Мокрецовой, В. П. Голубевой, А. В. Шамиса. – Москва, 1998.
4. Вехов В. Б. Компьютерные преступления: способы совершения, методики расследования / под ред. Б. П. Смагоринского. – Москва : Закон и право, 1996. С. 182.
5. Васильев, К. В. Криминологическая характеристика жертв дистанционного мошенничества / К. В. Васильев, К. В. Зубанова // Актуальные научные исследования в современном мире. – 2021. – № 12-5(80).

СВЕДЕНИЯ ОБ АВТОРЕ

Паутов Сергей Сергеевич.
Преподаватель кафедры криминалистики.
Воронежский институт МВД России.
E-mail: pautov-mvd@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Pautov Sergey Sergeevich.
Lecturer at the Department of Criminalistics.
Voronezh Institute of the Ministry of Internal Affairs of the Russian.
E-mail: pautov-mvd@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: преступник; потерпевший; личность; характеристика; анализ; мошенничество.

Keywords: criminal; victim; personality; characteristics; analysis; fraud.

УДК 343.9

ЦИФРОВЫЕ СЛЕДЫ В РАССЛЕДОВАНИИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

DIGITAL FOOTPRINTS IN THE INVESTIGATION OF TELEPHONE FRAUD

В статье представлен анализ механизма следообразования и цифровых следов, при совершении мошеннических действий с использованием телефонии.

The article presents an analysis of the mechanism of trace formation and digital traces when committing fraudulent actions using telephony.

Механизм следообразования при совершении мошеннических действий с использованием телефонии обладает своими специфическими признаками, поскольку деяние совершается удаленно. В подобной ситуации следователь должен исследовать не только традиционные материальные, но и электронно-цифровые следы. Ему необходимо обнаружить и исследовать следы, находящиеся во внутренней памяти устройства, а также те, которые остались в информационной системе оператора сотовой связи. Электронно-цифровые следы образуются при любом способе телефонного мошенничества. Исходя из этой информации отметим, что прежде всего нужно обращать внимание не внешнюю форму телефона, а на его внутреннее содержание. При этом целесообразно привлекать к сотрудничеству соответствующих специалистов [1].

Дистанционное мошенничество необходимо рассматривать как факт активного применения информационно-телекоммуникационных технологий при осуществлении хищения денежных средств обманным путем. Оно предполагает значительную трансформацию механизма классического типа преступления из-за отсутствия прямого контакта жертвы с преступником. По статистике по большей части уголовных дел по подобным фактам предварительное расследование приостанавливается, поскольку невозможно установить лицо, которое должно быть привлечено к ответственности в качестве обвиняемого. Раскрываемость мошенничеств, совершаемых с использованием телефонии, по-прежнему остается низкой [2].

Из практики раскрытия уголовных дел данной категории следует, что среди проблем, которые негативно влияют на эффективность обнаружения и установления преступников, выделяется вопрос выявления тех пользователей, которые используют информационно-телекоммуникационное оборудование. Получить криминалистически важные сведения почти невозможно из-за доминирования иностранных программных и аппаратных

средств, подменных IP-адресов, элементной базы, ресурсов, серверов, средств сокрытия личных данных пользователей в сети Интернет и др. [3]

Самые известные способы дистанционного мошенничества включают в себя различные действия. Например, преступники внедряют вредоносные программы в систему удаленного банковского обслуживания, выставляют поддельные РОБ-терминалы, совершают атаки в сети Интернет на банковские и брокерские системы и различные мобильные устройства, незаконно используют электронную цифровую подпись, применяют способы социальной инженерии (телефонный фрикинг, фишинг, «дорожное яблоко» и т.д.). В результате этих действий жертвы сами предоставляют конфиденциальную информацию (например, реквизиты карт), которая позволяет преступникам совершать хищение денежных средств.

Механизм образования следов телефонного мошенничества специфичен, в первую очередь из-за особенностей способов его совершения. Одни предполагают, например, замену адреса пользователя в сети Интернет, используются технологии «подменных» номеров с помощью IP-телефонии. Для такого способа характерно преобладание цифровых следов. Не подлежит сомнению тот факт, что использование цифровых следов в расследовании является весьма важным моментом.

Ученые криминалисты под цифровым следом понимают криминалистически важную информацию о действиях или событиях, которые отражены в материальной среде в процессе ее возникновения, обработки, хранения и передачи [4].

В. Б. Вехов отмечает, что при формировании следов, которые образуются при использовании компьютерной информации, на материальном носителе фиксируются не свойства физического процесса, а цифровые значения настроек математической модели, которая лежит в основе технического устройства регистрации его реального проявления. Помимо этого, стоит знать следующее. В цифровом или электронном следах может быть большое число отдельных элементов. Их могут записать на одном или нескольких электронных носителях, которые могут быть подключены к одному или нескольким компьютерам. Они в свою очередь объединены в информационно-телекоммуникационную сеть или информационную систему [5].

При расследовании фактов телефонных мошенничеств реализуются действия, которые направлены на обнаружение, фиксацию и изъятие цифровых следов, как в памяти компьютеров или мобильных устройств, так и линиях связи, а также на электронных носителях информации различных типов. Цифровые следы весьма специфичны, обладают отличительными свойствами: высокой скоростью изменения, легкостью уничтожения, быстротой распространения и доступностью. Стоит учесть, что локализируются эти следы не только в определенном одном месте (например, там, где находится преступник), а и на объектах, находящихся на всем пути про-

хождения сигнала (информационного взаимодействия). Это дает возможность выявлять данные следы несмотря на то, что их выявление довольно сложная задача. Фиксация осуществляется незамедлительно, в связи с высокой вероятностью их утраты. Сложность работы с подобными следами очевидна, предполагает специальную подготовку субъектов их обнаружения и исследования [6].

Недостаточный объем знаний оперативного работника или следователя в сфере высоких технологий не позволяет им эффективно, грамотно и самостоятельно работать с ними, требуется привлечение соответствующего специалиста. Но у следователя зачастую возникают сложности с выбором грамотного специалиста и определением его профессионализма. Важен тот факт, что известные на сегодняшний день критерии выявления компетенции недостаточно разработаны. Это сковывает правоохранителей в их действиях.

Е. Р. Россинская полагает, что необходимо расширить информационно-компьютерную составляющую в подготовке дознавателей и следователей. Сделать это можно, организовав курсы при основной образовательной программе. Второй вариант может предполагать повышение квалификации или профессиональную переподготовку в сфере расследования преступлений, которые сопряжены с привлечением компьютерных систем и средств [7].

По нашему мнению, это хорошо, но эти меры не убирают проблему недостатка в нужном количестве специалистов, которые обладали бы знаниями в сфере информационно-компьютерных технологий. Без участия таких сотрудников в подготовке и проведении следственных действий не получится грамотно определить важность цифровых следов и принять достаточные меры по их сохранности, а также изъять электронные носители данных в соответствии со статьей 164.1 УПК РФ. Специалист обязан разбираться в механизме следообразования в различных информационных системах, при действиях с файлами, в каждой операционной системе. Также необходимо уметь обращаться и грамотно применять современные компьютерно-технические средства. Немаловажным будет наличие опыта оценки и сравнения следов с предполагаемыми мошенническими действиями преступников, которые оставили эти следы [3, С. 20].

А. И. Семикаленова и И. А. Рядовский считают, для того чтобы произвести мероприятия, главная цель которых заключается в поиске и фиксации цифровых следов, необходимо привлекать к сотрудничеству специалистов широкой области познаний. В их сферу компетенции должно входить знание программирования, компьютерных устройств, эксплуатации сетевой инфраструктуры и т.д. Также можно сотрудничать сразу с несколькими экспертами, которые обладают углубленными познаниями в конкретных областях [8]. Соответственно, от следователя при обращении к таким специалистам требуется понимание того, по каким параметрам можно судить об их компетенции, какими знаниями и методиками они должны

владеть, насколько хорошо разбираются с техническими средствами для принятия всех необходимых мер по обнаружению важной информации для следствия.

Практика показывает, что при выборе специалиста недостаточно определить его компетентность, подтверждаемую документально (диплом о соответствующем образовании). Зачастую имеющаяся квалификация специалиста не всегда соответствует документам, которые он представляет. Считаем важным нормативно регламентировать компетенцию специалиста, его инструментарий, необходимый для обнаружения, фиксации и изъятия следов.

Чтобы обеспечить эффективность расследования телефонного мошенничества, которое предполагает образование достаточного количества электронно-цифровых следов, нужно понимать, что исследовать их можно лишь при использовании специальных средств и методов. В подобных ситуациях назначаются соответствующие компьютерные экспертизы.

Некоторые ученые высказывают мнение о возможности создания криминалистических учетов электронно-цифровых следов мобильных устройств, с последующей возможностью их идентификации. Вопрос о сборе, анализе и хранении цифровых следов в данном контексте весьма перспективен, так как любое устройство можно распознать по десяткам признаков, поэтому определить конкретный гаджет можно с высокой точностью [9].

Действующая подсистема «Дистанционное мошенничество» в настоящее время обеспечивает деятельность правоохранительных органов по раскрытию и расследованию рассматриваемого вида преступлений. Сбор и систематизация сведений аккумулируются и проверяются в режиме автоматизации информации, которая характеризует механизм образования следов. Системой проверяются: номера электронных кошельков и банковских карт, которые были использованы в момент преступления; данные ресурсов сети Интернет (адрес электронной почты, доменное имя сайта и пр.), которые были использованы мошенниками; идентификационные данные средств связи (IMSI и IMEI), которые были использованы при совершении деяния.

Как правило, чаще всего цифровые следы обнаруживают при осмотре, обыске, выемке и в ходе оперативно-розыскных действий. Результатом тщательной подготовки к процессу проведения следственных и оперативно-розыскных действий выступает эффективность обнаружения следов преступления. При этом учитывается специфичность преступления, которое совершено с помощью мобильного устройства или компьютерного оборудования; необходимость предварительного инструктажа сотрудников следственно-оперативной группы; слаженность совместной работы специалистов различного профиля; необходимость соблюдения мер предосторожности, которые обеспечивают сохранность следов.

СПИСОК ЛИТЕРАТУРЫ

1. Файзерахманова Н. Р. Некоторые аспекты криминалистической характеристики мошенничеств, совершаемых с использованием средств сотовой связи / Н. Р. Файзерахманова // Студенческие южноуральские криминалистические чтения : Сборник материалов Всероссийской научно-практической конференции, Уфа, 14 декабря 2020 года / Отв. редактор И. А. Макаренко. – Уфа : Башкирский государственный университет, 2020. – С. 8992.
2. В России число совершенных через мобильную связь и интернет преступлений выросло. – URL: <https://tass.ru/obschestvo/18417795>.
3. Давыдов В. О. Цифровые следы в расследовании дистанционного мошенничества / В. О. Давыдов, И. В. Тишутина // Известия ТулГУ. Экономические и юридические науки. – 2020. – № 3. – С. 38.
4. Россинская Е. Р. Концепция цифровых следов в криминалистике / Е. Р. Россинская, И. А. Рядовский // Аубакировские чтения : материалы Международной научно-практической конференции (19 февраля 2019 г.). – Алматы. – 2019. – С. 6–9.
5. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств её обработки / В. Б. Вехов. – Волгоград : Волгоградская академия МВД России, 2008. – С. 86.
6. Основы теории электронных доказательств : монография / под ред. С. В. Зуева. – Москва : Юрлитинформ, 2019. – С. 87.
7. Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации / Е. Р. Россинская // Вестник университета имени О. Е. Кутафина (МГЮА). – 2019. – № 5. – С. 35–36.
8. Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов : анализ современной практики / А. И. Семикаленова, И. А. Рядовский // Актуальные проблемы российского права. – 2019. – № 6 (103). – С. 182.
9. Сидоренко Е. По цифровым следам : в РФ раскрывается лишь четверть киберпреступлений / Е. Сидоренко // Известия. – URL: <https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rfraskrvvaetsialish-chetvert-kiberprestuplenii>.

СВЕДЕНИЯ ОБ АВТОРЕ

Пидусов Евгений Александрович.
Начальник кафедры криминалистики.
Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: pidusovea@vimvd.ru

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

Pidusov Evgeny Alexandrovich.

Head of the Department of Criminology.

Candidate of Law, Associate Professor.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: pidusovea@vimvd.ru

Russia. 394065, Voronezh, Prospect Patriotov, 53

Ключевые слова: телефонное мошенничество; цифровые следы; механизм следообразования; расследование.

Keywords: telephone fraud; digital footprints; the mechanism of trace formation; investigation.

УДК 67.99

Е. И. Пырьева, А. Е. Беляева

**МЕХАНИЗМ СЛЕДООБРАЗОВАНИЯ
ПРИ СОВЕРШЕНИИ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ
МОБИЛЬНЫХ СРЕДСТВ СОТОВОЙ СВЯЗИ**

**THE MECHANISM OF TRACE FORMATION IN THE COMMISSION
OF FRAUD USING MOBILE CELLULAR COMMUNICATIONS**

В данной статье выявлена специфика механизма следообразования при совершении преступления с использованием мобильных средств сотовой связи, а также рассмотрены некоторые способы совершения мошенничества с их использованием.

This article reveals the specifics of the mechanism of trace formation when committing a crime using mobile cellular communications, are also discusses some ways of committing fraud using them.

Мобильные средства сотовой связи стали важной составляющей нашей жизни. В настоящее время в России насчитывается около 260 млн пользователей сотовой связи. Если брать во внимание тот факт, что один человек может использовать несколько сотовых устройств, то проникновение сотовой связи к населению страны составило 152,5%. [1]

К сожалению, мобильные устройства имеют уязвимые места, чем и пользуются мошенники. Каждое третье преступление в 2023 году совершено с использованием информационно-телекоммуникационных технологий, о чем говорят статистические сведения о состоянии преступности,

предоставленные МВД России. Число таких преступлений выросло на 29,7% по сравнению с предыдущим 2022 годом.[2]

Каждый человек может стать жертвой мошенничества с использованием средств сотовой связи. Одной из особенностей является то, что жертва и преступник в момент совершения преступления находятся друг от друга на расстоянии и контактируют только посредством сотовой связи. Способов и схем совершения таких преступлений огромное множество, и постоянно появляются новые и новые, так как развитие технологий не стоит на месте. Это значительно затрудняет их раскрытие, так как некоторые методы расследования перестают быть актуальными, а на выработку новых приемов необходимо время.

В таких условиях возрастает актуальность проблемы эффективного расследования мошенничества с использованием средств сотовой связи. Важную роль в данном вопросе играет изучение механизма следообразования при совершении преступных действий.

Под механизмом следообразования следует понимать взаимодействие материальных объектов, завершающееся появлением следовотображений, содержащих криминалистически значимую информацию о событии преступления и его участниках. [3]

К отличительным чертам механизма следообразования при совершении преступлений с использованием средств сотовой связи можно отнести то, что значительный объем следовой информации мошенники оставляют при производстве звонков или отправке SMS. Следовая картина представлена не только материальными, идеальными, но и электронно-цифровыми следами. Сложность при выявлении электронно-цифровых следов служит одной из причин низкой раскрываемости преступлений, совершенных с использованием средств сотовой связи.

Особенности механизма следообразования обусловлены большими функциональными возможностями мобильных средств сотовой связи. На механизм следообразования влияет структура самой системы организации сотовой связи, в которую входит аппаратно-технические средства, средства вспомогательной поддержки и средства информационной поддержки.

Следует выделить несколько групп следов, образуемых при совершении исследуемых преступлений:

1. Материальные следы.

Особенностью преступлений, совершенных с использованием мобильных средств сотовой связи, является то, что материальных следов практически не образуется и чаще всего они не играют ключевую роль при расследовании. Это объясняется способами совершения преступных действий. Материальными следами в данном случае могут послужить банковские чеки, квитанции, а также оставляемые на них следы пальцев рук.

2. Электронно-цифровые следы.

По нашему глубокому убеждению, соглашаясь с мнением А. А. Жижилевой, электронно-цифровые следы – это совокупность элементов отображения события преступления в виртуальном пространстве в связи с созданием, удалением, копированием и другими действиями в отношении информации на электронных (компьютерных) устройствах, в электронных кошельках, облачных хранилищах и т.п. [4] Примерами электронно-цифровых следов могут служить данные о соединениях абонентов, о местонахождении абонента, информация о датах и длительности сеансов связи.

3. Следы, которые мошенники оставляют непосредственно на мобильных средствах сотовой связи. К ним можно отнести журнал вызовов, SMS, а также данные из мессенджеров (WhatsApp, Telegram и др.).

4. Идеальные следы.

При расследовании исследуемого вида преступлений зачастую они не играют большую роль, но могут предоставить какие-либо уточняющие детали. Примерами таких следов будут являться сохранившаяся в памяти жертвы информация об особых приметах внешности мошенника, об особенностях речи и голоса, о государственном регистрационном номере автомобиля мошенника и т.д.

Механизм слеодообразования будет иметь различные особенности исходя из способов совершения мошенничества. Рассмотрим непосредственно процесс передачи денег жертвой с использованием мобильных средств сотовой связи.

Первый способ предполагает непосредственную передачу денежных средств. В данном случае наиболее важную роль будут играть идеальные следы: информация об особых приметах, признаках одежды, манере речи. Кроме того, могут оставаться и материальные следы в виде следов обуви, пальцев рук.

Второй способ передачи денежных средств представляет собой передачу денежных средств в виде зачисления на счет мобильного телефона или перечисления банковским переводом.

Основными следами являются:

- электронно-цифровые следы в виде информации в мобильных телефонах мошенников и жертвы мошенничества; записи с камер системы видеонаблюдения в отделении банка, где был осуществлен перевод денежных средств;

- материальные следы – в виде документов, справок, квитанций, подтверждающих передачу и получение денежных средств;

- идеальные следы – в виде показаний свидетелей и жертвы мошенничества.

Рассмотрим подробнее электронно-цифровые следы, которые играют ключевую роль в расследовании исследуемого вида преступлений.

Они являются основными при совершении мошенничества с использованием средств сотовой связи. Их отличительной чертой является то, что

они остаются вне воли и желания человека, так как это происходит автоматически. Преступник может даже не подозревать об их существовании.

Электронно-цифровые следы можно также разделить на виды:

- информация, оставленная пользователями при использовании Интернета: история поиска, файлы cookie, IP-адреса и прочие;
- сообщения, отправленные на электронную почту, в мессенджерах;
- история вызовов, входящие и исходящие SMS;
- файлы, журналы, кэш и другие системные файлы;
- данные о соединениях абонентов, о местонахождении абонента;
- следы использования мобильных устройств: фотографии, аудиозаписи, открытые приложения и программы.

Одной из особенностей образования цифровых следов является то, что они возникают на различных уровнях системы: как на уровне аппаратного обеспечения, так и в приложениях и соцсетях. Кроме того, такие следы остаются не только на самом устройстве, но и в информационной системе сотового оператора. Следовательно, удалив на телефоне историю вызовов, он не стер ее совсем. Следователь может получить информацию о соединениях, отправив запрос сотовому оператору.

Также стоит отметить динамичность электронных следов. Они могут появляться, изменяться, исчезать в ходе использования устройства, а также посредством удаленного доступа к устройству.

Электронно-цифровые следы так же, как и материальные, могут попытаться скрыть. Это можно сделать, удалив файлы с устройства, очистив историю вызовов, отключив телефон или выбросив SIM-карту, с которой мошенник осуществлял звонки. Но особенность таких следов как раз в том, что не всегда попытки скрыть следы оказываются удачными, так как они остаются не только в истории вызовов, поиска и т.д., но и в самой системе, и после удаления никуда не исчезают с устройства. Специалист или эксперт, обладая специальными навыками, способны восстановить даже удаленные файлы, тем самым обнаружив следы преступления.

В заключение следует отметить, что мошенничество с использованием мобильных средств сотовой связи в современном мире совершается различными способами, как давно известными, так и новыми, появление которых связано со стремительным развитием новых технологий. Изучение механизма следообразования при совершении данного вида преступлений является одним из необходимых элементов совершенствования методики и повышения эффективности расследования.

СПИСОК ЛИТЕРАТУРЫ

1. 2024: В Минцифры назвали число пользователей мобильного интернета в России/. – URL: [https://www.tadviser.ru/index.php/Статья:Мобильный_трафик_%28российский_рынок_\(дата_обращения:_20.09.2024\)\)](https://www.tadviser.ru/index.php/Статья:Мобильный_трафик_%28российский_рынок_(дата_обращения:_20.09.2024)))
2. Статистические сведения о состоянии преступности в 2023 году. – URL:

<https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2023-godu/> (дата обращения: 20.09.2024)

3. Организация расследования хищений денежных средств, совершаемых с использованием компьютерных технологий : учебно-практическое пособие / под общ. ред. А. В. Шмолина. – Москва : Академия управления МВД России, 2018. – С. 195.

4. Жижилева А.А. О некоторых теоретических аспектах использования в криминалистике понятий цифровые, электронные, виртуальные следы // Вопросы российской юстиции. – Екатеринбург : ФГБОУВО «Уральский государственный юридический университет, 2019. – № 3. – С. 916.

СВЕДЕНИЯ ОБ АВТОРАХ

Пырьева Елена Ивановна.

Доцент кафедры криминалистики.

Кандидат юридических наук, доцент.

Воронежский институт МВД России.

E-mail: elena.pyreva@yandex.ru

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

Беляева Анастасия Евгеньевна.

Курсант Ю220 учебного взвода юридического факультета.

Воронежский институт МВД России.

E-mail: anastasiabel0401@gmail.com

Россия, 394065, г. Воронеж, пр-т Патриотов, д. 53.

Pyreva Helena Ivanovna.

Associate Professor, of the chair of Crimin.

Candidate of Law Sciences, Associate Professor.

Voronezh Institute the Ministry of the Interior of Russian.

E-mail: elena.pyreva@yandex.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Belyaeva Anastasia Evgenevna.

Cadet Yu220 training platoon of the law faculty.

Voronezh Institute of the Russian Ministry of Internal Affairs.

E-mail: anastasiabel0401@gmail.com

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: мошенничество; электронно-цифровые следы; следообразование; мобильная связь; идеальные следы.

Keywords: fraud; digital footprints; trail formation; mobile communications; perfect footprints.

УДК 343.98

ВСЕРОССИЙСКИЙ КРУГЛЫЙ СТОЛ
ПРОБЛЕМЫ АДАПТАЦИИ СОТРУДНИКОВ
ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ
НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ
И ПУТИ ИХ РЕШЕНИЯ

А. И. Алимова

НЕКОТОРЫЕ ВОПРОСЫ ВЗАИМОДЕЙСТВИЯ
ОРГАНОВ ПРОФИЛАКТИКИ С СОТРУДНИКАМИ
ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ

SOME ISSUES OF INTERACTION
BETWEEN PREVENTION AGENCIES
AND EMPLOYEES OF JUVENILE AFFAIRS UNITS

Полиция России занимается рядом сложных и многогранных задач, за которыми стоит большой опыт выполнения, многолетнее реформирование, стандарты и регламентация деятельности всех подразделений. Особую роль сотрудники играют в воспитании несовершеннолетних и в предупреждении совершения ими противоправных действий. Успешность и эффективность данного направления зависит и от отношений с государственными и муниципальными органами, где требуется комплексный подход, объединение усилий всех субъектов, превентивная работа на всех этапах взаимодействия.

The Russian police are engaged in a number of complex and multifaceted tasks, behind which there is extensive experience in implementation, many years of reform, standards and regulation of the activities of all departments. Employees play a special role in the education of minors and in preventing them from committing illegal acts. The success and effectiveness of this area also depends on relations with state and municipal authorities, which require a comprehensive approach, the unification of efforts of all entities, and preventive work at all stages of interaction.

На сегодняшний день органы внутренних дел Российской Федерации выполняют множество функций по предотвращению и снижению количества правонарушений, совершаемых несовершеннолетними. В частности, в своей деятельности с данной категорией лиц сталкиваются подразделения по делам несовершеннолетних (далее – ПНД). Однако для пресечения правонарушений, недостаточно применение только мер административного или уголовного характера. В современных условиях необходимо взаимодействие и с иными субъектами профилактики. Одно из главных направлений, которое отображает процессы взаимодействия различных объектов друг на друга – их взаимосвязь и взаимное влияние.

Профилактические мероприятия в сфере правонарушений и безнадзорности несовершеннолетних осуществляют органы и учреждения системы профилактики, в том числе службы и подразделения органов внутренних дел. Стоит отметить важность реализации социальных, правовых мер, осуществляемых сотрудниками ПДН по отношению к несовершеннолетним лицам.

Для эффективной работы инспекторов по делам несовершеннолетних с другими субъектами профилактики важно установить четкие механизмы взаимодействия и координации. Необходимо разработать план совместных мероприятий, определить роли и полномочия каждого участника, а также обеспечить обмен информацией и согласование действий. С помощью успешного взаимодействия между инспекторами и другими субъектами профилактики можно предотвратить правонарушения несовершеннолетних и осуществить защиту их прав.

Следует отметить нормативную правовую базу, регулирующую данную сферу правоотношений, среди которых:

- Конституция Российской Федерации, где в ст. 38 содержатся положения о защите государством семьи, материнства и детства, о заботе и воспитании детей;
- Федеральный закон «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» от 24 июня 1999 г. № 120-ФЗ;
- Федеральный закон «Об опеке и попечительстве» от 24 апреля 2008 г. № 48-ФЗ;
- Постановление Правительства Российской Федерации от 6 ноября 2013 г. № 995 «Об утверждении Примерного положения о комиссиях по делам несовершеннолетних и защите их прав»;
- законы субъектов о комиссиях по делам несовершеннолетних и защите их прав.

В ст. 4 Федерального закона «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» от 24.06.1999 г. № 120-ФЗ (далее – Закон) раскрывается перечень многочисленных органов и учреждений, которые осуществляют процесс профилактики правонарушений среди несовершеннолетних, а именно комиссии по делам несовершеннолетних и защите их прав, органы управления социальной защитой населения, федеральные органы государственной власти и органы государственной власти субъектов Российской Федерации, осуществляющие государственное управление в сфере образования, органы местного самоуправления, осуществляющие управление в сфере образования, органы опеки и попечительства, органы по делам молодежи, органы управления здравоохранением, органы службы занятости, органы внутренних дел, учреждения уголовно-исполнительной системы.

Взаимодействие комиссий по делам несовершеннолетних и защите их прав (далее – КДН и ЗП) с подразделениями по делам несовершеннолетних (далее – ПДН) и образовательными организациями заключается в

совместной деятельности. Данная деятельность направлена прежде всего на эффективное использование всех полномочий при выполнении задач, а также координирование всех направлений в целях предотвращения семейного неблагополучия.

Акцентируя внимание на взаимодействии субъектов системы профилактики, можно отметить:

- постоянное взаимодействие, которое выражается в непрерывном взаимодействии между различными органами, учреждениями и отдельными работниками, осуществляемое на протяжении всего периода выполнения ими своих функций;
- временное взаимодействие – характерно для организаций и органов, объединяющих свои силы для решения конкретных задач, в последующем прекращается.

Существует множество видов взаимодействия, которые включают в себя внешнее и внутреннее взаимодействие, непосредственное и опосредованное, а также вертикальный вид взаимодействия, который подразумевает взаимодействие между субъектами профилактики, находящимися на одном уровне с ними.

Взаимодействие всех вышеперечисленных органов системы профилактики согласно законодательству направлено на:

- 1) совместную информационно-аналитическую деятельность;
- 2) обследование условий жизни несовершеннолетних;
- 3) изучение личности несовершеннолетних;
- 4) обмен информацией.

В настоящее время в случае объединения усилий всех субъектов профилактики можно добиться максимального результата в предупреждении противоправного поведения несовершеннолетних. Необходима совместная работа сотрудников подразделений по делам несовершеннолетних, социальных педагогов, психологов, родителей по укреплению семейных, патриотических, нравственных, религиозных ориентиров у несовершеннолетних лиц.

Однако в рамках взаимодействия у органов и учреждений профилактики возникают трудности. В частности, существуют проблемы взаимодействия с комиссиями по делам несовершеннолетних и защите их прав при рассмотрении административных материалов по привлечению к ответственности несовершеннолетних, достигших возраста административной ответственности, которые распивали спиртные напитки дома, пользуясь отсутствием контроля со стороны родителей. Также к существующим проблемам следует отнести тот факт, что члены КДН и ЗП часто не имеют юридического образования, что влияет на грамотную квалификацию совершенного деяния. Количество лиц, которые присутствуют при рассмотрении дел об административных правонарушениях, законодательно не закреплено.

Стоит отметить проблемные моменты во взаимодействии, возникающие между сотрудниками ПДН и органами опеки и попечительства. На сегодняшний день актуальным остается вопрос, связанный с процедурой изъятия несовершеннолетнего из семьи. Согласно действующему законодательству, основанием для изъятия ребенка из семьи является решение (распоряжение) органа местного самоуправления, в котором говорится о том, что несовершеннолетний находится в крайне опасном для его здоровья и жизни положении, а также указ о немедленном отобрании ребенка у родителей или лиц, их заменяющих. Также в практической деятельности органов опеки и попечительства возникают трудности по установлению места нахождения законных представителей несовершеннолетних.

В рамках решаемых задач сотрудники ПДН взаимодействуют с другими органами и учреждениями профилактики, среди которых Центр временного содержания для несовершеннолетних правонарушителей (далее – ЦВСНП). Немаловажным является вопрос помещения несовершеннолетних, совершивших правонарушение, преступление, а также оставшихся без попечения родителей, личные данные которых, не известны.

Согласно Приказу МВД от 27 ноября 2023 года № 908 «Наставление по организации деятельности Центров временного содержания для несовершеннолетних правонарушителей органов внутренних дел» при доставлении в ЦВСНП несовершеннолетнего, личность которого не установлена, должностные лица ЦВСНП изучают обстоятельства его задержания, выясняют сведения, имеющие значение для установления личности; составляют описание внешности по методу словесного портрета, а также одежды и других имеющихся у него вещей.

В Российской Федерации функционирует Правительственная комиссия по делам несовершеннолетних и защите их прав, являющаяся координирующим органом, созданным для того чтобы решать проблемы защиты законных интересов детей. Координирующая роль вышеуказанной комиссии дает возможность глубоко и всесторонне исследовать происходящие процессы, вовремя выявлять негативные тенденции и решать проблемы, которые касаются защиты прав и интересов несовершеннолетних.

Анализируя вышеуказанное, справедливо будет отметить, что в современных условиях в действующем законодательстве возросла необходимость внесения дополнений и конкретизации указанных проблем по вопросам взаимодействия всех субъектов профилактики. Для разрешения проблем в сфере безнадзорности и предупреждения административных правонарушений необходимо совместное осуществление деятельности вышеуказанных служб, с учетом соблюдения всех норм права, выработкой методик и четким разграничением полномочий.

СПИСОК ЛИТЕРАТУРЫ

1. Шароян Ю. К. Предупреждение и профилактика правонарушений несовершеннолетних силами ОВД: проблемы и перспективы / Ю. К. Шароян. – Текст : непосредственный // Молодой ученый. – 2020. – № 6 (296). – С. 154–158. – URL: <https://moluch.ru/archive/296/67220/> (дата обращения: 10.10.2024).

2. Балашова Т. Н. Формы межведомственного взаимодействия органов, осуществляющих профилактику и защиту прав несовершеннолетних, проживающих в семьях группы риска и семьях, находящихся в социально опасном положении / Т. Н. Балашова, М. С. Власенко // Закон и право. – 2020. – № 3. – С. 32-35. – DOI 10.24411/2073-3313-2020-10106. – EDN MUNSFL. (дата обращения: 10.10.2024).

3. Ергашева Е. Г. Развитие законодательства в сфере деятельности комиссий по делам несовершеннолетних и защите их прав / Е. Г. Ергашева // Вопросы российского и международного права. – 2023. – Т. 13, № 8-1. – С. 61–68. – DOI 10.34670/AR.2023.16.85.007. – EDN TIKLSA. (дата обращения: 10.10.2024).

СВЕДЕНИЯ ОБ АВТОРЕ

Алимова Алина Ильдусовна.

Преподаватель кафедры административно-правовых дисциплин.

Уфимский юридический институт МВД России.

E-mail: alina30.04.1989@mail.ru

Россия, 450103, Уфа, ул. Муксинова, 2.

Alimova Alina Ildusovna.

Lecturer of the Department of Administrative and Legal Disciplines.

Ufa Law Institute of the Ministry of Internal Affairs of Russia.

E-mail: alina30.04.1989@mail.ru

Russia, 450103, Ufa, Muksinova str., 2.

Ключевые слова: несовершеннолетние; взаимодействие; подразделения по делам несовершеннолетних; комиссия по делам несовершеннолетних.

Keywords: minors; interaction; juvenile affairs units; juvenile affairs commission.

УДК 342

**СУЩНОСТЬ И ОСОБЕННОСТИ
ПРОФЕССИОНАЛЬНОЙ ПОЗИЦИИ КУРСАНТОВ
ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ
НА СОВРЕМЕННЫХ ЭТАПАХ**

**THE SIGNIFICANCE AND FEATURES
OF THE PROFESSIONAL OF CADETS
OF EDUCATIONAL ORGANIZATIONS OF THE MINISTRY
OF INTERNAL AFFAIRS OF RUSSIA AT MODERN STRANGES**

Профессиональное образование в образовательных организациях Министерства внутренних дел Российской Федерации должно не только базироваться на идее по реализации специальной подготовки, но и решать задачи по формированию личности курсанта, учить его приёмам и особенностям современного социального взаимодействия, воспитывать в нём необходимые морально-нравственные качества, развивать у него способность оперативно оценивать содержание практических ситуаций и принимать по ним соответствующие решения. Важнейшей задачей развития профессионально значимых личностных качеств курсантов в процессе обучения в образовательных организациях МВД России является формирование профессиональной позиции.

Professional education in educational organizations of the Ministry of Internal Affairs of Russia should be based not only on the ideas of implementing special training, but also to solve the problems of forming the personality of the cadet, to teach him the techniques and features of modern social interaction, to bring up in him the necessary moral and ethical qualities, to develop his ability to promptly assess the content of practical situations and make appropriate decisions on them.

Современные модернизационные процессы носят характер стремительных и динамичных явлений, которые затрагивают все сферы жизнедеятельности социума. Основная их цель базируется на идее совершенствования текущих механизмов либо их кардинальных преобразований. Преследование данной цели упирается в решение проблемы по созданию оптимальных условий, которые отвечали бы требованиям, предъявляемым социумом и государством в настоящее время.

Сфера образования на сегодняшний день выступает актуальным пространством, в рамках которого происходят непрерывные процессы по реализации идей и теорий эффективного преобразования образовательной системы во всех его направлениях. Образовательный процесс в системе МВД России выступает одним из основных блоков, содержание которого представлено ак-

тивными дискуссиями о наиболее эффективных способах повышения качества получаемого образования. Профессиональное образование выступает фундаментальной основой действий субъекта на пути освоения желаемой профессии. Оно представляет собой совокупность необходимых знаний, умений и навыков, осваиваемых в рамках получения конкретного профессионального образования. Профессиональное образование наделяет субъекта образовательного процесса необходимой компетенцией, руководствуясь которой он способен реализовывать свое функциональное предназначение в рамках профессионального статуса.

То есть в рамках формирования профессиональной компетенции обеспечивается процесс становления профессиональной личности обучающегося. Иначе говоря, становление профессиональной личности субъекта обучения связан с процессом наделения его соответствующими качествами как будущего профессионала в сфере реализации предстоящей профессии.

Профессионализм обучающихся обеспечивается качественной подготовкой в стенах образовательной организации при наличии соответствующих условий: компетентный профессорско-преподавательский состав, качественная материально-техническая база, современные образовательные программы [6].

Так, в своих исследованиях С. Н. Тихомиров справедливо отмечает, что «сегодня наиболее остро стоит проблема профессионализации курсанта образовательной организации МВД России на этапе получения высшего образования, что в обязательном порядке предполагает помощь в усвоении специфики профессии, а также исправление профессионально-личностной ориентации» [5].

Сотруднику полиции важно уметь грамотно сочетать в себе такие профессиональные качества, которые обеспечивали бы реализацию умений по эффективному противодействию преступности, а также отражали бы его морально-нравственную установку в социальном взаимодействии с гражданами.

Анализ нормативно-правовых источников в области образовательного процесса в системе МВД России позволил определить, что деятельность сотрудников полиции имеет морально-нравственный характер, вне зависимости от специфики выполняемых сотрудниками полиции профессионально-служебных задач. Морально-нравственный облик сотрудника правоохранительных органов должен реализовываться на постоянной основе в процессе выполнения им своих обязанностей.

Так, данная обязанность санкционируется законодателем в п. 3 ст. 13 Федерального закона «О полиции» от 7 февраля 2011 года № 3-ФЗ, где зафиксировано, что сотрудник полиции «проявлять уважение, вежливость, тактичность по отношению к гражданам» [4].

Стоит отметить тот факт, что необходимость в формировании профессиональной позиции курсантов, сочетающей в себе профессионализм и

соответствующий морально-нравственный облик, важно обеспечивать уже на первых этапах их обучения.

Качественный процесс по формированию профессиональной позиции курсантов образовательных организаций МВД России будет возможен в рамках грамотного педагогического сопровождения. Деятельность преподавателей должна ложиться в основу решения данной задачи: её решение важно определить в качестве основы педагогического целеполагания, определяющего образовательный результат их деятельности. Реализация данного подхода позволит повысить качество профессионального воспитания и обучения курсантов.

Образовательный процесс в системе МВД России сопряжён с двумя механизмами, взаимодействие которых и ложится в основу формирования профессиональной позиции обучающихся. В качестве этих механизмов выступают процессы обучения и воспитания, ориентированные прежде всего на становление личности курсанта, соответствующее всем тем требованиям, которые предъявляется современному сотруднику полиции.

Более того физическая готовность и выносливость, которая базируется на началах профессионально-служебной дисциплины и самодисциплины, выработанных благодаря психологической стойкости, также выступает крайне важным элементом формирования профессиональной позиции для будущего сотрудника полиции [7].

Другими словами, профессиональная позиция являет собой совместный оценочный результат общей работы по обучению и воспитанию курсантов, резюмируя их профессиональный потенциал и готовность к выполнению предстоящих профессионально-служебных задач.

Анализ научной литературы позволил отметить, что в педагогике понятие «позиция» представляет собой перечень психологических установок субъекта к окружающей его действительности через личную оценку выполняемой им деятельности.

Так, В. П. Бедерханова определяет позицию как «место, которое занимает человек в конкретных условиях; отношение человека к этим условиям; характер его деятельности в этих условиях» [1]. Тем самым автором подчеркивается важность активности субъекта в выполняемой им деятельности, поскольку она и определяет саму позицию личности.

Э. Ф. Зеер указывает, что «осознанная профессиональная позиция способствует возникновению особого эмоционального состояния – профессионального оптимизма» [2].

Профессионально-нравственная позиция ориентирует профессиональную деятельность субъекта на «идеал, нормы и эталоны должного в профессиональном поведении» [3].

Таким образом, профессиональная позиция курсанта представляет собой собирательный образ, который включает в себя следующие составляющие:

– профессиональные качества, которые формируются в процессе обучения под воздействием внешних объективных и внутренних субъективных факторов;

– система оценок и отношений (к себе как к носителю будущей профессии, к окружающим субъектам, связанным с профессиональным сообществом);

– перспектива и реальность социального и внутреннего опыта; личных притязаний, реализуемых в профессиональной деятельности полицейского.

Более того профессиональная позиция курсантов образовательной организации МВД России определяется системой нравственных отношений к обучению и будущей профессии, готовности исполнять свой долг, нести ответственность за свой выбор; знанием нравственных ценностей и наличием профессионально-значимых личностных качеств, практической реализации профессиональных обязанностей, стандартов поведения; уровнем мотивации к нравственному самоопределению, результатом которого является построение и реализации траектории профессионального развития.

СПИСОК ЛИТЕРАТУРЫ

1. Бедерханова В. П. Становление личностно-ориентированной позиции педагога. – Краснодар : Изд-во КубГУ, – 2001. – 218 с.

2. Зеер Э. Ф. Психология профессий : учебное пособие для студентов вузов. – Москва : Академический Проект; – Екатеринбург : Деловая книга, – 2003. – 336 с.

3. Скляренко, И.С. Педагогическая система формирования профессиональных ценностных установок у курсантов вузов МВД России : автореф. дис. ... д-ра пед. наук : 13.00.08 / И.С. Скляренко. – Москва, – 2014. – 52 с.

4. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации (с изм. И доп., вступ. в силу с 01.06.2024): Федеральный закон от 1 июня 2024 г. № 342-ФЗ (последняя редакция) // Собрание законодательства РФ. – 2024– № 49. – Ст. 7020. – Текст : непосредственный.

5. Тихомиров, С.Н. Когнитивный, компетентностный, личностно ориентированный и номадологический подходы к системе контроля и оценивания профессиональной подготовки специалиста в образовательной организации / С.Н. Тихомиров // Научные исследования и образование. – 2018. – № 1. – С. 29.

6. Фетисов, А. С. Формирование здоровьесберегающей позиции учащихся как педагогическая проблема / А. С. Фетисов, Н. В. Бирюкова // Проблемы современного педагогического образования. – 2021. – № 70-1. – С. 289-292. – EDN MVMFZG.

7. Фетисов, А. С. Развитие физической культуры как важное условие ориентации учащихся на профессии спортивной направленности : специальность 13.00.01 "Общая педагогика, история педагогики и образования" : диссертация на соискание ученой степени кандидата педагогических наук / Фетисов Александр Сергеевич. – Воронеж, 2002. – 154 с. – EDN NMCZMF.

СВЕДЕНИЯ ОБ АВТОРЕ

Короткова Анна Сергеевна.

Адъюнкт ФГКОУ ВО «Воронежского института МВД России».

Воронежский институт Министерства внутренних дел России.

E-mail: annielesnyh@yandex.ru

Россия, 394006, г. Воронеж, проспект Патриотов, 53.

Korotkova Anna Sergeevna.

Associate Professor at the Voronezh Institute of the Ministry of Internal Affairs of Russia.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: annielesnyh@yandex.ru

Russia. 394006, Voronezh, Prospect Patriotov, 53.

Ключевые слова: профессиональная позиция; образовательные организации МВД России; курсанты; образовательный процесс; образовательное пространство.

Keywords: professional position; educational organizations of the Ministry of Internal Affairs of Russia; cadets; educational process; educational space.

УДК 378.1

Н. В. Полякова

АКТУАЛЬНЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ ПРИОРИТЕТНОГО ПРОФИЛЯ ПОДГОТОВКИ «ДЕЯТЕЛЬНОСТЬ ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ»

TOPICAL ISSUES OF THE IMPLEMENTATION OF THE PRIORITY TRAINING PROFILE «ACTIVITIES OF JUVENILE AFFAIRS UNITS»

В статье изложены основные формы и методы реализации приоритетного профиля подготовки «Деятельность подразделений по делам несовершеннолетних» и возникающие при этом проблемы.

The article outlines the main forms and methods of implementing the priority of training profile «Activities of juvenile affairs units» and the problems that arise.

В соответствии с приказом МВД России от 29.08.2012 № 820 «О профилизации образовательных учреждений МВД России» образовательные организации МВД России наделены функциями по методическому обеспечению деятельности подразделений по делам несовершеннолетних, подготовке для них специалистов и научному исследованию проблем, возникающих в деятельности подразделений по делам несовершеннолетних (далее – ПДН). Воронежский институт МВД России наделен функциями учебно-научного центра по реализации приоритетного профиля подготовки «Деятельность подразделений по делам несовершеннолетних».

Как отмечает Д. В. Гуров, на современном этапе модернизации юридического образования одной из главных составляющих является практическая направленность обучения, формирование не просто умений, а компетенций, то есть умений, непосредственно сопряженных с опытом их применения в практической деятельности и достижения таким образом в полной мере реализации принципа связи обучения с жизнью [2].

В рамках реализации функций учебно-научного центра по указанному профилю в институте действует Координационный совет по приоритетному профилю подготовки, в состав которого входит профессорско-преподавательский состав кафедр института, представители Главного управления обеспечения охраны общественного порядка (далее – ГУОО-ОП), сотрудники ПДН территориальных органов.

В рамках реализации Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года, утвержденной распоряжением Правительства РФ от 22 марта 2017 г. № 520-р, осуществляется взаимодействие с центром профессионального развития специалистов системы профилактики ФГБНУ «Институт изучения детства, семьи и воспитания». Институтом разработаны методические материалы по программе повышения квалификации «Взаимодействие ПДН РФ с образовательными организациями в области профилактики правонарушений обучающихся».

Методическая работа выстраивается посредством учета в рабочих программах дисциплин административно-правового блока специфики деятельности подразделений по делам несовершеннолетних, проведения учебных занятий привлечением сотрудников ОУУП и ПДН ГУ МВД России по Воронежской области.

Институт взаимодействует с комиссиями по делам несовершеннолетних и защиты их прав, Уполномоченным по правам ребенка, органами прокуратуры и иными правоохранительными органами. Сотрудники института проходят обучение по дополнительной профессиональной программе повышения квалификации профессорско-преподавательского состава (стажировка в органах, организациях, подразделениях МВД России, а также в государственных органах и государственных организациях) на базе ПДН территориальных органов

МВД России. В период стажировки изучаются основные направления деятельности указанного подразделения и нормативные документы, их регламентирующие, аналитические обзоры и отчетно-статистическая документация, отражающая основные результаты работы подразделения.

По заявкам ГУОООП МВД России и территориальных органов МВД России, а также в инициативном порядке осуществляется выполнение научно-исследовательских работ с тематикой профиля.

Так, выполнялось исследование следующих тем:

- по организации деятельности подразделений по делам несовершеннолетних;
- по правовому обеспечению информационной безопасности несовершеннолетних;
- по действиям сотрудников полиции при обнаружении несовершеннолетних в обстановке, угрожающей их жизни и здоровью;
- правовые основы и организация психодиагностической и психокоррекционной работы в условиях центров временного содержания для несовершеннолетних правонарушителей, обеспечение взаимодействия с подразделениями по делам несовершеннолетних по вопросам профилактики безнадзорности и правонарушений несовершеннолетних»;
- по выявлению уровня профессиональных компетенций сотрудников подразделений по делам несовершеннолетних по организации работы с группами несовершеннолетних антиобщественной направленности»;
- по порядку действий сотрудников полиции при выявлении вовлечения несовершеннолетних в совершение антиобщественных действий»;
- особенности режима пребывания в Российской Федерации несовершеннолетних иностранных граждан: административно-правовые проблемы и пути их решения;
- административно-правовые основы деятельности органов внутренних дел по противодействию вовлечению несовершеннолетних в противоправную деятельность;
- применение норм КоАП РФ в отношении несовершеннолетних иностранных граждан и лиц без гражданства;
- профилактика правонарушений несовершеннолетних в Российской Федерации: административно-правовой аспект и другие.

Результатами стали учебные пособия, методические рекомендации, аналитические обзоры, которые внедряются в деятельность ПДН территориальных органов МВД России.

Ежегодно проводятся всероссийские научно-представительские мероприятия по различным проблемным аспектам деятельности подразделений по делам несовершеннолетних. Так, значимым мероприятием является Всероссийский круглый стол «Проблемы адаптации сотрудников подразделений по делам несовершеннолетних на первоначальном этапе профессиональной деятельности и пути их решения». Участие в нем принимают

территориальные органы МВД России по субъектам РФ, а также профессорско-преподавательский состав образовательных организаций. Обсуждаются проблемы, связанные с привлечением на службу специалистов в подразделения по делам несовершеннолетних и минимизацией увольнений в первые годы службы, повышением эффективности взаимодействия образовательных организаций и подразделений по делам несовершеннолетних территориальных органов МВД России в выработке единых стандартов оценки молодых специалистов в процессе их становления.

Активно ведется и научно-исследовательская работа курсантов и слушателей, их участие в научных конкурсах и научно-представительских мероприятиях. Темы по деятельности подразделений по делам несовершеннолетних учитываются и в научных кружках.

Ежегодно институтом проводится Всероссийский конкурс научно-исследовательских работ курсантов и слушателей образовательных организаций «Противодействие правонарушениям с участием несовершеннолетних».

Кроме того, кафедры организуют и проводят мероприятия, направленные на профилактику девиантного поведения, правовое просвещение несовершеннолетних и формирование положительного имиджа сотрудника полиции, приуроченные ко Дню знаний, Международному дню защиты детей и Всемирному дню ребенка.

Вместе с тем, следует отметить, что переход образовательных организаций с обучения по основным образовательным программам по 40.05.02 Правоохранительная деятельность, специализация – административная деятельность полиции, профиль образовательной программы – деятельность сотрудника подразделения по делам несовершеннолетних на программы бакалавриата не позволяет учитывать при подготовке специалистов узкой специализации для подразделений по делам несовершеннолетних, что значительно снижет эффективность такой подготовки курсантов.

СПИСОК ЛИТЕРАТУРЫ

1. О профилизации образовательных учреждений МВД России : приказ МВД России от 29.08.2012 № 820 // СТРАС «Юрист».
2. Гуров Д. В. Реализация требований профилизации образовательных учреждений МВД России кафедрой оперативно-розыскной деятельности и специальной техники Ставропольского филиала Краснодарского университета МВД России // Мир науки, культуры, образования. – 2015. – № 3. – С. 137–138.

СВЕДЕНИЯ ОБ АВТОРЕ

Полякова Наталья Викторовна.

Начальник кафедры административного права.

Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: n.v.poliyakova@list.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Polyakova Natalia Viktorovna.
Associate Professor of the chair of administrative law.
PhD in law , associate Professor.
Voronezh Institute of the Ministry of Interior of Russia.
E-mail: n.v.poliyakova@list.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: подразделения по делам несовершеннолетних; приоритетный профиль; профилизация; образовательные организации; правоохранительная деятельность; учебно-научный центр; координационный совет; правовое информирование; практическая направленность обучения.

Keywords: juvenile affairs units; priority profile; profiling; educational organizations; law enforcement; educational and scientific center; coordinating council; legal information; practical orientation of training.

УДК 342.92

Т. Н. Семенихина

О НЕКОТОРЫХ ОСОБЕННОСТЯХ СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКОЙ И ПРОФЕССИОНАЛЬНОЙ АДАПТАЦИИ ИНСПЕКТОРОВ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ

ON SOME FEATURES OF THE SOCIO-PSYCHOLOGICAL AND PROFESSIONAL ADAPTATION OF JUVENILE INSPECTORS AT THE INITIAL STAGE OF THEIR OFFICIAL ACTIVITIES

В настоящей статье автором рассматриваются основные особенности социально-психологической, а также профессиональной адаптации сотрудников подразделений по делам несовершеннолетних, впервые поступивших на службу в органы внутренних дел, а также после окончания ведомственного учебного заведения, проводящего подготовку кадров для замещения должностей в органах внутренних дел. Проанализированы основные моменты, необходимые для успешной адаптации сотрудников, а также выделены последствия, вызванные нарушением адаптации на службе.

In this article, the author examines the main features of the socio-psychological, as well as professional adaptation of employees of juvenile affairs units who first joined the internal affairs bodies, as well as after graduating from a departmental educational institution that trains personnel to fill positions in internal affairs bodies. The main points necessary for the successful adaptation of employees are analyzed, and the consequences caused by a violation of adaptation in the service are highlighted.

Деятельность сотрудников подразделений по делам несовершеннолетних (далее – ПДН) имеет своеобразную специфику, что требует определенной адаптации при прохождении службы в данном подразделении. Специфика деятельности инспекторов характеризуется такими чертами, как непосредственная работа с малолетними и несовершеннолетними правонарушителями, семьями, находящимися в социально-опасном положении, родителями, недобросовестно выполняющими свои родительские обязанности по воспитанию и содержанию своих несовершеннолетних детей. Для эффективного выполнения задач, возложенных на сотрудников ПДН, необходимо успешно пройти социально-психологическую, а также профессиональную адаптацию на первоначальном этапе служебной деятельности.

Термин «адаптация» (от лат. adapto, adaptare, adaptatio «приспособление») берет свое начало от второй половины XIX в. 1865 г. и связан с именем немецкого физиолога Германа Ауберта, который использовал его для характеристики явлений приспособления органов зрения к воздействию внешних раздражителей путем повышения или понижения порога чувствительности.

Социально-психологическая адаптация на первоначальном этапе представляет собой процесс социализации в новом коллективе на новом месте службы, который включает в себя активное приспособление сотрудника к специфике выполняемой работы и возложенных на него обязанностей в ходе осуществления служебной деятельности. Социально-психологическая адаптация на первоначальном этапе службы необходима для успешного выполнения поставленных задач, борьбой со стрессовыми ситуациями, принятия быстрого и правильного решения в нештатной ситуации и др.

Согласно трактовке Ф. Б. Березина, социально-психологическая адаптация представляет собой многоступенчатый процесс, в ходе которого индивидуум осваивает тот или иной социально-психологический статус и принимает на себя разнообразные ролевые функции в социуме [1]. Эта динамика развивается как в рамках самостоятельных систем психологических связей и взаимодействий, так и в контексте тех межличностных отношений, которые формируются при выполнении различных задач, относящихся к жизни в социальной среде.

В процессе адаптации личность учится овладевать новыми навыками и углубляется в свою деятельность, что позволяет ей интегрироваться в четко обозначенные социальные и психологические сети и взаимосвязи. В результате этого происходит не только профессиональная адаптация, но также и социально-психологическое преобразование индивидуума, которое может привести как к успеху, так и, наоборот, к дезадаптации.

Негативными последствиями, вызванными отсутствием социально-психологической адаптации, у действующих сотрудников рассматриваемого подразделения являются такие, как невроз, снижение иммунной системы, повышение риска заболеваемости, депрессия и иные психологические ответы организма на неблагоприятные факторы прохождения службы.

К психологическому аспекту прохождения службы в ПДН следует отнести следующие факторы, негативно сказывающиеся на психологическом состоянии сотрудников ПДН при несении службы: эмоциональное выгорание, повышенный уровень стресса, влияние преступной среды несовершеннолетних, нарушенная саморегуляции, эмоционально напряженная обстановка и т.д.

При наличии вышеперечисленных факторов осуществление служебной деятельности сотрудниками ПДН может носить рискованный характер и снижать эффективность выполнения служебных задач. Таким образом, возникает необходимость включения в систему социально-психологической и профессиональной адаптации инспекторов ПДН, мер, нейтрализующих указанные психологические факторы.

К данным мерам можно отнести следующие:

- 1) регулярная психологическая поддержка, которая может включать в свои рамки индивидуальные или групповые сеансы психотерапии, тренинги по управлению стрессом и эмоциональному выгоранию;
- 2) обеспечение права на отдых;
- 3) разработка тренировок, нацеленных на преодоление ситуаций, связанных с повышенной эмоциональной напряженностью.

Это будет способствовать:

- развитию у сотрудников ПДН саморегуляции, координации и эмоционального контроля;
- обучению сотрудников ПДН методам, направленным на разрешение и урегулирование конфликтных ситуаций;
- рациональному использованию современных технических средств, что позволит снизить возможные риски при выполнении сотрудниками ПДН повседневных задач в ходе несения службы.

Данные меры нацелены на создание благоприятных условий обеспечения представителям ПДН психологической безопасности, которая входит в систему социально-психологической и профессиональной адаптации сотрудников на первоначальном этапе прохождения службы.

В своих исследованиях, касающихся проблемы социально-психологической адаптации, А. А. Реан подчеркивает, что «структуры личности, являясь отражением формирующихся взаимосвязей и отношений», играют ключевую роль в процессе адаптации [2]. Адаптационные возможности личности в рамках правоохранительной системы представляют собой основополагающую индивидуально-психологическую характеристику, служащую её центральным ядром.

Как утверждает Д. А. Леонтьев, социально-психологическая адаптация отражает уровень личностной зрелости индивидуума и его способность справляться с внутренними конфликтами. Конфликты, возникающие в условиях нарушения равновесия, и внутренние противоречия формируют состояние нестабильности, решение которого требует значительных усилий по «преодолению» этих внутренних противоречий [3]. Успешность индивидуума в этой деятельности зависит от комплекса личностных характеристик, которые в научной литературе принято называть личностным адаптационным потенциалом.

Социально-психологическую, а также профессиональную адаптацию сотрудников ПДН следует воспринимать как динамичный процесс, который в свою очередь подразделяется на этапы. Профессиональная и социальная адаптация сотрудников органов внутренних дел – это жизненный период, который характеризуется активным и осознанным включением в новую сферу правоохранительной деятельности и соответствующую социальную среду.

Профессиональная адаптация инспекторов ПДН на первоначальном этапе служебной деятельности подразумевает под собой такие процессы, как: приспособление к распорядку дня, условиям службы, овладение необходимыми профессиональными качествами, способствующими в дальнейшем эффективному выполнению служебных задач в повседневной деятельности инспекторов ПДН в органах внутренних дел.

Нарушение адаптации хотя бы к одному из компонентов отрицает процесс успешной адаптации в целом, следствием чего может быть причина низкой эффективности и качества служебной деятельности, дисциплинарные проступки, психологическая дезадаптация и в крайних случаях формирование кризисных психологических состояний.

В системе межличностной адаптации у молодого сотрудника органов внутренних дел формируется чувство принадлежности к группе, складываются отношения с коллегами в коллективе, вырабатываются профессиональные склонности и интересы. Важным фактором воздействия на адаптацию молодого сотрудника органов внутренних дел являются сложившиеся традиции.

С. В. Косыгин и М. Ю. Охотников высказывают мнение, что «успешная социально-психологическая адаптация к учебно-профессиональной деятельности представляет собой ключевой элемент,

содействующий выявлению резервных возможностей индивидуума и формирующему у него готовность к преодолению разнообразных препятствий на пути к профессиональному становлению» [4].

Субъективное восприятие адаптированности проявляется через психическое благополучие и общее удовлетворение от труда, что служит внутренним показателем успешности данной адаптации.

Социально-психологическая и профессиональная адаптация сотрудников, впервые приходящих на службу в органы внутренних дел, требует значительных усилий со стороны личности и приводит к изменениям в индивидуально-психологических аспектах. Этот процесс включает перестройку психики под воздействием социальных и психологических условий. В рамках этого динамического процесса происходит трансформация привычной модели функционирования индивида на более оптимальную, соответствующую текущей ситуации. Новая модель находится в определенном диапазоне, который наиболее эффективен как для самого сотрудника, так и для его окружения.

Процесс социально-психологической и профессиональной адаптации сотрудников подразделений по делам несовершеннолетних является ключевым аспектом их подготовки к выполнению сложной и ответственной деятельности. Специфика работы с несовершеннолетними правонарушителями и их семьями требует не только профессиональных знаний, но и развитых психологических навыков, позволяющих справляться с эмоциональными и стрессовыми ситуациями.

Таким образом, создание условий для успешной адаптации, включая психотерапевтическую поддержку и обучение управлению стрессом, не только улучшает качество работы инспекторов, но и способствует общему благополучию в сфере защиты прав несовершеннолетних. Совершенствование данной области трудовой деятельности сотрудников органов внутренних дел является вложением в будущее, которое позволит эффективно решать возникающие проблемы и обеспечивать безопасность детей и подростков в обществе.

СПИСОК ЛИТЕРАТУРЫ

1. Березин Ф. Б. Психическая и психофизическая адаптация человека. – Ленинград : Наука, 1988. – 267 с.
2. Реан А. А. Психология адаптации личности. Анализ. Теория. Практика. – Санкт-Петербург : Прайм-Еврознак, 2006. – 479 с.
3. Леонтьев Д. А. Личностное в личности: личностный потенциал как основа самодетерминации // Учёные записки кафедры общей психологии МГУ им. М. В. Ломоносова. – Вып. 1 / под общ. ред. Б. С. Братуся, Д. А. Леонтьева. – Москва : Смысл, 2002. – С. 56–65.

4. Косыгина С. В., Охотников М. Ю. Профессиональная и социально-психологическая адаптация молодых специалистов-сотрудников ОВД : учебно-практическое пособие. – Москва : Московский ун-т МВД России имени В. Я. Кикотя, 2018. – 120 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Семенихина Татьяна Николаевна.
Преподаватель кафедры административного права.
Воронежский институт МВД России.
E-mail: fenix-omelia@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53,

Semenikhina Tatyana Nikolaevna.
Teacher of the Department of Administrative Law.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: fenix-omelia@yandex.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: социально-психологическая; профессиональная; адаптация; инспектор по делам несовершеннолетних.

Keywords: socio-psychological; professional; adaptation; juvenile affairs inspector.

УДК 342.95

А. С. Ситникова

ПРОФЕССИОНАЛЬНО-ПРАВОВАЯ КУЛЬТУРА СОТРУДНИКОВ ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ

PROFESSIONAL AND LEGAL CULTURE OF THE EMPLOYEES OF THE UNITS FOR MINORS

В современных условиях развития общества все более актуальной становится проблема подростковых девиаций. Формирование у сотрудников подразделений по делам несовершеннолетних профессионально-правовой культуры позволяет эффективно реагировать на подобные ситуации и своевременно их предотвращать, осуществлять поддержку несовершеннолетних и содействовать их скорейшей адаптации к социуму. Таким образом, профессионально-правовая культура является важным элементом в структуре подготовки сотрудников подразделений по делам несовершеннолетних ОВД России.

In the modern conditions of development of society, the problem of juvenile deviations is becoming increasingly urgent. Formation of professional and legal culture in employees of juvenile departments allows to effectively respond to such situations and prevent them in a timely manner, to support minors and to facilitate their rapid adaptation to society. Thus, professional and legal culture is an important element in the structure of training of employees of juvenile departments of the Russian Internal Affairs Directorate.

Будущее государства несомненно находится в прямой зависимости от подрастающего поколения, его ценностей и личностных смыслов. В нашей стране существует множество социальных институтов, направленных на развитие и поддержку современной молодежи, их развитие и самоопределение.

Однако не стоит забывать и про несовершеннолетних, с проявляющимися отклонениями в правомерном поведении. Данный факт активизирует подключение к процессу их воспитания специализированных органов (комиссии по делам несовершеннолетних и защите их прав; отдельных служб ОВД России, в частности подразделений по делам несовершеннолетних (далее – ПДН); органов опеки и попечительства и т.п.).

Для нашего исследования особый интерес представляет деятельность сотрудников ПДН, носящая многофункциональный характер и требующая наличия у сотрудника большого багажа знаний и навыков, позволяющих им взаимодействовать с одним из самых сложных, в силу возрастных особенностей, категорий населения – подростков с делинквентным поведением. Поэтому особую важность для страны представляет эффективная квалифицированная работа рассматриваемого подразделения по предупреждению и пресечению совершения несовершеннолетними противоправных действий. Данную задачу позволяет решить сформированная у сотрудников ПДН профессионально-правовая культура.

Логика исследования требует рассмотреть поочередно все составляющие дефиниции «профессионально-правовая культура» для более полного представления изучаемого феномена.

Термин «культура» возможно рассматривать в нескольких аспектах. С точки зрения антропологии, культура – это совокупность норм, ценностей, обычаев и традиций, которые передаются из поколения в поколение и определяют образ жизни социума. Психологический подход к культуре подчеркивает ее роль в формировании мышления, поведения и представлений о мире у членов общества. Социологический аспект культуры уделяет значительное внимание социальным институтам, ритуалам и обычаям, которые формируются в рамках конкретного общества и обеспечивают его согласованность и стабильность.

В целом культура рассматривается как многогранное комплексное понятие, которое включает в себя материальные и духовные ценности об-

щества, культура оказывает значительное влияние на развитие общества и формирование его идентичности.

Что касается правовой культуры, то под ней понимается совокупность норм, ценностей, знаний, умений и навыков, связанных с правовой системой общества. Уровень правовой культуры общества и его членов влияет на эффективность правовой системы, минимизирует в обществе количество противоправных деяний и стабилизирует общественный порядок.

По мнению А. А. Бондарева [1], правовая культура сотрудников ОВД представляется в качестве особой разновидности общей правовой культуры, которая отражает определенный уровень правосознания, законности, совершенства законодательства, юридической практики и охватывает те ценности, которые были созданы людьми в области права.

Профессиональная культура, по мнению Н. С. Мартусенко представлена как требование социума к культурному уровню людей, занятых той или иной профессиональной деятельностью, представляет собой упорядоченную совокупность общечеловеческих идей, профессионально-ценностных ориентаций и качеств личности, универсальных способов познания и гуманистической технологии деятельности [2].

Профессионально-правовая культура – это совокупность знаний, норм, ценностей и установок, отношения к праву и правовым ценностям, что формирует поведение и взаимодействие специалистов в определенной области профессиональной деятельности. В данном случае речь идет о сфере взаимодействия сотрудников ОВД с несовершеннолетними правонарушителями. Профессионально-правовая культура включает в себя не только знание законодательства Российской Федерации, но и понимание этических норм, психологических аспектов работы с детьми и подростками, а также навыки межличностного общения [3].

Сотрудники по делам несовершеннолетних сталкиваются с уникальными вызовами, выполняют высоконравственные задачи, которые перед ними ставит государство и общество. Работая с несовершеннолетними, они должны не только применять свои профессиональные знания, но также проявлять чуткость, эмпатию, умение устанавливать доверительный контакт. Профессионально-правовая культура позволяет им ориентироваться в сложных ситуациях, связанных с предупреждением и пресечением правонарушений, неблагополучием семей и социальными проблемами.

Профессионально-правовая культура каждого отдельного сотрудника способствует формированию имиджа всей правоохранительной системы и службы, повышению уровня доверия среди населения. Это является особенно важным в рамках работы с наиболее уязвимой группой населения – детьми и подростками, личность которых находится в активной стадии трансформации собственных ценностей, идеалов и жизненных принципов.

СПИСОК ЛИТЕРАТУРЫ

1. Бондарев А. А. Правовая культура и законность в механизме правомерного поведения сотрудника ОВД / А. А. Бондарев // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2018. – № 4(77). – С. 27–30.

2. Мартусенко С. Н. Формирование профессиональной культуры сотрудника органов внутренних дел в условиях начальной профессиональной подготовки / С. Н. Мартусенко // Мир науки, культуры, образования. – 2013. – № 4(41). – С. 94–96.

3. Яковлев М. В. Профессиональная правовая культура военнослужащих войск национальной гвардии России как объект правового воздействия: теоретико-правовой анализ / М. В. Яковлев // Правовая политика и правовая жизнь. – 2017. – № 2. – С. 143–148.

СВЕДЕНИЯ ОБ АВТОРЕ

Ситникова Анастасия Сергеевна.

Преподаватель кафедры теории и истории государства и права.

Воронежский институт МВД России.

E-mail: tyulya_n@mail.ru

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

Sitnikova Anastasia Sergeevna.

Lecturer in the Department of Theory and History of State and Law.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: tyulya_n@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: культура; профессиональная культура; правовая культура; профессионально-правовая культура; культура сотрудников подразделения по делам несовершеннолетних.

Keywords: culture; professional culture; legal culture; professional and legal culture; culture of employees of the juvenile affairs department.

УДК 378

**О ФОРМИРОВАНИИ
АДМИНИСТРАТИВНО-ОРГАНИЗАЦИОННОЙ КОМПЕТЕНТНОСТИ
У СОТРУДНИКОВ ПОДРАЗДЕЛЕНИЙ
ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ
В ОРГАНАХ ВНУТРЕННИХ ДЕЛ**

**ON THE FORMATION OF ADMINISTRATIVE
AND ORGANIZATIONAL COMPETENCE AMONG EMPLOYEES
OF JUVENILE AFFAIRS UNITS IN THE INTERNAL AFFAIRS BODIES**

В данной статье отмечена важность административно-организационной компетентности сотрудников подразделений по делам несовершеннолетних в органах внутренних дел. Это основа, которая определяет эффективность работы с молодежью, направленной на предотвращение правонарушений и преступлений среди подрастающего поколения. Формирование такой компетентности становится актуальной задачей для системы внутренних дел, требующей комплексного подхода и глубокого понимания как специфики работы с несовершеннолетними, так и методов организации административной деятельности.

This article highlights the importance of administrative and organizational competence of employees of juvenile affairs units in the internal affairs bodies. This is the basis that determines the effectiveness of work with young people aimed at preventing offenses and crimes among the younger generation. The formation of such competence is becoming an urgent task for the internal affairs system, which requires an integrated approach and a deep understanding of both the specifics of working with minors and the methods of organizing administrative activities.

Одной из важнейших задач, с которой на сегодняшний день сталкивается российское общество, является разработка эффективных методов снижения уровня преступности среди несовершеннолетних. Практика показывает, что несовершеннолетние, не получившие необходимой поддержки и внимания, склонны к совершению правонарушений уже на раннем этапе жизни, что в дальнейшем усложняет процесс их реабилитации. Эти молодые люди зачастую становятся основой для рецидива и участия в преступной деятельности взрослых. Поэтому так важно своевременно диагностировать и выявлять несовершеннолетних правонарушителей, а также принимать эффективные профилактические меры, чтобы помочь им избежать повторных противоправных действий.

По словам В. В. Путина [1], в области профилактики преступности среди молодежи нельзя действовать по шаблонам – «нужно искать новые,

современные подходы», видеть проблемы, сложности каждого молодого человека. В этой связи 17 февраля 2022 года на расширенном заседании коллегии Министерства внутренних дел Российской Федерации (далее – МВД России) Президентом определен курс на консолидацию усилий органов власти, всех субъектов системы профилактики по созданию единой государственной системы непрерывного социального сопровождения подростков, склонных к правонарушениям.

На одноименном заседании от 2 апреля 2024 года отмечена положительная динамика по рассматриваемому направлению работы и закреплена необходимость продолжения данной деятельности подразделениями по делам несовершеннолетних (далее – ПДН) в целях защиты подрастающего поколения от преступной среды [2].

Сегодня мы видим, что в предупреждении правонарушений несовершеннолетних участвуют многие субъекты системы профилактики, действующей в современной России, однако, основной объем работы возлагается на сотрудников полиции, а именно ПДН.

Роль сотрудника ПДН в работе с несовершеннолетними правонарушителями заключается в воздействии на их воспитание и предоставлении им психологической поддержки. В современных условиях функционирования подразделений по делам несовершеннолетних органов внутренних дел наиболее эффективным считается индивидуальный профилактический подход к работе с несовершеннолетними, состоящими на учете. Важно, чтобы сотрудники не придерживались стереотипов, а постоянно развивали новые методики воздействия. Но, к сожалению, в настоящее время из-за загруженности и отсутствия достаточного уровня компетенций, знаний, умений и навыков у сотрудников ПДН, достижение этой цели становится затруднительным [3].

Так, современные реалии жизни определяют кардинально новые требования, предъявляемые к профессиональной деятельности сотрудников ПДН, а качество образования должно быть адаптировано к новым компетенциям, знаниям, умениям и навыкам (далее – ЗУН), необходимым для успешного выполнения оперативно-служебных задач.

На пути к достижению высокого уровня профессионализма сотрудников подразделений по делам несовершеннолетних возникает ряд специфических проблем и вызовов. Основные из них связаны с необходимостью адаптации традиционных методов работы к постоянно меняющейся социальной среде и требованиям времени. Разработка эффективных программ обучения и повышения квалификации, которые будут способствовать формированию и развитию необходимых административно-организационных навыков, становится приоритетной задачей для руководителей и специалистов в данной области.

Административно-организационная компетентность (далее – АОК) сотрудника полиции представляет собой совокупность компетенций и

ЗУН, выражающихся в способности осуществлять действенное управление и упорядочение процессов, направленных на эффективную реализацию служебных задач и функций, возложенных на органы внутренних дел. Формирование АОК у сотрудников ПДН играет немаловажную роль в результативности работы органов внутренних дел в целом. Это обусловлено особенностью целевой аудитории – несовершеннолетних, требующих особого подхода, чуткости и профессионализма. Непосредственное влияние на социальную адаптацию и предотвращение правонарушений среди молодежи делает вопросы качественного наращивания таких компетенций актуальными. В контексте данных задач АОК охватывает знания законодательства, психологии, педагогики, а также умения и навыки эффективного управления, организации работы с молодежью и их семьями, межведомственного взаимодействия. Все это способствует поднятию уровня доверия и авторитета среди несовершеннолетних, обеспечивая тем самым успешную социализацию молодых граждан и минимизацию правонарушений и противоправных действий в подрастающем поколении. Осознание, насколько это важно, влечет за собой необходимость постоянного совершенствования и развития соответствующих компетенций среди работников данных подразделений.

Процесс формирования АОК сотрудников подразделений по делам несовершеннолетних включает в себя ряд практических мер, направленных на повышение профессионального уровня и развитие специфических навыков.

Во-первых, необходимо уделить внимание регулярному обучению и повышению квалификации через специализированные курсы и тренинги, охватывающие как теоретические аспекты работы, так и развитие коммуникационных навыков, необходимых для эффективного взаимодействия с несовершеннолетними.

Во-вторых, стажировки и обмен практическими знаниями с более опытными специалистами помогают не только обогатить собственный профессиональный багаж, но и способствуют формированию адаптированных подходов и методик работы в соответствии с современными требованиями и практиками. Кроме того, ролевые игры и симуляции реальных ситуаций служат эффективным инструментом для отработки навыков принятия быстрых и корректных решений в сложных и чрезвычайных обстоятельствах.

Наконец, наличие психологического консультирования для сотрудников ПДН играет ключевую роль в поддержании высокого уровня мотивации и профессионального выгорания.

Профессиональная деятельность сотрудников ПДН сопровождается сложными эмоциональными переживаниями и чувствами, что подтверждается исследованиями в области теории и практики. Психологическая уязвимость в профессии заключается в необходимости достижения постав-

ленных целей, что требует от сотрудников умения эффективно взаимодействовать с различными категориями несовершеннолетних правонарушителей, достигать желаемых результатов и при этом контролировать свои эмоции, чтобы уменьшить возможные стрессовые ситуации [3]. Такого самоконтроля возможно достичь за счет выработки собственной организованности, являющейся одним из компонентов АОК.

Для повышения административно-организационной компетентности сотрудников ПДН в органах внутренних дел важно сфокусироваться на систематическом применении комплексного подхода к обучению и развитию.

Первым шагом может стать разработка и внедрение специализированных программ обучения, включающих теоретические и практические модули, направленные на изучение административно-правовых норм, психологии несовершеннолетних, а также методик эффективного управления и коммуникации.

Вторым шагом является обеспечение возможности прохождения стажировок в опытных подразделениях, где сотрудники смогут на практике почерпнуть необходимые навыки и знания.

Третий критически важный аспект заключается в непрерывном мониторинге и оценке эффективности подготовки сотрудников, что позволит адаптировать программы обучения под актуальные задачи и изменения в законодательстве.

Помимо этого, рекомендуется формирование менторских программ, где опытные специалисты смогут передавать свои знания и практический опыт молодым сотрудникам, способствуя созданию сильной корпоративной культуры и повышению общей компетентности персонала.

Изложенное позволяет сделать вывод о необходимости и важности формирования административно-организационной компетентности у сотрудников ПДН органов внутренних дел. Именно благодаря АОК обеспечивается высокая степень готовности сотрудников ПДН к осуществлению эффективной работы с несовершеннолетними правонарушителями, включая умение разрабатывать профилактические мероприятия с «трудными подростками» и обеспечивать качественную организацию воспитательной работы.

СПИСОК ЛИТЕРАТУРЫ

1. Парламентская газета. – URL: <https://www.pnp.ru/social/putin-predlozhil-sozdat-sistemu-socialnogo-soprovozhdeniya-podrostkov.html> (дата обращения: 20.09.2024).
2. Президент России. – URL: <http://www.kremlin.ru/events/president/transcripts/deliberations/73770> (дата обращения: 22.09.2024).
3. Душкин А. С. К вопросу о повышении профессиональной психологической компетентности сотрудников подразделений по делам несовершеннолетних органов внутренних дел / А. С. Душкин // Психология и

педагогика: методика и проблемы практического применения, 2009. – № 9. – С. 68–72.

4. Тюлина А. С. Актуальные проблемы формирования профессиональной культуры в вузе / А. С. Тюлина // Традиции и новации в профессиональной подготовке и деятельности педагога : Сборник научных трудов VI Международной научно-практической конференции, посвященной Году семьи, Тверь, 28-30 марта 2024 года. – Тверь : Тверской государственный университет, 2024. – С. 110–113.

СВЕДЕНИЯ ОБ АВТОРЕ

Соломатина Ирина Николаевна.
Преподаватель кафедры административного права.
Воронежский институт МВД России.
E-mail: irinamwd@mail.ru
Россия, 394065, Воронеж, просп. Патриотов, 53.

Solomatina Irina Nikolaevna.
Lecturer at the Department of Administrative Law.
Voronezh Institute of the Ministry of the Interior of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: подразделения по делам несовершеннолетних; несовершеннолетний; административно-организационная компетентность; профилактика; формирование компетентности.

Keywords: juvenile affairs units; minor; administrative and organizational competence; prevention; competence formation.

УДК 37.013.46

Н. А. Швецова

ОСОБЕННОСТИ СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКОЙ И ПРОФЕССИОНАЛЬНОЙ АДАПТАЦИИ МОЛОДЫХ СОТРУДНИКОВ ПОДРАЗДЕЛЕНИЙ ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ К СЛУЖБЕ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

FEATURES OF SOCIO-PSYCHOLOGICAL AND PROFESSIONAL ADAPTATION OF YOUNG EMPLOYEES OF JUVENILE AFFAIRS UNITS TO SERVICE IN THE INTERNAL AFFAIRS BODIES

В статье рассматриваются особенности социально-психологической и профессиональной адаптации сотрудников подразделений по делам

несовершеннолетних, вновь прибывших на службу в органы внутренних дел, а также факторы, влияющие на эффективность осуществления служебной деятельности молодых сотрудников ОВД.

The article examines the peculiarities of socio-psychological and professional adaptation of employees of juvenile affairs units who have newly arrived to serve in the internal affairs bodies, as well as factors affecting the effectiveness of the performance of official activities of young police officers.

В существующих реалиях и в связи с постоянным реформированием системы органов внутренних дел (далее – ОВД), каждая профессия указанной сферы предъявляет особые требования к работнику, особенно к его физическим и психологическим качествам. В соответствии с постановлением Правительства РФ от 06.12.2012 г. № 1259 «Об утверждении Правил профессионально психологического отбора на службу в органы внутренних дел Российской Федерации», граждане, принимаемые на службу в ОВД, проходят профессиональный психологический отбор для определения способности данного гражданина по своим личным и деловым качествам выполнять служебные обязанности сотрудника ОВД [1]. Исходя из данного тезиса, одной из важных задач образовательных организаций системы МВД России выступает обеспечение психологической и физической подготовки будущих специалистов к выполнению предстоящих оперативно-служебных задач.

Профессиональная деятельность сотрудников полиции связана, прежде всего, с риском и высокими психоэмоциональными нагрузками. Для качественного и результативного выполнения служебных задач сотруднику полиции необходимо адаптироваться к среде, в которой ему предстоит работать. Если брать отдельные подразделения ОВД, то одним из наиболее подверженных и находящихся в группе риска находится подразделение по делам несовершеннолетних (далее – ПДН). Это связано, прежде всего, с гендерной принадлежностью, так как в большинстве случаев сотрудниками рассматриваемого нами подразделения являются лица женского пола.

На одном из совещаний министр внутренних дел В. А. Колокольцев сообщил о некомплекте личного состава, который стал критическим. Так, в июле 2023 года со службы в ОВД уволилось 5 тыс. сотрудников. Министр призвал местные отделы сделать всё, чтобы «минимизировать риски». В связи с массовыми увольнениями сотрудников, возникает кадровый «голод», что в последствии приводит к увеличению нагрузки на оставшийся личный состав. На сегодняшний день некомплект личного состава составляет 152 тыс. по всем регионам страны [2]. Впервые прибывший сотрудник ОВД (как правило, для подразделений ПДН – девушка) сталкивается с огромным количеством возложенных задач, которые превышают их

нормированность, вследствие чего, адаптация молодого сотрудника проходит для него тяжелее как в моральном, так и психологическом плане.

На социальную и психологическую адаптацию к службе влияет множество различных факторов (объективные и субъективные). Так, к объективным факторам следует отнести предоставляемые вновь прибывшему сотруднику условия труда, его оплата и различные формы стимулирования материального плана, санитарно-гигиенические условия и т.д. Что касается субъективных факторов, то они связаны с индивидуально-конкретной личностью, а также особенностями сотрудника в плане коммуникабельности, эмоциональной устойчивости и, безусловно, уровня теоретической и физической подготовки. Следует отметить, что морально-психологический климат внутри коллектива тоже играет определенную роль в период адаптации молодого сотрудника ОВД. Взаимоотношения в коллективе должны быть слажены и быть сугубо служебными, профессиональными, с соблюдением субординации.

Особенности психического состояния сотрудников ПДН во время службы зависят от множества деятельностных аспектов. Так, выполняя огромную работу с документацией, сотрудники подвергаются снижению работоспособности из-за монотонной работы. Помимо данного фактора инспекторы ПДН переутомляются вследствие масштаба обслуживаемой территории, количества несовершеннолетних и их родителей, состоящих на профилактическом учете, работы с «трудными семьями», ненормированного рабочего времени и т.п. На психологическую адаптацию также могут влиять факторы внешней среды – погодные условия, в которых сотрудник несет службу, например, в период проведения массовых мероприятий. Исходя из вышеперечисленных факторов, у инспектора ПДН отсутствует возможность психологической разгрузки.

Исходя из вышеизложенного, необходимо сделать вывод о том, что молодые сотрудники ОВД постоянно сталкиваются с ситуациями, подрывающими их морально-психологическое состояние, и адаптация к данной рабочей обстановке проходит гораздо медленнее, либо же сотрудники принимают крайние меры – решение об увольнении.

Для решения вопроса скорейшей адаптации сотрудника как социально-психологической, так и профессиональной, отделу по работе с личным составом, а также психологам необходимо проводить с подверженными риску и психоэмоциональным нагрузкам сотрудниками ПДН лектории по овладению навыками саморегуляции, аутотренингов и физической культуры – для снятия у них напряжения и стресса.

Таким образом, формирование готовности вновь прибывших сотрудников к службе в ОВД является важнейшей проблемой совершенствования системы профессиональной подготовки кадров для системы МВД России. Большую роль в процессе адаптации молодых сотрудников ПДН играет начальник подразделения, а также начальник территориального органа

МВД России, в котором сотрудник проходит службу. Создание благоприятного климата в коллективе – залог успешной и быстрой адаптации к условиям службы. Подчеркнем, что ответственность также ложится на сотрудников кадрового аппарата и на психологов.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении Правил профессионально психологического отбора на службу в органы внутренних дел Российской Федерации : постановление Правительства РФ от 06.12.2012 № 1259 (ред. от 06.03.2015) // СЗ РФ. – 2012. – № 50. – Ст. 7075.

2. Глава МВД Колокольцев сообщил о критической нехватке личного состава в полиции [Электронный ресурс] // Коммерсантъ. URL: <https://www.kommersant.ru/doc/6149807?ysclid=m36xwnjbn9995618838> (дата обращения: 25.10.2024).

СВЕДЕНИЯ ОБ АВТОРЕ

Швецова Надежда Алексеевна. Адъюнкт
Воронежский институт МВД России.
E-mail: naduysha.garanina02@mail.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Shvetsova Nadezhda Alexeevna. Postgraduate.
Voronezh Institute of the Ministry of the Internal affairs of the Russian Federation.

E-mail: naduysha.garanina02@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53

Ключевые слова: органы внутренних дел; профессиональная адаптация; психологический портрет; морально-психологический климат.

Keywords: internal affairs bodies; professional adaptation; psychological portrait; moral and psychological climate.

УДК 159.99

ВСЕРОССИЙСКИЙ СЕМИНАР
АКТУАЛЬНЫЕ ПРОБЛЕМЫ
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

И. С. Ивануха

**ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ДЛЯ ФИКСАЦИИ И ДОКУМЕНТИРОВАНИЯ ПРАВОНАРУШЕНИЙ
И ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ**

В статье рассмотрены программы, использование которых помогает сотрудникам ОВД по Омской области в раскрытии преступлений экстремистской и террористической направленности, а также дает возможность получать необходимые доказательства.

The article discusses programs whose use helps police officers in the Omsk region solve extremist and terrorist crimes, and also makes it possible to obtain the necessary evidence.

В последнее время в Российской Федерации происходит неуклонный рост правонарушений и преступлений экстремистской и террористической направленности. Согласно статистическим данным за 2021 г. было зарегистрировано 2136 преступлений террористического характера и 1057 преступлений экстремистской направленности, за 2022 г. – 2233 террористического характера и 1566 преступлений экстремистской направленности; в 2023 г. – 2382 преступления террористического характера и 1340 преступлений экстремистской направленности, в январе – мае 2024 года – 1364 и 677 преступлений соответственно, что подтверждает тенденцию дальнейшей активизации экстремистских посягательств. Несмотря на предпринимаемые правоохранительными органами усилия, экстремизм по-прежнему представляет серьезную угрозу стабильности и общественной безопасности в нашей стране.

Существенную угрозу безопасности личности, общества и государства представляет опубликование в информационно-телекоммуникационной сети «Интернет» информации, содержащей призывы к осуществлению экстремистской деятельности либо ее обосновывающей и оправдывающей. Характерной чертой данной категории преступлений является высокий уровень технической подготовки преступников, позволяющий им воздействовать на широкий круг людей при помощи информационно-телекоммуникационных технологий. Наиболее популярными источниками распространения экстремистских материалов являются такие социальные сети, как «ВКонтакте», «Одноклассники», «Инста-

грамм», мессенджер Telegram, Whatsapp а также видеохостинг YouTube. Основным инструментом выявления и раскрытия преступлений экстремистской направленности выступают оперативно-розыскные мероприятия (далее – ОРМ), следственные и иные процессуальные действия.

В связи с этим сотрудники ОВД должны знать организационно-тактическую основу и успешно применять навыки по осмотру страниц интернет-сайтов в целях фиксации и документирования правонарушений и преступлений экстремистской и террористической направленности.

Рассмотрим понятие административная ответственность.

Административная ответственность – наступает за совершение административного правонарушения, т.е. противоправного деяния (действия, бездействия), характеризующегося более низкой общественной опасностью, чем преступление. Так, Кодексом об административных правонарушениях установлена ответственность за некоторые правонарушения экстремистской и террористической направленности.

Следует отметить, что, пока правонарушения имеют место, сохраняется необходимость в применении правоохранительными органами государства принудительных мер в отношении правонарушителей, потому как «право есть ничто без аппарата, способного принуждать к соблюдению норм права».

Особое внимание также следует обращать на посредственное распространение материалов в социальных сетях, где «лайк» позволяет ранжировать материал, скрыто содержащий призыв или возбуждение ненависти либо вражды. Многие пользователи могут не пролистывать до конца пост (где содержится эта информация), а реагировать на актуальную социальную проблему. Кроме того, изложение нелицеприятных исторических фактов (правдивых) о какой-либо социальной группе (национальности, религиозной группе) не может рассматриваться, если отсутствуют явные призывы и не происходит обобщение на всю группу.

Проблематика раскрытия и расследования правонарушений и преступлений экстремистской направленности выражается в том, что такие деяния могут быть как явные, так и консперативные. Чаще всего сотрудники правоохранительных органов сталкиваются с последним, поскольку не удастся установить личность пользователя, специфика состава рассматриваемых преступлений и правонарушений характеризуется тайным, неочевидным характером деятельности. Поэтому чаще всего осмотр проводится не как следственное действие, а является частью оперативно-розыскных мероприятий, например, «сбор образцов для сравнительного исследования», «исследование предметов или документов» и пр., поскольку их производство значительно быстрее и проще, чем назначение и производство аналогичных следственных действий.

В рамках осмотра веб-страницы по рассматриваемой категории дел должна отсутствовать информация, содержащая личное мнение, личные оценки, не предназначенные к распространению или для публичного влияния.

В ходе осмотра веб-страниц обстоятельной фиксации подлежат сообщения о преступлениях и административных правонарушениях экстремистской и террористической направленности. Фиксация производится сотрудниками ОВД с использованием технических средств и систем.

Полагаем, в некоторых случаях в рамках осмотра интернет страниц, в том числе содержащих большое количество контента, необходимо его осуществлять с использованием специальных программ записи экрана, при котором сотрудник правоохранительных органов будет одновременно в присутствии участвующих лиц проговаривать ход его производства и вести аудио- и видеозапись.

К числу таких программ следует отнести следующие:

1. Icecream Screen Recorder

Простое в использовании приложение для записи с экрана с интуитивно понятным интерфейсом и широким набором функций. Среди них: запись экрана в полноэкранный режим или выделение определенной области, использование режима «Вокруг курсора», увеличение и уменьшение масштаба, захват экрана по расписанию и многое другое.

Добавляйте веб-камеру, захватывайте звук (как с динамиков, так и с микрофона) и добавляйте свои водяные знаки к медиафайлам.

Это программное обеспечение для записи экрана для Windows позволяет снимать видеоуроки, обзоры популярных продуктов, создавать качественные материалы для блога, сайта, аккаунта в социальной сети и т.д. Пользователям также доступны: обрезка видео и конвертирование, изменение скорости, добавление анимации для курсора мыши и отображение сочетаний горячих клавиш.

Данный отличный сервис записи экрана для коллективной работы позволяет загружать скриншоты и видео по ссылке. Ведь гораздо удобнее поделиться ссылкой, чем самим видеофайлом. Загружайте записанные видео в облако и получайте доступ к ним в любое время в режиме онлайн.

Плюсы:

- бесплатная программа для записи экрана для оперативной системы Windows;
- запись экрана с удобным интерфейсом;
- возможность рисования и добавления текста во время захвата экрана;
- бесплатное место в облачном хранилище для загруженных видео;
- функция создания скриншотов;
- поддержка добавления пользовательского водяного знака.

Минусы – функция размытия не доступна во время записи видео.

2. Xbox Game Bar

В Windows 10 и 11 уже есть предустановленная программа для записи экрана Windows, которую можно запустить, нажав комбинацию горячих клавиш «Win + G».

По умолчанию полученные файлы сохраняются в папке «Клипы» (Captures). Перед первым запуском Xbox Game Bar, программа для захвата видео с экрана предложит вам настроить несколько параметров: качество видео, FPS и т.д. Кроме того, в программе есть меню для выбора источника звука (микрофон или системные звуки), а также регулировки громкости звука.

Эта программа для записи видео с экрана персональных компьютеров и ноутбуков – отличный вариант для быстрой записи приложений или игр. Однако это не позволит записать экран целиком или отдельную его зону.

Плюсы:

- быстрый запуск с помощью горячих клавиш;
- абсолютно бесплатная программа для записи экрана;
- предустановлен на Windows 11 и 10;
- не требует мощного компьютера.

Минусы – запись экрана целиком недоступна. Вы можете записывать только программы или игры.

3. OBS Studio

OBS Studio – бесплатная программа для записи экрана с открытым исходным кодом для Windows, macOS и Linux предназначена в основном для стримеров. Она снимает экран или его определенную область для последующей онлайн трансляции. Кроме того, программа позволяет предварительно просматривать контент перед показом. Для плавного создания видео вам доступны различные фильтры и переходы. Вы можете использовать специальные эффекты и хромакей, а также выбрать тип потока (FLV, MP4, OGG и т.д.) для создания более качественного видео. Поскольку этот видео рекордер имеет открытый исходный код, вы можете использовать его бесплатно и даже настраивать при необходимости. Однако в OBS (Open Broadcaster Software) отсутствует видеоредактор для постобработки.

Плюсы:

- полностью бесплатное приложение для записи экрана;
- совместимость с большинством онлайн-сервисов потокового вещания;
- запись экрана с широкими настройками для хромакея;
- видеопоток из множества источников, которые можно комбинировать.

Минусы – интерфейс этого программного обеспечения для записи экрана с открытым исходным кодом может быть непонятен для начинающих пользователей.

По результатам производства осмотра интернет-страниц всегда прикладывается диск с аудио- или видеозаписью

Приведенный перечень программ для осуществления аудио-видеозаписи является примерным и может быть дополнен иными специальными программами, но многие из этих программ уже достаточно эффективно используются сотрудниками Центра по противодействию экстремизму Омской области. В заключение отметим, что эффективная работа сотрудников ОВД при проведении осмотра веб-страниц по указанным видам сообщений и преступлений с использованием данных программ способствует их раскрытию, а также дает возможность получать необходимые доказательства.

СПИСОК ЛИТЕРАТУРЫ

1. Шакирьянов М. М. Пути повышения эффективности расследования преступлений экстремистской направленности в сети Интернет / М. М. Шакирьянов // Вестник Казанского юридического института МВД России. – 2018. – №4 (34). – С. 549–555.
2. Смахтин Е. В. Тактические особенности деятельности следователя при проверке сообщения о преступлении экстремистской направленности / Е. В. Смахтин, С. В. Смагин // Юридическая наука и правоохранительная практика. – 2017. – № 4 (42). – С. 161–168.
3. Куватов В. И. Противодействие террористическим и экстремистским организациям в сети Интернет / В. И. Куватов, А. И. Примакин, Д. И. Якушев // Вестник Санкт-Петербургского университета МВД России. – 2015. – № 21 (65). – С. 91–92.
4. Кутузов А. В. Информационно-телекоммуникационная сеть Интернет как приоритетный источник получения оперативно-значимой информации при раскрытии преступлений экстремистской направленности / А. В. Кутузов // Ученые записки Крымского федерального университета имени В. И. Вернадского. – Юридические науки. 2019. – № 5 (71). – С. 154–162.

СВЕДЕНИЯ ОБ АВТОРЕ

Ивануха Иван Сергеевич.

Преподаватель кафедры информационных технологий в деятельности ОВД.
Омская академия МВД России.

E-mail: scorpion-6588@mail.ru

Россия, 644092, г. Омск, ул. Проспект Комарова, 7.

Ivanukha Ivan Sergeyevich.

Prepodavatel' kafedry informatsionnykh tekhnologiy v deyatel'nosti OVD.
Omsk Academy of the Ministry of Internal Affairs of Russia.

E-mail: scorpion-6588@mail.ru

Rossiia, 644092, Omsk, Prospect Komarova, 7.

Ключевые слова: сотрудники ОВД; осмотр веб-страниц; правонарушение; преступление; экстремистская направленность; программа записи экрана.

Keywords: police officers; browsing web pages; offense; crime; extremist orientation; Screen recording program.

УДК 004.051

Н. С. Кобяков

**ВОЗМОЖНЫЙ ПОДХОД К КЛАССИФИКАЦИИ АССН ОВД
ДЛЯ МОДЕЛИРОВАНИЯ ОЦЕНКИ ОПАСНОСТИ
ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ**

**A POSSIBLE APPROACH TO THE CLASSIFICATION OF ATS
FOR MODELING THE ASSESSMENT OF THE DANGER
OF DESTRUCTIVE SOFTWARE IMPACTS**

В статье рассматривается классификация автоматизированных систем специального назначения органов внутренних дел. Определены показатели безопасности информации и их значения, которые могут быть изменены в зависимости от рисков деструктивных воздействий на АССН.

The article examines the classification of automated special-purpose systems of internal affairs agencies. The indicators of information security and their values, which can be changed depending on the risks of destructive impacts on the ASSN, are determined.

Введение. В настоящее время деятельность сотрудников органов внутренних дел непрерывно связана с использованием средств автоматизации, сетей связи, реализующих возможности новейших достижений в области телекоммуникаций. Такое повсеместное использование информационных технологий при выполнении служебных задач повлекло за собой появление большого количества систем для автоматизации деятельности сотрудников. Вместе с тем, для обеспечения конфиденциальности, целостности и доступности данных сервисов необходимо выполнение комплекса организационно-технических мер. Вопросу обеспечения информационной безопасности сервисов ОВД посвящено множество работ [1-3], но в них не учтены особенности различных классов автоматизированных систем специального назначения ОВД при организации защиты от деструктивных воздействий.

Цель работы. Определить классификацию АССН ОВД для моделирования оценки опасности деструктивных воздействий и сформировать критерий для реагирования на них.

Постановка задачи. Для достижения цели работы необходимо решить следующие задачи:

1. Выполнить анализ существующих АССН ОВД;
2. Определить классы АССН ОВД;
3. Определить показатели безопасности информации в АССН, которые могут быть изменены в зависимости от рисков деструктивных воздействий.
4. Определить критерий для реагирования на появление новых вредоносных программ.

Основная часть. В настоящее время все автоматизированные системы специального назначения ОВД размещены в единой системе информационно-аналитического обеспечения деятельности (ИСОД МВД России) [4, 5]. В рамках данной системы функционируют следующие сервисы:

1. Сервисы обеспечения повседневной деятельности (Сервис электронной почты, Сервис электронного документооборота, и т. д.);
2. Сервисы обеспечения оперативно-служебной деятельности (Сервис централизованного учета оружия, Федеральная информационная система Госавтоинспекции и т. д.);
3. Прочие ресурсы (Картографическое обеспечение деятельности органов внутренних дел, Сервисы межведомственного взаимодействия и т. д.).

Целью защиты информации от деструктивных воздействий является обеспечение ее конфиденциальности, целостности и доступности. Конфиденциальность, целостность и доступность информации должны быть обеспечены в любых условиях обстановки и в любое время. Множество признаков безопасности информации может быть представлено в следующем виде:

$$B = \{r_1; r_2; r_3\}, \quad (1)$$

где:

B – множество признаков безопасности информации;

r_1 – конфиденциальность информации;

r_2 – целостность информации;

r_3 – доступность информации.

Но администраторы безопасности могут предпринимать организационно-технические меры для ограничения доступа к некоторым информационным ресурсам, в зависимости от опасности появившейся угрозы безопасности информации и ее актуальности для конкретной АССН.

Показатель доступности может принимать два значения:

$r_3 = 1$ – автоматизированная система специального назначения доступна;

$r_3 = 0$ – автоматизированная система специального назначения не доступна.

В рамках данной работы под угрозой безопасности информации понимаются вредоносные программы и их использование злоумышленниками для реализации тактики «внедрение и исполнение вредоносного программного обеспечения в системах и сетях» [6].

В зависимости от реализуемых функций АССН ОВД можно разделить на следующие классы:

1. Системы, ограничение доступа к которым влечет за собой невозможность выполнения должностным лицом отдельных видов служебной деятельности (в основном, это сервисы обеспечения деятельности).

2. Системы, ограничение доступа к которым влечет за собой выполнение должностным лицом своих обязанностей не в полном объеме (как правило, информационно-справочные системы).

3. Системы, ограничение доступа к которым влечет за собой выполнение должностных обязанностей в полном объеме, но уменьшит скорость выполнения задач (Сервис электронной почты, Сервис электронного документооборота).

Для каждого класса АССН ОВД необходимо определить предельный уровень опасности вредоносных программ, при превышении которого необходимо ограничить доступ к системе.

Следовательно, организационно-технические меры по ограничению доступности автоматизированной системы необходимо принимать, если опасность вредоносной программы превышает предельный уровень:

$$\begin{aligned} &\text{если для } S_i \rightarrow \{J_{\text{вп}} \gg T_i\}, \text{ то } r_{3i} = 0; \\ &\text{если для } S_i \rightarrow \{J_{\text{вп}} < T_i\}, \text{ то } r_{3i} = 1, \text{ где} \end{aligned} \quad (2)$$

S_i – класс автоматизированной системы специального назначения;

$J_{\text{вп}}$ – опасность вредоносной программы;

T_i – предельный уровень опасности вредоносной программы;

r_{3i} – показатель доступности для данного класса АССН.

Заключение. Таким образом, по результатам данной работы решены следующие задачи:

1. Выполнен анализ автоматизированных систем специального назначения органов внутренних дел (согласно руководящих документов АССН

разделяют на сервисы обеспечения повседневной деятельности, сервисы обеспечения оперативно-служебной деятельности и прочие ресурсы);

2. Определена классификация АССН для моделирования оценки опасности деструктивных воздействий (системы, ограничение доступа к которым влечет за собой невозможность выполнения должностным лицом отдельных видов служебной деятельности; системы, ограничение доступа к которым влечет за собой выполнение должностным лицом своих обязанностей не в полном объеме; системы, ограничение доступа к которым влечет за собой выполнение должностных обязанностей в полном объеме, но уменьшит скорость выполнения задач)

3. Определен показатель безопасности информации в АССН, который может быть изменен в зависимости от рисков деструктивных воздействий (доступность).

4. Сформирован критерий для реагирования на появление новых вредоносных программ (ограничение доступности АССН, в зависимости от опасности вредоносной программы).

В дальнейшем результаты работы могут быть использованы для моделирования оценки опасности вредоносных программ для АССН ОВД и принятия предупреждающих организационно-технических мер.

СПИСОК ЛИТЕРАТУРЫ

1. Бабкин А. Н. Модель информационной безопасности сегмента телекоммуникационной сети ОВД / А. Н. Бабкин, С. П. Алексенко, А. Ю. Куличенко // Вестник Воронежского института ФСИН России. – 2020. – № 2. – С. 34–40. – EDN NVCDNH.

2. Прекина Т. А. Проблемы организации информационного обеспечения деятельности в ОВД / Т. А. Прекина // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2020. – № 6-2. – С. 269–272. – EDN OVNPJL.

3. Канавин С. В. Анализ рисков нарушения информационной безопасности в информационных, телекоммуникационных системах ОВД / С. В. Канавин, Н. С. Хохлов // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2020. – № 6-2. – С. 174–177. – EDN LGWMEK.

4. Использование специальных учетов и автоматизированных информационных систем в деятельности подразделений по обеспечению безопасности дорожного движения : учебное пособие. – Москва : ДГСК МВД России, 2016. – 180 с.

5. Кобяков Н. С. Алгоритм классификации автоматизированных систем специального назначения / Н. С. Кобяков, В. Н. Париев // Альманах Пермского военного института войск национальной гвардии. – 2024. – № 2(14). – С. 15-21. – EDN PKWCCP.

6. Методический документ «Методика оценки угроз безопасности информации». Утвержден ФСТЭК России 5 февраля 2021 г., г. Москва.

СВЕДЕНИЯ ОБ АВТОРЕ

Кобяков Николай Сергеевич. Адъюнкт.
Воронежский институт МВД России.
E-mail: kkobyakov1234@gmail.com
Россия, 394065, Воронеж, проспект Патриотов, 53.
Kobyakov Nikolai Sergeevich. Postgraduate student.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: kkobyakov1234@gmail.com
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: автоматизированные системы; вредоносные программы; меры по защите информации.

Keywords: automated systems; malware; information protection measures.

УДК 004.056.57

К. А. Цыганов

СЦЕНАРИИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ВНЕШНИМ НАРУШИТЕЛЕМ С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ СТЕГАНОГРАФИЧЕСКИХ КАНАЛОВ

SCENARIOS OF REALIZATION OF INFORMATION SECURITY THREATS BY AN EXTERNAL INTRUDER USING HIDDEN STEGANOGRAPHIC CHANNELS

В статье рассмотрены виды угроз, реализуемых с использованием скрытых каналов, а также классификация скрытых каналов. Приведено понятие скрытого стеганографического канала, как скрытого канала, использующего механизм передачи информации по памяти. Рассмотрены основные тактики, используемые внешним нарушителем для реализации угроз безопасности информации с применением методов стеганографического погружения информации. Представлен обобщенный сценарий реализации угроз безопасности информации внешним нарушителем с использованием скрытых стеганографических каналов. Рассмотрены этапы представленного сценария, на которых применяется стеганографическое погружение информации. Также приведена схема реализации угроз безопасности информации внешним нарушителем с использованием скрытых стеганографических каналов на примере типовой локальной сети организации.

The article considers the types of threats realized using hidden channels, as well as the classification of covert channels. The concept of hidden steganographic channel is introduced as a covert channel that utilizes a memory-based information transfer mechanism. The main tactics used by an external intruder to realize information security threats using steganographic information immersion techniques are considered. A generalized scenario of realization of information security threats by an external intruder using hidden steganographic channels is presented. The stages of the presented scenario where steganographic information immersion is applied are considered. The scheme of realization of threats to information security by an external intruder using hidden steganographic channels on the example of a typical local network of the organization is also given.

Развитие и широкое распространение информационных технологий, внедрение информационных систем (ИС) и повсеместное использование телекоммуникационных сетей в повседневной человеческой жизни обуславливает рост количества угроз, направленных на информацию, обрабатываемую государственными учреждениями, частными организациями и гражданами с применением этих технологий. Рост количества угроз обрабатываемой информации в свою очередь влечет увеличение рисков, связанных с нанесением ущерба деятельности организации или государства. Основным источником угроз безопасности информации (УБИ) является несанкционированный доступ (НСД) с целью нарушения ее конфиденциальности, целостности или доступности. Источниками угроз такого рода являются деятельность преступных сообществ, разведывательных служб и террористических организаций. Только за период с 2019 по 2023 год количество преступлений в информационной сфере увеличилось более чем в 3 раза [1].

Одним из способов получения НСД к информации для нарушителя являются скрытые каналы. Область действия традиционных средств защиты информации (ЗИ), таких как средства обнаружения вторжений (СОВ), средства антивирусной защиты (САВЗ), межсетевые экраны (МЭ), DPI-системы (системы глубокого анализа пакетов) и др. ограничена контролем и фильтрацией информации, проходящей только по каналам, предназначенным для ее передачи. Возможность обмена информацией вне этих рамок посредством скрытых каналов данными средствами не учитывается, что делает их привлекательными для нарушителя пытающегося осуществить НСД.

В соответствии с [2] скрытые каналы могут применяться для реализации таких угроз как:

- внедрение вредоносных программ и данных;
- подача нарушителем команд вредоносному программному обеспечению (ВПО);
- утечка криптографических ключей или паролей;
- утечка отдельных информационных объектов.

Внутреннему нарушителю разумно использовать скрытые каналы только для реализации УБИ, связанных с утечкой информации, для предотвращения собственной компрометации. Внедрение вредоносных программ и управление ими с использованием скрытых каналов, имеет смысл в случае нахождения нарушителя за пределами контролируемой зоны (КЗ) или сегмента ИС, в котором обрабатывается конфиденциальная информация, для обхода средств защиты периметра, таких как DPI-системы, МЭ, СОВ, и т.п. и получения доступа в КЗ.

Таким образом УБИ, источником которых является внешний нарушитель, более разнообразны и включают в себя все виды угроз, реализуемые с применением СК. Внутренний же нарушитель является источником угроз, связанных только с утечкой информации.

Согласно [2] СК используют различные механизмы для передачи информации, так, существуют каналы, использующие механизм передачи информации по памяти, по времени и статистические СК.

В настоящее время в связи с развитием программного обеспечения (ПО) и распространением мультимедийной информации в сети Интернет широкое распространение получили СК с механизмом передачи информации по памяти. Такие каналы используют некоторую разделяемую память, в которую передающая сторона имеет возможность осуществлять запись, а принимающая считывать записанную информацию. В качестве разделяемой памяти могут выступать любые объекты информации, в которых представляется в цифровом виде – оперативная память, жесткий диск, информация, передаваемая через сетевой контроллер компьютера. Часто запись осуществляется в такие цифровые объекты как медиа файлы (изображения, видео-, аудиофайлы) с использованием методов стеганографического «погружения» информации [3]. Стеганография позволяет скрытно хранить или передавать информацию погрузив ее в безобидные объекты, которые не вызывают подозрения, называемые покрывающими объектами [4].

После погружения информации в медиа файл он передается по открытым каналам связи принимающей стороне, где происходит извлечение погруженной в него информации, таким образом образуя скрытый стеганографический канал (ССК).

Согласно методической документации ФСТЭК [5] при оценке УБИ рассматривают три основные тактики применения стеганографического погружения информации для построения сценариев реализации УБИ.

1. Управление ВПО и компонентами ИС, к которым ранее был получен доступ. Внедрив ВПО, нарушитель стремится автоматизировать управление инструментальными средствами, организовав взаимодействие со скомпрометированным компьютером и сервером управления, размещенным за пределами КЗ. При этом для сокрытия передачи управляющей информации нарушителем могут быть использованы стеганографические средства.

2. Соккрытие действий и применяемых при этом средств от обнаружения. Нарушитель стремится затруднить применение мер ЗИ, которые способны помешать его действиям или обнаружить их. Для чего производится упаковка с использованием стеганографических средств программного кода ВПО, в том числе при хранении этого кода в атакуемой системе или при передаче по сети.

3. Сбор и вывод из ИС информации, необходимой для дальнейших действий при реализации УБИ. В ходе реализации угроз нарушителю может потребоваться получить и вывести за пределы КЗ большие объемы информации, избежав при этом обнаружения или противодействия. Для этого производится погружение выводимой информации с использованием стеганографических средств.

Исходя из перечисленных тактик возможно рассмотреть некоторый обобщенный сценарий действий внешнего нарушителя, использующего ССК изображенный на рисунке 1.

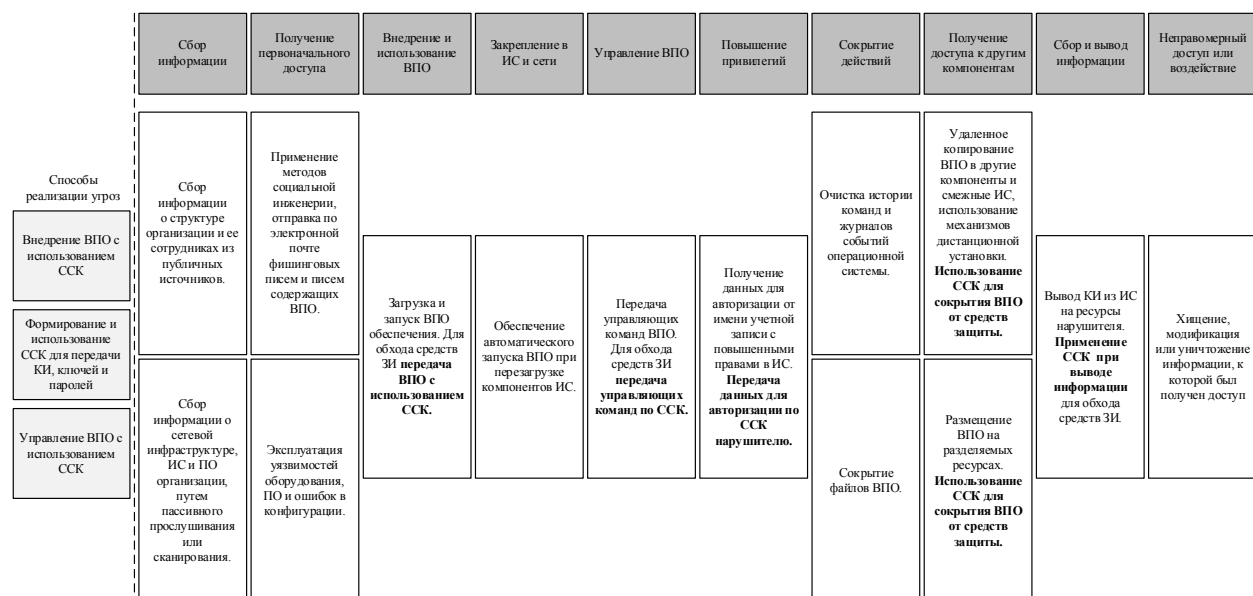


Рис. 1. Обобщенный сценарий реализации УБИ внешним нарушителем с использованием ССК

В различных сценариях реализации УБИ ССК может быть применен:

- на этапе внедрения ВПО;
- на этапе управления ВПО;
- на этапе повышения привилегий для вывода из атакуемой системы паролей и ключей привилегированных пользователей;
- на этапе получения доступа к другим компонентам системы и смежным системам, для скрытой передачи кода ВПО;
- на этапе сбора и вывода информации.

Согласно сценарию, изображенному на рисунке 1, в качестве примера, можно рассмотреть следующую последовательность действий наруши-

теля, реализующего угрозы внедрения ВПО, утечки конфиденциальной информации и управления ВПО.

На этапе сбора информации внешний нарушитель получает сведения о структуре организации, ее сотрудниках и клиентах с целью применения методов социальной инженерии для получения первоначального «виртуального» доступа в КЗ организации. Для этого могут использоваться поддельные аккаунты сотрудников в социальных сетях, службах обмена сообщениями или электронной почты, рассылка писем, содержащих ВПО или фишинговые ссылки. При этом для обхода средств ЗИ и доставки электронной корреспонденции, содержащей вредоносный код, могут быть применены ССК. Так, в письме может содержаться программа-сборщик, которая не распознается как ВПО, так как выполняет типичные для обработки медиафайлов операции. После запуска данная программа загружает на атакуемый компьютер покрывающие объекты с погруженным в них вредоносным кодом, осуществляет его извлечение и запуск. При этом код ВПО может быть передан даже в виде исходного текста, а затем осуществлена сборка и компиляция вредоносной программы уже на атакуемом компьютере [6] с использованием встроенных средств операционной системы. Применение данного метода позволяет обойти проверку электронной подписи ПО, проверку антивирусом и проверку электронной почты.

Также для получения первоначального доступа внешним нарушителем может осуществляться сканирование и сбор сведений о сетевой инфраструктуре организации, используемых программах или ИС с целью поиска уязвимостей в коде ПО или настройках используемых программ и оборудования. После обнаружения уязвимости нарушителем может быть осуществлена загрузка ВПО посредством ССК, для обхода COB, DPI-систем или других средств ЗИ.

Примеры таких атак были выявлены специалистами Kaspersky ICS Cert в 2020 году [7]. Так, от нарушителя приходило фишинговое письмо с просьбой открыть прикрепленный документ Excel, который запускал PowerShell скрипт, случайным образом выбирающий один из записанных в нем адресов, с которого загружалось изображение, содержащее вредоносный код.

После получения первоначального доступа ВПО делает записи в реестре операционной системы или планировщике задач для автоматического запуска в случае перезагрузки, атакуемой ИС или ее компонента. И начинает сбор информации о хранящихся в системе паролях и ключах, так же может осуществляться логирование нажимаемых пользователями клавиш на клавиатуре, для выявления парольных фраз. Среди полученных паролей и ключей осуществляется поиск данных для авторизации пользователя с повышенными привилегиями, что позволит расширить доступ в систему. На данном этапе также может осуществляться управление ВПО для определения атакуемых объектов, в которых необходимо осуществлять поиск данных для авторизации или конфиденциальной информации. Для

обхода средствЗИ и сокрытия действий вредоносной программы возможно применение ССК. Так, специалистами компании Trend Micro было обнаружено ВПО, которое загружало изображения из социальных сетей, в которых была погружена информация о серверах, принадлежащих нарушителю, но которые необходимо было загружать похищенную конфиденциальную информацию [8].

Все действия ВПО должны удаляться из истории команд и журналов операционной системы, для обеспечения скрытности присутствия программы в атакуемой системе. После окончания вредоносных действий программа, а также все следы ее присутствия должны удаляться из ИС.

Получение данных для авторизации привилегированного пользователя позволяет распространить действия вредоносной программы на другие компоненты системы. Для распространения могут быть использованы уязвимости в других компонентах системы, механизмы дистанционной установки, или размещение на общих ресурсах системы. Для сокрытия факта передачи вредоносного кода между компонентами ИС от средствЗИ, как и на этапе внедрения могут быть использованы ССК.

На последних этапах осуществляется сбор и вывод конфиденциальной информации из атакуемой системы, ее модификация или уничтожение. Для вывода информации из атакуемой ИС наиболее целесообразно применение ССК ввиду потенциального наличия в организации DLP, DPI-систем, COB и МЭ. Например, погружение информации в изображения и размещение их на общедоступных ресурсах в сети Интернет. Реальным примером такого использования ССК может служить атака на компании Microsoft, Intel и Cisco осуществленная в 2020 году, где для вывода похищенной информации использовались XML-файлы [9].

На рисунке 2 представлена схема реализации вышеуказанного сценария реализации УБИ на примере типовой локальной сети организации.

На первом этапе нарушитель отправляет фишинговое письмо или использует обнаруженные уязвимости для загрузки программы сборщика в локальную сеть организации. Затем на втором этапе сборщик осуществляет загрузку покрывающих объектов, извлечение из них ВПО и его запуск. Третий этап – это поиск конфиденциальной информации, паролей и ключей на скомпрометированном компоненте локальной сети. Четвертый – распространение ВПО на другие компоненты. После распространения осуществляется поиск конфиденциальной информации на всех компонентах сети, вывод полученной информации на общедоступные ресурсы сети Интернет. И на последнем этапе получение информации нарушителем.

Выявление фактов применения стеганографических средств осуществляется с использованием средств стегоанализа, но в настоящее время отсутствуют системыЗИ, позволяющие проводить стегоанализ автоматически в режиме реального времени. А представленные современные мето-

ды стегоанализа не выходят за рамки лабораторного применения и являются узконаправленными на выявление конкретных методов стеганографии.

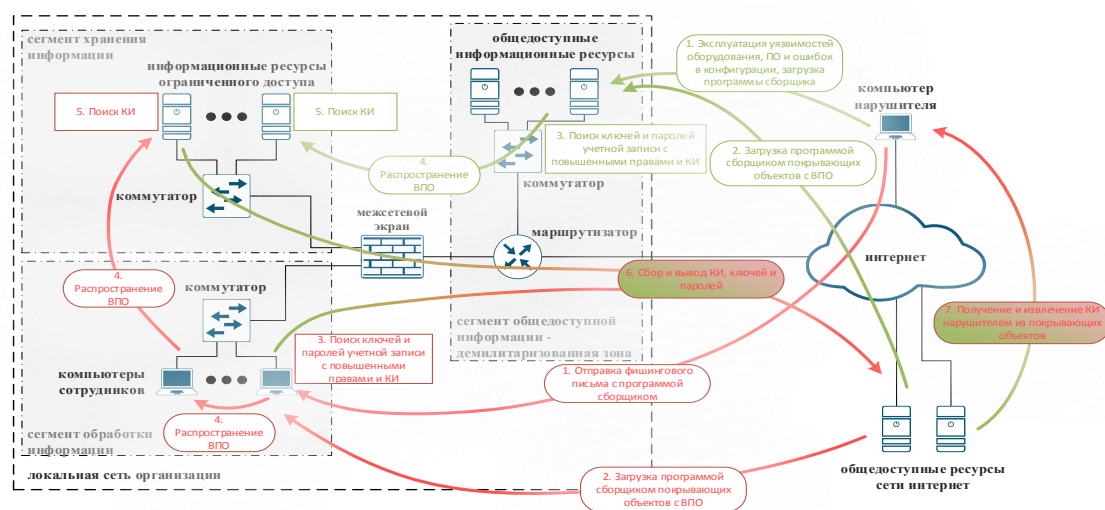


Рис. 2. Схема реализации УБИ внешним нарушителем с использованием ССК на примере типовой локальной сети организации

Таким образом, применение внешним нарушителем ССК представляет собой серьезную угрозу ввиду отсутствия в настоящее время средств ЗИ, позволяющих оперативно выявлять такие каналы и осуществлять их блокирование за время достаточное для предотвращения или минимизации ущерба организации от деятельности нарушителя.

Разработка моделей таких средств ЗИ, позволяющих оценить эффективность применяемых в них методов стегоанализа, является предметом дальнейших исследований автора.

СПИСОК ЛИТЕРАТУРА

1. Терентьев, А. А. Построение алгоритма прогнозирования числа киберпреступлений / А. А. Терентьев, А. С. Лукьянов // Вестник Воронежского института МВД России. – 2024. – № 3. – С. 106–115. – EDN RWVFTO.
2. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. – Москва : Стандартинформ. 2018.
3. Цифровая стеганография и цифровые водяные знаки: монография: в 2 ч.: Часть 1. Цифровая стеганография / В. И. Коржик, К. А. Небаева, Е.

Ю. Герлинг [и др.]. – Санкт-Петербург : СПбГУТ, 2016. – 226 с. – ISBN: 978-5-89160-125-3. – EDN: WJYYGJ.

4. Коржик В. И., Красов А. В. Цифровая стеганография : учебник (Бакалавриат и магистратура). – Москва : КНОРУС, 2023. – 324 с. – ISBN: 978-5-406-10970-0. – EDN: KNKBXU.

5. Методика оценки угроз безопасности информации: методический документ : утвержден ФСТЭК России 5 февраля 2021 г. – URL: <http://fstek.ru> (дата обращения: 30.11.2023).

6. Чистая Windows и разработка «без всего» – Хабр – 2024 – URL: <https://habr.com/ru/articles/837570/> (дата обращения: 23.10.2024).

7. Стеганография в атаках на промышленные предприятия – Kaspersky ICS CERT – 2020 – URL: https://ics-cert.kaspersky.ru/media/KASPERSKY_Steganography_in_attacks_RU.pdf (дата обращения: 23.10.2024).

8. Мемы в твиттере оказались скрытыми командами для трояна – N+1 – 2018. – URL: <https://nplus1.ru/news/2018/12/18/memes> (дата обращения: 23.10.2024).

9. A «Worst Nightmare» Cyberattack: The Untold Story of The SolarWinds Hack – NPR – 2021. – URL: <https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack> (дата обращения: 23.10.2024).

СВЕДЕНИЯ ОБ АВТОРЕ

Цыганов Кирилл Алексеевич.

Старший инженер-программист.

Орловский юридический институт МВД России имени В. В. Лукьянова.

E-mail: tsyganov-ka@yandex.ru

Россия, 302027, Орел, ул. Игнатова, 2.

Tsyganov Kirill Alekseevich.

Senior software engineer.

Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.

E-mail: tsyganov-ka@yandex.ru

Russia, 302027, Orel, st. Ignatova, 2.

Ключевые слова: стеганография; стегоанализ; угроза утечки информации; скрытый канал.

Keywords: steganography; steganalysis; information leakage threat; hidden channel.

УДК 004.056.53

ВСЕРОССИЙСКИЙ СЕМИНАР

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОХРАНЯЕМЫХ ТЕРРИТОРИЙ И ОБЪЕКТОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Е. М. Абросимова

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ И АНАЛИТИКИ ДАННЫХ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

USING A VIDEO SURVEILLANCE SYSTEM AND DATA ANALYTICS TO IMPROVE THE SECURITY OF INTERNAL AFFAIRS FACILITIES

В настоящей статье рассмотрен вопрос использования систем видеонаблюдения и аналитики данных для повышения безопасности объектов органов внутренних дел. Приведены ключевые аспекты данного вопроса.

This article discusses the use of video surveillance systems and data analytics to improve the security of objects of internal affairs agencies. The key aspects of this issue are given.

Использование систем видеонаблюдения и аналитики данных для повышения безопасности объектов органов внутренних дел (ОВД) представляет собой важный аспект в современном подходе к обеспечению общественного порядка и безопасности. В условиях растущих угроз, таких как терроризм, организованная преступность и вандализм эффективные меры по охране требуют интеграции высоких технологий. Рассмотрим ключевые аспекты данного вопроса.

1. *Современные системы видеонаблюдения* обладают рядом преимуществ, которые делают их незаменимыми в работе органов внутренних дел:

- качество изображения: современные камеры обеспечивают высокое разрешение, что позволяет распознавать лица, номера автотранспортных средств и другие детали;

- круглосуточный мониторинг: системы могут работать круглосуточно, что позволяет осуществлять постоянный контроль за охраняемыми объектами, такими как полицейские участки, тюрьмы и административные здания;

- интеллектуальные функции: многие современные камеры оснащены функциями распознавания лиц, детекцией движения и анализа поведенческих паттернов, что позволяет автоматически выявлять подозрительную активность.

2. *Аналитика данных* в сочетании с видеонаблюдением позволяет достичь новых уровней безопасности:

- сбор и хранение данных: видеопотоки могут быть записаны и проанализированы для выявления преступных схем и тенденций. Хранение данных также делает возможным последующий анализ инцидентов;

- прогнозирование преступлений: используя алгоритмы машинного обучения, можно анализировать исторические данные о преступлениях и предсказывать вероятность их совершения в определённых районах. Это помогает в распределении полицейских ресурсов;

- интеграция с другими системами: видеонаблюдение может быть интегрировано с другими системами безопасности, такими как сигнализация, контроль доступа и системы управления инцидентами, что повышает общую эффективность.

3. *Этические и правовые аспекты*, которые необходимо учитывать при использовании систем видеонаблюдения и аналитики данных:

- конфиденциальность: важно обеспечить защиту личных данных граждан. Разработка ясных политик по обращению с данными и соблюдению законодательства о защите персональной информации является критически важной. Важно соблюдать законы о защите личной информации и обеспечить, чтобы данные использовались только в легальных рамках;

- прозрачность: работа систем видеонаблюдения должна быть прозрачной для населения, что помогает избежать недовольства и недоверия к действиям ОВД. Это включает в себя информирование граждан о том, где и как используется видеонаблюдение, а также о целях его использования;

- обучение персонала: сотрудники должны быть обучены правильно использовать данные системы, понимать их возможности и ограничения, а также следить за соблюдением правил и норм.

- может возникнуть предвзятость: автоматизированные системы распознавания лиц могут проявлять предвзятость в зависимости от образовательных и социальных факторов. Это может привести к стереотипизации определённых групп населения.

4. *Внедрение технологий и обучение*. Чтобы обеспечить эффективное использование технологий в ОВД, необходимо обратить внимание на следующие аспекты:

- обучение сотрудников: полицейские и другие работники ОВД должны проходить обучение по использованию видеонаблюдения и аналитических инструментов. Это включает как технические аспекты, так и правовые рамки;

- инфраструктура: необходима соответствующая инфраструктура для хранения и анализа больших объемов данных. Это может включать облачные решения или локальные серверы с достаточной вычислительной мощностью;

- сотрудничество с частным сектором: ОВД могут сотрудничать с технологическими компаниями для создания более эффективных решений по использованию видеонаблюдения и аналитики. Частный сектор может предложить инновационные технологии, которые помогут в борьбе с преступностью.

Таким образом, использование систем видеонаблюдения и аналитики данных является важным инструментом для повышения безопасности объектов органов внутренних дел. Однако успешное внедрение этих технологий требует комплексного подхода, включая техническое обеспечение, вопросы правового регулирования и взаимодействие с обществом. Важно, чтобы современные технологии использовались для обеспечения безопасности и защиты прав граждан, что является основой доверия к правоохранительным органам.

Использование систем видеонаблюдения и аналитики данных в работе органов внутренних дел открывает новые возможности для повышения безопасности и профилактики преступлений. Однако важно балансировать между эффективностью технологий и соблюдением прав граждан на конфиденциальность. ОВД должны стремиться к прозрачному, этичному и эффективному использованию видеонаблюдения, чтобы создать безопасную и справедливую среду для всех граждан.

СПИСОК ЛИТЕРАТУРЫ

1. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ МВД России от 31 декабря 2014 № 1152. – Режим доступа: Специализированная территориально распределенная система СТРАС «Юрист».

2. 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 февраля 2013 г. № 21. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения: 10.10.2024). – Режим доступа: официальный сайт ФСТЭК России. – Текст : электронный.

3. Официальный сайт Аргус-Спектр : [сайт] / ООО «Аргус-Спектр». – Санкт-Петербург, 2024. – URL: <https://argus-spectr.ru/> (дата обращения : 10.10.2024).

4. НИКИРЭТ – комплексное обеспечение безопасности объектов : [сайт] / АО «НИКИРЭТ» государственной корпорации по атомной энергии «Росатом». – ЗАТО г. Заречный, 2024. – URL: <https://nikiret.ru/> (дата обращения : 10.10.2024).

СВЕДЕНИЯ ОБ АВТОРЕ

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.

Abrosimova Evgeniya Mikhailovna.

Lecturer in electronic systems and complexes of security monitoring.

Candidate of technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: chip_ik@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: видеонаблюдение; аналитика данных; повышение безопасности; объекты органов внутренних дел.

Keywords: video surveillance; data analytics; security improvement; objects of internal affairs bodies.

УДК 681.772.7

О. В. Багринцева

ОСОБЕННОСТИ ВНЕДРЕНИЯ МОНИТОРИНГОВЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТЬ ПОДРАЗДЕЛЕНИЙ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

FEATURES OF THE IMPLEMENTATION OF MONITORING SYSTEMS IN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

В настоящей статье рассматриваются основные положения систем мониторинга автотранспорта при транспортировке имущества в правоохранительных органах, а также рассмотрена оптимальная структура системы спутникового определения местоположения автотранспорта.

This article discusses the main provisions of vehicle monitoring systems for the transportation of property in law enforcement agencies, as well as the optimal structure of the satellite positioning system for vehicles.

В современных условиях многие ведомства и организации сталкиваются с необходимостью отслеживать местоположение и состояние мобильных транспортных средств, будь то для рабочих задач или для оперативной передачи деловой информации.

Практически все диспетчерские службы используют технологии для контроля и мониторинга перемещения объектов. Однако существующие инструменты не идеальны: они часто недостаточно автоматизированы и не всегда надежны.

В последние годы назрела острая необходимость в создании новых, надежных технических средств, способных автоматически собирать диспетчерскую информацию как с подвижных объектов, так и с объектов, находящихся на месте. Для решения этой задачи предлагаются различные методы, включая традиционные и спутниковые. Однако на сегодняшний день ни одна из таких систем в России не была реализована.

Разработка такой системы обеспечит автоматизированный сбор информации о местоположении подвижных объектов, участвующих в системе, независимо от их местонахождения на Земле, то есть в глобальном масштабе.

В такой системе оборудование автоматически определяет географические координаты объекта и передает их в диспетчерский центр пользователя. Кроме того, диспетчер может инициировать запрос информации с объекта и передавать необходимые данные обратно.

Помимо решения коммерческих задач, система повышает безопасность при перемещении объектов и может способствовать защите человеческой жизни. Информация о местонахождении объектов, попавших в аварию, может быть оперативно передана в соответствующие поисково-спасательные службы.

Исследования, проведенные в России, выявили основные категории потенциальных пользователей, заинтересованных в получении оперативной информации с подвижных и стационарных объектов:

1. Администрации, эксплуатирующие автомобильный транспорт.
2. Организации, эксплуатирующие подвижной железнодорожный состав и специальные средства.
3. Организации, эксплуатирующие подвижные автомобильные объекты.
4. Научные организации, проводящие с помощью подвижных технических средств изучение окружающего пространства.
5. Организации, эксплуатирующие магистральные трубопроводы и иные удаленные объекты.
6. Предприятия топливно-энергетического комплекса.
7. Сельскохозяйственные предприятия.
8. Коммерческие структуры.

Анализ требований потенциальных пользователей к системам сбора оперативной информации позволил выявить следующее:

1. Важным требованием является автоматическое определение географического положения объекта без участия оператора. При этом точность определения может варьироваться от нескольких метров до десятков километров, в зависимости от конкретных задач.

Некоторые объекты, такие как поезда и автомобили движутся по заранее определенным маршрутам, в то время как другие имеют большую свободу перемещения.

2. Скорость доставки информации от устройства до пункта сбора данных пользователя может варьироваться от нескольких минут до нескольких часов.

3. Количество определений – от нескольких раз в месяц до нескольких раз в час.

4. Система должна обеспечивать передачу не только данных о местоположении, но и дополнительной информации с подвижного объекта и на него. При этом существует широкий спектр информации, которую необходимо передавать.

5. Наличие простых и недорогостоящих оконечных устройств пользователей, которые при необходимости могли бы работать от автономных источников питания.

Ряд ведомств и организаций, таких как МВД России, МЧС России и другие, выразили заинтересованность в использовании системы слежения за местоположением подвижных объектов.

Отдельно стоит отметить заинтересованность в приобретении средств мониторинга автотранспортными предприятиями.

Система должна обеспечивать отслеживание в реальном времени перемещения ценных грузов, пассажирских транспортных средств и других движущихся объектов с точностью до 50 метров. Кроме того, система должна позволять получать информацию о возникновении аварийных ситуаций на движущихся объектах.

Оптимальная структура системы спутникового определения местоположения автотранспорта должна включать в себя:

1. Система должна использовать конstellляцию спутников, включающую достаточное количество спутников, расположенных на разных орбитальных плоскостях. Это позволит обеспечить глобальное покрытие и высокую точность позиционирования.

2. Система должна включать в себя наземную инфраструктуру, состоящую из станций слежения и контроля, которые отслеживают спутники и передают корректирующую информацию для повышения точности позиционирования.

3. Транспортные средства должны быть оборудованы антенной, приемником и процессором, которые принимают сигналы со спутников и вычисляют местоположение транспортного средства.

4. Система должна включать в себя центр управления данными, который обрабатывает, хранит данные о местоположении и обеспечивает доступ к ним для пользователей и приложений.

При реализации спутниковых систем определения местоположения транспортных средств важно учитывать конкретные потребности и бюджетные

ограничения каждого проекта, чтобы создать оптимальную структуру.

Изучив структуру спутниковых систем, можно сказать о том, что для оптимальной работы спутниковых систем позиционирования необходимо учитывать конфигурацию созвездия, характеристики сигнала и данных, технологии обнаружения, инфраструктуру наземного сегмента, стандартизацию, а также функциональность, безопасность и экономическую эффективность.

При разработке таких систем важно найти баланс между точностью, надежностью, функциональностью и стоимостью.

Использование систем мониторинга автотранспорта при транспортировке имущества в подразделениях вневедомственной охраны в наши дни является крайне актуальным по следующим причинам:

- повышение безопасности грузов;
- соблюдение требований законодательства;
- улучшение координации и оперативного реагирования;
- оптимизация маршрутов и сокращение транспортных расходов;
- увеличение эффективности работы;
- обеспечение сохранности транспортных средств;
- повышение прозрачности и отчетности.

Таким образом, использование систем мониторинга автотранспорта при транспортировке имущества в подразделениях вневедомственной охраны Росгвардии в наши дни является не только актуальным, но и необходимым для обеспечения безопасности перевозимых ценностей, соблюдения законодательства и повышения эффективности работы.

СПИСОК ЛИТЕРАТУРЫ

1. Аппаратно-программные комплексы охранного мониторинга : учебное пособие / С. А. Винокуров [и др.]. – Воронеж : Воронежский институт МВД России, 2020. – 209 с.

2. Организация комплексных систем мониторинга и управления силами и средствами объектов охраны / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков, Д. А. Сошнева. – Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2020. – 115 с.

3. Багринцева, О. В. Принципы построения системы охранного мониторинга / О. В. Багринцева // Охрана, безопасность, связь. – 2022. – № 7-1. – С. 14–18.

СВЕДЕНИЯ ОБ АВТОРЕ

Багринцева Оксана Владимировна.

Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.
E-mail: bagrinceva-oksana@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Bagrintceva Oksana Vladimirovna.
Lecturer in electronic systems and complexes of security monitoring.
Candidate of technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: bagrinceva-oksana@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: система мониторинга; безопасность; автотранспорт; защита жизни; спутниковые системы.

Keywords: monitoring system; safety; motor transport; life protection; satellite systems.

УДК 351.74; 614.8

Е. С. Бондаренко

**К ВОПРОСУ О МЕТОДАХ И СРЕДСТВАХ ОРГАНИЗАЦИИ
ОБЕСПЕЧЕНИЯ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ
ОБЪЕКТОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ON THE ISSUE OF METHODS AND MEANS OF ORGANIZING
THE PROVISION OF ANTI-TERRORIST PROTECTION OF OBJECTS
OF THE INTERNAL AFFAIRS BODIES OF THE RUSSIAN FEDERATION**

В данной работе рассмотрены современное состояние охраны объектов органов внутренних дел Российской Федерации. Описаны источники угроз обеспечения безопасности на современном этапе деятельности террористических организаций, группировок и отдельных лиц, которая направлена на подрыв нормального функционирования органов внутренних дел.

In this paper, the current state of protection of objects of the internal affairs bodies of the Russian Federation is considered. The sources of threats to security at the present stage of the activities of terrorist organizations, groups and individuals, which are aimed at undermining the normal functioning of internal affairs bodies, are described.

Современная обстановка показывает, что объекты органов внутренних дел Российской Федерации остаются в числе объектов повышенной террористической опасности. В целях нарушения

функционирования органов внутренних дел, устрашения населения, представители террористических организаций, группировок или отдельные лица совершают террористические акты на объектах территориальных органов МВД России. При этом подобные террористические акты отличаются серьезной подготовкой, повышенной опасностью, а также тяжкие последствия в виде человеческих жертв и материального ущерба.

Текущая ситуация обусловлена несколькими факторами, выделяющимися как основные угрозы безопасности для сооружений, попадающих под ведомство внутренних дел. Во-первых, затрудняющим обстоятельством является отсутствие детально разработанных планов, охватывающих необходимость оперативного реагирования с учётом предполагаемых ресурсов и потенциальных сил. В контексте имеющихся планов, проблема склоняется к их формализованному характеру. Во-вторых, наблюдается несоответствующий уровень компетенции среди руководящего звена и сотрудников комендантских отделений в аспекте эффективности предотвращения и контрмер действиям агрессоров. В-третьих, обостряющим моментом выступает инженерно-техническая укреплённость отдельных объектов, что делает единицы инфраструктуры более уязвимыми перед преступником.

В связи с этим, обеспечение антитеррористической защищённости объектов органов внутренних дел, усовершенствование их инженерно-технической укреплённости является одним из приоритетных направлений в деятельности МВД России.

Антитеррористическая защищённость объекта (территорий) – состояние защищённости здания, строения, сооружения, иного объекта, места массового пребывания людей, препятствующее совершению террористического акта [1].

Первоочередная цель защищённости территориальных органов МВД России от антитеррористических угроз включает в себя обеспечение их защиты от преступных посягательств. Следующим шагом является пресечение и нейтрализация возможных предпосылок и факторов, что могут привести к осуществлению террористических деяний, а также обеспечение готовности руководящего состава и сотрудников к действиям по предупреждению, предотвращению и пресечению террористических актов на объектах территориальных органов МВД России.

В рамках действующего нормативного правового регулирования, направленного на укрепление антитеррористической защиты подразделений органов внутренних дел, ключевыми задачами выступают:

- усовершенствование правовых основ такой деятельности;

- анализ и пресечение потенциальных угроз, направленных на минимизацию возможного риска;
- повышение эффективности инженерно-технических решений для укрепления объектов, с учётом требований нормативных актов;
- организация систематического обучения управленческого состава и сотрудников методам противодействия противоправным актам экстремизма через практические занятия;
- непрерывный мониторинг сохранения антитеррористической защищенности зданий и сооружений, находящихся в ведении органов внутренних дел.

В условиях нарастающей угрозы терроризма, акцентируется важность проведения комплексных инженерно-технических действий для повышения защищённости объектов под юрисдикцией территориальных подразделений МВД России. Данные мероприятия должны быть осуществлены заблаговременно и направлены на то, чтобы инфраструктура учреждений внутренних дел соответствовала установленным стандартам, определённым в нормативных правовых документах.

Защита объектов, входящих в систему территориальных подразделений органов внутренних дел Российской Федерации, от террористических угроз и организация их защиты в случае агрессии зависит от грамотной организации управления силами и средствами органа внутренних дел, ее устойчивости и скрытности, умелых и слаженных действий личного состава, которые отрабатываются в ходе учебно-практических мероприятий.

Повышение антитеррористической защищенности объектов органов внутренних дел, будучи важнейшей задачей в условиях как в режиме повседневной деятельности, так и при возникновении чрезвычайных ситуаций, требует обустройства эффективной системы обеспечения безопасности. Полученный опыт показывает, что детально выстроенная стратегия охраны и обороны позволяет органам внутренних дел успешно выполнять задачи по обеспечению антитеррористической безопасности собственных объектов.

Вместе с тем можно выделить имеющиеся проблемные вопросы:

1. В системе органов внутренних дел антитеррористическая защищенность небольших объектов, таких как участковые пункты полиции, которые зачастую находятся в жилых домах или плотной городской застройке. В своей штатной численности они не имеют должностей для обеспечения пропускного режима и досмотровых мероприятий, тем не менее обязаны обеспечить доступ граждан и иных лиц, желающих обратиться в органы внутренних дел с заявлением или сообщением.

2. В случае на объекте отсутствующих дежурных смен и комплексных систем видеонаблюдения, доступ на объект реализуется через интерактивное взаимодействие по домофонной связи.

3. Объекты, не оборудованные системами видеоконтроля и отсутствием круглосуточных дежурств, регламентируют доступ к своим помещениям через интерактивное взаимодействие с домофонными устройствами.

4. Инженерно-техническая укрепленность не всех объектов территориальных органов МВД России полностью соответствует требованиям приказа МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств» [2].

5. Проводимые контрольные проверки и целевые выезды в территориальные органы внутренних дел показывают, что руководящий состав и сотрудники не всегда уверено знают порядок действий и умеют действовать при нападении (угрозе) нападения.

6. Внезапные проверки сотрудников комендантских подразделений территориальных органов МВД России по обеспечению пропускного режима, проведению досмотровых мероприятий и контролю за прилегающей территорией, показывают, что факты проноса муляжей взрывных устройств на объекты органов внутренних дел по-прежнему возможны.

В рамках существующих границ штатной численности органов внутренних дел и финансовых ограничений, решение актуальных проблем представляются возможным следующими путями:

1. Необходимость проведения инженерно-технических мероприятий, нацеленных на повышение уровня антитеррористической безопасности объектов, определена актуальностью их применения без существенных финансовых вложений и без необходимости осуществления капитального ремонта. Данный анализ направлен на выявление таких мероприятий и исключает работы, требующие высоких финансовых затрат.

2. Средства видеонаблюдения и досмотра являются ключевым фактором в обеспечении безопасности объектов территориальных органов внутренних дел. Развертывание и усовершенствование такого оборудования следует проводить с учётом переменной степени террористической угрозы. Эффективная защита подразумевает гибкую адаптацию к текущим рискам, а также превентивное обновление систем в ответ на эволюционирующие тактики ведения террористической деятельности.

3. Обучение руководящего состава и сотрудников действиям, связанным с отражением нападения (угрозы нападения) на объекты органов внутренних дел в ходе проведения учебно-практических мероприятий, исключаящее формальный подход к их проведению.

Проведения незапланированных внезапных проверок объектов органов внутренних дел МВД России на предмет бдительности сотрудников комендантских подразделений при осуществлении пропускного и досмотрового режимов, контроля за прилегающей территорией.

СПИСОК ЛИТЕРАТУРЫ

1. О противодействии терроризму : Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 10.07.2023)// СПС «КонсультантПлюс».

2. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ МВД России от 31.12.2014 № 1152 (ред. 05.03.2024) // СПС «КонсультантПлюс».

СВЕДЕНИЯ ОБ АВТОРЕ

Бондаренко Евгений Сергеевич.

Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: bondarenko-92-92@mail.ru

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

Bondarenko Evgeny Sergeevich.

Lecturer at the Department of Radio Engineering Systems and Security Monitoring complexes.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: bondarenko-92-92@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: антитеррористическая защищенность; дело; территориальный орган МВД России; орган; обеспечение безопасности; инженерно-техническая укрепленность; пропускной режим; угроза нападения.

Keywords: anti-terrorist protection; case; territorial body of the Ministry of Internal Affairs of Russia; body; security; engineering and technical fortification; access control; threat of attack.

УДК 351.74

**К ВОПРОСУ О ПРИМЕНЕНИИ «УМНЫХ ЗАМКОВ»
В КАЧЕСТВЕ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ**

**ON THE ISSUE OF THE USE OF «SMART LOCKS»
AS TECHNICAL MEANS OF PROTECTION**

В работе рассматривается возможность использования «умных замков» для охраны объектов, проводится анализ представленных на рынке Российской Федерации «умных замков», а также отмечаются имеющиеся проблемы для подобных изделий.

The paper considers the possibility of using «smart locks» for the protection of objects, analyzes the «smart locks» presented on the market of the Russian Federation, and also notes the existing problems for such products.

Современный рынок технических средств безопасности предлагает широкий спектр решений, направленных на защиту объектов от различных угроз. Неподдельный интерес представляют изделия, обладающие дополнительным (расширенным) функционалом, способствующим противодействию противоправным посягательствам. Одним из таких решений являются замки, оборудованные средствами раннего обнаружения несанкционированных воздействий.

На рынке Российской Федерации представлен широкий ассортимент «умных замков», функционал которых в том числе включает раннее реагирование на несанкционированное воздействие. Самыми простыми «умными замками» с функцией раннего реагирования можно считать различные навесные замки, имеющие встроенную сигнализацию.

Одним из таких вариантов являются навесные замки со встроенной системой сигнализации производства AlarmLock и Maximum.

Оба замка имеют стандартный и увеличенный размер дужки, что позволяет установить замок почти в любом требуемом месте. Если в режиме охраны переместить или тронуть замок, то средство обнаружения вибрации передаст сигнал на систему сигнализации и прозвучит три предупредительных звуковых сигнала. Если манипуляции с замком не прекратятся, то на 10 сек включится громкая тональная сирена, которая будет работать с интервалом в 10 сек до тех пор, пока продолжаются действия злоумышленника. Система сигнализации станет в первоначальное состояние охраны только в том случае, если состояние покоя замка продлится более 35 сек.

Кроме навесных «умных замков» на рынке Российской Федерации представлены варианты врезных «умных замков». К таким, например, относится *Xiaomi Mijia Smart Door Lock* производства Xiaomi Corporation.

Комплект из замка и пары дверных ручек с длинным основанием. *Mijia Smart Door Lock* поддерживает шесть методов открытия:

- по отпечатку пальца;
- постоянным кодом;
- временным кодом;
- через приложение по NFC;
- через приложение по Bluetooth;
- механическим ключом.

Многие «умные замки» открываются запасным физическим ключом, в том числе *Mijia Smart Door Lock*. Для этого «умные замки» оснащаются механической частью с цилиндром и ключом, которая нужна на случай отказов остальных систем. Замочную скважину прикрывает круглая заглушка. Предполагается, что если злоумышленник разрушит переднюю панель, ему придется затратить время на преодоление механизма внутри двери.

С наружной стороны замка предусмотрен светодиодный дисплей для ввода кода. Замок питается от восьми элементов питания типа АА. Внутри замка встроены следующие устройства:

- детектор наличия ключа;
- детектор положения косого язычка;
- детектор положения прямоугольного язычка;
- детектор положения углового язычка;
- детектор положения язычка запираения;
- детектор вскрытия лицевой панели;
- детектор давления на ручку.

Встроенные устройства следят за состоянием замка и направляют уведомления о подозрительных ситуациях. Для этого потребуется подключить замок к «умному дому Mihome» через Bluetooth-шлюз.

На оси ручки находится сканер отпечатков пальцев, по заявлению изготовителя способный отличать реальные отпечатки от «неживых», а также идентифицировать мокрые пальцы. Кроме того, производителем отмечается, что замок защищен от электромагнитного воздействия, а также что в режиме ожидания от элементов питания заряда хватит на 15 месяцев (приложение для «умного замка» предупреждает, когда требуется их заменить).

Похожие замки, но с меньшим защитным функционалом, предлагает фирма SmartBase. Дверные замки для входных металлических дверей *Smart Lock Base* и *Smart Lock Prime* оборудованы встроенными видеокамерами, которая сохраняет изображение на CD карте и передает на мобильное приложение. Мобильное приложение USmart Go работает по беспроводной сети Wi-Fi. В замки встроена сигнализация, которая оповещает на мобильном приложении о попытке несанкционированного входа.

Еще несколько подобных вариантов «умных замков» врезного типа предлагаются компанией Philips. Замки *Philips Easykey 7300* и *Philips Easy Key 9300* предназначены для использования в домах, офисах и квартирах.

Замки оснащены функцией «антипаника» [1]: при нажатии на ручку происходит разблокировка запертой двери. При закрывании двери, засов (ригель) [2] выдвигается автоматически и блокирует дверь или происходит оповещение владельца о не полностью прикрытой двери. Дополнительно в замки встроена сигнализация от взлома при помощи рычага, наружная сигнализация от принудительного запираения и сигнализация при неисправности замка-защелки. Доступ снаружи возможен только при вводе мастер-кода, принадлежащего хозяину квартиры.

Компанией Zhejiang Dahua Technology предлагается интеллектуальный дверной замок *Imou K2 Smart Lock*, использующий для отпираения замка технологию RFID. Устройство состоит из трех элементов. Первый – внешняя панель, на которой расположен считыватель RFID-карт, сканер отпечатка пальца и сенсорная клавиатура с цифровыми клавишами и кнопкой дверного звонка. Вторая часть – это внутренняя панель, устанавливаемая внутри запираемого помещения. На ней расположена завертка для механического управления засовом (ригелем), отсек на 4 батарейки типа АА и динамик звонка. На обеих панелях присутствуют ручки механической защелки. Третий элемент – врезной механический блок с защелкой и засовом (ригелем).

По заявлению изготовителя одного комплекта батареек хватает примерно на год использования, в зависимости от интенсивности работы. Кроме того, на внутренней панели находится разъем Micro USB для аварийного питания устройства. При падении напряжения блока элементов питания до 4,8 В замок подает предупреждение о необходимости их замены. Замок предназначен для установки в отапливаемых помещениях и работает при температуре среды от минус 10°C. Умный дверной замок *Imou K2 Smart Lock* имеет 5 способов открытия с использованием: приложения Imou, картой Mifare, пароля, отпечатка пальца, механической защелки. В замок дополнительно встроены звонок. При попытке несанкционированного доступа или попытках повреждения обеспечивается блокировка замка с уведомлением владельца.

Еще одним вариантом «умного замка», для открывания которого применяется технология RFID, является дверной замок *Samsung SHS-1321* производства компании Samsung Electronics.

Этот «умный замок» накладного типа с одинарным засовом (ригелем). Устройство имеет высокочувствительный дисплей, который защищен ударопрочным ABS-пластиком, он обеспечивает не только антивандальную функцию, а еще и предохраняет от различных погодных условий. Таким образом, замок можно устанавливать не только в помещении, но и на улице. Устройство рассчитано на работу при температуре от минус 20°C до

плюс 60°C и влажности 80%. Эта модель замка подходит для любой двери толщиной (40–50) мм, с любым типом и сторонностью открытия.

Для открывания замка *Samsung SHS-1321* может использоваться цифровой код, либо RFID-карта. Устройство хранит в памяти один цифровой код и до 20 RFID-карт. Система защищена от подбора пароля, поэтому при пятикратном ошибочном введении, замок подаст звуковой сигнал и автоматически заблокируется на три минуты. Если требуется дополнительная защита, то в замке может использоваться режим двойной авторизации. Для открытия двери в этом режиме необходимо ввести цифровой пароль и использовать RFID-карту.

Замок *Samsung SHS-1321* оснащен функцией охраны. Эта функция включает сигнализацию при попытке отпереть замок изнутри или снаружи (в зависимости от того, как она настроена). Таким образом, имеется возможность максимально контролировать не только доступ в помещение, а еще и попытки его покинуть. Помимо этого, устройство оснащено функцией обнаружения вторжений. При попытке несанкционированного отпирания изнутри или снаружи, будет активирована сигнализация.

Кроме того, этот «умный замок» оснащен функцией обнаружения пожара. При возникновении пожара, температурный датчик обнаружит возгорание и активирует сигнализацию, после чего автоматически откроет дверь. Эта функция срабатывает при нагреве воздуха до плюс 65°C. Когда температура вокруг нормализуется, замок вернется в состояние стабильного функционирования.

Работу *Samsung SHS-1321* обеспечивают 4 элемента питания типа АА, что делает его автономным от единой электросети. Благодаря этому имеется возможность его установки в любое место, вне зависимости от кабелей питания. Изготовитель утверждает, что в среднем батареек хватает на год стабильного использования. Если своевременно не заменить батарейки и они полностью разрядятся, то всегда есть возможность использовать резервную батарею аварийного питания.

Несмотря на разнообразие представленных на рынке «умных замков», которые могут быть достаточно высокотехнологичными (управляться по отпечатку пальца, постоянным кодом, временным кодом, через приложение по NFC, через приложение по Bluetooth, открываться с использованием технологии RFID, а также с помощью специального приложения на смартфоне и тому подобного), в настоящее время вопрос надежности таких замков для обеспечения охраны объектов остается открытым.

Представленные технологии имеют уязвимости и подвержены кибератакам [3]. В случаях взлома других элементов «умного дома» (например, «умная лампочка» или «умный пылесос») последствия могут быть незначительными. Но взлом «умного замка», который может быть установлен и на входную дверь, напрямую влияет на степень защищенности охраняемого объекта.

Таким образом, на рынке Российской Федерации представлен широкий ассортимент «умных замков», в основном применяющихся в составе «умного дома». Технологии, задействованные для реализации функции раннего реагирования в «умных замках», имеют уязвимости и подвержены кибератакам, что напрямую влияет на степень защищенности. Для обеспечения охраны объектов целесообразным представляется применение замков, исключающих возможность дистанционного вмешательства в тактику работы механизма запирающего устройства, а также имеющих соответствующие документы, подтверждающие соответствие изделия требованиям, установленным нормативными правовыми актами Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 31471-2021 «Устройства экстренного открывания дверей эвакуационных и аварийных выходов. Технические условия».
2. ГОСТ Р 52582-2006 «Замки для защитных конструкций. Технические требования и методы испытаний на устойчивость к криминальному отмыканию и взлому».
3. Повышение безопасности и надежности умных замков / А. Ухов, В. Герасимов, Л. Селиванов, В. Симон // Электроника: Наука, технология, бизнес. – 2020. – № 6(197). – С. 60–63.

СВЕДЕНИЯ ОБ АВТОРАХ

Волкова Виктория Геннадьевна.

Старший научный сотрудник отделения лабораторных исследований и испытаний.

Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: vikgennn91@mail.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Зубова Наталья Вячеславовна.

Старший научный сотрудник отделения лабораторных исследований и испытаний.

Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: zubava@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Volkova Viktoriya Gennadievna.

Senior Researcher at the Laboratory Research and Testing Department.

Federal State Institution «Scientific Research Center «OKHRANA» of the Federal service of National Guard of the Russian Federation.
Russia, 111539, Moscow, Reutovskaya, 12B.

Zubova Natalia Vyacheslavovna.
Senior Researcher at the Laboratory Research and Testing Department.
Federal State Institution «Scientific Research Center «OKHRANA» of the Federal service of National Guard of the Russian Federation.
Russia, 111539, Moscow, Reutovskaya, 12B.

Ключевые слова: умные замки; безопасность; несанкционированный доступ; обнаружение; сигнализация; умный дом; защита объектов.

Keywords: smart locks; security; unauthorized access; detection; alarm; smart home; protection of objects.

УДК 654

С. А. Гречаный

**ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОХРАНЫ ОБЪЕКТА
ПРИ УГРОЗЕ ПРИМЕНЕНИЯ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ
В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ**

**FEATURES OF THE ORGANIZATION OF OBJECT PROTECTION
IN CASE OF THREAT OF USE OF UNMANNED AIRCRAFT
FOR TERRORIST PURPOSES**

В статье рассматриваются вопросы комплексного обеспечения безопасности объектов, учитывая специфику угроз применения беспилотных летательных аппаратов.

The article deals with the issues of comprehensive security of facilities, taking into account the specifics of threats to the use of unmanned aerial vehicles.

Беспилотное воздушное судно (далее – БВС) представляет собой летательный аппарат, не имеющий на борту экипажа, способный перемещаться самостоятельно или под дистанционным управлением оператора. Это устройство может автономно выполнять различные задачи в воздушном пространстве благодаря заложенной в нем программе автопилота или же может управляться человеком-оператором с помощью пульта дистанционного управления [1].

Сегодня существует реальная угроза использования данных аппаратов в незаконных целях. Злоумышленники способны применять их для сбора информации и наблюдения, например, в видимом и инфракрасном диапазонах, а также для длительного отслеживания объектов. Кроме того, БВС могут доставлять опасные грузы, такие как взрывчатые или ядовитые вещества, опасные для жизни и здоровья человека, взрывные устройства в охраняемые места, превращаясь, таким образом, в инструмент для противоправных действий, такие как террористические атаки. Классификация, например, беспилотных воздушных аппаратов, как одного из видов беспилотных аппаратов, имеет обширную классификацию, учитывая цель применения, размер, массу, дальность полета и способ управления [2].

Современные беспилотники представляют потенциальную угрозу для безопасности различных объектов. Их присутствие над территорией требует немедленного реагирования со стороны сотрудников охраны. При обнаружении неизвестного дрона, сотрудники охраны обязаны сразу же сообщить об этом руководству, которое должно оперативно связаться с правоохранительными органами и территориальным подразделением Росгвардии. Важно предоставить полную информацию: данные о себе, адрес объекта, где был замечен БВС, источник и время поступления информации о беспилотнике, особенности его поведения, наличие видеозаписей с камер видеонаблюдения, а также иные запрошенные уполномоченными органами сведения.

Необходимо организовать наблюдательный пункт для слежения за воздушными перемещениями над территорией объекта и в районе, прилегающем к этой территории, также стоит отметить, что необходимо избегать размещения поста в местах массового скопления людей. Важно зафиксировать время и место обнаружения БВС, их высоту полета, скорость и направление полета, а также количество и примерную форму летательных аппаратов, осуществить фото- и видеосъемку. Усилить меры безопасности, а также пропускной и внутриобъектовый режимы. Проводить регулярные обходы территории для выявления подозрительных предметов или лиц. Если на территории объекта обнаружен беспилотник, следуйте установленным инструкциям по обнаружению подозрительных объектов. При появлении аппарата в воздухе над территорией отслеживайте его траекторию и сообщайте руководству о любых изменениях его поведения.

При поступлении дополнительных указаний от местных органов власти и территориальных органов Росгвардии, действовать согласно им. По указанию должностного лица, управляющего деятельностью работников объекта, или уполномоченного им лица, при возникновении угрозы жизни и здоровью, предупредить находящихся на объекте людей

о потенциальной опасности и при необходимости организовать укрытие, либо эвакуировать личный состав.

Таким образом, для обеспечения надежной работы охраняемых объектов необходимо комплексное обеспечение безопасности, одним из ключевых элементов которого является защита от террористических угроз. Все действия по охране должны быть нацелены на выявление и нейтрализацию потенциальных угроз в максимально короткие сроки.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении Порядка принятия решения о пресечении функционирования беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов в целях отражения нападения либо угрозы нападения на объекты, охраняемые военизированными и сторожевыми подразделениями федерального государственного унитарного предприятия "Охрана" Федеральной службы войск национальной гвардии Российской Федерации, работников военизированных и сторожевых подразделений федерального государственного унитарного предприятия "Охрана" Федеральной службы войск национальной гвардии Российской Федерации или лиц, находящихся на этих объектах, а также Перечня должностных лиц федерального государственного унитарного предприятия "Охрана" Федеральной службы войск национальной гвардии Российской Федерации, уполномоченных на принятие такого решения : приказ Федеральной службы войск национальной гвардии Российской Федерации от 16.10.2023 № 378.

2. Обзор Главного центра научных исследований Федеральной службы войск национальной гвардии Российской Федерации «Классификация и единые требования к образцам средств противодействия робототехническим комплексам (системам) иностранных государств», 2022 г.

СВЕДЕНИЯ ОБ АВТОРЕ

Гречаный Сергей Анатольевич.

Начальник кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук, доцент.

Воронежский институт МВД России.

E-mail: grechan7777@mail.ru.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Grechanyi 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.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотное воздушное судно; меры безопасности; инструкции; подозрительный объект.

Keywords: unmanned aircraft; security measures; instructions; suspicious object.

УДК 654.9

М. А. Гудков, А. А. Гапеев, Д. Ю. Калков, И. С. Никитин

К ВОПРОСУ МЕТОДИКИ ОЦЕНКИ БЕЗОПАСНОЙ ЗОНЫ ПО ДЕЙСТВИЮ ВОЗДУШНОЙ УДАРНОЙ ВОЛНЫ

ON THE ISSUE OF THE METHODOLOGY FOR ASSESSING THE SAFE ZONE BY THE ACTION OF AN AIR SHOCK WAVE

В статье рассматриваются существующие методы оценки пожаровзрывоопасных свойств пиротехнических изделий. В ходе проверочного эксперимента установлено, что существующие подходы не позволяют провести оценку безопасной зоны по действию ударной волны для пиротехнических изделий малой мощности (до 0,05 кг в тротиловом эквиваленте). Предлагается в качестве критерия безопасности ввести такое значение давления ударной волны, которое, по численной величине, должно быть меньше 14 709,6 Па. Данное значение соответствует целостности барабанной перепонки человека.

The article discusses the existing methods for assessing the fire and explosive properties of pyrotechnic products. During the verification experiment, it was found that existing approaches do not allow for an assessment of the safe zone by the impact of a shock wave for pyrotechnic products of low power (up to 0.05 kg in TNT equivalent). It is proposed to introduce as a safety criterion such a value of the shock wave pressure, which, numerically, should be less than 14 709,6 Pa. This value corresponds to the integrity of the human eardrum.

В средствах массовой информации часто встречаются заметки и статьи о многочисленных загораниях, пожарах и случаях гибели и травматизма, особенно среди детей, вызванных нарушениями правил пожарной безопасности при обращении с пиротехническими изделиями. Данная проблема становится еще более актуальной в канун Нового года и в период зимних каникул.

Риски поражения и гибели людей при обращении с пиротехническими изделиями еще весьма высоки, так как многие вопросы, связанные с обеспечением пожаровзрывобезопасности при транспортировании, хранении, применении пиротехнических изделий, не решены.

Современный рынок гражданской пиротехники формировался с 90-х годов прошлого века. Кроме бенгальских огней и хлопушек в розничной продаже появились петарды, ракеты, фонтаны, салюты. На отечественный рынок хлынул поток импортной пиротехнической продукции, зачастую весьма низкого качества и поэтому весьма пожаровзрывоопасной.

Пиротехнические изделия (далее ПИ) являются пожароопасными и (или) взрывоопасными. Продукты сгорания ПИ могут оказывать вредные воздействия на людей и окружающую среду. Внешние воздействующие факторы [ВВФ (удар, нагрев, электромагнитное излучение, детонационный импульс и др.)] могут вызывать несанкционированное срабатывание ПИ или потерю их работоспособности, если уровни ВВФ выше допустимых.

Превышение установленных уровней внешних воздействий, использование изделий не по назначению или не в соответствии с инструкцией по применению (эксплуатации), а также несоответствие параметров и характеристик ПИ и используемого пускового оборудования могут приводить к аномальной работе, разрушению и разлету за пределы установленной опасной зоны элементов конструкций и горящих пиротехнических, возникновению ударных волн.

В зависимости от назначения и конструктивных особенностей ПИ их действие сопровождается проявлением одного или нескольких опасных факторов (табл. 1), характеризующихся уровнями опасности.

Таблица 1

Опасные факторы и опасные зоны пиротехнических изделий

Опасный фактор	Определяющий параметр, единица величины	Уровень опасности (размер зоны)
1. Пламя или высокотемпературная струя продуктов сгорания	Размеры пламени, м	Все пламя
2. Разбрасываемые пожароопасные элементы конструкции (горящие таблетки, раскаленные шлаки, искры и пр.)	Радиус разлета, м	Вся площадь, ограниченная радиусом разлета
3. Тепловое (инфракрасное) излучение	Поверхностная плотность, Вт/м	540
4. Ударная волна при взрыве	Давление, Па	35–10
5. Разлетающиеся поражающие осколки	Радиус разлета, м	Вся площадь, ограниченная радиусом разлета

6. Движущиеся за счет начальной скорости выброса или под действием реактивной силы ПИ или ПЭ	Кинетическая энергия, Дж	20
7 Акустическое излучение	Уровень звука, дБА:	
	- импульсный	140
	- длительный	120
8 Оптическое излучение	Плотность потока, Дж/м	1·10
9 Продукты сгорания или диспергирования в аэрозольном состоянии	Определяют по нормативной и технической документации на ПИ	
10 Специфическое воздействие продуктов сгорания на человека и окружающую среду	То же	

Методы оценки пожаровзрывоопасности пиротехнических изделий:

1. Метод определения размеров пламени. Метод позволяет определять размеры пламени или(и) радиус разлета горящих элементов при работе малогабаритных ПИ. Сущность метода заключается в видеорегистрации пламени работающего ПИ и сравнении размеров пламени с размерами изображения эталона на экране монитора или телевизора. Погрешность измерений не более 10% [1].

2. Метод измерения размеров пламени и температуры поверхностей пиротехнических изделий [1]. По данному методу проводят измерения и расчеты, позволяющие установить распределение яркостных температур на поверхности излучающего объекта, визуализируемого инфракрасной камерой. Объектом определения полей яркостных температур являются возникающие при горении пиротехнического состава тепловые зоны: пламени и корпуса ПИ. В основу метода положен принцип зависимости интенсивности теплового излучения объекта от температуры его поверхности. Метод обеспечивает измерение полей яркостных температур, значения которых составляют от 20°C до 2400°C, на поверхности нагретых объектов.

3. Определение размера опасной зоны для ПИ. Метод позволяет определять размеры опасной зоны для ПИ, предназначенных для применения в помещениях или в руках и не имеющих опасных факторов, кроме пламени и разлетающихся искр. Метод заключается в органолептической регистрации загорания индикаторного вещества (ваты) в ячейках, размещенных на координатной площади. Погрешность метода не превышает 20% [1].

4. Метод костровой пробы. Метод основан на способности ПИ в упаковке или без нее загораться или взрываться [2] под действием открытого огня.

Предварительное сравнение экспериментальных и теоретических результатов, для ПИ малой мощности (до 0,05 кг в тротиловом эквиваленте) показало, что традиционные подходы по определению безопасного расстоя-

яния от эпицентра взрыва не подходят. В качестве критерия безопасности предлагается ввести такое значение давления ударной волны, которое, по численной величине, должно быть меньше 14 709, 6 Па, что соответствует целостности барабанной перепонки человека.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 33732-2016 Изделия пиротехнические. Общие требования безопасности СПС «КонсультантПлюс».

2. Определение параметров взрыва смеси горючих газов / И. А. Терин, В. А. Сулименко, М. А. Гудков, Э. Б. Гафарова. В сборнике: Гражданская оборона на страже мира и безопасности. Материалы VII Международной научно-практической конференции, посвященной Всемирному дню гражданской обороны в Год 90-летия со дня образования Академии ГПС МЧС России. В 5-ти частях. – Москва, 2023. – С. 212–215.

СВЕДЕНИЯ ОБ АВТОРАХ:

Гудков Максим Андреевич.

Доцент кафедры процессов горения и экологической безопасности (в составе учебно-научного комплекса процессов горения и экологической безопасности).

Кандидат технических наук.

Академия Государственной противопожарной службы МЧС России.

E-mail: M.Gudkov@academygps.ru.

Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Гапеев Артём Александрович.

Заместитель начальника кафедры процессов горения и экологической безопасности (в составе учебно-научного комплекса процессов горения и экологической безопасности).

Кандидат химических наук.

Академия Государственной противопожарной службы МЧС России.

E-mail: A.Gapeev@academygps.ru.

Россия, 129366, Москва, ул. Бориса Галушкина, 4.

Калков Дмитрий Юрьевич.

Доцент кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: dmitreyrus@mail.ru.

Россия, 394065, Воронеж, проспект Патриотов, 53.

Никитин Иван Сергеевич.
Доцент кафедры комплексной безопасности в строительстве.
Кандидат химических наук.
Национальный исследовательский Московский государственный
строительный университет.
E-mail: nikitinivan@inbox.ru.
Россия, 129337, г. Москва, Ярославское шоссе, д. 26.

Gudkov Maxim Andreevich.
Docent of the Department of Combustion processes and Environmental
Safety (as part of the educational and scientific complex of combustion process-
es and environmental safety).
Candidate of Technical Sciences.
State Fire Academy of EMERCOM of Russia.
Moscow, 129366, Russia, Borisa Galushkina street, 4.

Gapeev Artem Alexandrovich.
Deputy head of the Department of Combustion Processes and Environ-
mental Safety (as part of the educational and scientific complex of combustion
processes and environmental safety).
Candidate of Chemical Sciences.
State Fire Academy of EMERCOM of Russia.
Moscow, 129366, Russia, Borisa Galushkina street, 4.

Kalkov Dmitry Yurievich.
Associate Professor of the Department of radio engineering systems and
security monitoring complexes.
Candidate of Technical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Nikitin Ivan Sergeevich.
Associate Professor of the Department of Integrated Safety in Construction.
Candidate of Chemical Sciences.
National Research Moscow State University of Civil Engineering.
Moscow, 129337, Russia, Yaroslavskoye shosse, 26.

Ключевые слова: пиротехнические изделия; давление взрыва; тро-
тиловый эквивалент.

Keywords: pyrotechnic products; explosion pressure; TNT equivalent.

УДК 62-756.62

УГРОЗЫ ПЕРИМЕТРАЛЬНОЙ ЗАЩИТЫ ТЕРРИТОРИЙ И ОБЪЕКТОВ ОВД

THREATS TO THE PERIMETER PROTECTION OF TERRITORIES AND ATS FACILITIES

В статье рассматривается угроза применения роботизированных комплексов злоумышленниками.

The article discusses the threat of the use of robotic complexes by intruders.

В настоящий момент основной проблемой защиты территорий и объектов ОВД является угроза применения преступниками роботизированных комплексов. Прежние угрозы безопасности были связаны с наземным проникновением злоумышленников, поэтому системы защиты были ориентированы на своевременное обнаружение человека, пытающегося пробраться на охраняемую территорию [1].

Появление новых технологий привело к увеличению угроз, связанных с роботизированными комплексами. Применение БПЛА, надводных дронов, подводных дронов увеличивает число моделей возможных нарушителей. При этом нарушитель сам физически не проникает за периметр и на охраняемый объект. Для этого он использует роботизированные комплексы, что в свою очередь уменьшает риски для нарушителя, а также уменьшает риски быть пойманным и наказанным. Применение роботизированных комплексов злоумышленниками не разрушает инженерные заграждения охраняемой территории и объектов ОВД и не воздействует на технические средства охраны периметра, что затрудняет обнаружение роботизированных комплексов. Для их обнаружения и противодействия должны быть приняты другие кардинальные меры.

Для противодействия роботизированным комплексам, действующим в воздухе, на воде и под водой, применяются различные технологии, включая локаторы, пеленгаторы радиосигналов и радиочастотные глушилки. Активное развитие и внедрение видеоаналитики также играет важную роль. Системы охранного телевидения, оснащенные алгоритмами обнаружения, позволяют оценивать объекты, приближающиеся к охраняемой территории, и своевременно активировать меры защиты, такие как подавление каналов управления и создание помех. Не исключается также возможность физического устранения угрозы со стороны роботизированных комплексов.

В настоящее время основными эффективными и доступными методами обнаружения роботизированных комплексов:

– Радиолокационное обнаружение. Радиолокатор способен выявлять БПЛА, определять их местоположение и параметры движения, а также анализировать их свойства и характеристики, используя радиоволны, которые излучаются или отражаются от объектов.

– Радиотехническое обнаружение. Эта система проводит сканирование радиозэфира для поиска сигналов, исходящих от БПЛА. После обнаружения сигнала происходит его идентификация, а также вычисление координат и траектории движения аппарата.

– Оптическое обнаружение. Данный метод использует оптоэлектронные датчики с высоким разрешением для выявления БПЛА.

– Акустическое обнаружение. Для обнаружения БПЛА применяются акустические системы, которые улавливают звуки, издаваемые движущимися аппаратами, с помощью высокочувствительных микрофонов.

На текущий момент производители систем обнаружения воздушных целей объединяют различные устройства в одном комплексе, сочетая радиолокационные станции с оптико-электронными и/или радиотехническими средствами. Это комбинирование технологий повышает вероятность выявления БПЛА, учитывая недостатки отдельных методов, и способствует более точному распознаванию аппаратов, а также снижению числа ложных срабатываний. Однако такая интеграция увеличивает стоимость оборудования для охраняемых объектов.

Дополнительные трудности возникают при попытках задержания оператора роботизированного комплекса. Он может находиться в автомобиле, жилом помещении или другом укрытии, что затрудняет его обнаружение и задержание. В то же время для поиска задействуются значительные ресурсы.

Из выше сказанного перспективной технологией, которая начнет оказывать существенное влияние на защиту территорий и объектов ОВД будет искусственный интеллект. Искусственный интеллект значительно повысит возможность сбора, обработки и глубокого анализа полученной информации для дальнейшего обеспечения объективного принятия решений, сведя к минимуму ошибку человека. На наш взгляд, это наиболее перспективное направление развития защиты территорий и объектов ОВД. В сложившейся ситуации, когда угрозы появляются быстрее, чем разрабатываются методы защиты, необходимо осуществлять дистанционное обнаружение на предмет угроз не на периметре, а на дальних подступах к первому рубежу охраны.

Для эффективной защиты территорий и объектов ОВД необходимо учитывать эти угрозы и применять комплексный подход, который должен включать:

– многоуровневую систему защиты, включающую инженерные и технические средства;

– регулярное техническое обслуживание инженерных и технических средств;

- постоянный мониторинг работоспособности технических средств;
- проведение инструктажей и тренировок с сотрудниками, обслуживающими инженерные и технические средства;
- постоянный мониторинг с последующим анализом потенциальных угроз и адаптацию всей системы защиты к изменяющимся угрозам [2].

Периметральная защита территорий и объектов органов внутренних дел (ОВД) играет ключевую роль в обеспечении безопасности и защиты важных государственных и общественных ресурсов. Тем не менее, существует множество потенциальных угроз, которые могут поставить под сомнение эффективность этих систем.

Технические угрозы. Современные технологии позволяют злоумышленникам использовать различные средства и устройства для обхода периметральной защиты. Это могут быть беспилотные летательные аппараты, системы подавления сигналов или даже взломы имеющихся охранных систем.

Физические угрозы. Необходимо учитывать возможность несанкционированного проникновения через периметр. Это может быть достигнуто как путем применения физической силы, так и с использованием специальных инструментов, таких как отмычки или кислота для разрушения заборов.

Психологические угрозы. Угрозы не всегда проявляются в физической форме. Психологический аспект не следует недооценивать, поскольку действия, направленные на запугивание персонала или провокации конфликты, могут серьезно сказаться на боеготовности и работе службы.

Координация и коммуникация. Качество обмена информацией между различными службами и подразделениями ОВД также может оказать влияние на эффективность периметральной защиты. Неполная информация о потенциальных угрозах или задержки в реагировании могут привести к серьезным последствиям.

Элементы внутренней угрозы. Существуют риски, связанные с внутренними факторами, такими как недовольство сотрудников или коррупция, что может привести к саботажу или предательству.

Для эффективного противодействия этим угрозам, необходимо внедрение комплексного подхода, включающего регулярную оценку защищенности, использование современных технологий и обеспечение надежной подготовки персонала. Важно также развивать механизмы взаимодействия с другими службами и органами правоохранительной системы для своевременного обмена информацией о потенциальных угрозах.

СПИСОК ЛИТЕРАТУРЫ

1. Р 78.36.026-2012. Рекомендации по использованию технических средств обнаружения, основанных на различных физических принципах, для охраны огражденных территорий и открытых площадок.

2. Винокуров С. А. Организация периметральных систем безопасности : курс лекций / С. А. Винокуров, С. А. Гречаный, Н. И. Меркулова. – Воронеж : Воронежский институт МВД России, 2021.

СВЕДЕНИЯ ОБ АВТОРЕ

Дуплякин Петр Михайлович.

Преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Воронежский институт МВД России.

E-mail: 00008540@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Duplyakin Pyotr Mikhailovich.

Lecturer at the Department of Radio Engineering Systems and Security Monitoring complexes.

Voronezh Institute of the Ministry of the Interior of Russia.

Russia, 394006, Voronezh, Lenin Str., 86.

Ключевые слова: роботизированные комплексы; надводные дроны; подводные дроны; безопасность периметра ОВД.

Keywords: robotic complexes; surface drones; underwater drones; security of the ATS perimeter.

УДК 654.9

И. С. Ивануха, Д. Ю. Калков

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРИ ПРОВЕДЕНИИ ОБСЛЕДОВАНИЯ СОБСТВЕННЫХ ОБЪЕКТОВ МВД РОССИИ НА ПРЕДМЕТ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ

PROBLEMATIC ISSUES WHEN CONDUCTING A SURVEY OF THE RUSSIAN INTERIOR MINISTRY'S OWN FACILITIES FOR ANTI-TERRORIST PROTECTION

В статье рассматриваются проблемные аспекты, связанные с проведением контрольных проверок по антитеррористической защищенности территориальных органов МВД России.

The article discusses the problematic issues, associated with conducting control checks on anti-terrorism security of the territorial bodies of the Ministry of Internal Affairs of Russia.

Известно, что объекты органов внутренних дел Российской Федерации являются объектами повышенной террористической опасности. Деятельность террористических организаций, группировок и отдельных лиц направлена на подрыв нормального функционирования органов государственной власти, в том числе органов внутренних дел, что является источником угроз при обеспечении их безопасности. Совершаются данные террористические акты, как правило, с целью устрашения населения. Сам по себе террористический акт влечет за собой как правило тяжкие последствия в виде серьезного социального и материального ущерба [1].

Причинами, способствующими успешному совершению террористических атак, могут послужить формальный подход при разработке специальных планов, отражающих расчеты сил и средств, отсутствие таких планов на объектах, неграмотные действия личного состава из-за недостаточного уровня подготовленности к действиям, связанным с угрозой нападения на объект, а также недостаточная инженерно-техническая укрепленность объектов органов внутренних дел. Именно поэтому повышение инженерно-технической укрепленности объектов органов внутренних дел, обеспечение их антитеррористической защищенности является одним из приоритетных направлений в деятельности МВД России [1].

Ежегодно в каждом регионе Российской Федерации проходит контроль антитеррористической защищенности объектов территориальных органов МВД России. Антитеррористическая защищенность объекта или территории – состояние защищенности здания, строения, сооружения, иного объекта, места массового пребывания людей, препятствующее совершению террористического акта. Проводится данное мероприятие комиссионно.

В комиссии принимают участие специалисты разных областей и направлений, и, как показывает практика, сотрудники, входящие в ее состав, не всегда обладают компетенциями, позволяющими давать объективную оценку по всем вопросам, касающимся поставленной задачи. В первую очередь это относится к специалистам инженерной службы.

Стоит отметить, что раньше в комиссии по обследованию и категорированию объектов территориальных органов МВД России входили сотрудники вневедомственной охраны, квалификация и род деятельности которых направлены на решение задач по обеспечению безопасности объектов с помощью технических средств охраны. Отсутствие на сегодняшний день таких специалистов также сказалось на качестве обследования объектов и решению задач по антитеррористической защите.

Ещё одним фактором является время, затрачиваемое на обследование объектов. Порой временные сроки обследования достаточно сжаты. Происходит это по той причине, что комиссия может проводить за сутки обследование нескольких объектов, находящихся на значительном расстоянии друг от друга. Соответственно достаточно много времени затрачивается на перемещение членов комиссии и перерыв для приема пищи.

Следующим фактором хотелось бы отметить, что некоторые объекты такие, как, например, изолятор временного содержания не сразу планировались при постройке районного отдела.

Важным аспектом также является тот факт, что у всех членов комиссии обязательно должна быть форма допуска к информации с грифом секретности, чтобы ознакомиться с актом и поставить свою подпись. Иными словами, нельзя назначать в комиссию сотрудников без формы допуска к государственной тайне.

Особое внимание при обследовании объектов комиссия уделяет инженерно-техническим мероприятиям, проводимым на объектах органов внутренних дел, на их соответствие требованиям приказа МВД России от 31 декабря 2014 № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств».

Говоря о проведении инженерно-технических мероприятий на объектах ОВД, мы ведем речь о сооружениях и конструкциях, которые препятствуют или затрудняют проникновение (приближение) на объект.

Стоит также упомянуть, что в соответствии с Федеральным законом «О полиции» от 7 февраля 2011 года № 3-ФЗ личный состав органов внутренних дел имеет право на применение специальных средств, а также огнестрельного оружия для отражения нападения на свои объекты. Охрана объектов, а также их оборона при угрозе нападения напрямую зависит от накопленного практического опыта по обеспечению безопасности объектов органов внутренних дел, который нарабатывается в ходе проведения учебно-практических мероприятий. Это позволяет четко и грамотно организовать управление силами и средствами органов внутренних дел, действовать личному составу умело и слаженно. Весь накопленный опыт они применяют в режиме повседневной деятельности. В случае возникновения чрезвычайных ситуаций антитеррористическая безопасность собственных объектов МВД России возможна лишь благодаря четкой организации системы охраны и обороны. Именно эти аспекты позволяют успешно решать задачи, возложенные на личный состав органов внутренних дел [4].

Еще одной немаловажной проблемой в настоящее время выступают беспилотные летательные аппараты, управление которыми осуществляется либо автоматически, либо оператором с пункта управления, либо совместное использование обоих способов. На сегодняшний день беспилотные летательные аппараты получили большую популярность и все чаще используются в различных сферах жизни. Использование беспилотных летательных аппаратов можно разделить по назначению на: гражданские (для строительства), потребительские (для видеосъемки), боевые (для военных целей). Поскольку беспилотные летательные аппараты общедоступны, то можно сделать вывод, что они скрывают в себе большую опасность. Они могут быть использованы в различных противоправных целях [3].

Стоит отметить, что в законодательстве сегодня не существует запрета нахождения беспилотных летательных аппаратов в воздушном пространстве над объектами территориальных органов МВД России. То есть объекты территориальных органов МВД России никак не защищены от полетов беспилотных летательных аппаратов. Для решения этой проблемы было бы эффективно использовать для защиты объектов акустический, оптический, инфракрасный и радиоканал, а также данные радиоразведки для обнаружения и обезвреживания беспилотных летательных аппаратов [2].

Также считаем необходимым внесение изменений, поправок в Приказ МВД России от 31 декабря 2014 года № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств», где стоит указать алгоритм действий по защите собственных объектов ОВД от беспилотных летательных аппаратов. Следует также разработать меры пресечения в отношении беспилотных летательных аппаратов при совершении ими полетов в закрытом для полетов воздушном пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ МВД России от 31 декабря 2014 г. № 1152 – Доступ из справочно-правовой системы «КонсультантПлюс» (дата обращения: 21.10.2024)

2. Аниськов Р. В. К вопросу борьбы с незаконным использованием беспилотных летательных аппаратов коммерческого типа / Р. В. Аниськов, Е. В. Архипова, А. А. Гордеев, А. Н. Пугачев // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2017. – № 9-10 (111–112). – С. 71–75.

3. Демьянович М. А. Использование беспилотных летательных аппаратов в преступных целях: методы противодействия и борьбы / М. А. Демьянович // Правопорядок: история, теория, практика. – 2019. – № 2 (21). – С. 108–112.

4. Олейник А. С. Методы и модели принятия решений по охране и обороне важных государственных объектов : монография. Москва : Академия управления МВД России, 2017.

СВЕДЕНИЯ ОБ АВТОРАХ

Ивануха Иван Сергеевич.

Преподаватель кафедры информационных технологий в деятельности ОВД.

Омская академия МВД России.

E-mail: scorpion-6588@mail.ru
Россия, 644092, г. Омск, ул. Проспект Комарова, 7.

Калков Дмитрий Юрьевич.
Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.
Кандидат технических наук.
Воронежский институт МВД России.
E-mail: DmitreyRUS@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Ivanukha Ivan Sergeyevich.
Lecturer of the Department of Information Technology in the activities of the Department of Internal Affairs.
Omsk Academy of the Ministry of Internal Affairs of Russia.
E-mail: scorpion-6588@mail.ru
Russia, 644092, Omsk, Prospect Komarova str., 7.

Kalkov Dmitry Yurievich.
Senior lecturer of the Department of Radio Engineering Systems and Security Monitoring Complexes.
Candidate of Technical Sciences.
Voronezh Institute of the Ministry of internal Affairs of Russia.
E-mail: DmitreyRUS@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: безопасность объектов; преступные посягательства; инженерно-технические мероприятия; антитеррористическая защищенность; беспилотный летательный аппарат.

Keywords: security of objects; criminal attacks; engineering activities; anti-terrorism security; unmanned aerial vehicle.

УДК 351.74

Д. Ю. Калков, М. А. Гудков, И. С. Ивануха

К ВОПРОСУ ОХРАНЫ ОБЩЕСТВЕННОГО ПОРЯДКА И ОБЕСПЕЧЕНИЮ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ МАССОВЫХ МЕРОПРИЯТИЙ

ON THE ISSUE OF PROTECTING PUBLIC ORDER AND ENSURING PUBLIC SAFETY DURING MASS EVENTS

Работа посвящена рассмотрению нормативно-правовой базы, порядка обеспечения безопасности, применения современных технологий, а также важности взаимодействия различных служб и организаций на всех этапах подготовки и проведения мероприятий. Углубленный подход к данной теме поможет организаторам мероприятий и правоохранителей лучше понять, как предотвратить угрозы и создать безопасное пространство для всех участников.

This work is devoted to the consideration of the regulatory framework, the procedure for ensuring safety, the use of modern technologies, as well as the importance of interaction between various services and organizations at all stages of preparation and holding events. An in-depth approach to this topic will help event organizers and law enforcement officers better understand how to prevent threats and create a safe space for all participants.

Обеспечение безопасности массовых мероприятий – это одна из актуальнейших задач современного общества, имеющая множество аспектов и особенностей. В условиях растущих угроз, от террора до стихийных бедствий, организаторы крупных мероприятий сталкиваются с необходимостью создания надежной системы защиты участников и обеспечением комфортных условий для их пребывания. Каждый концерт, фестиваль, спортивное событие или культурное собрание не только приносит положительный социальный эффект, но и требует внимательного анализа рисков и четкого плана действий в случае возникновения чрезвычайных ситуаций.

Современные технологии играют значительную роль в повышении уровня безопасности. Использование систем видеонаблюдения, беспилотных летательных аппаратов для мониторинга территорий, а также программного обеспечения для анализа данных о посетителях и их поведении позволяет заранее выявлять потенциальные угрозы. Интеграция таких технологий в общий план безопасности мероприятия помогает создать более надежную систему защитных мер.

Ключевым моментом в организации безопасности массовых мероприятий является взаимодействие с местными правоохранительными органами и службами экстренной помощи. Установление четкого канала связи

и координация действий в экстренных ситуациях способствуют более эффективному реагированию на потенциальные угрозы.

Правоохранительные органы в свою очередь сталкиваются с задачей расчета необходимого и достаточного количества сил и средств для обеспечения безопасности массовых мероприятий. В современных условиях высокой неукомплектованности подразделений решение подобных задач действительно становится непростым.

Большинство массовых мероприятий имеет публичный характер. Целью публичного мероприятия является свободное выражение и формирование мнений, а также выдвижение требований по различным вопросам политической, экономической, социальной и культурной жизни страны и вопросам внешней политики.

Правовую основу деятельности граждан, общественных объединений, органов государственной власти, органов местного самоуправления, а также их должностных лиц при подготовке и проведении массовых мероприятий составляют положения Конституции Российской Федерации, общепризнанные принципы и нормы международного права, Федеральный конституционный закон «О чрезвычайном положении», федеральные законы «О собраниях, митингах, демонстрациях, шествиях и пикетированиях», «О политических партиях», «Об общественных объединениях», «О безопасности», «О полиции» и другие, конституции (уставы), законы, другие правовые акты субъектов Российской Федерации, а также правовые акты органов местного самоуправления, принятые ими в пределах своих полномочий.

Для получения разрешения на проведение массового мероприятия его организатор должен подать в органы исполнительной власти субъекта РФ или орган местного самоуправления в письменной форме соответствующее уведомление (за исключением собрания и пикетирования, проводимого одним участником) в срок не ранее 15 и не позднее 10 дней до дня проведения массовой акции. При проведении пикетирования группой лиц уведомление о проведении публичного мероприятия может подаваться в срок не позднее трех дней до дня его проведения [1].

Уведомление о проведении публичного мероприятия должно содержать в себе следующую информацию: цель мероприятия, место и время проведения, продолжительность, предполагаемое количество участников, маршруты передвижения участников мероприятия и иную важную информацию.

Если уведомление о проведении публичного мероприятия не было подано в установленный законодательством срок, организатор не имеет право на его проведение.

Организация охраны общественного порядка (ООП) и обеспечения общественной безопасности (ООБ) во время проведения массовых мероприятий в зависимости от их значения и масштаба обеспечивается силами и средствами органов внутренних дел в тесном взаимодействии с органами

государственной власти, органами местного самоуправления, прокуратуры и безопасности, в частности с подразделениями Росгвардии

Организация деятельности органов внутренних дел при проведении массовых мероприятий включает в себя три взаимосвязанных между собой периода их функционирования: подготовительный, исполнительный, заключительный [2].

В подготовительный период, который начинается с момента получения задачи на ООП и ООБ, уточняются программа, место, время, вид и характер предстоящего массового мероприятия, возможное количество и состав участников, зрителей, а также наличие или отсутствие факторов, требующих не принимать уведомление о проведении массовой акции.

Наряду с этим, органами внутренних дел осуществляются дополнительные мероприятия по усилению борьбы с преступностью, пьянством, наркоманией и другими антиобщественными проявлениями:

1) организуется подготовка личного состава и технических средств к несению службы по ООП и ООБ в местах их проведения и на прилегающей территории;

2) проводится инструктаж, на котором разъясняются обязанности и права соответствующих должностных лиц, особенности их реализации при проведении массовых мероприятий;

3) организуется взаимодействие служб и подразделений ОВД с другими правоохранительными органами, органами государственной власти, органами местного самоуправления, а также с общественными объединениями, трудовыми коллективами и гражданами, участвующими в охране правопорядка.

Расчет сил и средств, необходимых для эффективного несения службы, производится в каждом территориальном или линейном органе внутренних дел и является важным элементом организации охраны общественного порядка.

Исполнительный период, охватывающий действия нарядов полиции и управление ими во время проведения массового мероприятия включает в себя: введение в зоне проведения мероприятий, ограничений движения транспорта и пешеходов, в работе торговых и других предприятий, удаление из зоны оцепления случайно оказавшихся там людей, выставление нарядов по периметру зоны проведения массового мероприятия, а также на прилегающей к ней территории.

Для охраны общественного порядка и безопасности при проведении массового мероприятия используются, как правило, два вида нарядов охраны общественного порядка – обычные и специальные.

Обычные наряды используются для решения повседневных задач, как на прилегающей территории, так и в местах проведения массовых мероприятий, к ним относятся пешие посты, пешие патрули и патрули на автомобилях, посты регулирования движения и другие виды нарядов.

Специальные наряды: полицейские цепочки, группы сопровождения, посты охраны объектов, посты наблюдения, заслоны, резерв, наряды заграждения, группы ограничения движения транспорта, группы разъяснения законов, группы обеспечения связи, группы оцепления (блокирования), группы фиксации правонарушений (документирование противоправных действий), группы разбора с задержанными и составления документов и другие группы, предусмотренные нормативными актами МВД России.

В заключительный период обеспечивается беспрепятственный выход участников и зрителей публичного мероприятия из зоны его проведения. Ответственный за ООП и ООБ снимает (переводит в резерв) освободившиеся наряды или передислоцирует их с целью обеспечения общественного порядка на прилегающей к месту проведения массового мероприятия территории. Организуется работа нарядов сопровождения, патрульных групп и экипажей автопатрулей с целью усиления несения службы на маршрутах движения колонн участников (зрителей), входах на станции метрополитена, остановках общественного транспорта.

При решении задачи по охране общественного порядка и обеспечении общественной безопасности при проведении массовых мероприятий руководителю органа внутренних дел необходимо на подготовительном этапе провести тщательный анализ оперативной обстановки на подконтрольной территории, выявить уязвимые места, оценить риски и определить необходимый объем сил и средств, в том числе резерв. При этом важно учитывать деятельность сотрудников, несущих службу согласно плану единой дислокации постов и маршрутов патрулирования в период проведения массовых мероприятий и на следующие сутки, которым, в свою очередь, также необходимо выделить время на отдых. Дополнительные трудности в решении поставленной задачи накладывает существенный некомплект личного состава, в частности младшего начальствующего состава, который наблюдается во многих подразделениях.

Охраной общественного порядка и обеспечением общественной безопасности в первую очередь занимаются подразделения МВД России. Однако существенную поддержку им оказывает Росгвардия, в частности подразделения вневедомственной охраны.

Участие частных охранников в обеспечении общественного порядка стало актуальной темой в последние годы. С ростом преступности и необходимости обеспечения безопасности, многие муниципалитеты стали привлекать частные охранные структуры для поддержки государственных органов.

В заключение хочется отметить, что задача обеспечения безопасности – это не только реакция на угрозы, но и создание спокойной, комфортной атмосферы, способствующей всеобъемлющему взаимодействию. Вовлекая общественность в диалог по вопросам безопасности, можно значи-

тельно повысить уровень доверия и взаимопонимания, что в конечном итоге принесет пользу всему обществу.

Важным аспектом в обеспечении безопасности является использование инновационных подходов к планированию мероприятий. К примеру, применение концепций риск-менеджмента [3] позволяет заранее выявить потенциальные угрозы и разработать соответствующие стратегии реагирования. Это включает в себя не только технические меры, но и социальные инициативы, направленные на повышение осведомленности граждан о возможных рисках. Применение методов расчета оптимального количества сил и средств органов безопасности позволит максимально эффективно использовать имеющиеся ресурсы для охраны общественного порядка и обеспечению общественной безопасности.

Помимо этого, создание партнерств между частным сектором и государственными органами может стать катализатором для внедрения новейших технологий и подходов. Частные компании, обладая экспертизой и ресурсами, могут внести значительный вклад в разработку эффективных решений, которые позволят улучшить уровень безопасности на массовых мероприятиях.

Таким образом, комплексный подход к безопасности на массовых мероприятиях строится на принципах вовлеченности, диалога и инноваций, что в итоге способствует созданию безопасной и комфортной общественной среды.

СПИСОК ЛИТЕРАТУРЫ

1. О собраниях, митингах, демонстрациях, шествиях и пикетированиях : Федеральный закон от 19 июня 2004 года № 54 // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru>.
2. Беженцев А. А. Охрана общественного порядка : учебное пособие. – 2-е изд., перераб. и доп. – Москва : ИНФРА-М, 2025. – 252 с.
3. Бокадаров, С. А. Риск-ориентированный подход к функционированию аппаратно-программного комплекса «Безопасный город» / С. А. Бокадаров, Д. Ю. Калков, М. А. Гудков // Техника и безопасность объектов уголовно-исполнительной системы : Сборник материалов Международной научно-практической конференции, Воронеж, 23–24 мая 2018 года. – Воронеж : Научная книга, 2018. – С. 113–114. – EDN YAFUDB.

СВЕДЕНИЯ ОБ АВТОРАХ

Калков Дмитрий Юрьевич.

Старший преподаватель кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: DmitreyRUS@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Гудков Максим Андреевич.
Доцент кафедры процессов горения и экологической безопасности (в составе учебно-научного комплекса процессов горения и экологической безопасности).

Кандидат технических наук.
Академия ГПС МЧС России.
E-mail: Gudokmaksim@yandex.ru
Россия, 129366, г. Москва, улица Бориса Галушкина, 4.

Ивануха Иван Сергеевич.
Преподаватель кафедры информационных технологий в деятельности
ОВД.
Омская академия МВД России.
E-mail: scorpion-6588@mail.ru
Россия, 644092, г. Омск, ул. Проспект Комарова, 7.

Kalkov Dmitry Yurievich.
Senior lecturer of the Department of Radio Engineering Systems and Security Monitoring Complexes.
Candidate of Technical Sciences.
Voronezh Institute of the Ministry of internal Affairs of Russia.
E-mail: DmitreyRUS@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Gudkov Maxim Andreevich.
Docent of the Department of Combustion processes and Environmental Safety (as part of the educational and scientific complex of combustion processes and environmental safety).
Candidate of Technical Sciences.
The Academy of the Ministry of Emergency Situations of Russia.
E-mail: Gudokmaksim@yandex.ru.
Russia, 129366, Moscow, Boris Galushkin Street, 4.

Ivanukha Ivan Sergeyevich.
Lecturer of the Department of Information Technology in the activities of the Department of Internal Affairs.
Omsk Academy of the Ministry of Internal Affairs of Russia.
E-mail: scorpion-6588@mail.ru
Russia, 644092, Omsk, Prospect Komarova, 7.

Ключевые слова: охрана общественного порядка; обеспечение общественной безопасности; массовые мероприятия; безопасность; взаимодействие правоохранительных органов.

Keywords: protection of public order; ensuring public safety; mass events; security; interaction of law enforcement agencies.

УДК 351.74

Н. И. Меркулова

**АСПЕКТЫ ФОРМИРОВАНИЯ У ПЕРСОНАЛА ПЦО ЗНАНИЙ,
УМЕНИЙ И НАВЫКОВ ПО КОНФИГУРИРОВАНИЮ УСТРОЙСТВ
ОКОНЕЧНЫХ ОБЪЕКТОВЫХ**

**ASPECTS OF THE FORMATION OF KNOWLEDGE, SKILLS AND
ABILITIES AMONG THE PERSONNEL OF THE CONTROL CENTER
FOR CONFIGURING TERMINAL FACILITY DEVICES**

В данной статье рассмотрены вопросы формирования у персонала ПЦО знаний и навыков работы по настройке, конфигурированию и подключению устройств объектовых оконечных в составе систем передачи извещений по каналам Ethernet и мобильным сетям сотовой связи.

This article discusses the issues of formation of knowledge and skills among the personnel of the control center for setting up, configuring and connecting object terminal devices as part of notification transmission systems over Ethernet channels and mobile cellular networks.

В настоящее время на объектах, охраняемых подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации, для организации централизованной охраны, применяются системы передачи извещений (далее – СПИ) тринадцати предприятий-производителей. Программное обеспечение каждой из систем отличается последовательностью настройки и конфигурирования объектового оборудования на пульте централизованного наблюдения, интерфейсом, терминологией. Системы передачи извещений – это сложные программно-аппаратные комплексы, программное обеспечение содержит несколько программных продуктов, каждый из которых имеет определенное назначение и описание. Настройка и конфигурирование объектового оборудования на пульте централизованного наблюдения (далее – ПЦН) проводится в нескольких модулях программного обеспечения системы, для чего необхо-

димо изучить большой объем технической документации программного обеспечения комплекса средств автоматизации ПЦО. Кроме того, при установке нескольких СПИ на ПЦО, однотипная информация отображается и одни и те же операции для разных систем выполняются по-разному, что влечет за собой возможные ошибочные действия персонала. Это усложняет процесс и увеличивает время обучения инженерно-технического персонала ПЦО при настройке, конфигурировании и подключении устройств оконечных объектов к пультовому оборудованию разных систем централизованного наблюдения. В справочно-методическом пособии «Настройка, конфигурирование и подключение устройств объектов оконечных в составе систем передачи извещений по каналам Ethernet и мобильным сетям сотовой связи на пульт централизованного наблюдения подразделений вневедомственной охраны войск национальной гвардии Российской Федерации» [1] рассмотрены особенности настройки объектового оборудования СПИ, приведена краткая информация с описанием необходимых автоматизированных рабочих мест для подключения объектовых приборов на ПЦН, примеры построения дерева конфигурации, проверки связи объектового оборудования и ПЦН, а также создания карточки объекта. Целью справочно-методического пособия является формирование у персонала ПЦО знаний и навыков работы по настройке, конфигурированию и подключению устройств объектов оконечных в составе систем передачи извещений по каналам Ethernet и мобильным сетям сотовой связи. Обобщим ряд ключевых положений настоящего документа.

Централизованная охрана объектов силами подразделений вневедомственной охраны войск национальной гвардии Российской Федерации осуществляется в соответствии с положениями: приказа Росгвардии от 25 февраля 2019 г. № 59 «Об утверждении Руководства по организации службы пунктов централизованной охраны подразделений вневедомственной охраны войск национальной гвардии Российской Федерации»; приказа Росгвардии от 28 декабря 2018 г. № 669 «Об утверждении Правил охраны имущества физических и юридических лиц по договорам войсками национальной гвардии Российской Федерации»; методических рекомендаций «Отдельные вопросы деятельности инженерно-технической службы подразделений вневедомственной охраны войск национальной гвардии Российской Федерации при организации охраны имущества с использованием технических средств», утвержденных ГУВО Росгвардии от 4 октября 2021 г. В части, касающейся настройки и конфигурирования объектового оборудования, указанные документы разграничивают функции проектно-монтажных организаций и подразделений вневедомственной охраны. Так, монтажные и пусконаладочные работы на объектах, принимаемых под охрану, проводятся проектно-монтажной организацией, выбранной заказчиком, в соответствии с согласованной подразделением вневедомственной охраны проектной документацией или актом первичного обследования

объекта. После проведения монтажа ТСО представитель подразделения вневедомственной охраны совместно с заказчиком и представителем монтажной организации проверяет соответствие монтажно-наладочных работ проекту или акту первичного обследования, проверяет работоспособность ТСО при подключении к ПЦН, а также заводит в базу данных сведения о принимаемом под охрану объекте, заполняет оперативную карточку объекта.

СПИСОК ЛИТЕРАТУРЫ

1. Настройка, конфигурирование и подключение устройств объектовых оконечных в составе систем передачи извещений по каналам Ethernet и мобильным сетям сотовой связи на пульт централизованного наблюдения подразделений вневедомственной охраны войск национальной гвардии Российской Федерации : справочно-методическое пособие. – Москва : ГУВО Росгвардии, 2022. – 244 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Меркулова Наталья Ивановна.
Доцент кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.
Воронежский институт МВД России.
E-mail: gomova.nata2008@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Merkulova Natalia Ivanovna.
Docent in electronic systems and complexes of security monitoring. Candidate of Engineering Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: gomova.nata2008@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: устройства оконечные объектовые; конфигурирование; пункт централизованной охраны.

Keywords: terminal object devices; configuration; centralized security point.

УДК 004.9

**ДЕЯТЕЛЬНОСТЬ СОТРУДНИКОВ ПОЛИЦИИ
ПО ПРЕСЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ
РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ
И БЕСПИЛОТНЫХ ВОЗДУШНЫХ СУДОВ (ДРОНОВ)
В ВОЗДУШНОМ ПРОСТРАНСТВЕ НАД ОБЪЕКТАМИ ТРАНСПОРТНОЙ
ИНФРАСТРУКТУРЫ:
ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ И ПРОБЛЕМНЫЕ АСПЕКТЫ**

**POLICE OFFICERS' ACTIVITIES TO SUPPRESS
THE OPERATION OF ROBOTIC COMPLEXES
AND UNMANNED AIRCRAFT (DRONES) IN THE AIRSPACE ABOVE
TRANSPORTATION INFRASTRUCTURE FACILITIES:
LEGAL REGULATION AND PROBLEM ASPECTS**

Автором рассматриваются проблемные аспекты, связанные с деятельностью сотрудников полиции по пресечению функционирования робототехнических комплексов и беспилотных воздушных судов (дронов) в воздушном пространстве над объектами транспортной инфраструктуры, а также правовая регламентация такой деятельности

The author considers problematic aspects related to the activities of police officers to suppress the operation of robotic complexes and unmanned aircraft (drones) in the airspace over the objects of transport infrastructure, as well as legal regulation of such activities.

Научно-технический прогресс, происходящий в последние десятилетия, стал основой качественных изменений во всех сферах жизнедеятельности человека. Его результаты определяют развитие общества и непосредственно связаны с интеллектуальной научной деятельностью. Внедрение новых технологий и передовой техники стало повсеместным процессом, используемым для роботизации и комплексной автоматизации производства продукции, предоставления услуг и организации быта.

В условиях серийной технологической индустрии наиболее целесообразной формой роботизации стало создание робототехнических комплексов, представляющих собой совокупность программно-алгоритмических и аппаратных решений, направленных на автоматизированное выполнение целого ряда поставленных задач. Сегодня практически невозможно назвать количество используемых типов роботизированных техник и технологий, а их модификации поражают своим разнообразием.

Создание и развитие робототехнических систем и средств (далее – РТС) в интересах силовых структур стало необходимым по различным ос-

нованиям, в частности, для сохранения человеческой жизни, ускорения и упрощения реализации возложенных на эти структуры функций. С каждым годом их технические характеристики и возможности заметно увеличиваются. Динамичность, анонимность, нечувствительность к рискам, автономность и широкая возможность эффективного использования сделали применение РТС тотальным. Наблюдается стремительный рост их использования при проведении боевых и контртеррористических операций.

Однако, есть обратная сторона – они используются в преступных целях, как средство совершения преступлений и иных противоправных деяний, либо как орудие преступления. Причем их применение в криминальной действительности весьма разнообразно (для доставки взрывчатых и отравляющих веществ, наркотических средств, контрабанды, повреждения имущества, для наблюдения за объектами с целью хищения или шантажа, совершения террористических актов и т.д.). Особенно это актуально в последнее время, в частности, с начала проведения специальной военной операции на Украине. Весьма заметно, что сегодня число преступлений, совершенных с применением беспилотных летательных аппаратов (далее – БПЛА), заметно увеличилось. Новости об атаках дорнов на различные объекты инфраструктуры стали ежедневными. Чаще всего удары наносятся по нефтехранилищам, промышленным предприятиям России, объектам энергоснабжающей, транспортной и иной жизнеобеспечивающей инфраструктуры.

Безусловно большая часть БПЛА (дронов) ликвидируется до прилета к намеченной цели (системами ПВО, с использованием РЭБ и т.д.), либо они не долетают до нее по техническим причинам (нехватка топлива, потеря управления оператором, поломка и т.д.). Однако обнаружение и уничтожение малоразмерных целей (мини и микро БПЛА) радиолокационными станциями частей и подразделений войск ПВО малоэффективно, поскольку «летающие на высоте 100 метров БПЛА со скоростью 100 км/ч воспринимаются как летящая птица» [1. С. 84], а применение РЭБ не всегда гарантирует возможность предотвращения прорыва БПЛА к контролируемому периметру. Здесь требуется дополнительные механизмы, средства и способы пресечения их функционирования.

Правом пресечения незаконного нахождения РТК и БПЛА (дронов) в воздушном пространстве путем их повреждения или уничтожения наделены сотрудники целого ряда силовых ведомств РФ (УФСИН, ФСБ, СВР, МВД, Росгвардия, ФСО). Данное право дополнено Федеральным законом от 2 декабря 2019 г. № 404 «О внесении изменений в отдельные законодательные акты Российской Федерации» в положения нормативных правовых актов, определяющих направления деятельности соответствующих ведомств и перечень полномочий их сотрудников.

В частности, согласно п. 40 ч. 1 ст. 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» (далее – Закон о полиции), сотрудники полиции при исполнении своих обязанностей имеют право «пре-

секать функционирование беспилотных аппаратов в целях защиты жизни, здоровья и имущества граждан, сотрудников органов внутренних дел, в том числе в месте проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-розыскных мероприятий». Принятие такого решения осуществляется согласно порядку [2], изложенному в Приказе Министерства Внутренних дел Российской Федерации от 16 ноября 2023 г. № 865, должностными лицами, перечень которых также предусмотрен в тексте данного документа.

Основные трудности по пресечению сотрудниками полиции нахождения РТК и БПЛА (дронов) заключается в том, что их использование в противоправных целях в основном осуществляется в темное время суток, поскольку в этот период затрудняется их визуальное обнаружение и противодействие им стрелковым оружием и иными средствами (в ночное время суток БПЛА не видно уже с высоты 12 м, шум винтов не слышен с высоты выше 70 м.). К тому же высокая скорость движения БПЛА, которая может колебаться от 50 км/ч (малоскоростные БПЛА) до 400 км/ч и достигать скорости звука в воздухе – число Маха (сверхзвуковые) [3], и изменяющаяся траектория осложняют попадание сотрудником полиции какими-либо средствами и орудиями по данному объекту. Определение исходной установки для принятия мер по пресечению полета также является одной из проблем. Не стоит забывать и то, что многие БПЛА, используемые в преступных целях, являясь орудием преступления, снабжены взрывчатыми устройствами или взрывными веществами (дроны-камикадзе). Поэтому при принятии решения о его обезвреживании необходимо «оценить возможные риски от результатов пресечения его функционирования» (п. 5 Порядка).

Если вести речь об особенностях отдельных объектах, на целостность и деятельность которых осуществляется покушение с помощью РТК и БПЛА (дронов), то это тоже является определяющим фактором для принятия решения по их обезвреживанию.

Так, объекты транспортной инфраструктуры имеют свои особенности в конструкции и производственных процессах, их доступность и масштабность делают такие объекты особенно уязвимыми для ряда угроз террористического характера, а расположение критических элементов объекта (вокзалы, порты, аэропорты и аэродромы, мосты и т.д.) может препятствовать обеспечению безопасности, усложнить своевременное принятие соответствующих мер, в том числе по обезвреживанию РТК и БПЛА (дронов), покушающихся на целостность данных объектов.

К тому же сам процесс принятия решения, предусмотренный указанным Порядком, видится проблематичным в соблюдении и не конкретизированным в содержании. Как подчеркнули В. В. Копылов и А. А. Субботин, «данный порядок пресечения сотрудниками ОВД РФ

нахождения беспилотных воздушных судов в части управления неэффективный и сложный, во многом зависит от «человеческого фактора» (ошибки при выполнении сотрудником своих функций), исправности средств связи и т. п., и самое главное, он не учитывает «фактора внезапности» [1, С. 86].

Но самый проблемный вопрос заключается в определении способов и средств, используемых сотрудником полиции для пресечения нахождения РТК и БЛА (дронов) в воздушном пространстве, в том числе и над объектами транспортной инфраструктуры.

Согласно ч. 5 ст. 23 Закона «О полиции» для пресечения нахождения беспилотных воздушных судов в воздушном пространстве сотрудник полиции имеет право применять огнестрельное оружие, но с оговоркой о том «если иными средствами прекратить их нахождение в воздушном пространстве не представляется возможным». В число последних можно отнести, согласно вышеупомянутому порядку, «посредством подавления или преобразования сигналов их дистанционного управления, воздействия на пульты управления». Спецсредства для непосредственного повреждения или уничтожения не определены.

Если все-таки говорить о применении сотрудниками полиции огнестрельного оружия для пресечения функционирования РТК и БЛА (дронов), то стоит обозначить ряд проблемных аспектов. Во-первых, для этого необходимо наличие специализированной подготовки сотрудников по выработке навыков ведения прицельной стрельбы по движущей цели с упреждением, в том числе с учетом погодных условий. Здесь также важно обладать знаниями и умениями по определению направления и скорости ветра. Во-вторых, немаловажно быть знакомым с техническими характеристиками, типами и модификациями РТК и БЛА (дронов). В-третьих, особо значимо наличие у сотрудника полиции умения оперативно определять риски и возможные последствия применения огнестрельного оружия для пресечения нахождения РТК и БЛА (дронов) в воздушном пространстве, в частности над объектами транспортной инфраструктуры, поскольку чаще всего это небезопасно, так как там могут быть граждане или скопление людей (аэропорты, вокзалы, пассажирские поезда), сами объекты, на которые осуществляется атака, могут являться огнеопасными (цистерны с топливом, химикатами и т.д.), а стрельба по цели, движущейся со скоростью, например, 100 км/ч с меняющейся траекторией на высоте 50-90 м., не всегда гарантирует попадание по ней. В итоге стрельба может спровоцировать панику людей, либо сотрудник может произвести попадание в сами объекты транспортной инфраструктуры, что может причинить большой вред, либо создать угрозу жизни и здоровью граждан либо окружающей среде. К тому же имеется ч. 6 ст. 23 Закона «О полиции» прямо предусматривает запрет на применение огнестрельного оружия «при значительном скоплении граждан, если в результате его применения могут пострадать случай-

ные лица». Обеспечение сотрудников полиции иными специальными средствами, с помощью которых возможно обезвреживание БПЛА более безопасным способом, весьма финансово затратно, ввиду их дороговизны. К тому же применение специальных средств требует особой подготовки.

Таким образом, резюмируя вышесказанное, стоит отметить тот факт, что ограниченность вариантов действий сотрудников полиции для пресечения функционирования РТК и БПЛА (дронов) в воздушном пространстве над объектами критической инфраструктуры, в том числе транспортной, и недостаточная правовая регламентация порядка принятия ими соответствующего решения, требует выработки конкретных мер в целях повышения результативности уничтожения РТК и БПЛА (дронов), являющихся средством совершения противоправных деяний и создающие опасность для нормального функционирования объектов жизнедеятельности, а также для жизни и здоровья людей и окружающей среды. В число таких мер необходимо включить разработку алгоритма действий сотрудника полиции с учетом особенностей охраняемых объектов транспортной инфраструктуры, а также принятие на вооружение конкретных изделий, предназначенных для обнаружения и уничтожения РТК и БПЛА (дронов), с последующей подготовкой сотрудников к разнообразным подходам к организации и тактике их применения в действительности.

СПИСОК ЛИТЕРАТУРЫ

1. Копылов В. В., Субботин А. А. Проблемы в организации пресечения сотрудниками ОВД РФ несанкционированного нахождения беспилотных летательных аппаратов (БПЛА) в воздушном пространстве // Вестник Экономической безопасности. – 2023. – № 6. – С. 83–88.

2. Об утверждении Порядка принятия решения о пресечении функционирования беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов в целях защиты жизни, здоровья и имущества граждан, сотрудников органов внутренних дел, в том числе в месте проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-розыскных мероприятий и Перечня должностных лиц полиции, уполномоченных на принятие такого решения : приказ Министерства внутренних дел Российской Федерации от 16 ноября 2023 г. № 865 // СПС «КонсультантПлюс» (дата обращения: 07.07.2024).

3. БПЛА: Классификация, типы, сферы применения. – URL: <https://3mx.ru/articles/bpla-konstruktsiya-tipy-sfery-primeneniya>

СВЕДЕНИЯ ОБ АВТОРЕ

Миллер Андрей Александрович.
Начальник Отдела МВД России по Городищенскому району
(слушатель 2 курса, группы 2 ГЗ-2326 Академии управления МВД России).
Академия управления МВД России.
Россия, 125171, г. Москва, ул. Зои и Александра Космодемьянских, 8

Miller Andrey Aleksandrovich.
Head of the department of the Ministry of Interior of Russia for
Gorodishchensky district (1st year student, group 2 GZ-2326 of the Academy of
Management of the Ministry of Interior of Russia)
Academy of Management of the Ministry of Interior of Russia.
Russia, 125171, Moscow, Zoe and Alexandra Kosmodemyanskikh st., 8.

Ключевые слова: БПЛА; сотрудники полиции; объекты
транспортной инфраструктуры.

Keywords: drones; police officers; transportation infrastructure facilities.

УДК. 351.74

А. В. Сидоров

СОВЕРШЕНСТВОВАНИЕ АНТИТЕРРОРИСТИЧЕСКОЙ ЗАЩИЩЕННОСТИ ОХРАНЯЕМЫХ ОБЪЕКТОВ В УСЛОВИЯХ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ВОЗДУШНЫМ СУДАМ

ANTI-TERRORIST SECURITY'S IMPROVEMENT OF PROTECTED OBJECTS IN CONDITIONS OF COUNTERING UNMANNED AIRCRAFT

В данной статье проведен анализ защищенности охраняемых объектов от угроз, связанных с применением беспилотных воздушных судов. Предложены решения и разработаны рекомендации по обеспечению безопасности охраняемых объектов с целью повышения уровня антитеррористической защищенности в условиях противодействия беспилотным воздушным судам.

This article analyzes the security of protected facilities from threats associated with the use of unmanned aircraft. Solutions are proposed and recommendations are developed to ensure the security of protected facilities in order to increase the level of anti-terrorist security in the context of countering unmanned aircraft.

В настоящее время, в связи с осложняющейся внешнеполитической обстановкой, которая может неукоснительно сказаться на росте актов терроризма и преступных посягательств, все больше возрастает

актуальность и значимость обеспечения безопасности охраняемых объектов различного функционального назначения.

В соответствии с Федеральным законом от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму», антитеррористическая защищенность объекта (территории) – состояние защищенности здания, строения, сооружения, иного объекта, места массового пребывания людей, препятствующее совершению террористического акта [1]. Состояние защищенности охраняемого объекта определяется уровнем инженерной и технической укрепленности, а также соблюдением требований организационных, административных, технических мер безопасности.

В связи с проведением специальной военной операции, беспилотные воздушные суда (БВС) стали основной угрозой безопасности объектам различного функционального назначения.

Несомненно, БВС являются одним из самых современных достижений в военной технике. Они представляют собой автономные устройства, управляемые дистанционно, что позволяет значительно снизить риск для лица, его применяющего и увеличить их возможности в боевых условиях.

Преимущества использования БВС на поле боя очевидны. Во-первых, они способны осуществлять широкий спектр разведывательных операций. Благодаря своей автономной системе навигации и оснащению современными средствами разведки, они могут проникать на территорию противника, собирать информацию и передавать ее безопасно и эффективно.

Кроме того, БВС стали незаменимым средством для нанесения точных и мощных ударов по вражеским объектам. Они обладают возможностью нести различные виды вооружения и могут выполнять задачи, которые раньше требовали мобильности и смелости пилотов.

В данной статье будут рассмотрены охраняемые объекты, имеющие стратегическое значение для государства в условиях проведения специальной военной операции. К таким объектам можно отнести: объекты топливно-энергетического комплекса, объекты жизнеобеспечения, особой важности, производственного кластера и другие.

Угрозы, связанные с применением БВС, условно можно разделить на 2 группы:

- угрозы безопасности зданий и сооружений, а также жизни и здоровья сотрудников, при применении ударных БВС;
- потеря сведений, составляющих государственную или иную охраняемую законом тайну, выявление постов и маршрутов патрулирования, выявление другой информации с применением разведывательных БВС.

Учитывая специфику рассматриваемых объектов, необходимо определить комплекс мероприятий, который позволит повысить антитеррористическую защищенность охраняемых объектов, и тем самым свести к минимуму возможный ущерб от реализации угроз, связанных с применением БВС. Необходима разработка и внедрение комплексных систем защиты, которые включают в себя как технические, так и

организационные меры. Среди технических решений можно выделить внедрение радиолокационных систем и систем подавления сигналов управления БВС, а также создание специализированных средств физического уничтожения или захвата БВС.

Для противодействия БВС необходимо выполнить две задачи, сначала обнаружить его, а потом подавить или безопасно уничтожить. Существуют несколько методов обнаружения БВС, отличающихся физическим способом выявления их присутствия: акустический, оптический, тепловой, радиочастотный и радарный.

На рисунке 1 представлены расчетные значения максимального расстояния обнаружения БВС системами, использующими различные методы обнаружения.

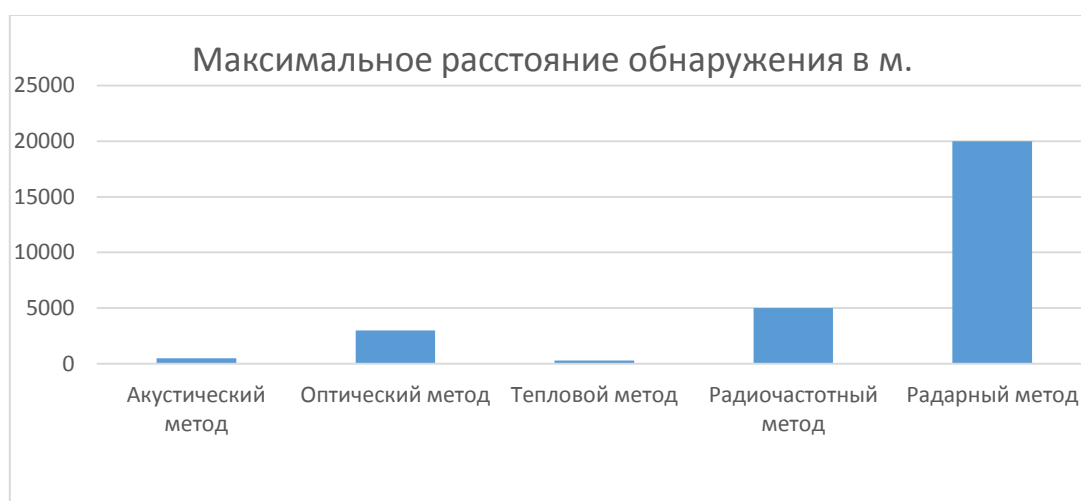


Рис. 1. Максимальные расстояния обнаружения БВС системами, использующими различные методы обнаружения

Можно сделать вывод, что первые три метода обнаружения БВС нецелесообразно использовать ввиду малого радиуса обнаружения и неэффективности применения в условиях городской застройки. Радарный и радиочастотный методы имеют свои плюсы и минусы.

Таким образом, при оборудовании объекта радиолокационной системой необходимо определить расстояние, на котором она будет обнаруживать БВС.

Сегодня на рынке достаточно большое количество таких систем, например: подавитель дронов GroZZa, мобильная система обнаружения БВС «Н1С», «1С» стационарное оборудование обнаружения и позиционирования БВС, комплекс обнаружения БВС «РАДЕСКАН-АНТИДРОН» и другие.

С целью повышения эффективности вышеперечисленных систем целесообразно применять спуфинг. Спуфинг – это подмена сигнала GPS, транслируемого спутниками, другим, более сильным сигналом, транслируемым с наземной станции. Сигнал от наземной станции спуфинга вносит

корректуру в определение приемником собственного расположения, что приводит к нарушению позиционирования. Проще говоря, наземная станция спуфинга заменяет сигнал спутника и дает БВС неверные данные о его местонахождении и положении.

Также применимы для небольших БВС (дронов) антидроновые ружья, они могут быть оснащены различными типами систем, такими как радиоинтерференция, лазерное подавление, электромагнитное воздействие и другие. Они могут нейтрализовать дроны, либо заставлять их вернуться на базу, либо вынуждать к аварийной посадке. Однако практика применения показала низкую эффективность этих устройств противодействия БВС.

Защитные экраны и сети, наоборот, все чаще используются для обеспечения безопасности локальных объектов защиты. Они имеют каркасную конструкцию и состоят обычно из вертикальных опорных стоек, закрепленных между собой стальными тросами, и антидроновой сети. Пример защитного экрана компании «ЦеСИС» представлен на рисунке 2.



Рис. 2. Внешний вид защитного экрана от дронов-камикадзе

Важным вопросом совершенствования антитеррористической защищенности является правомерность применения на объекте средств противодействия БВС.

В соответствии с Федеральным законом от 4 августа 2023 г. № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» определен перечень органов и организаций, наделенных правом пресекать функционирование не только беспилотных воздушных судов, но и подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов, в том числе посредством подавления или преобразования сигналов дистанционного управления беспилотными аппаратами, воздействия на их пульта управления, а также повреждения или уничтожения беспилотных аппаратов, в целях защиты собственных объектов, сил, средств и информации или охраняемых объектов по договорам [2].

К этим органам и организациям относятся: подразделения Федеральной службы безопасности, Федеральной службы охраны, Службы внешней разведки, Министерства внутренних дел, Федеральной службы войск национальной гвардии, Федеральной службы исполнения наказаний, ведомственной охраны, Министерства по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и др.

На основании вышеизложенного можно сделать вывод, что на объекте должен быть как минимум пост(ы) охраны, вышеуказанных подразделений. Поэтому обеспечение безопасности объекта охраны не только задача собственника, но и соответствующих подразделений.

Предложенные решения будут способствовать повышению уровня антитеррористической защищенности охраняемых объектов в условиях противодействия беспилотным воздушным судам.

СПИСОК ЛИТЕРАТУРЫ

1. О противодействии терроризму : Федеральный закон от 06.03.2006 № 35-ФЗ (с изм. от 10.07.2023) // СПС «КонсультантПлюс» (дата обращения: 28.10.2024).

2. О внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 04.08.2023 № 440-ФЗ // СПС «КонсультантПлюс» (дата обращения: 28.10.2024).

СВЕДЕНИЯ ОБ АВТОРЕ

Сидоров Александр Викторович.

Заместитель начальника кафедры радиотехнических систем и комплексов охранного мониторинга.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: asidic@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Sidorov Aleksandr Viktorovich.
Deputy Head of the Department of Radio Engineering Systems and Security Monitoring Complexes.
Candidate of Engineering Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: asidic@mail.ru.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: угроза безопасности; антитеррористическая защищенность; беспилотное воздушное судно; инженерно-техническая укрепленность; охраняемый объект.

Keywords: security threat; anti-terrorism protection; unmanned aircraft; engineering and technical strength; protected object.

УДК 699.81:654.924

О. В. Толстых

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВОПРОСОВ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ВОЗДУШНЫМ СУДАМ НА ОБЪЕКТАХ ОХРАНЫ

LEGAL REGULATION OF THE ISSUES OF COUNTERING UNMANNED AIRCRAFT AT SECURITY FACILITIES

В статье представлены основные нормативные правовые акты, регламентирующие противодействие беспилотным воздушным судам на охраняемых объектах.

The article presents the main regulatory legal acts regulating the counteraction to unmanned aircraft at protected facilities.

Беспилотные воздушные суда (БВС) становятся всё более распространёнными, и с этим ростом возникает необходимость в создании системы регулирования, которая бы обеспечивала безопасность и защиту охраняемых объектов.

Анализ нормативных правовых актов в области противодействия БВС – это сложный процесс, требующий учета ряда аспектов, связанных с безопасностью, законодательством и технологическими достижениями.

Вопрос регулирования использования БВС на таких объектах затрагивается следующими законами и подзаконными актами, основными из которых являются:

1. Воздушный Кодекс Российской Федерации от 19.03.1997 г. № 60-ФЗ. – закон основополагающий для регулирования воздушного пространства России, включая правила эксплуатации гражданской и государственной авиации. Он также устанавливает основные принципы, касающи-

еся использования БВС, таких как необходимость регистрации и получения разрешений на полеты.

2. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» – в контексте использования БВС для террористических атак. Он устанавливает меры, которые должны быть приняты для предотвращения террористических актов с использованием беспилотников.

3. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 10.07.2023) «О безопасности» – определяет подходы к обеспечению безопасности на объектах, включая разработку и реализацию мер по противодействию угрозам, исходящим от БВС. Упоминаются риски, связанные с террористической деятельностью и шпионажем.

4. Федеральный закон от 04.08.2023 № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» – предусмотрены изменения, касающиеся регулирования БВС, определяет пресечение функционирования БВС на охраняемых территориях.

5. Постановление Правительства Российской Федерации от 11.03.2010 № 138 (ред. от 29.03.2024) «Об утверждении Федеральных правил использования воздушного пространства Российской Федерации» – для БВС предусмотрен только разрешительный порядок использования воздушного пространства независимо от класса воздушного пространства.

А также нормативные акты правоохранительных органов. Внутренние инструкции и нормы безопасности, принятые правоохранительными органами, которые содержат указания по взаимодействию с другими структурами. В них указаны методики выявления и нейтрализации потенциальных угроз, связанных с БВС, а также протоколы действий в случае обнаружения подозрительных объектов в воздушном пространстве.

Таким образом, правовая основа для противодействия БВС представлена многоуровневой системой нормативных актов, включая федеральные законы, правила и внутренние распоряжения. Эти документы регламентируют не только операции с БВС, но и рекомендации по обеспечению безопасности на охраняемых объектах. Правовая база постоянно обновляется в связи с развитием технологий и угроз безопасности, что требует от участников рынка и правоохранительных органов высокой степени бдительности и готовности к изменениям.

Комплексный подход к противодействию беспилотным воздушным судам на охраняемых объектах включает многочисленные законодательные акты и внутренние регламенты. Эффективная координация между разными ведомствами, а также интеграция современных технологий являются ключевыми факторами для обеспечения безопасности таких объектов. Применение комплексных мер, как технических, так и юридических, позволяет более эффективно защищать критически важные объекты от потенциальных угроз со стороны БВС.

СПИСОК ЛИТЕРАТУРЫ

1. URL:<http://www.consultant.ru> – Официальный сайт компании «КонсультантПлюс».
2. URL:<http://www.garant.ru/> – Информационно-правовое обеспечение Гарант.
3. URL:<http://www.pravo.gov.ru> – Официальный интернет-портал правовой информации.

СВЕДЕНИЯ ОБ АВТОРЕ

Толстых Ольга Владимировна.
Доцент 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.

Tolstikh Olga Vladimirovna.
Associate Professor of the Department of Radio Engineering Systems and Security Monitoring Complexes.
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.

Ключевые слова: беспилотное воздушное судно;, правовое регулирование; правоохранительные органы.

Keywords: unmanned aircraft; legal regulation; law enforcement agencies.

УДК 342; 623.746

А. И. Янгиров, И. М. Янгиров, С. Б. Ахлюстин, Н. А. Садчикова

ОРГАНИЗАЦИЯ ОХРАНЫ ОБЪЕКТОВ С ПРИМЕНЕНИЕМ СПУТНИКОВОГО КАНАЛА СВЯЗИ

ORGANIZATION OF THE PROTECTION OF FACILITIES USING A SATELLITE COMMUNICATION CHANNEL

В статье рассматривается подход к охране объектов, основанный на применении спутникового канала связи, на примере объектов, расположенных в труднодоступных районах. В настоящее время описанное решение

представляется перспективным, за счет своей эффективности и многофункциональности.

The article considers an approach to the protection of objects based on the use of a satellite communication channel, using the example of objects located in hard-to-reach areas. Currently, the described solution seems promising, due to its effectiveness and multifunctionality.

При организации охраны объектов в труднодоступных районах со сложными климатическими и географическими условиями оптимальным является применение средств передачи извещений (далее – СПИ), использующих беспроводные каналы связи, и дополнительного специального оборудования и/или современных методов эксплуатации систем централизованного наблюдения. Это обусловлено значительной удаленностью охраняемых объектов от районных центров, слабой развитостью инфраструктуры, сложным рельефом местности, резкими перепадами и экстремальными показателями температур, экономической рентабельностью и другими факторами.

Для построения систем централизованного наблюдения с применением средств передачи извещений, использующих в качестве основного канала связи интернет-соединение, применяются средства передачи извещений, осуществляющие передачу извещений по цифровым каналам связи.

Такие средства передачи извещений имеются в «Списке технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» [1, 2].

Организация централизованного наблюдения в труднодоступных районах с применением СПИ, использующих в качестве основного канала связи маршрутизируемые IP-сети, возможна при подключении СПИ к беспроводному интернет-соединению.

Достаточно интересным современным решением в данной области является использование спутниковых каналов передачи данных.

Спутниковая связь – это один из видов радиосвязи, основанный на использовании искусственных спутников Земли в качестве ретрансляторов. Спутниковая связь осуществляется между земными станциями, которые могут быть как стационарными, так и подвижными.

В настоящее время практическое применение на рынке услуг спутниковой связи имеют геостационарные спутники [3]. Услуги, предоставляемые с помощью геостационарных спутников, ориентированы как на предприятия малого и среднего бизнеса, так и на крупные коммерческие и государственные структуры. Операторы, предоставляющие данные услуги, предлагают отраслевые решения для организаций, использующих спутниковую связь в качестве основного или резервного канала передачи данных, вплоть до организации магистральных каналов для интернет-провайдеров.

В интересах государственных учреждений операторы, предоставляющие услуги спутниковой связи, уже имеют готовые решения для оперативной организации систем связи в труднодоступных районах для ведомств, отвечающих за предупреждение и ликвидацию чрезвычайных ситуаций.

Данные цели достигаются за счёт применения VSAT технологий. VSAT – технология двухстороннего (симметричного) спутникового интернета. В основе способа подключения лежит использование двух каналов связи, каждый из которых спутниковый: «запросы» и «ответы» идут через спутник. Технология позволяет передавать через спутник различные виды информации и поддерживает надежную работу с любыми IP-сервисами, включающими в себя передачу голоса, данных, видео, выход в интернет, доступ к корпоративным сетям и актуальной отраслевой информации (базам данных и приложениям) для оперативного управления и взаимодействия специалистов удаленных подразделений.

Спутниковая связь VSAT не имеет ограничений по привязке к местности и позволяет организовать телекоммуникационные каналы там, где построение других систем нерентабельно или невозможно: малозаселенные или незаселенные регионы, территории без наземной инфраструктуры, морские транспортные пути. Спутниковые каналы позволяют получить полноценный доступ в интернет также и вне зоны действия наземных сетей связи с входящей скоростью до 45 Мбит/с и исходящей – до 10 Мбит/с.

В основном компании, предоставляющие услуги спутниковой технологии VSAT, используют группировки искусственных спутников Земли (далее – ИСЗ):

- российские – «Ямал-401», «Ямал-402», «Ямал-300К», «Ямал-601», «Экспресс-AM8», «Экспресс-AM103», «Экспресс-AMU1», «Экспресс-AM5»;
- зарубежные – NSS12, Eutelsat 172B.

В случае выхода из строя одного из ИСЗ имеется возможность быстрого перехода на другой без потери связи для абонента на территориях Российской Федерации, стран СНГ, Европы и Ближнего Востока.

Операторы, предоставляющие услуги с применением спутниковой связи, применяют следующие виды технологий:

- технология с применением фиксированных спутниковых систем связи VSAT;
- технология морского VSAT;
- мобильная спутниковая связь.

Фиксированные спутниковые системы связи VSAT состоят из двух и более терминалов, взаимодействующих между собой через геостационарные спутники-ретрансляторы, которые расположены на геостационарной орбите (36000 км) над экватором и вращаются синхронно с Землей.

Таким образом, спутники находятся в неподвижном положении для наблюдателя с Земли, и это позволяет использовать фиксированные антенны, нацеленные в постоянную точку на орбите. Основными характери-

ками спутника являются количество бортовых передатчиков, их мощность и диапазоны радиочастотных каналов.

Основным узлом в спутниковых сетях является центр управления сетями (далее – ЦУС) оператора. В состав ЦУС входит: каналообразующее оборудование – спутниковая приемо-передающая антенна диаметром 4,5–11 м с мощным приемопередатчиком до 400 Вт; HUB – аппаратура для коммутации и обработки информации в сети VSAT.

В общем случае, сигнал от VSAT-терминала абонента поступает на спутник, который усиливает и отправляет его в ЦУС. Оператор обрабатывает запрос и, получив ответные данные из сети, передает информацию обратно через спутник на малую земную станцию абонента.

Дополнительно на основе спутниковой связи VSAT возможна организация видеонаблюдения за удаленными объектами, автоматизированных сетей управления и телекоммуникационных сетей связи.

Принцип работы фиксированной спутниковой системы связи VSAT представлен на рисунке 1.

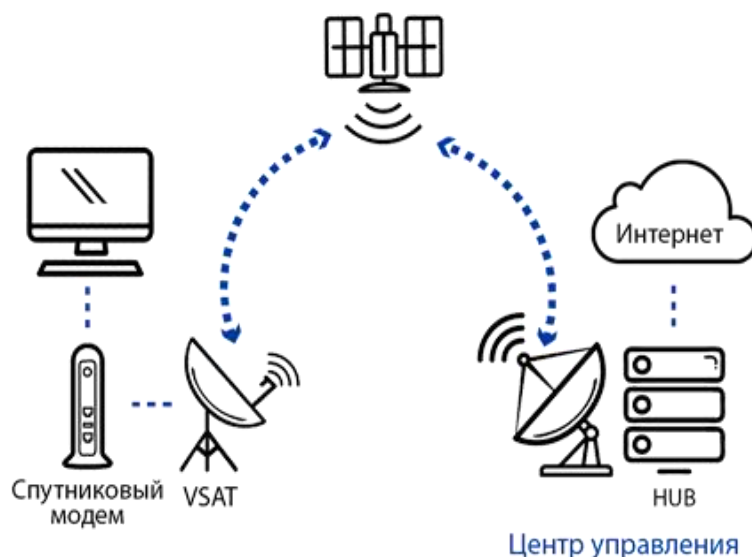


Рис. 1. Принцип работы фиксированной спутниковой системы связи VSAT

На базе двусторонней фиксированной спутниковой системы связи VSAT доступа можно обеспечить связью отдаленные и крупные объекты, к станции можно подключить сеть из множества компьютеров, для которых требуется выход в интернет, а также решить множество других задач [4].

Фиксированные спутниковые системы связи VSAT могут быть построены на основе следующих топологий:

- «звезда» (ЦУС располагается на стороне оператора или клиента);
- сети с мигрирующей топологией (малые локальные сети, бесхабовые сети, гибридные сети);
- полносвязные сети;
- выделенные каналы связи по технологии SCPC/CnC («точка-точка») [5].

В большинстве случаев сети VSAT строятся по топологии Star (звезда): ЦУС оператора является центром сети, и взаимодействие абонентских станций происходит через него. Сигнал с пользовательского VSAT-терминала направляется на спутник, где он усиливается и перенаправляется на ЦУС спутникового оператора, который подключен к глобальным сетям высокоскоростными наземными каналами связи. Обратный сигнал проходит тот же путь. Сеть топологии «звезда» – оптимальное решение для организации широкополосного доступа и построения корпоративных сетей для компаний с разрозненными объектами. Но для некоторых онлайн приложений или IP-протоколов данная топология не подходит из-за неизбежной задержки сигнала. Современные телекоммуникационные технологии позволяют избежать данной проблемы, так как ЦУС распределяет частотный ресурс таким образом, что абонентские VSAT станции могут взаимодействовать через спутник напрямую друг с другом. Это позволяет обеспечивать надежные каналы связи без системы стороннего управления.

В зависимости от задач возможна реализация смешанной или вложенной топологии, когда в архитектуре сети применяются оба решения.

Для организации надежного канала связи с помощью VSAT-технологии необходимо установить малую земную спутниковую станцию связи. Комплект VSAT включает в себя спутниковую антенну от 0,78 м до 2,4 м, приемо-передающее устройство, спутниковый модем-маршрутизатор, необходимый набор кабелей, систему крепления антенны. Комплект оборудования устанавливается в любом месте, а его размещение не привязано к наземным и сотовым линиям связи.

Согласно принятой классификации, оборудование VSAT-станции подразделяют на:

- внешнее, устанавливаемое на открытом воздухе – спутниковая антенна в сборе и приемоопередатчик (ODU);
- внутреннее, устанавливаемое в помещении – спутниковый модем (IDU).

Внешнее и внутреннее оборудование фиксированной спутниковой системы связи VSAT представлены на рисунке 2.

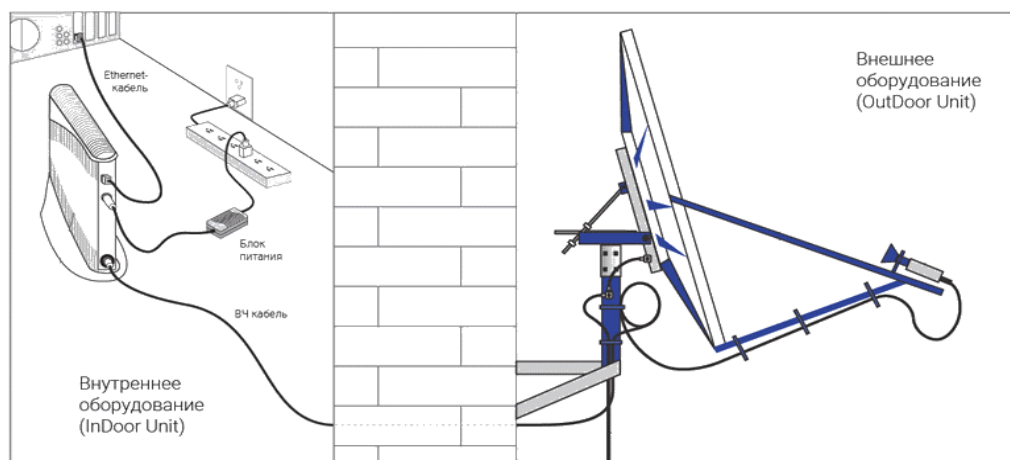


Рис. 2. Внешнее и внутреннее оборудование фиксированной спутниковой системы связи VSAT

На базе такого комплекта возможна организация более широкого спектра услуг: IP-телефония, видеонаблюдение, коллективный доступ в Интернет и прочие услуги, где требуется скоростной входящий и исходящий каналы передачи данных.

Таким образом, система централизованного наблюдения в труднодоступных районах с применением спутниковой VSAT-технологии приобретает вид, представленный на рисунке 3.

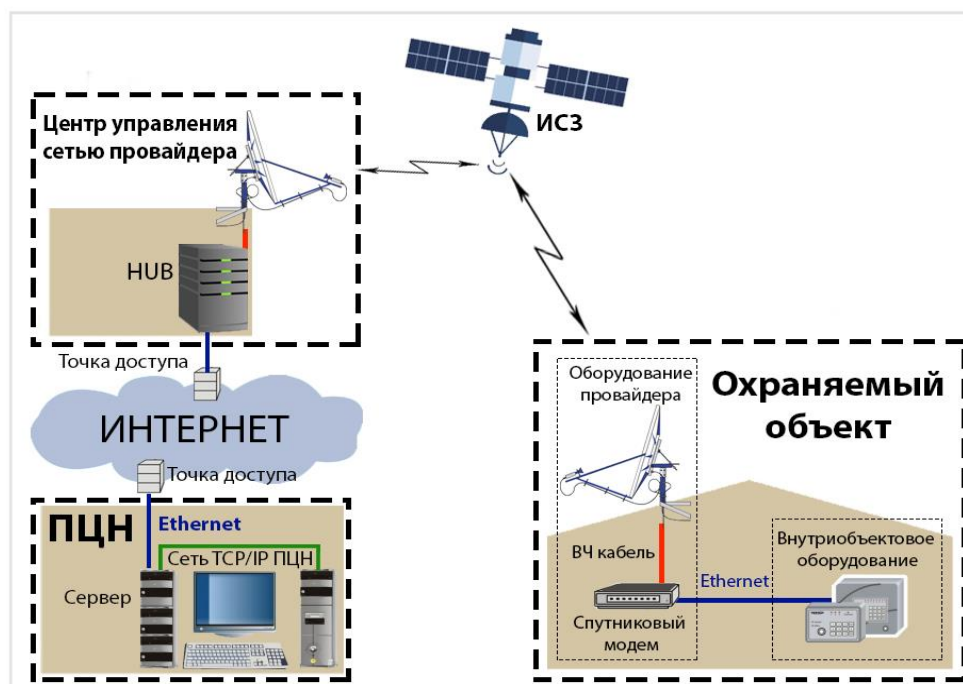


Рис. 3. Организация системы централизованного наблюдения в труднодоступных районах с применением спутниковой VSAT-технологии

Таким образом, организация устойчивой работы СПИ в труднодоступных районах с применением СПИ, использующих в качестве основного канала связи маршрутизируемые IP-сети с каналом передачи данных Ethernet, возможна при подключении средства передачи извещений к беспроводному интернет-соединению. Перспективным решением данной задачи представляется использование спутниковых каналов передачи данных с применением VSAT-технологии.

Выделяют следующие преимущества спутниковой VSAT-технологии:

- доступность практически в любой точке Российской Федерации;
- оптимальный вариант решения проблемы со связью на временных объектах;
- быстрота демонтажа и монтажа на новом объекте;
- весь спектр приложений и возможностей современных информационных технологий на одной платформе;
- возможность объединения удаленных объектов в единую сеть;

- возможность обеспечения мониторинга и управление процессами удаленных объектов в режиме online;
- возможность организации полного контроля и видеонаблюдения для удаленных объектов.

Вместе с тем при организации централизованной охраны с применением спутниковой VSAT-технологии необходимо учитывать следующие недостатки:

- необходимость затрат средств и времени на обеспечение конфиденциальности передачи данных, на предотвращение возможности перехвата данных «чужими» станциями;
- наличие задержки приема радиосигнала наземной станцией из-за больших расстояний между спутником и базовой станцией. Это может вызывать проблемы, связанные с реализацией канальных протоколов, а также временем ответа;
- возможность взаимного искажения радиосигналов от наземных станций, работающих на соседних частотах;
- подверженность сигналов на участках Земля-спутник и спутник-Земля влиянию различных атмосферных явлений.

СПИСОК ЛИТЕРАТУРЫ

1. Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально–противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации, утверждены решением расширенного заседания Технического совета ГУВО Росгвардии (Протокол № 1 от 27–30 мая 2024 г.).

2. Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально–противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации», рекомендован решением расширенного заседания Технического совета ГУВО Росгвардии (Протокол № 1 от 27–30 мая 2024 г.).

3. Михайлов Р. Л. Описательные модели систем спутниковой связи как космического эшелона телекоммуникационных систем специального назначения : монография. – Санкт-Петербург : Наукоемкие технологии, 2019. – 150 с.

4. Евлушина Д. А., Гильманов И. И. Технология построения сетей спутниковой связи VSAT // Форум молодых ученых. – 2017. – №7 (11).

5. Зинкин С. В., Каркаев Р. М., Перетрухин В. С. Теоретический анализ топологий сетей спутниковой связи // Вестник ПензГУ. – 2022. – № 1 (37).

СВЕДЕНИЯ ОБ АВТОРАХ

Янгиров Адиль Илдарович.

Начальник отделения лабораторных исследований и испытаний.

Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: Adil-Yan@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б.

Янгиров Илдар Мухаматович.

Научный сотрудник отдела развития средств обнаружений.

Федеральное казенное учреждение «Научно-исследовательский центр «Охрана» Федеральной службы войск национальной гвардии Российской Федерации.

E-mail: YIMufa@yandex.ru

Россия, 111539, г. Москва, ул. Реутовская, 12Б,

Ахлюстин Сергей Борисович.

Начальник кафедры тактико-специальной подготовки.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: cerg7676@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Садчикова Наталия Александровна.

Следователь специализированного отдела по расследованию преступлений общеуголовной направленности – «дистанционного хищения»

Следственное управление УВД по ЮБАО ГУ МВД России по г. Москве.

E-mail: nsadchikova6@mail.ru

Россия, 109443, г. Москва, ул. Юных Ленинцев, 79, корп. 2.

Yangirov Adil Ildarovich. Head of the Laboratory Research and Testing Department.

Federal State Institution «Scientific Research Center «OKHRANA» of the Federal service of National Guard of the Russian Federation.

Russia, 111539, Moscow, Reutovskaya, 12B.

Yangirov Ildar Mukhamatovich.

Researcher at the Department of Development of Detection Tools.

Federal State Institution «Scientific Research Center «OKHRANA» of the Federal service of National Guard of the Russian Federation.

Russia, 111539, Moscow, Reutovskaya, 12B.

Ahlyustin Sergey Borisovich.

Head of the department of tactical and special training.

Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Sadchikova Natalia Alexandrovna.

Investigator of the Specialized Department for the Investigation of Crimes of a General Criminal Orientation - «Remote Theft».

Investigative Department of the Department of Internal Affairs for the Southern Administrative District of the Ministry of Internal Affairs of Russia in Moscow.

E-mail: nsadchikova6@mail.ru

Russia, 190443, Moscow, st. Yunykh Lenintsev, 79, bldg. 2.

Ключевые слова: охрана объектов; труднодоступные районы; спутниковый канал связи; VSAT.

Keywords: security of facilities; hard-to-reach areas; satellite communication channel; VSAT.

УДК 654

ВСЕРОССИЙСКИЙ СЕМИНАР

УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ СРЕДИ НЕСОВЕРШЕН- НОЛЕТНИХ

А. И. Бадретдинов

ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В СИСТЕМАТИЧЕСКОЕ УПОТРЕБЛЕНИЕ АЛКОГОЛЬНОЙ ПРОДУКЦИИ В СЕЛЬСКОЙ МЕСТНОСТИ

FEATURES OF PREVENTING THE INVOLVEMENT OF MINORS IN THE SYSTEMATIC CONSUMPTION OF ALCOHOL PRODUCTS IN RURAL AREAS

Статья посвящена некоторым аспектам системы профилактики вовлечения несовершеннолетних в употребление алкогольной продукции в сельской местности. Приводится и анализируется статистическая информация о деятельности территориальных органов внутренних дел и комиссий по делам несовершеннолетних в Республике Башкортостан, особое значение отводится вопросу профилактической работы в семье и школе.

The article is devoted to some aspects of the system of prevention of involvement of minors in the use of alcoholic beverages in rural areas. Statistical information on the activities of territorial bodies of internal affairs and commissions for juvenile affairs in the Republic of Bashkortostan is given and analyzed; special importance is given to the issue of preventive work in the family and school.

Проблема потребления алкоголя несовершеннолетними является одной из наиболее острых и насущных в современном обществе. Интерес подростков к алкоголю не является случайным явлением. Для многих молодых людей, вступающих в период полового созревания, употребление спиртных напитков ассоциируется с признаком взрослости, поскольку чаще всего происходит в семейном кругу во время совместных застолий. Стоит заметить, что таким образом родители порой сами способствуют развитию у своих детей пагубной привычки. Во время праздничных мероприятий некоторые взрослые считают безобидным, если ребенок попробует напиток из бокала, причём не придавая значение возрастным особенностям и возможным негативным последствиям. Вопреки расхожему мнению о том, что наиболее подверженными алкоголизацией являются дети из неблагополучных семей, данные социальных опросов позволяют установить, что риск возникновения таких проблем актуален для представителей всех социальных групп.

Причины, побуждающие подростков к употреблению алкоголя, многообразны.

Среди наиболее часто встречающихся можно выделить следующие:

- 1) формирование привычки к употреблению спиртных напитков в семейном кругу в связи с праздниками;
- 2) широкая доступность алкогольной продукции в торговых точках;
- 3) низкая самооценка и стремление к поиску способов повышения уверенности в себе;
- 4) сильное влияние со стороны сверстников, практикующих употребление алкоголя;
- 5) недостаток возможностей для организации досуга и поиска альтернативных форм времяпрепровождения.

Потребление спиртных напитков оказывает разрушительное воздействие не только на физическое здоровье индивида, но и влечет за собой серьёзные негативные последствия для общества в целом. К ним относятся: рост уровня преступности, увеличение общей смертности населения, а также распространение беспризорности среди детей.

Согласно статье 20.20 и 20.21 Кодекса об административных правонарушениях Российской Федерации [1] (далее – КоАП РФ), подростки, достигшие шестнадцатилетнего возраста, несут административную ответственность за употребление алкоголя. Статья 20.22 КоАП РФ устанавливает административную ответственность в виде штрафа для родителей несовершеннолетних граждан в возрасте до шестнадцати лет, замеченных в состоянии опьянения. В соответствии с законодательством Российской Федерации, вовлечение несовершеннолетних в употребление пива и напитков, произведенных на его основе, влечет за собой административную ответственность, предусмотренную статьей 6.10 КоАП РФ. Если данные действия совершают родители, то их действия квалифицируются по части 2 статьи 6.10 КоАП РФ.

Подростковое употребление алкоголя представляет собой серьезную проблему, которая требует пристального внимания. Одним из ключевых аспектов профилактики является ограничение доступа подростков к алкогольной продукции. К сожалению, на практике мы сталкиваемся с ситуациями, когда продавцы пренебрегают своими обязанностями и продают алкоголь несовершеннолетним, руководствуясь исключительно корыстными мотивами.

В соответствии с законодательством Российской Федерации, розничная продажа алкоголя несовершеннолетним влечет за собой административную ответственность по статье 14.16 КоАП РФ в случае единичного нарушения. Повторное нарушение данного запрета влечет уголовную ответственность, предусмотренную статьей 151.1 Уголовного Кодекса Российской Федерации [2].

К сожалению, на сегодняшний день статистические данные весьма печальные. По словам А. И. Бастрыкина, на профилактическом учете в

подразделениях по делам несовершеннолетних территориальных органов внутренних дел Российской Федерации состоит свыше 400 тысяч подростков [3]. В 2023 году на территории Республики Башкортостан органами и учреждениями системы профилактики проводилась индивидуальная профилактическая работа с 19229 несовершеннолетними, с 1537 несовершеннолетними, совершившими правонарушение, повлекшее применение мер административного взыскания, и с 1215 (в 2022 г. – 1313) несовершеннолетними [4], совершившими правонарушение до достижения возраста, с которого наступает административная ответственность.

Согласно отчету о работе по профилактике безнадзорности и правонарушений несовершеннолетних на территории Республики Башкортостан по итогам 2023 года [4] на втором месте среди наиболее часто совершаемых несовершеннолетними административных правонарушений правонарушения, связанные с употреблением спиртных напитков: ст. 20.20 КоАП РФ – 189 (в 2022 г. – 266); ст. 20.21 КоАП РФ – 419 (в 2022 г. – 453). Особое беспокойство вызывает употребление спиртных напитков подростками, не достигших возраста 16 лет – 494 чел. (ст. 20.22 КоАП РФ в 2022 г. – 553).

Незанятость и отсутствие полноценного досуга среди подростков является одним из ключевых факторов риска развития алкогольной зависимости. Данная проблема обусловлена, в первую очередь, недостаточной ответственностью родителей, которые пренебрегают своими обязанностями по воспитанию, образованию и материальному обеспечению своих детей.

Одним из существенных факторов, осложняющих социально-педагогическую работу в поселке, является его удаленность от культурных центров и недостаточность системы дополнительного образования. Эффективность работы поселковой школы по всестороннему развитию подростков напрямую коррелирует с ее географическим расположением и социально-экономическими условиями проживания населения. Близость сельской школы к районному центру или городу предоставляет ей больше возможностей для интеграции подростков в социальную и культурную жизнь, способствует более успешному решению кадровых вопросов, укрепляет профессиональные связи социального педагога школы со специалистами различных областей, обеспечивает свободный доступ к актуальной информации и культурным ресурсам.

В отдаленных населенных пунктах качество образования страдает от ограниченных возможностей как школы, так и ее преподавательского состава. Это негативно сказывается на всестороннем развитии учащихся. Сельская местность, к сожалению, не располагает достаточным количеством ресурсов для организации полноценного досуга подростков. Основную нагрузку по этому направлению несут Дом культуры, поселковый спорткомплекс и школа. Дом культуры предлагает кружки танцев и изобразительного искусства, спорткомплекс – спортивные секции, а школа организует кружки по интересам. Несмотря на то, что школьные кружки

планируются с учетом пожеланий и интересов подростков, следует отметить, что их уровень, как и во многих других внешкольных учреждениях, оставляет желать лучшего. Основная проблема поселения заключается в нехватке квалифицированных специалистов по работе с подростками.

На данный момент организацию досуга и работу с молодежью осуществляют в основном педагоги без достаточной квалификации или пенсионеры, которым физически сложно организовывать активный отдых, походы и секции. Отсутствие перспектив развития не привлекает молодых специалистов, способных обеспечить полноценное и разностороннее досуговое сопровождение подростков.

В поселении проживает значительное количество талантливых молодых людей, но дефицит учреждений, способствующих развитию их способностей, увлечений и интересов, остается серьезной проблемой. Численность населения поселка стремительно сокращается в результате миграции жителей в городские центры. Несмотря на то, что школа продолжает функционировать, изменившиеся социально-экономические условия требуют коренных преобразований в ее социально-педагогической деятельности. Школе необходимо адаптироваться к инновационным процессам, происходящим в социально-экономической сфере общества. В настоящее время образовательный и воспитательный процесс в поселке отстает от требований современной жизни, поскольку не уделяет должного внимания формированию у учащихся личностных качеств, ценностных ориентиров, социально значимых знаний, соответствующих динамике изменений в обществе и необходимых для организации самостоятельной и полноценной жизни в поселке.

Борьба с алкоголизмом предполагает комплексную реализацию мероприятий, направленных на предотвращение употребления несовершеннолетними спиртных напитков. Основополагающими принципами профилактики подросткового алкоголизма являются пропаганда здорового образа жизни и противоалкогольная агитация.

Одним из средств профилактики вовлечения несовершеннолетних в употребление алкогольной продукции являются меры административно-правового характера в отношении родителей, не исполняющих обязанностей по содержанию и воспитанию несовершеннолетних. В рамках производства по делам об административных правонарушениях на территории Республики Башкортостан муниципальными комиссиями за 2023 год рассмотрено 15 644 (в 2022 – 15 820) административных материалов в отношении родителей (законных представителей) несовершеннолетних. В 2023 году наблюдается снижение количества родителей, привлеченных к административной ответственности за неисполнение родителями или иными законными представителями несовершеннолетних обязанностей по содержанию и воспитанию несовершеннолетних 14762 (2022 г. – 14 835) родителей.

В 2023 году на профилактический учет в ПДН территориальных органов внутренних дел поставлено 2 277 (в 2022 г. – 2 401) родитель и иной

законный представитель. По состоянию на 1 января 2024 года на профилактическом учете состояло 4 930 (в 2022 г. – 5 070) родителей (иных законных представителей). Объектом особого внимания являются неблагополучные семьи, многие из которых находятся в социально опасном положении. В числе подучетных «неблагополучных родителей» под профилактическим контролем находилось: употребляющих спиртные напитки – 3 392, употребляющих наркотические средства или психотропные вещества и их прекурсоры, либо новые потенциально опасные психоактивные вещества – 82, ранее лишенные родительских прав – 69.

Таким образом, можно сделать вывод, что формирование у детей и подростков нетерпимого отношения к употреблению алкоголя является неотъемлемой частью их нравственного воспитания. Для достижения положительных результатов антиалкогольная пропаганда должна быть систематической, целенаправленной и охватывать все доступные формы и методы работы. Государство также должно содействовать распространению информации о мерах противодействия данным деструктивным проявлениям [5]. Важную роль в этом процессе играет пропаганда здорового образа жизни, физической культуры и спорта, закаливания организма. Проведение подобных мероприятий целесообразно на уроках, во внеурочной деятельности и на занятиях по основам безопасности жизнедеятельности. При планировании работы необходимо учитывать возрастные и психологические особенности учащихся. Значительный вклад в формирование негативного отношения к алкоголизму вносят приглашенные специалисты: врачи, представители правоохранительных органов и юристы. Они проводят беседы и лекции на темы, связанные с последствиями употребления алкоголя, такими как «Алкоголизм и потомство», «Влияние малых доз алкоголя на способности человека» и «Последствия однократного сильного опьянения несовершеннолетнего». Возможно также привлечение самих учащихся к подготовке отдельных тем. В этом случае им должна быть оказана необходимая помощь.

СПИСОК ЛИТЕРАТУРЫ

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 08.08.2024) // Официальный интернет-портал правовой информации : [сайт]. – URL: <http://www.pravo.gov.ru> (дата обращения 21.09.2024).

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 02.10.2024) // Официальный интернет-портал правовой информации : [сайт]. – URL: <http://www.pravo.gov.ru> (дата обращения 21.09.2024).

3. Стало известно число подростков в России, которые состоят на профилактическом учёте // [сайт]. – URL: <https://www.gazeta.ru/social/news/2024/04/16/22796894.shtml?updated> (дата

обращения 21.10.2024).

4. Отчет о работе по профилактике безнадзорности и правонарушений несовершеннолетних на территории Республики Башкортостан по итогам 2023 года // [сайт]. – URL: <https://pravitelstvorb.ru/upload/uf/063/ucvsj9zp7an7cvl0cwww36vyw1uxqsns/Otchet-po-rabote-profilaktike-beznadzornosti-i-pravonarusheniy-nesovershen... .pdf> (дата обращения 21.10.2024).

5. Сибагатуллин Ф. Ф. Пропаганда насилия в сети Интернет: пути противодействия / Ф. Ф. Сибагатуллин // Санкт-петербургские встречи молодых ученых : Материалы I всероссийского конгресса адъюнктов, аспирантов и соискателей ученых степеней, Санкт-Петербург, 15 июня 2023 года. – Санкт-Петербург г: Санкт-Петербургский университет МВД России, 2023. – С. 329–334.

СВЕДЕНИЯ ОБ АВТОРЕ

Бадретдинов Айнур Ильдарович. Адъюнкт.
Уфимский юридический институт МВД России.
E-mail: badretdinov.ainur@rambler.ru
Россия, 450047, г. Уфа, ул. Муксинова, 2..

Badretdinov Ainur Ildarovich. Adjunct.
Ufa Law Institute of the Ministry of Internal Affairs of Russia.
E-mail: badretdinov.ainur@rambler.ru
Russia, 2, Muxinova str., Ufa, 450047.

Ключевые слова: профилактика; несовершеннолетние; алкогольная продукция; употребление алкоголя; сельское поселение; предупреждение вовлечения.

Keywords: prevention; minors; alcoholic beverages; alcohol consumption; rural settlement; prevention of involvement.

УДК 343.976

**НЕКОТОРЫЕ КРИМИНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ
ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ НЕСОВЕРШЕННОЛЕТНИМИ**

**SOME CRIMINOLOGICAL FEATURES
OF PREVENTING CRIMES COMMITTED BY MINORS**

В настоящей статье раскрыты некоторые криминологические особенности преступлений, совершенных несовершеннолетними. Рассмотрены такие элементы криминологической характеристики преступлений несовершеннолетних, как состояние и динамика преступлений, личность несовершеннолетнего преступника (психофизиологическая структура, возрастные группы), детерминанты. Предложен комплекс мер профилактики и предупреждения преступности среди несовершеннолетних.

This article reveals some criminological features of crimes committed by minors. The following elements of the criminological characteristics of crimes committed by minors are considered: the state and dynamics of crimes, the personality of a juvenile offender (psychophysiological structure, age groups), determinants. A set of measures for the prevention and warning of crime among minors is proposed.

Преступность несовершеннолетних является острой проблемой, имеющей множество граней, исследование которых способствует всестороннему изучению причин возникновения подростковой преступности и выбору наиболее эффективных мер противодействия ей.

Несмотря на прогнозы, анализ динамики общего количества зарегистрированных преступлений в Российской Федерации среди несовершеннолетних показывает положительную тенденцию. Статистические данные о состоянии преступности в Российской Федерации с января по октябрь 2024 года свидетельствуют о снижении числа зарегистрированных преступлений. Необходимо отметить, что количество уголовно наказуемых деяний, совершенных несовершеннолетними за указанный период времени, уменьшилось на 9,7%. Среди лиц, совершивших преступления, было выявлено 21 023 несовершеннолетних [1]. Данный положительный результат несомненно обеспечен эффективной работой по профилактике и предупреждению преступлений, проведенной инспекторами по делам несовершеннолетних и участковыми уполномоченными полиции.

Преступления, совершенные несовершеннолетними, имеют ряд особенностей. Во-первых, это связано с психофизиологическими качествами несовершеннолетних, так как они во многом отличаются от взрослых лиц.

Во-вторых, это влияние старших по возрасту, условия жизни, кругозор и род занятий несовершеннолетних лиц.

Личность преступника является главным звеном. Верное и успешное предупреждение любого вида преступлений зависит от личности преступника. Именно личностные особенности являются основной причиной, которая ведет к совершению конкретного преступления, поэтому на личности преступника стоит акцентировать внимание.

Как отмечает Л. С. Голубничая в несовершеннолетнем возрасте сознание и психика человека только начинают формироваться, поэтому подростки крайне восприимчивы как к положительному так и отрицательному влиянию, соответственно изучение личности несовершеннолетнего преступника имеет весомое криминологическое и уголовно-правовое значение [2].

Возраст несовершеннолетнего преступника играет важную роль, который связан с социологическими, биологическими и духовными характеристиками. Возраст обуславливает не только интеллектуальное, но и физическое развитие, что позволяет несовершеннолетнему лицу совершить определенного рода преступление.

Возрастные особенности несовершеннолетнего преступника стоит разделить на две группы:

- от 14 до 15 лет – подростково-малолетняя;
- от 16 до 17 лет – несовершеннолетние.

Исследования многих ученых-криминологов показали, что удельный вес несовершеннолетнего преступника зависит от их образовательного уровня, от занятости во внеурочное время, так как часто такие несовершеннолетние остаются на второй год учебы либо перестают ходить на учебные занятия в школу [3].

Также следует обратить внимание на влияние старших по возрасту лиц. Все качества несовершеннолетнего закладываются в его семье, то как с ним общаются, чем занимаются родители. Именно в семье происходит становление личности несовершеннолетнего. Большинство несовершеннолетних преступников воспитываются в семьях, где пьянство, скандалы, причинение физической боли являются неотъемлемой частью воспитания. Исследования криминологов показывают, что старшие братья, сестры, родители вовлекают несовершеннолетнего в преступную деятельность, либо способствуют формированию асоциального отношения к установленному порядку поведения в обществе [4].

В обыденной жизни несовершеннолетний преступник имеет больше свободного времени, примерно в 2-3 раза больше, нежели его сверстники. Связано это с тем, что несовершеннолетний не занимается каким-то определенным родом занятий, т.е. не посещает спортивные секции, не ходит на творческие кружки, не помогает родителям, не готовится к занятиям и т.д.

Немаловажным значением является правовое сознание несовершеннолетнего, совершающего преступления. Такой несовершеннолетний не

развивается (в интеллектуальном плане), относится пренебрежительно к нормам морали, правовым актам и указанным в них предписаниям [5].

Далее целесообразно рассмотреть предмет преступного посягательства со стороны несовершеннолетних лиц. Достаточно интересной является его характеристика, в первую очередь по той причине, что по некоторым видам преступлений предмет не отличается от преступлений, совершаемых совершеннолетним контингентом, а по другим видам преступлений предмет может иметь свою индивидуальность. К первому случаю мы можем отнести преступления против личности в части преступлений против жизни и здоровья. Не менее интересным является предмет преступлений против собственности, в частности наиболее популярного вида преступления среди несовершеннолетних – хищение чужого имущества (кража, грабеж, разбой). Часто предметом в указанном виде преступлений среди несовершеннолетних становятся стандартные вещи: деньги, золотые украшения, бытовая техника, то есть те вещи, которые представляют ценность в обществе. В то же время ввиду непонимания ценности некоторых вещей очень редко предметом хищения у несовершеннолетних становятся меховые изделия и произведения искусства. Данный факт может свидетельствовать о наивности и экономической необразованности субъектов данного вида преступлений.

Время совершения преступления в зависимости от определенного вида преступления не отличается от того случая, когда такие преступления совершают совершеннолетние субъекты. Например, квартирные кражи совершаются в большей степени в дневное время, когда владельцев квартиры нет дома, грабеж и разбой чаще всего совершаются в раннее утреннее либо позднее вечернее время, когда в общественных местах еще нет массового скопления граждан.

Место совершения преступления может незначительно отличаться от места совершения их совершеннолетними. Например, если у совершеннолетних субъектов наиболее популярным местом совершения кражи являются квартиры, то для несовершеннолетних часто местом совершения кражи являются торговые центры, магазины продуктов и других товаров. В остальных случаях место совершения преступления зачастую совпадает.

Анализируя способ совершения преступлений, стоит отметить, что данный критерий состоит из 3 стадий – подготовки, совершения противоправного деяния, маскировки. Здесь необходимо рассмотреть способ совершения преступлений по представленной структуре в наиболее часто встречаемом виде преступлений среди несовершеннолетних – кражи.

На этапе подготовки осуществляется подбор соучастников, выбор объекта посягательства, приобретение технических средств, выбор времени совершения преступного деяния, а также поиск мест хранения. Стоит отметить, что подбор соучастников среди несовершеннолетних осуществляется достаточно быстро, так как в качестве соучастников в большей степени участвуют люди с ближайшего окружения: одноклассники, соседи, а

также лица, находящиеся в дружеских отношениях с совершеннолетним. Кроме того, определенной особенностью является незаинтересованность несовершеннолетних преступников в поиске мест хранения похищенного, это связано с тем, что совершение таких преступлений носит спонтанный характер, что приводит к плохой организованности совершения данного преступления.

Маскировка, уничтожение или укрытие орудий совершения преступлений, сбыт похищенного, выбрасывание похищенного при угрозе разоблачения в наименьшей степени осуществляется несовершеннолетними, это связано с отсутствием у них чувства ответственности и страха наказания за содеянное.

Проанализированные выше некоторые данные позволяют выделить наиболее результативные меры профилактики и предупреждения преступности среди несовершеннолетних.

Многие меры, которые предпринимаются субъектами профилактики являются продуктивными формально, ведь та информация, которая преподносится несовершеннолетним в большей степени их не интересует. Для доступности представляемой информации и возможности усвоения полученных знаний со стороны несовершеннолетних необходимо использовать ряд психологических приемов и методов, которые помогут отчетливо донести до подростка основные положения законодательства. Проведение подобных мероприятий «для галочки» приводит к неосознанному совершению преступлений, к отсутствию понимания закономерных последствий совершения противоправных деяний несовершеннолетними.

Исследуя такой способ профилактики преступности, на наш взгляд, самым продуктивным является встреча несовершеннолетних правонарушителей с теми лицами, которые уже находятся в исправительных учреждениях. На несовершеннолетних в таком случае будет оказано колоссальное влияние людей, которые сами пережили сложные моменты, допустили ошибки в жизни. Учитывая психологические особенности рассматриваемой категории лиц, стоит прогнозировать внушительное воздействие на правосознание молодых людей.

Конечно, использование одного метода для эффективного воздействия на несовершеннолетнего недостаточно. Профилактическая работа должна иметь комплексный характер и распространяться не только на конкретное лицо, но и затрагивать сферы его жизнедеятельности. В качестве одного из основных методов можно проанализировать поддержание контакта с родителями или опекунами проблемного подростка. Такая мера способствует четкому формированию у старших лиц ответственности за несовершеннолетнего, ощущению контроля со стороны правоохранительных органов за действиями по отношению к нему.

Нельзя не сказать о деятельности по разобщению круга лиц антиобщественной направленности, в который включен подопечный несовер-

шеннолетний. Разрыв связей с криминогенными элементами и лицами, которые ранее привлекались в ответственности, посредством демонстрация подростку сущности совершенных такими лицами деяний. Данная мера способствует утрачиванию желая подростка подражать антисоциальным авторитетам, что благоприятно сказывается на его правовом сознании.

Помимо рассмотренных способов профилактики, стоит выделить отдельные аспекты, изучение которых также необходимо при предупреждении как общеуголовных преступлений, так и противоправных деяний, совершенных несовершеннолетними:

- прямая и непосредственная причина совершения несовершеннолетним преступления;
- причины сформированности антиобщественной направленности личности несовершеннолетнего преступника;
- объективные и субъективные условия, которые способствовали формированию, закреплению у несовершеннолетнего антиобщественной направленности;
- причины и условия совершения конкретного преступления несовершеннолетним.

Подводя итог сказанному, необходимо отметить, что в данной сфере кроме множества особенностей, существуют определенный перечень проблем, которые нуждаются в скорейшем решении. Такая оперативность необходима в связи с тем, что общество не стоит на месте и происходит активное развитие различных сфер жизнедеятельности человека. Соответственно, с каждым годом подростковая преступность подвергается трансформации ее качественной составляющей. Такая динамика требует незамедлительного вмешательства в совершенствование профилактических и предупредительных мер преступности несовершеннолетних.

СПИСОК ЛИТЕРАТУРЫ

1. Статистика и аналитика / Состояние преступности (архивные данные) // Официальный сайт МВД России [Электронный ресурс]. – URL: <https://xn--b1aew.xn--p1ai/folder/101762> (дата обращения: 11.11.2024).
2. Голубничая Л. С. Криминологическая характеристика личности несовершеннолетнего преступника / Л. С. Голубничая // Амурский научный вестник. – 2015. – № 1. – С. 158–172.
3. Свечников Н. И. Преступность несовершеннолетних: личность преступника, причины, профилактика / Н. И. Свечников, А. Ю. Князькина // Вестник Пензенского государственного университета. – 2020. – № 3 (31). – С. 85–95.
4. Медведева Д. Д. Вовлечение несовершеннолетних в преступную среду как уголовно-правовая категория: вопросы теории и практики

/ Д. Д. Медведева // Правопорядок: история, теория, практика. – 2024. – № 2 (41). – С. 186–193.

5. Кулешов А. А. Детерминанты вовлечения несовершеннолетних в совершение преступлений / А. А. Кулешов, В. В. Ильиных // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2022. – № 8-1. – С. 52–56.

СВЕДЕНИЯ ОБ АВТОРАХ

Колесников Роман Викторович.
Доцент кафедры уголовного права и криминологии.
Кандидат юридических наук.
Воронежский институт МВД России.
E-mail: rkolesnikow@mail.ru
Россия, 394065, Воронеж, просп. Патриотов, 53.

Польшиков Александр Васильевич.
Доцент кафедры уголовного права и криминологии.
Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: polschikow@mail.ru
Россия, 394065, Воронеж, просп. Патриотов, 53.

Kolesnikov Roman Viktorovitch.
Assistant professor of the Criminal law and Criminology.
Candidate of Legal Sciences.
Voronezh institute of the Ministry of the Interior of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Polshikov Alexander Vasilievich.
Associate Professor of the Department of Criminal Law and Criminology.
Candidate of Legal Sciences, Associate Professor.
Voronezh institute of the Ministry of the Interior of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: несовершеннолетний; подросток; преступность; криминологическая характеристика; особенности; личность преступника; возраст.

Keywords: minor; teenager; crime; criminological characteristics; features; personality of the criminal; age.

УДК 343.85

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНЕГО В СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЯ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ

INVOLVEMENT OF A MINOR IN THE COMMISSION OF A CRIME: PROBLEMS OF QUALIFICATION

В статье анализируются проблемы квалификации вовлечения несовершеннолетних в преступную деятельность, включая отсутствие разграничения между вовлечением несовершеннолетних и малолетних, а также правовые пробелы в отношении вовлечения в укрывательство преступлений. Предложены рекомендации по совершенствованию законодательства для более точной защиты прав несовершеннолетних.

The article analyzes the problems of qualification of the involvement of minors in criminal activity, including the lack of differentiation between the involvement of minors and minors, as well as legal gaps in relation to involvement in the concealment of crimes. Recommendations on improving legislation for more accurate protection of the rights of minors are proposed.

Актуальность исследования уголовно-правовых аспектов вовлечения несовершеннолетнего в совершение преступления обусловлена несколькими важными факторами, имеющими как теоретическое, так и практическое значение. Прежде всего, следует отметить, что преступления, связанные с вовлечением несовершеннолетних, представляют собой серьезную угрозу не только для личности пострадавшего, но и для общества в целом, поскольку они подрывают основы воспитания и социализации подрастающего поколения [1, с. 251]. Учитывая высокую степень виктимности несовершеннолетних, обусловленную их психофизиологическими и социальными особенностями, исследование проблем квалификации подобных преступлений приобретает особую значимость.

Такое преступное воздействие зачастую направлено на формирование у несовершеннолетнего устойчивых антиобщественных установок, что может стать причиной вовлечения его в криминальную субкультуру. В условиях информационного общества влияние различных факторов, таких как интернет-пространство, групповые психологические механизмы и неблагоприятная социальная среда, значительно усложняет профилактику и выявление таких преступлений. Более того, специфика психологии несовершеннолетнего – его повышенная внушаемость, недостаточная критичность мышления и стремление к самореализации в группе – способствует уязвимости перед манипулятивным воздействием со стороны взрослого преступника [2, с. 275].

Одна из проблем, связанных с квалификацией вовлечения несовершеннолетнего в совершение преступления, возникает в ситуациях, когда между вовлекающим и вовлекаемым существует незначительная разница в возрасте, составляющая от нескольких месяцев до одного года. На практике суды зачастую рассматривают подобные случаи исключительно с формально-юридической точки зрения, не принимая во внимание социальные и психологические аспекты взаимодействия таких лиц.

При таком подходе упускается из виду важное обстоятельство: в случаях минимальной возрастной разницы стороны могут находиться в схожей стадии психофизиологического и социального развития. Это существенно затрудняет выделение одного из участников как лица, обладающего властью или влиянием, достаточным для «вовлечения» другого. Например, вовлекающее лицо в возрасте 18 лет и вовлекаемый несовершеннолетний в возрасте 17 лет могут поддерживать дружеские, а не иерархические отношения, что делает спорным утверждение о наличии признаков манипуляции, уговоров или иного преступного воздействия, а, следовательно, и повышенной общественной опасности деяний, позволяющей дополнительно квалифицировать действия злоумышленника по ст. 150 УК РФ.

Еще одной серьезной проблемой квалификации вовлечения несовершеннолетних в совершение преступления является отсутствие различий в правовом регулировании между вовлечением несовершеннолетнего лица, достигшего возраста привлечения к уголовной ответственности, и малолетнего лица, которое по определению не является субъектом преступления. Данная проблема обусловлена унифицированным подходом статьи 150 УК РФ, который не учитывает фундаментальных различий в психофизиологических, социальных и правовых характеристиках этих категорий лиц.

С юридической точки зрения, привлечение к уголовной ответственности за вовлечение малолетнего лица требует более жесткой оценки действий виновного, поскольку малолетние не обладают даже минимальным уровнем осознания противоправности своих поступков и полностью зависят от влияния взрослого. В то же время действующее законодательство не делает различий между вовлечением малолетнего и несовершеннолетнего, что приводит к одинаковой квалификации действий, несмотря на значительные различия в степени общественной опасности таких деяний [3, с. 115].

Проблема отсутствия различий между вовлечением несовершеннолетнего лица и малолетнего лица, не являющегося субъектом преступления, особенно ярко проявляется в контексте применения положений статьи 150 УК РФ и части 2 статьи 33 УК РФ. Согласно действующему законодательству, лицо, вовлекшее несовершеннолетнего, который достиг возраста уголовной ответственности, может быть привлечено к ответственности за вовлечение как самостоятельное преступление. Однако в случае, если во-

влекаемым является малолетнее лицо, не достигшее возраста уголовной ответственности, правоприменение сталкивается с юридическим парадоксом.

С одной стороны, формально лицо, вовлекшее малолетнего, несет ответственность за преступление, совершенное этим лицом, в качестве исполнителя через посредственное причинение. Данный подход основан на том, что малолетнее лицо не может быть субъектом преступления, а его действия расцениваются как инструмент, использованный вовлекателем. С другой стороны, юридическая природа вовлечения предполагает, что лицо склоняет другого субъекта к совершению преступления, тогда как малолетнее лицо по определению не может совершить преступление ввиду отсутствия у него субъектного статуса. Следовательно, говорить о вовлечении малолетнего в совершение преступления с точки зрения строгой юридической логики неправомерно.

Данная правовая коллизия приводит к двум важным последствиям. Во-первых, применение статьи 150 УК РФ к случаям вовлечения малолетнего становится теоретически некорректным, так как отсутствует ключевой элемент состава преступления – субъективное участие вовлекаемого в преступной деятельности. Во-вторых, ответственность за действия вовлекателя, связанная с применением части 2 статьи 33 УК РФ, не учитывает специфики вовлечения малолетних, требующих особой правовой защиты в силу их полной зависимости от взрослого. Это приводит к смешению понятий «вовлечение» и «использование», что создает сложности в квалификации.

Таким образом, отсутствие четкого законодательного разграничения между вовлечением несовершеннолетнего и действиями, связанными с использованием малолетнего лица, приводит к юридической неопределенности. Для устранения этой проблемы целесообразно пересмотреть подход к квалификации таких деяний, выделив отдельный состав преступления, связанный с использованием малолетнего лица для совершения преступных действий, либо внести дополнительные разъяснения в статью 150 УК РФ, исключив возможность применения термина «вовлечение» к малолетним.

Еще одним значительным пробелом в законодательстве является отсутствие правового регулирования ситуации, связанной с вовлечением несовершеннолетнего в заранее не обещанное укрывательство преступлений небольшой или средней тяжести. Такая ситуация возникает, когда несовершеннолетний, не являясь соучастником преступления, вовлекается в действия, направленные на сокрытие его следов, такие как уничтожение вещественных доказательств, перемещение предметов преступления или оказание иной помощи виновному. В действующем законодательстве отсутствуют нормы, которые бы четко регламентировали ответственность за вовлечение несовершеннолетнего в такие действия, что создает значительные сложности в правоприменительной практике.

Согласно действующим положениям уголовного закона, заранее не обещанное укрывательство преступлений (ст. 316 УК РФ) относится к са-

мостоятельным преступлениям лишь в случае укрывательства некоторых тяжких и особо тяжких преступлений. Соответственно вовлечение несовершеннолетних в укрывательство преступлений, если такое деяние содержит признаки преступления, предусмотренного ст. 316 УК РФ, влечет привлечение взрослого лица дополнительно к уголовной ответственности по ст. 150 УК РФ. В свою очередь, вовлечение несовершеннолетнего в заранее не обещанное укрывательство преступлений небольшой или средней тяжести не является «вовлечением в совершение преступления». Это приводит к юридической неопределенности, так как действия виновного лица, манипулирующего несовершеннолетним, фактически остаются вне рамок уголовной ответственности.

В ходе проведенного исследования выявлены ключевые проблемы уголовно-правового регулирования, связанные с вовлечением несовершеннолетних в преступную деятельность. Наиболее значимые из них включают отсутствие четкого законодательного разграничения между вовлечением несовершеннолетних и малолетних, не являющихся субъектами преступления, формализм в подходах к квалификации действий при минимальной разнице в возрасте между вовлекающим и вовлекаемым, а также правовая неопределенность в отношении вовлечения несовершеннолетних в заранее не обещанное укрывательство преступлений.

Предлагается внести изменения в статью 150 УК РФ, выделив отдельный состав преступления, связанный с использованием малолетних для совершения преступных действий, а также дополнить законодательство нормами, регулирующими вовлечение несовершеннолетних в укрывательство преступлений. Устранение обозначенных пробелов будет способствовать повышению эффективности уголовно-правовой защиты несовершеннолетних, укреплению справедливости в правоприменении и усилению профилактической роли уголовного законодательства.

СПИСОК ЛИТЕРАТУРЫ

1. Пучнина М. Ю. Факторы, способствующие вовлечению несовершеннолетних в совершение преступлений экстремистской направленности и террористического характера / М. Ю. Пучнина, А. В. Пучнин // Вестник Воронежского института МВД России. – 2024. – № 2. – С. 250–255.

2. Родин С. Г. Противодействие вовлечению несовершеннолетних в совершение действий, представляющих опасность для их жизни: обоснованность криминализации и проблемы квалификации / С. Г. Родин, Р. В. Колесников // Вестник Воронежского института МВД России. – 2022. – № 3. – С. 274–280.

3. Буданова Е. А. О необходимости оптимизации уголовно-правовой нормы об ответственности за вовлечение несовершеннолетнего в совершение преступления (ст. 150 УК РФ) / Е. А. Буданова, А. В. Польшиков,

М. М. Буслов // Современное общество и право. – 2022. – № 6 (61). – С. 112–117.

СВЕДЕНИЯ ОБ АВТОРЕ

Кулешов Антон Александрович.
Преподаватель кафедры уголовного права и криминологии.
Воронежский институт МВД России.
E-mail: kuleashov@yandex.ru
Россия, 394065, Воронеж, Проспект Патриотов, 53.

Kuleshov Anton Alexandrovich.
Lecturer at the Department of Criminal Law and Criminology.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: kuleashov@yandex.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: несовершеннолетний; малолетний; уголовная ответственность; квалификация преступлений; укрывательство преступлений; субъект преступления; уголовно-правовая защита.

Keywords: minor; juvenile; criminal liability; qualification of crimes; concealment of crimes; the subject of the crime; criminal legal protection.

УДК 343.2

А. В. Максименко, А. С. Лимарь

ПРЕДУПРЕЖДЕНИЕ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В ДИВЕРСИОННУЮ ДЕЯТЕЛЬНОСТЬ

CURRENT TRENDS IN IMPROVING THE CRIMINAL LEGISLATION OF THE RUSSIAN FEDERATION

В данной статье исследуется состояние ювенольной преступности. Основная цель исследования заключается в анализе причин, способствующих вовлечению несовершеннолетних в диверсионную деятельность. Актуальность данной темы обусловлена необходимостью выработки криминологических мер, направленных на защиту несовершеннолетних от вовлечения в преступную деятельность.

Объектом исследования является совокупность взаимосвязанных общественных отношений, направленных на защиту прав несовершеннолетних и обеспечение правового воспитания.

This article examines the state of juvenile delinquency. The main purpose of the study is to analyse the reasons contributing to the involvement of minors in subversive activities. The relevance of this topic is due to the need to develop criminological measures aimed at protecting minors from involvement in criminal activity.

The object of the study is a set of interrelated social relations aimed at protecting the rights of minors and providing legal education.

Преступность среди несовершеннолетних всегда привлекала внимание общества, поскольку нарушения уголовно-правовых норм подрастающим поколением, их распространенность и разнообразие выступают в качестве одного из элементов характеристики преступности в целом.

Существует взаимосвязь между процессами, протекающими в отдельных сферах общества, и состоянием преступности несовершеннолетних как ответной реакцией на происходящее.

Преступность несовершеннолетних – показатель нестабильности в обществе, свидетельствующий о противоречиях в политической и социально-экономической сферах, которые выступают основным фактором зарождения криминогенных процессов в стране [1]. Как отмечают сотрудники правоохранительных органов, несовершеннолетние, совершившие преступления, создают основной резерв для развития будущей преступности.

Сегодняшнее состояние ювенальной преступности в Российской Федерации, которое характеризуется ростом не только количества преступлений, но и ужесточением форм преступной деятельности (если в 2022 году было возбуждено 8 573 уголовных дела, то в 2023 году – уже 8 757), отражает неэффективность реализуемых государственными органами мер, направленных на духовное и патриотическое воспитание подрастающего поколения.

К сожалению, отдельные ситуации, в особенности проведение специальной военной операции, демонстрируют, что современная правовая система и сложившаяся правоприменительная практика сотрудников правоохранительных органов и отдельных спецслужб оказалась неготовой к новым вызовам и угрозам, которые несет в себе, к примеру, диверсионная деятельность, которая за короткий промежуток времени видоизменилась в организационном и техническом аспектах.

Вовлечение несовершеннолетних в осуществление деятельности, заключающейся в совершении взрыва, поджога, действиях, направленных на разрушение или повреждение предприятий, сооружений, объектов транспортной инфраструктуры, средств связи, объектов жизнеобеспечения населения в целях подрыва экономической безопасности и обороноспособности Российской Федерации трудно спрогнозировать, оно постепенно развивается, приобретая все новые формы и невероятный масштаб. Невоз-

можно противостоять диверсии без систематического и подробного учета и анализа этого явления.

Таблица 1

Количество преступлений, предусмотренных ст. 281 УК РФ,
зарегистрированных за 2016-2024 гг.

Год	Количество преступлений, возбужденных по ст. 281 УК РФ
2016	2
2017	3
2018	1
2019	-
2020	-
2021	1
2022	23
2023	127

С 2022 года, по данным Генпрокуратуры, отмечается рост числа диверсий. Стоит отметить, что большинство данных преступлений зарегистрировано в граничащих с Украиной регионах: Белгородской области (три), Курской и Воронежской (по две).

По данным МВД России, с начала специальной военной операции совершено 184 диверсии на железной дороге, за их совершение задержан 141 человек, среди которых 59 подростков (15 несовершеннолетних привлечены к уголовной ответственности за поджоги военкоматов).

К примеру, 13-летний, 14-летний и 16-летний школьники за плату в размере 70 тысяч рублей сожгли оборудование на железной дороге в Смоленской области, повредив три релейных шкафа на станции Гусино [2].

В мае 2024 года трое подростков за денежное вознаграждение, которое так и не получили, подожгли релейный шкаф на ст. Бочаты Кемеровской области. В настоящее время им предъявлено обвинение в совершении преступления по п. «а» ч. 2 ст. 281 УК РФ. Следствием установлено, что действиями несовершеннолетних руководили зарубежные координаторы [3].

Со стремительным развитием информационных технологий, а именно сети Интернет, на преступность несовершеннолетних стала влиять виртуальная реальность как самостоятельная социальная сфера. На современном этапе её выделяют наравне с традиционными социальными сферами [4]. Директор ФСБ А. В. Бортников на заседании Национального антитеррористического комитета (НАК) заявил, что украинские спецслужбы посредством мессенджеров и сети Интернет вербуют российских граждан, включая молодежь, для осуществления диверсий и терактов.

В конце февраля 2023 г. президент РФ В. В. Путин в ходе выступления на расширенной коллегии ФСБ поставил задачу пресекать использование

соцсетей для вовлечения в террористическую и экстремистскую деятельность граждан Российской Федерации, особое внимание уделив уязвимой категории населения – молодежи.

По мнению генерального прокурора И. В. Краснова, пресечение фактов вовлечения в экстремистскую и иную противоправную деятельность молодежи является приоритетной задачей правоохранительных органов. По его словам, это актуально, потому что из 127 зарегистрированных в прошлом году террористических актов 13 совершены с участием несовершеннолетних [5].

Так, Верховный суд Татарстана вынес приговор трем местным жителям за диверсии на железной дороге. В марте 2023 года Б. Ибрагимов нашел подростков и уговорил их поджечь релейный шкаф на перегоне Автозаводская – Сидоровка в Тукаевском районе. Подростки осуждены на пять лет с отбыванием в воспитательной колонии. Ранее судимый за кражу 20-летний житель Набережных Челнов Б. Ибрагимов осужден к 17 годам лишения свободы за диверсию и вовлечение подростков в преступную деятельность [6].

Вовлечение в преступную среду несовершеннолетнего происходит в силу его не до конца сформированной психики, жизненных установок и принципов в отличие от взрослого, имеющего жизненный опыт и социальные установки [7].

Воспитание подрастающего поколения в современных условиях развития немыслимо без работы, направленной на противодействие преступности несовершеннолетних и в идеале ее искоренение. В первую очередь, преступность среди детей и подростков неизбежно ведет к распространению подобного поведения и среди нормальной, социально не дезориентированной подростковой среды, помимо этого неизбежно наносится вред формированию личности несовершеннолетнего, что, в конечном счете, будет способствовать его дальнейшей криминальной деятельности.

По нашему мнению, А. Михайлова наиболее точно и полно сформулировала причины преступности несовершеннолетних и указала пути их решения. Исследователь выделила семь основных причин, влияющих на возникновение и развитие преступности несовершеннолетних: слабая профилактика правонарушений среди несовершеннолетних и плохая организация общественной работы с несовершеннолетними; отсутствие воспитательной функции в системе обучения; недостаточная организация системы безопасности учебных заведений; **проблемы межведомственного взаимодействия; излишне мягкая ответственность за совершение преступления и отсутствие системы пробации.**

Как утверждает член Общественной палаты Российской Федерации С. Симак, вся система образования в России ориентирована на дрессировку, на натаскивание знаний[8]. Такой фактор доказывает, что при ориентировании преподавателя на целевые показатели в учёбе любыми способами

повлечёт за собой отсутствие контроля над обучающимися и появление безнадзорности несовершеннолетних.

Многие общественные деятели (например, Олег Зыков, а также член Совета при Президенте РФ по развитию гражданского общества и правам человека **Андрей Бабушкин**) придерживаются мнения, что появление в России системы пробации, *когда лицо совершило преступление небольшой тяжести – это более плодотворный путь, чем повышение наказания*, поможет решить проблему подростковой преступности.

Перечисленные причины наиболее точно и полно отражают специфику формирования преступности несовершеннолетних, благодаря чему можно выделить основные пути их разрешения и устранения.

Несомненно, что современные меры профилактики нуждаются в качественном изменении и касательно момента их «включения», и по их форме-содержанию, и по длительности воздействия.

Эффективность проведенных мероприятий должна рассчитываться не с точки зрения количества «поставленных на учет» и «проведенных бесед», но с учетом конкретных результатов проведенной работы [9].

Для реализации этих задач необходима разработка качественно иной системы профилактики преступлений и правонарушений несовершеннолетних, базирующейся на новых принципах и, главное, с учетом новых реалий.

С положительной стороны стоит отметить развитие Федерального проекта «Патриотическое воспитание граждан Российской Федерации на 2021-2026 годы», который на сегодняшний день объединяет более 1 800 000 участников, 1 660 000 подростков участвуют во всероссийских, окружных и межрегиональных мероприятиях патриотической направленности, 1 750 000 детей вовлечены в деятельность детско-юношеского военно-патриотического общественного движения «ЮНАРМИЯ», во многих образовательных учреждениях созданы отряды «Юные друзья полиции». Указанные отряды имеют правоохранительную направленность и ставят основной задачей профилактику правонарушений несовершеннолетних.

В этой связи задачей науки является не только исследование теоретических проблем уголовной ответственности несовершеннолетних и их проявления на практике, но и разработка программ духовно-нравственного и идеологического воспитания, а также сохранение и укрепление традиционных ценностей. От эффективности профилактики преступности несовершеннолетних в настоящее время «во многом зависят состояние и тенденции преступности в будущем и даже более широко – нравственный климат в обществе» [10].

СПИСОК ЛИТЕРАТУРЫ

1. Филиппова Е. О. Несовершеннолетняя преступность как объект криминологического исследования / Е. О. Филиппова // Юридические науки. – 2021. – № 1. – С. 258–260.
2. В Смоленской области задержали трех подростков за поджог релейных шкафов [Электронный ресурс] – URL: <https://ria.ru/20240423/ufsb-1941702222.html> (дата обращения: 22.10.2024).
3. В Кузбассе трое подростков за деньги подожгли релейный шкаф на железной дороге. – URL: <https://tass.ru/proisshestviya/20868161> (дата обращения: 22.10.2024).
4. Демидова-Петрова Е. В. Исследование преступности несовершеннолетних в России / Е. В. Демидова-Петрова // Вестник Санкт-Петербургского университета. Право. – СПб., 2021. – Т. 12. – № 1. – С. 4–16.
5. Генпрокурор заявил о росте рисков диверсий и терактов в России. – URL: <https://www.vedomosti.ru/politics/news/2023/04/26/972640-genprokuror-zayavil-o-suschestvennom-roste-riskov-diversii> (дата обращения: 22.10.2024).
6. Троим жителям Татарстана вынесли приговор за диверсии на железной дороге. – URL: <https://ria.ru/20240606/tatarstan-1950993982.html> (дата обращения: 22.10.2024).
7. Карчаева К. А. Некоторые размышления о преступности несовершеннолетних: особенности и детерминанты / К. А. Карчаева // Образование и право. – 2022. – № 1. – С. 224–226.
8. Михайлова А. 7 основных причин подростковой преступности и пути их решения // ГАРАНТ.РУ. – URL: <http://www.garant.ru/article/526482/#ixzz3nDzTsK3k> (дата обращения: 12.10.2024).
9. Муртазалиева М. М. Социально-педагогическая профилактика правонарушений несовершеннолетних детей : диссертация кандидата педагогических наук: 13.00.01. – Махачкала, 2005. – 175 с.
10. Алексеев А. И. Криминология. Курс лекций. – Москва, 1999. – С. 208.

СВЕДЕНИЯ ОБ АВТОРАХ

Максименко Александр Владимирович.
Начальник кафедры уголовно-правовых дисциплин.
Кандидат юридических наук, доцент.
Белгородский юридический институт МВД России им. И. Д. Путилина.
E-mail: Mav1202@yandex.ru
Россия, 308004, г. Белгород, ул. Горького, 71.

Лимарь Анна Сергеевна.
Доцент кафедры уголовно-правовых дисциплин.

Кандидат юридических наук.

Белгородский юридический институт МВД России им. И. Д. Путилина.

E-mail: ani.limar@yandex.ru

Россия, 308004, г. Белгород, ул. Горького, 71.

Alexander Vladimirovich Maksimenko.

Head of the Department of Criminal Law Disciplines.

Candidate of Legal Sciences, Associate Professor.

Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation named after I. D. Putilina.

Russia, 308004, Belgorod, Gorkogo str., 71.

Anna Sergeevna Limar. Associate Professor of the Department of Criminal Law Disciplines.

Candidate of Legal Sciences.

Belgorod Law Institute of the Ministry of Internal Affairs of the Russian Federation named after I. D. Putilina.

Russia, 308004, Belgorod, Gorkogo str., 71.

Ключевые слова: несовершеннолетний; подросток; интернет диверсия; преступность; экономическая безопасность; обороноспособность.

Keywords: minor; teenager; internet; sabotage; crime; economic security; defense capability.

УДК 343.85

А. Р. Нугуманов

БУЛЛИНГ: УГОЛОВНО-ПРАВОВЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ

BULLYING: CRIMINAL LEGAL REMEDIES

В настоящей работе раскрыты вопросы уголовной ответственности за совершение травли (буллинга) в отношении несовершеннолетних. Проанализированы нормы Уголовного кодекса РФ, содержащие признаки отдельных проявлений травли (буллинга).

This work reveals issues of criminal liability for committing bullying (bullying) against minors. The norms of the Criminal Code of the Russian Federation containing signs of individual manifestations of bullying (bullying) are analyzed.

Буллинг (от английского bullying – «запугивание», «издевательство», «травля») – это систематические акты агрессии (словесной, психологической или физической), направленные против одной или нескольких жертв.

Буллинг и травля – это синонимы, описывающие одно и то же явление.

Официальное закрепление понятия нашло отражение в распоряжении Минпросвещения России, в соответствии с которой буллинг – проявление агрессии, в том числе физическое насилие, унижение, издевательства в отношении обучающегося образовательной организации со стороны других обучающихся и/или учителей [1].

Общественная опасность буллинга заключается не в способности жертвы травли защитить себя. Травля в отличии от конфликта, где силы сторон примерно равны, в среде несовершеннолетних происходит группой лиц. Также, если конфликт – это единичное происшествие, которое тоже может быть довольно жёстким, то буллинг – это долгосрочное и обдуманное насилие, которое жертва не может остановить самостоятельно.

Травля может проявляться как в физической (драки, повреждения или кражи личных вещей), так и в психологической форме в виде оскорблений, угроз, бойкота, психологического давления. Одной из разновидностей буллинга является «кибербуллинг». Кибербуллинг – это вербальное издевательство в сети, в том числе угрозы, вызывания чувств стыда, враждебное отношение, обидные высказывания, связанные с внешним видом, умственными способностями, умениями и т.д. [2].

Таким образом, буллинг можно определить как разновидность физического и психического насилия. Также следует указать на системный характер применяемого такого насилия в отношении жертвы буллинга. Опасность данного явления заключается не только в нанесении физического или психического вреда потерпевшему, а также в нарушении общественных отношений, обеспечивающих безопасное нахождение обучающегося в учебном заведении и реализацию права на получение образования.

Специальные нормы, предусматривающие ответственность за буллинг в КоАП РФ и УК РФ не содержатся. КоАП РФ устанавливает административную ответственность за отдельные проявления буллинга – оскорбление, то есть унижение чести и достоинства другого лица, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме (статья 5.61), клевету, то есть распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (статья 5.61.1), мелкое хулиганство, то есть нарушение общественного порядка, выражающее явное неуважение к обществу, сопровождающееся нецензурной бранью в общественных местах, оскорбительным приставанием к гражданам, а равно уничтожением или повреждением чужого имущества (статья 20.1).

По мнению специалистов, уголовная ответственность за буллинг возможна при наличии признаков составов преступлений, предусмотренных ст.ст. 128.1, 213, 137, 119 УК РФ, в случае совершения кибербуллинга ст. 137 УК РФ, в случае доведении жертвы интернет-травли до самоубийства

или в склонении к совершению самоубийства, влечет ответственность по ст. ст. 110 - 110.1 УК РФ [3, 4].

В соответствии с методическими рекомендациями для сотрудников образовательных организаций высшего образования, курирующих воспитательную работу с молодежью, по профилактике буллинга (травли) среди обучающихся уголовно-правовые признаки буллинга охватываются положениями сразу нескольких статей УК РФ: статья 110 «Доведение до самоубийства», статья 115 «Умышленное причинение легкого вреда здоровью», статья 116 «Побои», статья 117 «Истязание», статья 128.1 «Клевета», статья 148 «Нарушение права на свободу совести и вероисповеданий» (кибербуллинг в отношении вероисповедания), статья 161 «Грабеж», статья 163 «Вымогательство», статья 213 «Хулиганство», статья 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» [5].

Таким образом, уголовный закон содержит широкий круг норм, позволяющих противодействовать буллингу. Следует согласиться с экспертами и специалистами в области профилактики буллинга в школах, рассматривающих комплекс правовых норм, применимых для привлечения к уголовной ответственности за буллинг.

Анализ данных норм позволяет сделать вывод о том, что законодатель усиливает уголовную ответственность за данный круг деяний, совершенных в отношении несовершеннолетних, а также с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет). Вместе с тем основным местом совершения буллинга является школа (в широком смысле), где осуществляется процесс воспитания и обучения несовершеннолетних. На наш взгляд, совершение буллинга в образовательной организации повышает общественную опасность деяния, так как причиняется вред общественным отношениям, связанным с получением образования. В связи с этим следует подумать об установлении повышенной уголовной ответственности за совершение деяний, содержащих признаки буллинга, в образовательных организациях в квалифицированных (особо квалифицированных) составах данных норм, либо включения нового обстоятельстваотягчающего наказание – совершение преступления в образовательной организации.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении методологии (целевой модели) наставничества обучающихся для организаций, осуществляющих образовательную деятельность по общеобразовательным, дополнительным общеобразовательным и программам среднего профессионального образования, в том числе с применением лучших практик обмена опытом между обучающимися : распоряжение Минпросвещения России от 25.12.2019 № Р-145 // СПС «КонсультантПлюс».

2. Инфографика по буллингу и кибербуллингу. Официальный сайт уполномоченного при Президенте Российской Федерации по правам ребенка. – URL: <https://deti.gov.ru/Deyatelnost/documents/211> (дата обращения 01.10.2024).

3. Курбенков В. А. Буллинг в российских школах: правовые проблемы профилактики / В. А. Курбенков, А. Ю. Новосельцев // Журнал российского права. – 2020. – № 3. – С. 95–102.

4. Гусев А. Ю. Ответственность за травлю (буллинг) / А. Ю. Гусев // СПС «КонсультантПлюс».

5. О направлении методических рекомендаций» (вместе с «Методическими рекомендациями для сотрудников образовательных организаций высшего образования, курирующих воспитательную работу с молодежью, по профилактике буллинга (травли) среди обучающихся : письмо Минобрнауки России от 13.12.2022 № МН-6/1873 // СПС «КонсультантПлюс».

СВЕДЕНИЯ ОБ АВТОРЕ

Нугуманов Азат Римович.

Заместитель начальника кафедры уголовного права и криминологии.

Кандидат юридических наук.

Уфимский юридический институт МВД России.

E-mail: ugp@csu.ru

Россия, 450047, г. Уфа, ул. Муксинова, 2.

Nugumanov Azat Rimovich.

Deputy Head of the Department of Criminal Law and Criminology.

Candidate of Legal Sciences.

Ufa Law Institute of the Ministry of Internal Affairs of Russia.

E-mail: ugp@csu.ru

Russia, 450047, Ufa, Muksinova St., 2.

Ключевые слова: профилактика правонарушений; буллинг; травля; уголовная ответственность за буллинг.

Keywords: crime prevention; bullying; criminal liability for bullying.

УДК 343.4

**СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ ИЗМЕНЕНИЯ
ПРЕСТУПНОСТИ В РОССИИ, СВЯЗАННОЙ СО СКЛОНЕНИЕМ
ПОДРОСТКОВ К УПОТРЕБЛЕНИЮ НАРКОТИКОВ**

**THE CURRENT STATE AND TRENDS IN CRIME
IN RUSSIA RELATED TO THE TENDENCY
OF ADOLESCENTS TO USE DRUGS**

В представленной статье рассматриваются современное состояние и тенденции изменения преступности в России, связанной со склонением подростков к употреблению наркотиков. По итогам проведенного авторами анализа научной литературы, статистических сведений, опроса сотрудников правоохранительных органов и судей, судебной-следственной практики и публикаций по заявленной теме из открытого доступа, сформулированы основные выводы с учетом современных реалий и угроз безопасности.

The present article examines the current state and trends in crime in Russia related to the tendency of adolescents to use drugs. Based on the results of the authors' analysis of scientific literature, statistical information, a survey of law enforcement officers and judges, judicial and investigative practice and publications on the stated topic from open access, the main conclusions are formulated taking into account modern realities and security threats.

В юридической литературе «склонение» рассматривается как процесс, порой – достаточно длительный, преследующий достижение конечного результата: сделать несовершеннолетнего потребителем (думается, на постоянной основе) наркотических средств (или, как вариант, психотропных веществ) и/или их аналогов. Среди способов склонения ученые-криминологи чаще всего отмечают (выделяют) словесные (вербальные) [1], т.е. без использования насилия. Поэтому, с нашей точки зрения, преступность, непосредственно связанную со склонением лиц, не достигших совершеннолетнего (т.е. восемнадцатилетнего) возраста, к употреблению наркотических средств (а также их аналогов и прекурсоров), вполне обоснованно можно считать организованной и даже носящей транснациональный характер (если принимать во внимание факт изготовления вышеуказанных средств из наркосодержащих растений (т.е. из растительного сырья), произрастающих, главным образом, в государствах Южной (Латинской) Америки).

Проведенное изучение материалов судебной-следственной практики, научных и иных публикаций по теме, мнений практических сотрудников правоохранительных органов показывает, что в настоящее время Одной из самых распространенных разновидностей организованной преступности в

настоящее время является наркопреступность. Многими отечественными исследователями данное негативное социальное явление рассматривалось сквозь призму совокупности преступлений в сфере незаконного оборота наркотических средств (а также психотропных веществ). На наш взгляд, это представляется в корне неверным, поскольку наркопреступность – это специфическая организация отдельного (узкоспециализированного) вида преступной деятельности, угрожающей, прежде всего, жизни и здоровью человека.

Современную наркопреступность с участием несовершеннолетних в России условно можно охарактеризовать следующим криминологически значимым признаками: во-первых, такая наркопреступность связана незаконным оборотом как наркотических средств, так и психотропных веществ (соответственно, предметом выступают предметы как естественного, т.е. растительного происхождения, так и искусственного – химического, синтетического); во-вторых, такая наркопреступность связана с высоким уровнем наркотизма, поскольку вызывает на практике быструю зависимость от «синтетических наркотиков» (таблеток, капсул, транквилизаторов, курительных смесей, порошков и т.п.); в-третьих, таким преступлениям присущ особый состав – это склонение лиц в возрасте до 18 лет к употреблению наркотических средств и психотропных веществ (деяния квалифицируются п. «а» ч. 3 ст. 230 УК РФ) [2].

Вместе с тем, следует учитывать, что равно как и любому другому социальному явлению, преступности, имеющей непосредственное отношение к различным незаконным процессам (операциям) с наркотическими средствами, присущи определенные тенденции и собственная динамика на современном этапе развития. Необходимо заметить, что и преступность, связанная со склонением лиц, не достигших восемнадцатилетнего возраста, к употреблению наркотических средств, в полной мере испытывает на себе воздействие стремительно меняющейся международной обстановки и природно-климатических изменений.

В свою очередь, следует охарактеризовать ключевые тенденции и динамику изменения криминологических показателей наркопреступности в течение периода с 2021 по 2024 гг. (последние пять лет статического наблюдения), связанной так или иначе со склонением несовершеннолетних к употреблению наркотиков, которые имеют важное значение при выборе мер раннего профилактического воздействия.

Так, в качестве общих тенденций развития выделим следующие аспекты и вопросы:

- ситуация в сфере незаконного оборота наркотических средств в РФ по-прежнему контролируется правоохранительными органами различных уровней; переориентация поставок наркотических средств в РФ с европейского направления на центральноазиатские и ближневосточные маршруты;
- активное задействование для доставки наркотических средств на

территорию РФ автомобильного и иных видов транспорта из государств-участников СНГ, а также почтовых и курьерских компаний, продолжающих свою деятельность на российской территории независимо от запретов и ограничений, предусмотренных пакетами западных санкций;

– в некоторых южноамериканских и европейских государствах возобладали либерализация политики в отношении употребления наркотических средств (руководствуясь пропагандистской нарколиберальной риторикой, органы высшей государственной власти и высшие руководящие должностные лица принимают на законодательном уровне акты относительно: а) активного культивирования каннабиса; б) выращивания отдельных наркосодержащих растений для личного пользования; в) изъятия из национальных уголовных законодательств наказаний за обладание наркотическими средствами, не используемыми для продажи (сбыта). В конечном итоге, такая ситуация может привести к резкому росту употребления «слабых наркотиков»);

– с одной стороны, сокращение объемов перемещаемых на территорию РФ наркотических средств в связи с значительными затруднениями перемещения товаров через Государственную границу РФ в зарубежные государства и обратно;

– с другой стороны, положительная динамика увеличения количества подпольных лабораторий по изготовлению, главным образом, «искусственных», синтетических наркотиков с помощью химических реактивов и специализированного оборудования, как ни странно, из дружественных России стран – Китая, Турции, Египта;

– расширение посевов наркосодержащих растений в районах Дальнего Востока, Забайкалье с благоприятными природно-климатическими условиями;

– блокировка (запрещение) ряда иностранных Интернет-ресурсов на территории РФ способствует широкому использованию мессенджера Telegram, а также отечественных социальных сетей и сервисов (в частности – ВКонтакте, Одноклассники и др.) с целью распространения пропаганды потребления и распространения наркотических средств в среде молодежи, в том числе – несовершеннолетних лиц;

– значительный рост употребления метадона в качестве заменителя «тяжелого наркотика» – героина.

При этом динамике развития наркопреступности присущи определенные черты и особенности:

1) вышеназванная динамика достаточно сильно зависит от политико-экономических процессов, прежде всего – санкционных ограничений, введенных странами Запада в отношении РФ, сокращения площадей наркосодержащих растений – как в Южной Америке, так и в Центральной Азии, вооруженных конфликтов между различными преступными группировками и крупными преступными формированиями с целью установления кон-

троля за районами культивирования вышеназванных растений, а также за их трафиком;

2) в контексте существенных изменений логистических маршрутов и цепочек транспортировки грузов представляется вероятным сокращение, в количественном выражении, поставок ряда «европейских» наркотиков, таких как ЛСД, МДМА или амфетамин, а также других запрещенных веществ, которые традиционно транзитом перевозились через государства Европейского Союза; вместе с тем, скорее всего, увеличатся поставки наркотических средств из государств Азиатского континента – Таиланда, Лаоса, Мьянмы, Вьетнама, Камбоджи и др.; не исключено, что территория РФ может быть использована как перевалочный пункт в плане транспортировки опийных наркотических средств из Афганистана в страны Европейского континента;

3) значительному росту наркопреступности способствует достаточно большое количество нелегальных мигрантов из государств Средней и Центральной Азии – потенциальных членов организованных преступных формирований, имеющих хорошо налаженные связи на межэтническом, межрегиональном и международном уровнях, специализацией которых являются контрабандные поставки наркотических средств и сбыт запрещенных законом психотропных веществ;

4) специалисты практически едины во мнении о том, что усилению позиции наркопреступности в подростковой и молодежной среде способствует негативное влияние фактора расширения Интернет-пространства (в том числе использование преступниками для целей сетевой наркоторговли и склонения несовершеннолетних запрещенных в настоящее время в России ресурсов Даркнет и Discort, а точнее – нахождение в его информационном поле организационных структур, предлагающих представителям различных возрастов наркотические средства «по сходной цене» [3-7].

На основании вышесказанного, сформулируем общие выводы:

1) состояние преступности, связанной со склонением несовершеннолетних к употреблению наркотиков (т.е. наркопреступности), характеризуется положительной динамикой роста, усилением воздействия на физическое и психическое здоровье (состояние) лиц, не достигших восемнадцатилетнего возраста;

2) в структуре наркопреступности преобладают преступления, предусмотренные ст. ст. 228, 228.1 и 228.2 УК РФ; при этом, подавляющее количество преступлений непосредственно связано с незаконным сбытом наркотических средств;

3) динамика развития наркопреступности носит нестабильный, волнообразный характер: количество наркопреступлений то снижается, то вновь – после 2022 года – возрастает; в то же время, удельный вес тяжких и особо тяжких наркопреступлений демонстрирует устойчивые показатели роста;

4) среди тенденций развития наркопреступности следует отметить (выделить): сохранение уровня латентности на достаточно высоком уровне; увеличение поставок наркотических средств через центрально-азиатские и юго-восточные направления и пути (в том числе, транзитные); сокращение поставок так называемых «европейских наркотиков»; увеличение количества подпольных лабораторий и объемов производства «синтетических наркотиков»; широкое использование организованной наркопреступностью Интернет-ресурсов (главным образом, социальных сетей) для пропаганды наркотических средств, для привлечения к их сбыту и распространению несовершеннолетних лиц; все большее вовлечение мигрантов (прежде всего, из Средней и Центральной Азии) в преступную наркодеятельность на территории РФ; продолжение преступной деятельности и акцентирование внимания на системной активизации действий в сети Интернет и реальной жизни по склонению подростков к употреблению так называемых «слабодействующих» наркотических средств (психотропных веществ) и/или их аналогов.

Данные факторы следует учитывать сотрудникам ПДН ОВД и другим субъектами профилактики наркотизма в подростковой и молодежной среде.

СПИСОК ЛИТЕРАТУРЫ

1. Овчинко О. А. Склонение несовершеннолетнего к употреблению наркотиков: нужны ли российскому уголовному закону статьи-казусы? // Научный компонент. – 2022. – № 3 (15). – С. 17.

2. Герман Л. Г. Понятие, виды, общественная опасность наркопреступности // Молодой ученый. – 2022. – № 13 (408). – С. 178.

3. Доклад о наркоситуации в Российской Федерации в 2022 году. – Москва : Государственный Антинаркотический Комитет, 2023. – 60 с.

4. Жидконожкина О. Н. Актуальные проблемы деятельности органов внутренних дел по предупреждению вовлечения несовершеннолетних в совершение правонарушений и антиобщественных действий // Полиция и общество: проблемы и перспективы взаимодействия. – 2023. – № 5. – С. 71–75.

6. Герасимова Е. В., Жидконожкина О. Н. Социально-правовые аспекты профилактики правонарушений несовершеннолетних, совершаемых под воздействием деструктивных интернет-контентов // Вестник Воронежского института МВД России. – 2021. – № 1. – С. 265

5. Рыбокитова Ж. И. Основные направления повышения эффективности ранней профилактики преступности студентов профессиональных образовательных организаций и образовательных организаций высшего образования // Вестник Воронежского института МВД России. – 2023. – № 2. – С. 302–306.

7. Буданова Е. А., Буданов С. А., Кушнарев М. А. Факторы, препят-

ствующие повышению уровня доверия к деятельности сотрудников ПДН ОВД, связанной с профилактикой подростковой преступности // Современное общество и право. – 2023. – № 6 (67). – С. 111–118.

СВЕДЕНИЯ ОБ АВТОРАХ

Польшиков Александр Васильевич.
Доцент кафедры уголовного права и криминологии.
Кандидат юридических наук, доцент.
Воронежский институт МВД России.
E-mail: polschikow@mail.ru
Россия, 394065, Воронеж, просп. Патриотов, 53.

Кушнарёва Анна Васильевна.
Заместитель начальника научно-исследовательского отдела.
Кандидат юридических наук.
Воронежский институт МВД России.
E-mail: akushnareva@mvd.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Polshikov Alexander Vasilyevich.
Associate Professor of the Department of Criminal Law and Criminology.
Candidate of Law, Associate Professor.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: polschikow@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kushnareva Anna Vasilyevna. Deputy head of the Research Department.
Candidate of Legal Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: akushnareva@mvd.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: несовершеннолетние; ребенок; подросток; школа; наркопреступность; склонение; потребление наркотиков; наркотизм; взрослый; куратор; социальные сети; мессенджеры; Интернет; комплексная профилактика; предупреждение; полиция; органы внутренних дел.

Keywords: minors; child; teenager; school; drug crime; persuasion; drug use; narcosis; adult; curator; social networks; messengers; Internet; comprehensive prevention; prevention; police; internal affairs agencies.

УДК 343.97

**ФАКТОРЫ, СПОСОБСТВУЮЩИЕ СОВЕРШЕНИЮ ПРЕСТУПЛЕНИЙ,
СВЯЗАННЫХ СО СКЛОНЕНИЕМ ПОДРОСТКОВ
К УПОТРЕБЛЕНИЮ НАРКОТИКОВ**

**FACTORS CONTRIBUTING TO THE COMMISSION
OF CRIMES RELATED TO THE PROPENSITY
OF ADOLESCENTS TO USE DRUGS**

В представленной статье рассматриваются ключевые факторы, способствующие совершению преступлений, связанных со склонением подростков к употреблению наркотиков в России. По итогам проведенного авторами комплексного исследования сформулированы основные выводы о причинах и условиях наркотизма подростков с учетом современных реалий.

The presented article examines the key factors contributing to the commission of crimes related to the propensity of adolescents to use drugs in Russia. Based on the results of a comprehensive study conducted by the authors, the main conclusions about the causes and conditions of drug addiction in adolescents are formulated, taking into account modern realities.

С позиции криминологической науки, совершению практически всех без исключения преступлений, включая наркопреступления, против несовершеннолетних, предшествуют определенные причины, условия и обстоятельства (в целом характеризующиеся как факторы): причем, первые могут носить внутренний характер, вторые и третьи – внешний характер.

Так, в качестве общих причин и условий Н. Ю. Жилина справедливо формулирует следующие:

1) отрицательный вектор развития молодежной политики, выраженный в коммерциализации детских и юношеских кружков и секций, подростковых клубов, занятий различными видами спорта, ликвидации малокомплектных общеобразовательных школ – главным образом, в сельской местности;

2) снижение, в финансовом отношении, жизненного уровня несовершеннолетних – как в сельских, так и в городских поселениях;

3) отсутствие системности, синхронности и четкости в деятельности общественных и государственных институтов и структур, занимающихся различными вопросами, аспектами и проблемами жизнедеятельности несовершеннолетних лиц;

4) конфликтные отношения (на почве взаимной неприязни, непонимания, отсутствия умения слышать и слушать друг друга, навязывания

устаревших или исключительно новых (антиобщественных) моделей поведения) между различными поколениями, возрастными категориями;

5) утрата семьей одного из основных своих предназначений в обществе – воспитания детей;

6) негативное воздействие «информационного негатива» на неокрепшее сознание подростков [1].

При этом И. Н. Коновалова подчеркивает следующие основные причины, имеющие непосредственное отношение к проблеме склонения подростков к употреблению наркотических средств и психотропных веществ:

- *психологические*: потребность несовершеннолетних в изменении своего эмоционального состояния посредством удовлетворения интереса к необычным ощущениям и переживаниям, возможности забыть о личных проблемах;

- желание получить особое удовольствие, повысить настроение, развлечься; рассмотрение употребления наркотических средств в качестве способа адаптации к проблемной ситуации и снятия психологической нагрузки;

- *социальные*: стремление приспособиться к жизни в обществе, найти в ней свое место;

- оказание прямого и поэтому наиболее сильного воздействия на решение несовершеннолетних употреблять наркотики со стороны непосредственного социального окружения, главным образом, родственников, близких лиц, друзей и знакомых [2].

Со своей стороны, А. Ю. Заболоцких детализирует рассматриваемые нами причины, классифицируя их на следующие виды: психологические; социально-психологические; образовательные; воспитательные: абстрагирование родителей от повседневной жизни собственных детей; отсутствие взаимопонимания между родителями и детьми, переживающими «переходные периоды»; предоставленность несовершеннолетних самим себе; правовые: слабое правовое сознание и практически сведенная к минимуму правовая культура; отсутствие понимания у последствий вследствие совершения общественно опасных преступных деяний [3].

Л. С. Радькова в качестве ключевых факторов определяет:

- заметно ухудшившуюся в последние два-три года экономическую обстановку в Российской Федерации (прежде всего, довольно ощутимый рост цен на продукты первой необходимости, проезд в общественном транспорте, тарифы на оплату жилищно-коммунальных услуг и др.);

- использование организованными преступными формированиями (сообществами) технологии вовлечения несовершеннолетних в незаконный оборот наркотических средств посредством снабжения их последними – первоначально, на безвозмездной основе;

- недостаточность и неэффективность мер противодействия наркопреступности со стороны органов государственной власти и управления

различных уровней, руководящих должностных лиц (в том числе правоохранительных органов);

- отрицательное воздействие внутрисемейных отношений на становление и развитие личности несовершеннолетних, недостаточность времени у родителей на их воспитание и формирование культурного уровня, нестабильность материального благосостояния большинства семей, употребление родителями алкогольных напитков и/или наркотических средств;

- усиление дефицита духовного и нравственного воспитания подрастающего поколения;

- внутриобразовательные проблемы: отсутствие эффективного механизма преодоления (предотвращения) возникших в школе конфликтов педагогическими и воспитательными методами, и др.;

- незанятость несовершеннолетних в досуговых организациях по причине перевода кружков, спортивных секций, объединений военной ориентации, детских площадок на платную основу, а также отсутствие желания у них заниматься социально-позитивными формами досуга;

- популяризация наркотических средств и психотропных веществ, демонстрация соответствующих сцен в кинофильмах, телевизионных передачах, видеороликах, связанных с наркотиками, в средствах массовой информации и информационных ресурсах глобальной сети Интернет [4].

Стремится определить наиболее вероятные причины и условия, способствующие совершению наркопреступлений с участием подростков, О. В. Богущ. Таковыми, по мнению автора, могут являться: стремление несовершеннолетнего к материальному благополучию за счет распространения наркотических средств; формирование доверительных, дружеских отношений между распространителями наркотиков и несовершеннолетними; формирование наркодилерами у несовершеннолетних правового нигилизма, отрицательного отношения к правоохранительным органам, соблюдению правовых норм и правил [5].

На наш взгляд, в настоящее время особое внимание необходимо уделить таким психологическим факторам, способствующим росту наркопреступности среди несовершеннолетних, имеющим криминогенное значение, как экстремальное мышление; нравственная невоспитанность; ощущение собственной незначимости и ненужности, недостаточный самоконтроль; неумение предвидеть последствия своих поступков. Необходимо отметить и «информационный фактор», который связан с распространением негативной информацией, содержащейся в Интернет-публикациях, имеющую непосредственное отношение к причинам и условиям, способствующим совершению преступлений в плане склонения несовершеннолетних к употреблению наркотиков: среди них пропаганда бессмысленного времяпрепровождения, толерантного отношения (в частности, проявления понимания и сострадания) к их потребителям; рост популярности наркотических средств синтетического происхождения; стимулирование желания несо-

вершеннолетних к «легкому заработку» путем распространения наркотиков через ресурс сети Интернет среди своих сверстников; пропаганда со стороны криминальных сообществ легкости, важности и доступности получение новых ощущений в результате употребления наркотиков различными способами, отсутствие должного межведомственного взаимодействия субъектов профилактики [6-10].

СПИСОК ЛИТЕРАТУРЫ

1. Жилина Н. Ю. Вовлечение несовершеннолетних в незаконный оборот наркотических средств (уголовно-правовой и криминологический аспекты) / Н. Ю. Жилина : дисс. ... канд. юрид. наук. – Тамбов, 2009. – С. 9.
2. Коновалов И. Н. Методические рекомендации для комиссий по делам несовершеннолетних и защите их прав по координации межведомственного взаимодействия органов и учреждений системы профилактики безнадзорности и правонарушений несовершеннолетних, употребляющих наркотические средства и психотропные вещества, алкогольную и спирто-содержащую продукцию. – Саратов, 2015. – С. 26.
3. Заболоцких А. Ю. Социально-психологические причины преступности несовершеннолетних и молодежи в сфере незаконного оборота наркотиков. – URL: <https://izron.ru/articles> (дата обращения: 25.10.2024).
4. Радькова Л. С. Факторы, обуславливающие вовлечение несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов // Вестник Воронежского Государственного Университета. Серия: Право. – 2017. – № 4. – С. 248.
5. Богуш О.В. Вовлечение несовершеннолетних в процесс реализации наркотических средств // NovaInfo.ru. – 2023. – № 135. – С. 75.
6. Иванченко Р. Б., Польшиков А. В. Специфика ранней профилактики наркотизма среди несовершеннолетних школьников // Проблемы противодействия преступности в современных условиях : сборник статей / Редколлегия: А. Н. Подчерняев [и др.]. – Орел : Орловский юридический институт МВД России имени В. В. Лукьянова, 2017. – С. 39–42.
7. Иванченко Р. Б., Польшиков А. В. Медико-социологические, уголовно-правовые и криминологические аспекты понятия «криминальный суицид» // Вестник Воронежского института МВД России. – 2017. – № 4. – С. 45–51.
8. Иванченко Р. Б., Польшиков А. В. Наркотизация несовершеннолетних: современное состояние и тенденции // Вестник Воронежского института МВД России. – 2016. – № 4. – С. 68–76.
9. Лелеков В. А. Наркопреступность женщин в Российской Федерации // Вестник Воронежского института МВД России. – 2024. – № 1. – С. 161–165.
10. Буданова Е. А., Буданов С. А., Кушнарев М. А. Факторы, препятствующие повышению уровня доверия к деятельности сотрудников ПДН ОВД, связанной с профилактикой подростковой преступности // Современное общество и право. – 2023. – № 6 (67). – С. 117–118.

СВЕДЕНИЯ ОБ АВТОРАХ

Прохонов Василий Степанович.

Старший преподаватель кафедры уголовного права и криминологии.

Воронежский институт МВД России

E-mail: eliza2666@mail.ru

Россия, Воронеж, 394065, проспект Патриотов, 53.

Демидова Оксана Васильевна.

Профессор кафедры уголовно-исполнительного и уголовного права.

Кандидат юридических наук, доцент.

Воронежский институт ФСИН России.

E-mail: oks-dem.78@mail.ru

Россия, 394072, Воронеж, ул. Иркутская, 1а.

Prokhonov Vasily Stepanovich.

Senior Lecturer at the Department of Criminal Law and Criminology.

Voronezh Institute of the Ministry of Internal Affairs of Russia

E-mail: eliza2666@mail.ru

Russia, 394065, Voronezh, Prospect Patriots, 53.

Demidova Oksana Vasilievna – the professor of criminal-executive and criminal law department of the Voronezh institute of the Russian Federal Penitentiary Service, candidate of law, associate professor.

E-mail: oks-dem.78@mail.ru

Russia, 394072, Voronezh, Irkutskaya St., 1a.

Ключевые слова: несовершеннолетние; ребенок; подросток; школа; наркопреступность; склонение; потребление наркотиков; наркотизм; взрослый; куратор; социальные сети; мессенджеры; Интернет; комплексная профилактика; предупреждение; полиция; органы внутренних дел.

Keywords: minors; child; teenager; school; drug crime; persuasion; drug use; narcosis; adult; curator; social networks; messengers; Internet; comprehensive prevention; prevention; police; internal affairs agencies.

УДК 343.97

**ТЕНДЕНЦИИ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ
В СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ
ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА
И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ**

**TRENDS OF INVOLVEMENT OF MINORS IN THE COMMITTION
OF CRIMES OF A TERRORIST AND EXTREMIST NATURE**

В статье рассматриваются факторы, способствующие вовлечению несовершеннолетних в совершение преступлений террористического характера и экстремистской направленности. Приводятся некоторые профилактические меры, способные повысить эффективность борьбы с распространением экстремистских и террористических идей среди молодого поколения.

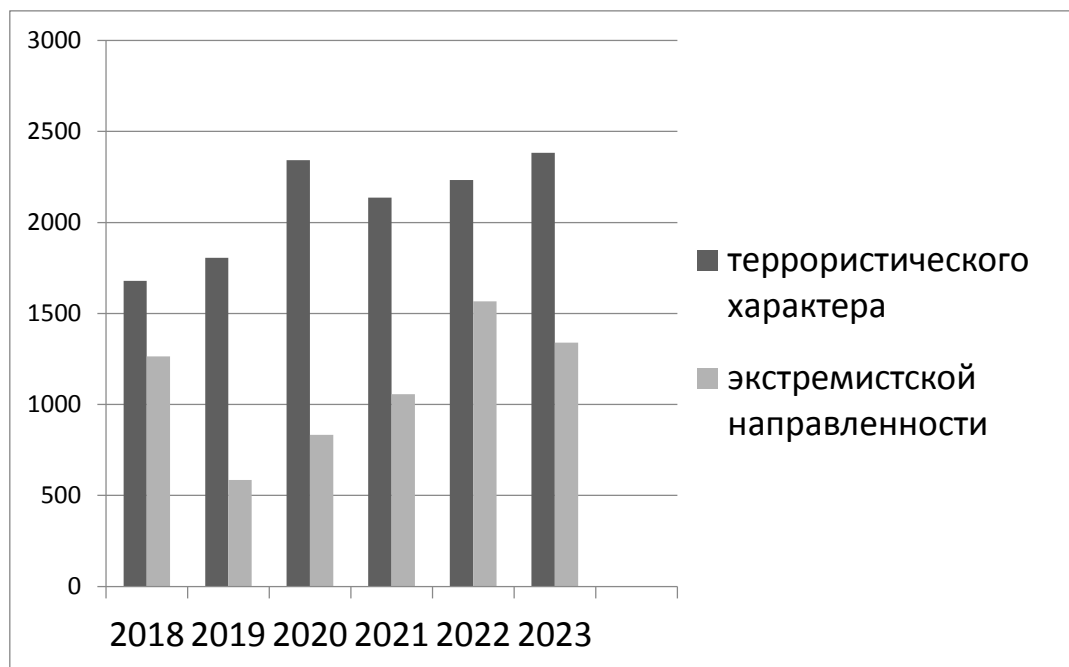
The article examines factors that contribute to the involvement of minors in committing crimes of a terrorist nature and extremist nature. Some preventive measures are given that can increase the effectiveness of the fight against the spread of extremist and terrorist ideas among the younger generation.

С начала XXI века экстремизм сумел трансформироваться из негативного регионального явления в глобальную проблему, захлестнувшую все современное общество. Существует множество проявлений экстремизма: от распространения с помощью сетевых интернет-ресурсов национализма и религиозной нетерпимости, как следствие этого искажение таких понятий как – Родина, патриотизм, национальность в отдельно взятых социальных группах, до создания экстремистских или террористических вооруженных формирований и повсеместного внедрения террора и насилия.

«Экстремизм и терроризм – нельзя сравнить с вирусом, который подхватило человечество [1]. Это его внутренний недуг, порождаемый главным образом дисгармоничным развитием в социальной, политической и культурной областях». В настоящее время именно молодежь наиболее подвержена этому социальному вирусу в силу многих определяющих факторов: возрастной активности, желания быть принятым и понятым в своей среде, юношеского максимализма, любопытства, в силу специфической обстановки в гражданском обществе, начавшегося возрождения активного влияния таких регуляторов правопорядка в обществе как: политическая активность, развитие национального самоопределения и возрастающей роли религии.

К сожалению, данные статистики показывают, что тенденции к уменьшению количества рассматриваемых деяний в настоящее время не наблюдается (см. гистограмму).

Гистограмма



Из приведенной гистограммы мы видим, что в стране наблюдается рост преступлений экстремистской направленности и террористического характера. Для преступлений экстремистской направленности исключение составляет 2019 год, когда произошла декриминализация ряда деяний, а также был применен такой юридический прием как административная преюдиция за возбуждение ненависти либо вражды, а равно унижение человеческого достоинства. На некоторое время это позволило снизить уровень такого рода преступности, но, тем не менее, достаточно быстро она дошла до прежних пороговых значений [2]. Конечно, основным фактором, влияющим на данную обстановку, выступает обострение взаимоотношений Российской Федерации со странами Запада, введение санкций, а также проведение Россией специальной военной операции на Украине (далее – СВО).

Высокий рост совершения деяний, связанных с преступлениями террористической и экстремистской направленности, наблюдается в Курской, Белгородской областях (по всей видимости из-за ухудшающейся обстановки на границе с Украиной в зоне проведения СВО), г. Севастополь, Республике Ингушетия. Чаще всего подростки совершают преступления в Новгородской области, Республике Тыва, Забайкальском крае, Еврейской автономной области [3].

Конечно, нельзя не отметить тот факт, что несовершеннолетние вовлекаются в совершение подобного рода преступлений достаточно часто в силу свойственных им виктимологических особенностей.

Вовлечение несовершеннолетних в совершение преступлений террористического характера – это прежде всего результат деформации нравственного и правового сознания личности подростков под воздействием различных негативных факторов. А благодаря процессу цифровизации общества, связанному с масштабным внедрением цифровых технологий во все значимые социальные сферы [4], уровень виктимности несовершеннолетних еще более возрос, поскольку в сети Интернет они становятся более уязвимы и подвержены криминогенному влиянию извне.

Следующим моментом выступает излишняя детская самоуверенность, что они все понимают и могут сами себя защитить в информационном пространстве, на чем, собственно, и попадают под воздействие кураторов экстремистских и террористических организаций. Несовершеннолетние пользователи податливы на чужое мнение, которое, как правило, лишено адекватных ценностных ориентиров и содержит антиобщественные призывы. Информация воспринимается ими как игра или развлекательный квест, потому они легко вовлекаются в преступную деятельность и учатся обращаться с оружием или вовсе его создавать, не осознавая всю серьезность и общественную опасность, которую могут повлечь за собой их действия [5].

Конечно, все это говорит о низком уровне информационной и цифровой грамотности населения. Обратим внимание, что речь идет именно о населении в целом, а не об отдельно взятой категории несовершеннолетних, поскольку последним, зачастую, некуда обратиться за помощью, их близкое взрослое окружение не понимает всю опасность, которую таит в себе интернет-пространство.

Система предупреждения вовлечения несовершеннолетних в совершение преступлений экстремистской направленности недостаточно эффективна в условиях постоянного совершенствования технологий, развития теневого интернета, повсеместной глобализации [6]. Кроме того, на современном этапе наблюдается обострение проблемы «отцов и детей» в ее современной интерпретации – родители должны объяснять подростку происходящие в обществе перемены, новую культуру, безопасное освоение интернет-пространства, однако современная общественная нестабильность, борьба за удовлетворение первичных потребностей не позволяет старшему поколению своевременно освоить технические и информационные технологии, поддерживать своих детей и способствовать их социализации.

Лидеры экстремистской или террористической организации, свободно ориентирующиеся в современных технологиях и интернет-пространстве, с легкостью могут вовлечь подростков в совершение преступлений. Они расширяют и синтезируют современную идеологию экстремизма для реализации собственных целей, а государственные органы, призванные осуществлять борьбу с вовлечением несовершеннолетних в совершение экстремистских преступлений не успевают освоить и обрабо-

тать огромный массив информации и организовать взаимодействие между органами, призванными осуществлять противодействие экстремизму.

Несовершеннолетние воспринимают огромные объемы информации, проявляют большой интерес ко всему новому [7]. По нашему мнению, проведение профилактики экстремизма среди учащихся средних общеобразовательных учреждений будет особенно эффективным при условии использования интерактивных материалов, короткометражных фильмов и творчества. Такую профилактику должны осуществлять не только инспекторы ПДН, но и педагоги, воспитатели, психологи и социальные работники. В свою очередь нам представляется достаточно эффективным осуществление подобных мероприятий студентами и курсантами юридических клиник, существующих при образовательных организациях высшего образования.

СПИСОК ЛИТЕРАТУРЫ

1. Дробижева Л. М. Политический терроризм и экстремизм // Полис. – 2012. – № 2. – С. 100.
2. Официальный сайт Министерства внутренних дел Российской Федерации. – URL: http://www.crimestat.ru/offenses_table (дата обращения: 17.03.2024).
3. Состояние преступности за январь-декабрь 2023 года, рассчитанное ФКУ «Главный информационно-аналитический центр» МВД России. – URL: <https://мвд.рф> (дата обращения: 17.03.2024).
4. Осипенко А. Л., Соловьев В. С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. – 2021. – Т. 15, № 6. – С. 681–691.
5. Алтухов Е. И. Проблемы противодействия вовлечению несовершеннолетних в террористическую деятельность // Научно-образовательные дискуссии: фундаментальные и прикладные исследования. Материалы XXX Всероссийской научно-практической конференции. – Ростов-на-Дону. – 2021. – С. 337–339.
6. Игнатов А. Н., Кашкаров А. А. Тенденции проявлений экстремизма и терроризма в Крымском федеральном округе и пути повышения эффективности деятельности правоохранительных органов по противодействию им // Библиотека уголовного права и криминологии. – 2016. – № 2(14). – С. 127–137.
7. Кулешов А. А. Профилактика вовлечения несовершеннолетних посредством сети интернет в совершение экстремистских преступлений // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : Сборник материалов Международной научно-практической конфе-

ренции: в 2-х частях, Воронеж, 25 мая 2017 года. Том Часть 1. – Воронеж : Воронежский институт МВД России, 2017. – С. 93–94.

СВЕДЕНИЯ ОБ АВТОРЕ

Пучнина Маргарита Юрьевна.
Преподаватель кафедры уголовного права и криминологии.
Кандидат юридических наук.
Воронежский институт МВД России.
E-mail: epasyaeva@mail.ru
Россия, 394065, Воронеж, просп. Патриотов, 53.

Puchnina Margarita Yuryevna.
Lecturer of the chair of Criminal Law and Criminology.
Candidate of Law.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: masloy100@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: вовлечение несовершеннолетних; терроризм; экстремизм; противодействие терроризму; сеть Интернет.

Keywords: involvement of minors; terrorism; extremism; counter-terrorism; Internet.

УДК 34.03

М. Ю. Пучнина, Д. Ю. Кузнецова

КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В СКУЛШУТИНГ

CRIMINOLOGICAL ANALYSIS OF THE INVOLVEMENT OF MINORS IN SCHOOLSHOOTING

Несовершеннолетние являются наиболее уязвимой группой населения из-за своих психофизиологических характеристик, в связи с чем они более всего подвержены криминогенному воздействию. В статье рассматривается вопрос вовлечения несовершеннолетних в такое субкультурное течение как «колумбайн», в частности посредством использования информационно-коммуникационных технологий.

Minors are the most vulnerable group of the population due to their psychophysiological characteristics, and therefore they are most susceptible to criminogenic effects. The article examines the issue of involving minors in such a subcultural movement as «Columbine», in particular through the use of information and communication technologies.

Распространение радикальных идей субкультуры «колумбайн» (скулшутинг) представляет собой одну из самых крайних форм деструктивного поведения. В России и по всему миру его приверженцами уже было совершено множество резонансных преступлений. Скулшутинги и случаи, связанные с «колумбайном», обычно относятся к инцидентам вооруженных нападений на студентов и (или) педагогов, а также других сотрудников образовательных учреждений.

К сожалению, современное молодое поколение воспринимает «колумбайн» не как ужасную трагедию, в которой гибнут невинные люди, а как хайповую (хайп (англ. hype) – это шум в медиа и социальных сетях, ажиотаж, кратковременная популярность) тему для обсуждения. Нападавшие на образовательные учреждения популярны и зачастую становятся объектами культа в определенных молодежных кругах. Несмотря на то что инцидент 1999 года в штате Колорадо [1] не является первым, он стал ключевой точкой для этого идейного течения и приобрел множество последователей по всему миру.

В России крупнейшим аналогичным инцидентом стало вооруженное нападение на политехнический колледж в Керчи, которое произошло 17 октября 2018 года и было осуществлено подражателем американских преступников. В дальнейшем в России были задержаны лица, планировавшие атаки на учебные заведения, чьи действия напоминали алгоритм, использованный керченским стрелком. Вторым наиболее крупным инцидентом в России стало вооруженное нападение 26 сентября 2022 года в ижевской школе № 88, совершенное бывшим выпускником этой школы, в результате которого погибли 18 человек, 11 из них – дети, пострадали более двадцати пяти человек [2]. Нападавший покончил с собой. Годом ранее, 20 сентября 2021 года было совершено нападение в Пермском государственном университете, в результате которого погибло шесть человек, более сорока пострадало. Стрелок (студент вышеуказанного учебного заведения) был задержан [3]. Пермский нападавший стал кумиром у современной молодежи, часть из которых даже организовали сбор средств с целью оплатить ему другого адвоката.

В качестве последних наиболее известных, но, к счастью, менее трагических инцидентов, приведем следующие:

– 11 сентября 2023 года в Ростовской области подросток с ножом попытался зайти в школу (учеником которой он являлся), однако попытка не удалась, но в результате ее пресечения им было ранено четыре человека [4];

– 16 сентября 2024 года в Челябинске ученик общеобразовательной школы № 68 напал с молотком на сверстников и педагога. В результате четверо человек пострадали, подросток был задержан сотрудниками Росгвардии [5].

Примечательно, что накануне этого события, 4 сентября 2024 года 14-летний ученик средней школы Апалачи (штат Джорджия) устроил стрельбу. В результате вооруженного нападения четыре человека погибли и девять получили ранения. Стрелок был задержан.

Обратите внимание, что большая часть инцидентов совершается именно осенью – в начале учебного года.

Опираясь на исследования зарубежных экспертов, можем выделить формальные признаки скулшутинга, которые соответствуют уже произошедшим инцидентам в России:

- нападающий (или нападающие) имели связь с учебным заведением (обычно это действующие студенты);
- убийства или ранения осуществлялись умышленно, без корыстных побуждений, имели демонстративный характер и были направлены на неопределённый круг людей;
- нападение не было спонтанным, а заранее спланированным и подготовленным.

В качестве дополнения к вышеизложенным признакам, отметим, что, как правило, у колумбайнеров отсутствует политическая и религиозная мотивации, они имеют собственную идеологию – своеобразное восприятие и позицию по поводу событий вокруг [6]. Их идея о том, что именно они имеют право «влиять на судьбы других», является частью их искаженного мировоззрения, однако это не имеет отношения к религиозным аспектам.

Действия террористов направлены на достижение своих целей через привлечение общественного внимания, запугивание населения и властей. Скулшутеры имеют более ограниченный характер, ими движет чувство мести, желания показать свое превосходство, на что и делается упор при вовлечении в данную деятельность несовершеннолетних посредством сети Интернет [7]. В процессе общения несовершеннолетнего подталкивают к индуктивному рассуждению, в результате которого он переходит от отдельных людей к обществу в целом.

«Колумбайнерами» движет две основные вещи: стремление к славе – желание «оставить свой след в истории», и идеологическая установка, согласно которой они считают, что своими действиями способствуют естественному отбору. Они полагают, что могут решать, кто должен жить, а кто – умереть. По этой причине некоторые из нападавших предварительно предупреждали определенных людей о своих намерениях, чтобы те могли избежать гибели. Они прибегают к определенной символике и атрибутике, а также действуют по заранее разработанному плану.

Рассмотрим характеристики, характерные как для терроризма в целом, так и для феномена «колумбайн» в частности:

- основная цель – привлечение внимания общества;
- активное вовлечение несовершеннолетних (главные идеи распространяются через сеть Интернет: оказывается деструктивное влияние, осуществляется вербовка и привлечение людей к антисоциальным действиям);
- высокая степень общественной опасности, связанная с прямой угрозой жизни людей;
- равнодушие к жертвам;
- действия направлены на неопределённые группы людей;
- тенденция перехода от конкретных целей к бесцельным убийствам;
- нападения тщательно планируются заранее (включая обучение, покупку или изготовление оружия, разработку плана действий и т.д.).

Изучение идеологии «колумбайнеров» позволяет прийти к выводу, что она во многом обусловлена низким уровнем участия молодежи в общественно полезной деятельности. Это усугубляется недостатками в социальной политике и профилактической работе с несовершеннолетними. Данные, полученные в результате эмпирического анализа и контент-анализа социальных сетей, подтверждают это. Результаты показывают, что идеология «колумбайна» вызывает массовый интерес среди подростков и молодежи и ее распространение происходит с нарастающей скоростью. Особенно тревожно, что в случае отсутствия эффективных мер противодействия этому явлению создаются условия для перехода множества людей из просто увлеченных фэндомом в активные последователи данной идеологии. Участие в колумбайн-сообществах постепенно изменяет мышление и мировосприятие несовершеннолетнего [8].

Характеристики «колумбайна», его массовый характер и скорость распространения в 2021 году поспособствовали развитию вопроса о возможности признания пропагандируемых идей как одной из форм терроризма, что и было сделано 2 февраля 2022 года [9].

В настоящее время мы фактически наблюдаем появление нового типа молодежной террористической активности, не связанного с религиозными аспектами или политическими мотивами (требования к государственным властям не выдвигаются). В этом случае на передний план выходит идеология, распространение которой представляет собой реальную и серьезную угрозу для национальной безопасности. Признание актов «колумбайна» террористическими открыло возможности для применения эффективных уголовно-правовых мер, направленных на предотвращение их дальнейшего распространения.

СПИСОК ЛИТЕРАТУРЫ

1. Массовое убийство в школе Колумбайн. – URL: <https://ru.wikipedia.org/> (дата обращения: 20.10.2024).
2. Массовое убийство в школе № 88. – URL: <https://ru.wikipedia.org/> (дата обращения: 20.10.2024).
3. Массовое убийство в Пермском государственном университете. – URL: <https://ru.wikipedia.org/> (дата обращения: 20.10.2024).
4. Дети не пострадали в результате нападения подростка на ростовскую школу. – URL: <https://ria.ru/20230911/shkola-1895472349.html> (дата обращения: 20.10.2024).
5. Росгвардия задержала ученика школы в Челябинске после нападения. – URL: <https://ria.ru/20240916/uchenik-1972910896.html> (дата обращения: 20.10.2024).
6. Миненко П. В., Поправко А. С. Противодействие экстремистским сообществам в сети Интернет // Актуальные вопросы противодействия экстремизму и терроризму : Сборник материалов межвузовского круглого стола, Воронеж, 12 ноября 2014 года. – Воронеж : Воронежский институт МВД России, 2015. – С. 39–42.
7. Кулешов А. А. Профилактика вовлечения несовершеннолетних посредством сети интернет в совершение экстремистских преступлений // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : Сборник материалов Международной научно-практической конференции: в 2-х частях, Воронеж, 25 мая 2017 года. Том Часть 1. – Воронеж : Воронежский институт МВД России, 2017. – С. 93–94.
8. Игнатов А. Н., Торопов С. А. Социальная напряженность как фактор терроризма и экстремизма // Современные проблемы теории и практики борьбы с преступностью : Материалы V Всероссийской научно-практической конференции, Краснодар, 23 декабря 2019 года / Отв. редактор Н В. Генрих. – Краснодар : Издательский Дом - Юг, 2020.
9. Верховный суд признал движение «колумбайн» террористическим. – URL: <https://ria.ru/20220202/kolumbayn-1770691723.html> (дата обращения: 20.10.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Пучнина Маргарита Юрьевна.

Преподаватель кафедры уголовного права и криминологии.

Кандидат юридических наук.

Воронежский институт МВД России.

E-mail: masloy100@mail.ru

Россия, 394065, Воронеж, просп. Патриотов, 53.

Кузнецов Дмитрий Юрьевич.

Старший преподаватель кафедры уголовного права и криминологии.

Кандидат юридических наук.
Орловский юридический институт МВД России им. В. В. Лукьянова.
E-mail: demetrio.k@yandex.ru
Россия, 302027, Орёл, ул. Игнатова, д. 2.

Puchnina Margarita Yuryevna.
Lecturer of the chair of Criminal Law and Criminology.
Candidate of Law.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: masloy100@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Kuznetsov Dmitry Yurievich.
Head lecturer of the chair of Criminal Law and Criminology.
Candidate of Law.
Lukyanov Orel Law Institute of the Ministry of the Interior of Russia.
E-mail: demetrio.k@yandex.ru
Russia, 302027, Orel, st. Ignatova 2.

Ключевые слова: колумбайн; скулшутинг; несовершеннолетние; информационно-коммуникационные технологии; сеть Интернет; вовлечение; терроризм; социальные сети.

Keywords: columbine; schoolshooting; minors; information and communication technologies; Internet; involvement; terrorism; social networks.

УДК 343.85

Д. Н. Соловьев

НЕКОТОРЫЕ УГОЛОВНО-ПРАВОВЫЕ МЕРЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ СРЕДИ НЕСОВЕРШЕННОЛЕТНИХ

SOME CRIMINAL LEGAL MEASURES TO COMBAT JUVENILE CRIME

В представленной статье говорится о том, что борьба с преступностью несовершеннолетних требует комплексного подхода, включающего меры профилактики, раннего вмешательства, образования и судебной системы. Важно помнить, что каждый подросток уникален, и для успешной борьбы с преступностью необходим индивидуальный подход к каждому случаю. Только совместными усилиями общества, государства и семьи можно создать условия для формирования законопослушной личности и успешной интеграции молодых людей в общество.

The article presents that the fight against juvenile delinquency requires a comprehensive approach, including measures of prevention, early intervention, education and the judicial system. It is important to remember that each teenager is unique, and for the successful fight against crime, an individual approach to each case is necessary. Only through the joint efforts of society, the state and the family can we create conditions for the formation of a law-abiding personality and the successful integration of young people into society.

По данным аналитического обзора состояния преступности в Российской Федерации по итогам 2023 года 22 340 несовершеннолетних совершили преступления [1]. Преступность всегда являлась одним из основных дестабилизирующих факторов в стране, представляющих реальную угрозу успешному осуществлению социально-экономических реформ. Вопрос противодействия преступности несовершеннолетних и защиты от преступлений, совершенных в отношении их, в течение последних лет оставался актуальным, находился на постоянном контроле.

К причинам преступности несовершеннолетних можно отнести:

1. Социальные факторы:

- семейная обстановка: неблагоприятные семейные условия, отсутствие внимания и заботы со стороны родителей, насилие в семье.
- образование: недостаточное или некачественное образование, отсутствие интереса к учёбе.
- социальное окружение: влияние сверстников, участие в асоциальных группах и субкультурах.
- экономические условия: низкий уровень жизни, безработица среди родителей.

2. Психологические факторы:

- психологические проблемы: эмоциональные и поведенческие расстройства, низкая самооценка.
- импульсивность: неспособность контролировать свои эмоции и поведение.
- поиск идентичности: желание утвердиться в группе сверстников, поиск своего места в обществе.

3. Биологические факторы:

- генетическая предрасположенность: наличие у родителей или близких родственников криминального прошлого.
- гормональные изменения: влияние гормональных изменений в подростковом возрасте на поведение.

В качестве приоритетов организации работы правоохранительных органов по борьбе с преступлениями, совершаемыми несовершеннолетними, выступает направленность на индивидуальный подход к каждому несовершеннолетнему и, в зависимости от его личности и установленных

обстоятельств деяния, на применение конкретных процедур уголовного судопроизводства.

Уголовное преследование несовершеннолетних всегда должно исходить из неукоснительного приоритета соблюдения прав несовершеннолетних, объективной оценки формы умысла и мотивов инкриминируемых деяний и в целом из общественной опасности содеянного. Нельзя забывать, что подростки не всегда способны адекватно оценивать общественную опасность и контролировать свои поступки, и именно поэтому законодатель предусматривает для них особые условия и механизм уголовного судопроизводства и назначения наказания. В то же время позиция следственных органов и надзирающих прокуроров должна формироваться исходя из приоритета обеспечения безопасности окружающих граждан от преступных действий несовершеннолетнего. Иными словами, при своевременном принятии мер, направленных на изоляцию подростков с устойчивой криминальной направленностью, можно предотвратить наступление общественно опасных последствий, в том числе тяжких и особо тяжких, тем самым обеспечив конституционное право граждан на защиту от преступных посягательств [2].

В борьбе с преступностью среди несовершеннолетних очень важное значение имеет профилактика правонарушений среди указанной категории лиц, которая сегодня становится главной задачей всего общества. Профилактика – деятельность по недопущению нарушений норм законодательства, в частности уголовного права, выявление причин преступлений, условий и обстоятельств, способствующих их совершению, выявление лиц, которые могут совершить преступление в силу их антисоциальной направленности и поведения [3].

Уголовно-правовые меры борьбы с преступностью среди несовершеннолетних направлены на предотвращение противоправных деяний и воспитание законопослушных граждан.

Они включают в себя следующие аспекты:

1. Предупреждение преступлений. Одной из основных задач уголовно-правовых мер является предупреждение совершения преступлений несовершеннолетними. Это достигается путём воздействия на сознание молодых людей, формирования у них понимания недопустимости противоправного поведения и уважения к закону.

2. Ответственность за совершение преступлений. Несовершеннолетние, совершившие преступления, подлежат уголовной ответственности в соответствии с законодательством. Это включает в себя назначение наказания, применение мер воспитательного воздействия и контроль за поведением несовершеннолетних после отбытия наказания.

3. Применение мер воспитательного воздействия. Вместо наказания за некоторые преступления несовершеннолетним могут быть назначены меры воспитательного воздействия, такие как предупреждение, передача под

надзор родителей или специализированных органов, возложение обязанностей загладить причинённый вред, ограничение досуга и установление особых требований к поведению.

4. Контроль за поведением несовершеннолетних. После отбытия наказания или применения мер воспитательного воздействия, несовершеннолетние находятся под контролем специализированных органов, которые следят за их поведением и помогают адаптироваться к жизни в обществе.

5. Профилактика преступности. Одной из важных задач уголовно-правовых мер является профилактика преступности среди несовершеннолетних. Это достигается путём проведения разъяснительной работы, организации досуга, создания условий для получения образования и профессиональной подготовки.

6. Сотрудничество с семьёй и образовательными учреждениями. Для эффективной борьбы с преступностью среди несовершеннолетних необходимо сотрудничество с семьёй, образовательными учреждениями и другими организациями, работающими с молодёжью. Это позволяет выявить причины противоправного поведения и разработать меры по их устранению.

7. Реабилитация и социальная адаптация. Несовершеннолетние, совершившие преступления, нуждаются в реабилитации и социальной адаптации. Это включает в себя оказание помощи в трудоустройстве, получении образования, восстановлении социальных связей и формировании позитивных жизненных установок.

8. Международное сотрудничество. В борьбе с преступностью среди несовершеннолетних важную роль играет международное сотрудничество. Это позволяет обмениваться опытом, разрабатывать совместные программы и оказывать помощь странам, столкнувшимся с проблемой роста преступности среди молодёжи.

Таким образом, предпосылки к преступности среди несовершеннолетних, как и преступность в целом, носят социально обусловленный характер. Чтобы не допускать совершения преступлений несовершеннолетними, нужно доводить до подрастающего поколения основные положения законодательства об ответственности. Уголовно-правовые меры борьбы с преступностью среди несовершеннолетних направлены на создание условий для формирования законопослушного поведения молодых людей и их успешной интеграции в общество.

СПИСОК ЛИТЕРАТУРЫ

1. Аналитический обзор «Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 года и ожидаемые тенденции её развития» подготовлен авторским коллективом ФГКУ «ВНИИ МВД России». – Москва, 2024. – С. 10.

2. Махош М. Б., Медведев С. С. Меры профилактики и борьбы с преступностью несовершеннолетних // Отечественная юриспруденция. – 2019. – № 4 (36). – С. 34–37.

3. Маркина Э. В., Сосновская Ю. Н. К вопросу о профилактике правонарушений среди несовершеннолетних // Современная наука. – 2020. – № 2. – С. 43–46.

СВЕДЕНИЯ ОБ АВТОРЕ

Соловьев Данил Николаевич.

Доцент кафедры уголовного права и криминологии.

Кандидат юридических наук.

Уфимский юридический институт МВД России.

E-mail: soloviev-danil@mail.ru

Россия, 450103, г. Уфа, ул. Муксинова, 2.

Soloviev Danil Nikolaevich.

Associate Professor of the Department of Criminal Law and Criminology.

Candidate of Legal Sciences.

Ufa Law Institute of the Ministry of Internal Affairs of Russia.

Russia, 450103, Ufa, Muksinova St., 2.

Ключевые слова: уголовно-правовые меры; борьба с преступностью; несовершеннолетние; профилактика правонарушений.

Keywords: criminal law measures; fight against crime; minors; crime prevention.

УДК 343.54 (470)

С. А. Солодина

К ВОПРОСУ О НЕОБХОДИМОСТИ КРИМИНАЛИЗАЦИИ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В АЗАРТНЫЕ ИГРЫ

ON THE QUESTION OF THE NEED TO CRIMINALIZE THE INVOLVEMENT OF MINORS IN GAMBLING

В настоящей статье рассмотрен вопрос о необходимости криминализации вовлечения несовершеннолетнего в азартные игры, в связи с наличием общественной опасности деяния. Автором проведены исследования материалов судебно-следственной практики, данных уголовной статистики и мнений респондентов, в связи с чем, рассматривается вопрос о совершенствовании уголовно-правовых норм, связанных с вовлечением

несовершеннолетних в азартные игры, так как дети и подростки чаще подвержены различным пагубным влияниям с различных сторон, государству необходимы соответствующие рычаги, усиливающие контроль в правовом поле игорного бизнеса.

This article discusses the need to criminalize the involvement of a minor in gambling, due to the presence of a public danger of the act. The author conducted research on materials of judicial and investigative practice, criminal statistics data and opinions of respondents, in connection with which, the issue of improving criminal law norms related to the involvement of minors in gambling is being considered, since children and adolescents are more often exposed to various harmful influences from various sides, the state needs appropriate levers that strengthen control in the legal field of gambling.

Технологическое развитие принесло не только преимущества для современного общества, но и ряд негативных последствий. Право на участие в азартных играх без ограничений способствовало возникновению множества социальных проблем и развитию новых психологических зависимостей. В настоящий момент лудомания представляет собой одну из наиболее актуальных проблем российского общества, ведь азартные игры в жизни детей – это серьезная тема, требующая внимания и обсуждения всех структур общества. Тем не менее, проблема лудомании не воспринимается столь серьезно, как, например, вопросы, связанные с алкогольной или наркотической зависимостями в стране. Это обусловлено тем, что многие люди не осознают значимость данной проблемы и ее потенциальную угрозу для общества. Для многих граждан лудомания представляется менее опасной по сравнению с другими социальными проблемами.

«Лудомания – болезнь, проявляющаяся в склонности к азартным играм, которая приводит к ее преобладанию в жизни субъекта и к упадку материальных, духовных, профессиональных, социальных и семейных ценностей» [1]. Игра, способствует психологическому расслаблению, давая человеку уйти от иных значимых социальных проблем в жизни. Она втягивает, поглощая всю жизнь человека и ведет к зависимости равной наркотической или алкогольной.

На сегодняшний день существует множество аспектов, связанных с воздействием азартных игр на детей как непосредственно, так и через образы азартных игр в культуре и медиа. В условиях глобальной безопасности казино рассматривается как арена международной политики, с пересечением интересов государств и культур. В литературе и кинематографе данные места служат не только местом развлечений граждан, но и заведениями, где происходит агентурное общение и различная разведывательная деятельность, в том числе шпионаж.

В мире представлено множество видов азартных онлайн-игр, и их разнообразие постоянно увеличивается. Обычно все азартные игры делятся на два основных типа: первый тип – игры, где выигрыш зависит исключительно от удачи (например, игровые автоматы, кости и другие онлайн-казино), а второй тип – это игры, в которых успех зависит не только от удачи, но и от мастерства игроков (такие как видеоигры, тотализаторы и покер).

В результате анализа проблемы азарта в жизни людей можно выделить несколько этапов игровой аддиктивности:

1. Втягивание в игру. Здесь игрок способен управлять своими поступками и имеет возможность легко остановить игру.

2. Игра важнее выигрыша. Лудоман только с помощью своих усилий и силы воли может прекратить игру.

3. Тотальная зависимость от игры. Игра – это смысл жизни. На данной стадии четко сформировано расстройство личности.

Лудомания относится к поведенческой зависимости (нехимическая зависимость), т.е. это аддикция, при которой объектом зависимости становится какой-либо поведенческий паттерн, а не психоактивное вещество. Для такой зависимости характерны «сверхценность», синдром отмены, резкое изменение настроения, рост толерантности, межличностные и внутриличностные конфликты и частые рецидивы.

Основная проблема заключается в том, что в последнее время азартные онлайн-игры быстро набирают популярность среди детей и подростков, становясь одной из самых популярных форм досуга. Онлайн-ставки в онлайн-казино и спортивные тотализаторы представляют собой серьезную угрозу не только для родителей и близких, но и педагогов, сотрудников правоохранительных органов, а также представителей других учреждений, занимающиеся профилактикой правонарушений и безнадзорности среди несовершеннолетних. Дети тратят на это свои карманные деньги, крадут средства с банковских карт родителей и даже совершают преступления, чтобы, например, купить персонажа в какой-нибудь игре или занять рейтинговое место, получив игровой выигрыш. Патологическое влечение становится настолько интенсивным, что человек перестает замечать окружающих, проблемы и события в своей жизни. Дети, увлеченные азартными играми, могут развить зависимость, что негативно сказывается на их психическом здоровье, вызывая стресс, тревожность и депрессию.

Несовершеннолетние представляют собой одну из наиболее уязвимых и криминогенно-подверженных групп населения, т.к. обладают низким уровнем социальной защиты. Они характеризуются эмоциональной неустойчивостью и недостаточной социальной адаптацией. У подростков существует высокая вероятность формирования зависимостей, что делает их легкой мишенью для вовлечения их в азартные игры. Согласно

статистике, зависимость у несовершеннолетних выявляется в три раза чаще, чем у взрослых. «По данным Росстата на 1 января 2023 г. численность населения (постоянных жителей) России составляет 146 447 424 человек, в том числе детей в возрасте до 6 лет – 14 579 283, подростков (школьников) в возрасте от 7 до 17 лет – 17 243 332» [2]. Таким образом, не менее $\frac{1}{2}$ подростков являются активными потребителями индустрии азартных игр, которая развивается стремительно в виртуальном пространстве интернета. Азартные игры оказывают разрушительное воздействие на еще несформировавшуюся психику молодежи. Результаты анкетирования показали, что 52% студентов-респондентов имеют негативное отношение к азартным играм; 42,7% – относятся к ним равнодушно; а 1,3% не смогли дать ответ и только 4% выражают положительное мнение о данном виде досуга.

В современном российском обществе проблема вовлечения несовершеннолетних в азартные игры остается актуальной и недостаточно изученной на данный момент времени. Для гемблинговой индустрии (азартные игры на деньги) в современности характерно массовое внедрение новых технологий. Многие игры вовлекают большое количество несовершеннолетних игроков с тем, чтобы они могли соревноваться друг с другом в сети Интернет. Даже играющий на таких сайтах без денег находит Интернет-гемблинг привлекательным, волнующим и захватывающим. Например, казино-игры перемежаются с другими более безобидными играми, часто используется яркая графика и реальные звуки, узнаваемые образы из знаменитых фильмов, мультфильмов, что способствует красочному восприятию азартной игры [3]. Исследователи проблемы как в России, так и за рубежом, пришли к неутешительному выводу о том, что современные дети и подростки, вовлеченные в гемблинговые онлайн-игры и имитирующие гемблинговые видеоигры, находятся в зоне риска, так как эти симуляторы включают в себя принятие гемблинга как обычного нормального, и даже позитивного, развлечения и времяпрепровождения; формирование ложного чувства безопасности онлайн-игр и уверенности (на уровне психологической зависимости) в обязательном успехе с каждым новым этапом и получении значительной большой по сумме выигрыша (применяются рекламные технологии, постоянно демонстрирующие в сети крупные победы пользователей, а также использование системы активных беспроигрышных бонусов в первых играх и крупный «Джек-пот» – наиболее показательные примеры массового навязывания гемблинговых технологий онлайн-казино «Вулкан» или тотализатором спортивных ставок «СпортБэт», позволяющие выводить деньги на банковскую карту или электронные кошельки); формирование ложной уверенности на среднесрочную и длительную перспективу (прежде всего, систематическое получение прибыли от онлайн-игры, которые могут заменить профессию взрослому

человеку и обеспечить высокий постоянный доход, в том числе приобрести жилье, автомобиль или обеспечить собственную семью).

Соответствующие меры по борьбе с такими формами азартных онлайн-игр со стороны государства принимаются. Достаточно вспомнить, что «с 2007 г. в России запрещена деятельность онлайн-лотерей и прочих азартных игр в интернете, а с 2018 г. – переводы средств в пользу нелегальных организаторов таких сервисов. Исключение составляет работа букмекеров и тотализаторов, заключивших договор с Единым центром учета перевода ставок букмекерских контор и тотализаторов (ЦУПИС или «Мобильная карта»), который ведет учет и перевод денежных средств от игроков, обработку этих платежей и удерживает целевые отчисления на поддержку отечественного спорта (в сентябре 2021 г. стала единым центром учета перевода ставок букмекерских контор и тотализаторов (Единый ЦИПУС).

Обращаясь к диспозиции действующей нормы ст. 171.2 УК РФ, отметим, что в ней несовершеннолетние лица не указаны как особая категория потерпевших (как правило, отечественный законодатель, понимая повышенную общественную опасность таких деяний и их последствий, массовость их совершения предусматривает отдельно в уголовно-правовой норме Особенной части квалифицирующий признак, отягчающий ответственность и наказание). При буквальном толковании ст. 171. 2 УК РФ и других норм действующего уголовного закона, факт вовлечения несовершеннолетних в незаконные организацию и проведение азартных онлайн-игр не является преступлением, хотя основные критерии криминализации деяний на лицо: во-первых, упомянутая повышенная общественная опасность деяний, совершенных в отношении детей и подростков и, во-вторых, массовость совершения таких деяний в современных российских условиях и прогноз на существенный рост.

На целесообразность введения в современных российских условиях уголовной ответственности за сам факт вовлечения несовершеннолетних лиц в незаконные организацию и проведение азартных онлайн-игр (как оптимальный вариант новой нормы – ч. 4 ст. 171.2 УК РФ) прямо указало 88,5% опрошенных респондентов из числа действующих сотрудников различных территориальных подразделений по делам несовершеннолетних органов внутренних дел – представителей одного из ключевых субъектов профилактики безнадзорности, административных правонарушений и преступности с участием несовершеннолетних (всего в рамках исследования опрошено 84 человек из 15 регионов Российской Федерации, в том числе проходивших обучение и повышение квалификации в Воронежском институте МВД России). Представляется, что на практике, введение такой запретительной уголовно-правовой нормы и правильное применение ее в комплексе с другими действенными общими и специальными мерами системы ранней профилактики позволит

стабилизировать криминогенную ситуацию в этой сфере за счет минимизации масштабов вовлечения детей и подростков в организацию и проведение незаконных онлайн-игр.

СПИСОК ЛИТЕРАТУРЫ

1. Ахрамейко А. В. Современные аспекты лечения игровой зависимости / А. В. Ахрамейко, В. А. Куташов // Молодой ученый. – 2016. – № 2. – С. 143–151.

2. Росстат зафиксировал снижение численности населения России на полмиллиона за год. – URL: <https://rg.ru/2023/02/01/rosstat-zafiksiroval-snizhenie-chislennosti-naseleniia-rossii-na-polmilliona-za-god.html> (дата обращения: 10.11.2024).

3. Колесникова Л. И. К вопросу о негативных последствиях вовлечения подростков в современные азартные игры в сети интернета / Л. И. Колесникова // Мир науки, культуры, образования. – 2015. – № 6 (55). – С. 161–164.

СВЕДЕНИЯ ОБ АВТОРЕ

Солодина София Антоновна. Адъюнкт адъюнктуры.
Воронежский институт МВД России.
E-mail: olgasonia1999@gmail.com
Россия, 394065, Воронеж, проспект Патриотов, 53.

Solodina Sofia Antonovna. Adjunct Adjunct.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: несовершеннолетний; подросток; дети; азартные игры; индустрия развлечений; вовлечение; склонение; общественно опасное деяние; преступление; негативные последствия; криминализация.

Keywords: minor; teenager; children; gambling; entertainment industry; involvement; inducement; socially dangerous act; crime; negative consequences; criminalization.

УДК 343.53

ВСЕРОССИЙСКИЙ СЕМИНАР
ИСПОЛЬЗОВАНИЕ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ
В СОЗДАНИИ ТЕХНИЧЕСКИХ УСТРОЙСТВ И ПОДГОТОВКЕ СПЕЦИАЛИСТОВ
ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

С. Л. Анисимов

**ПРОГНОЗИРОВАНИЕ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

**FORECASTING OF CRIMES COMMITTED USING INFORMATION
AND TELECOMMUNICATION TECHNOLOGIES**

В статье рассматриваются примеры совершения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, и применение искусственного интеллекта в прогнозировании преступлений.

The article discusses examples of crimes committed using information and telecommunication technologies and the use of artificial intelligence in crime forecasting.

За три месяца 2023 года в России заблокировано почти 100 тысяч телефонных номеров, которые использовали мошенники. Однако вычислять и блокировать звонки из мессенджеров пока не удастся. Этим и пользуются аферисты. Как мошенники убеждают своих жертв?

Неизвестный представится лейтенантом полиции, следователем прокуратуры или майором ФСБ. Скажет, что звонит по зашифрованной линии, будет убеждать, что ваши деньги под угрозой и нужно срочно перевести их на безопасный счет. На аватаре фото человека в форме или эмблема силового ведомства. Неужели это мошенник? Никаких сомнений. Важно знать, сотрудники правоохранительных органов, как и работники банков никогда не звонят и не пишут в мессенджерах, а фото на аватаре – подделка.

Следующий пример, голос в трубке звучит зловеще: «Вы подозреваетесь в государственной измене, с вашей карты поступали денежные средства врагу, вам грозит огромный срок с конфискацией имущества». Важно знать. Это мошенники. Их задача напугать людей и заставить отдать круглую сумму.

Еще, пример, звонок с портала «Госуслуг». Вежливый голос уверяет, что ваш аккаунт взломан и вот-вот случится беда, на ваше имя оформят кредит, украдут все данные, зарегистрируют несколько симкарт и используют их в преступной деятельности. Но злоумышленнику можно поме-

шать, если сменить пароль и номер телефона на госуслугах, а собеседник подскажет, как это сделать прямо сейчас под его чутким руководством. Важно знать. Это мошенники. Их задача получить доступ к аккаунту людей на госуслугах чтобы сделать все то, о чем они подробно рассказывают.

Мошенники придумывают все новые схемы обмана, пугают уголовной ответственностью, обещают баснословные выигрыши, привлекают легким заработком и все с одной целью – выманить денежные средства [1, 2].

В данной ситуации следует помнить, что сотрудники правоохранительных органов никогда не будут звонить в телефонном режиме и предлагать участие в каких-либо операциях по поимке других преступников. Также не будут присылать фотографии своих служебных удостоверений, потому что это является конфиденциальной информацией.

В 2024 году на территории Российской Федерации участились случаи телефонного мошенничества. Так, в сравнении с аналогичным периодом прошлого года преступлений возросло примерно на 20%. При этом преступники действуют по самым разнообразным схемам, в том числе участились случаи, когда преступники представляются сотрудниками Центрального банка России. Они предлагают потерпевшим принять участие в операции по поимке мошенников, при этом потерпевшим прилагается взять на себя кредит либо занять денежные средства у родственников и перевести их на безопасный счет, тем самым оказать содействие следствию.

В настоящее время российские ученые разрабатывают программу на основе искусственного интеллекта, она будет искать мошенников. Нейросеть обучают с помощью данных, из уже раскрытых дел [3]. Программа преступности делит карту на небольшие квадраты. Места, где риск нарваться на неприятности высокий, выделяются красным цветом. Искусственный интеллект предсказывает не только район, но и время предполагаемого преступления. В расчет берут все, что ранее происходило в конкретном месте. По мнению многих аналитиков, повсеместное использование искусственного интеллекта для предсказаний – дело недалекого будущего, но эта технология еще нуждается в контроле живых людей.

СПИСОК ЛИТЕРАТУРЫ

1. Обзор мошеннических схем, направленных на получение денежных средств путем незаконных манипуляций в интернет-сервисах и многопользовательских компьютерных играх / Э. А. Томилова, А. О. Ефимов, С. Л. Анисимов, Е. А. Печенин // Вестник Воронежского института ФСИН России. – 2024. – № 3. – С. 222–227.

2. Поликарпов Е. С. О защищенности сайта сети Интернет от автоматизированного сбора данных / Е. С. Поликарпов, С. Л. Анисимов, А. А. Толстых // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 77–84.

3. Попов А. В. Перспективы применения нейросетевых технологий в деятельности органов внутренних дел / А. В. Попов, С. Л. Анисимов // Актуальные проблемы кибербезопасности в сети Интернет : Сборник научных трудов Всероссийской конференции, Москва, 23 апреля 2020 года. – Москва : Московский университет Министерства внутренних дел Российской Федерации им. В. Я. Кикотя, 2020. – С. 111–113.

СВЕДЕНИЯ ОБ АВТОРЕ

Анисимов Сергей Леонидович.
Доцент кафедры физики и радиоэлектроники.
Кандидат технических наук.
Воронежский институт МВД России.
E-mail: anisimov12@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Anisimov Sergey Leonidovich.
Associate Professor of the Department of Physics and Radioelectronics.
Candidate of technical sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: anisimov12@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: угроза; мошенники; конфиденциальная информация; защита.

Keywords: threat; fraudsters; confidential information; protection.

УДК 004.056, 343.72

А. О. Авсентьев

ТЕХНИЧЕСКИЕ АСПЕКТЫ МОДЕЛИ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СИСТЕМЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

TECHNICAL ASPECTS OF THE COMPUTER SYSTEM PROTECTION MODEL AGAINST UNAUTHORIZED ACCESS

В статье рассматриваются технические аспекты моделей защиты компьютерных систем от несанкционированного доступа, использующие методы шифрования, биометрическую аутентификацию, межсетевые экраны и системы обнаружения вторжений.

The article discusses the technical aspects of models for protecting computer systems from unauthorized access using encryption methods, biometric authentication, firewalls and intrusion detection systems.

Современные технологии защиты компьютерных систем органов внутренних дел (ОВД) от несанкционированного доступа включают многослойные меры безопасности [1]. Они используют передовые методы шифрования, биометрическую аутентификацию, межсетевые экраны и системы обнаружения вторжений. Более того, технологии искусственного интеллекта и машинного обучения эффективно применяются при изучении человеческого поведения – стремлении выявить аномалии. Это значительно повышает уровень безопасности, создавая более активный щит, подавляющий угрозы в зародыше.

В сфере информационной безопасности ключевую роль играет техническая защита компьютерных систем от несанкционированного доступа. Это действительно важно, ведь риски, связанные с потерей данных или взломом системы, могут иметь серьезные последствия. Давайте подробнее рассмотрим различные технические подходы и механизмы, которые помогают обеспечить надежную многоуровневую защиту.

Одним из основных элементов является система управления доступом. Эта система, как правило, базируется на введении строгих правил, ролей и политик безопасности. Важную роль играют инструменты контроля доступа, например, списки контроля доступа или ACL. Они помогают четко определить, кто и к каким ресурсам системы может получить доступ, что делает защиту более гибкой и адаптируемой к различным угрозам.

Следующий важный аспект – это система регистрации и контроля критических событий. Она не только фиксирует все важные события и действия пользователей в системе, но и предоставляет возможность для проведения тщательного аудита [2]. Это позволяет не только улучшить общую безопасность системы, но и своевременно обнаруживать и анализировать попытки несанкционированного доступа.

Не менее важной является система контроля целостности данных. Она защищает данные от несанкционированного изменения, используя различные механизмы проверки целостности, включая хеширование. Это гарантирует, что любые изменения в данных будут замечены и проверены на предмет их законности и соответствия установленным стандартам [3].

Наконец, система криптографической защиты играет центральную роль в обеспечении безопасности данных. С помощью шифрования информация защищена от несанкционированного доступа и утечек. Применяются разнообразные алгоритмы и методы шифрования, как симметричные, так и асимметричные, чтобы обеспечить как конфиденциальность, так и целостность данных. Интеграция этих технических методов создает

крепкую защиту для информационных систем, минимизируя риски и усиливая уверенность в безопасности ценной информации.

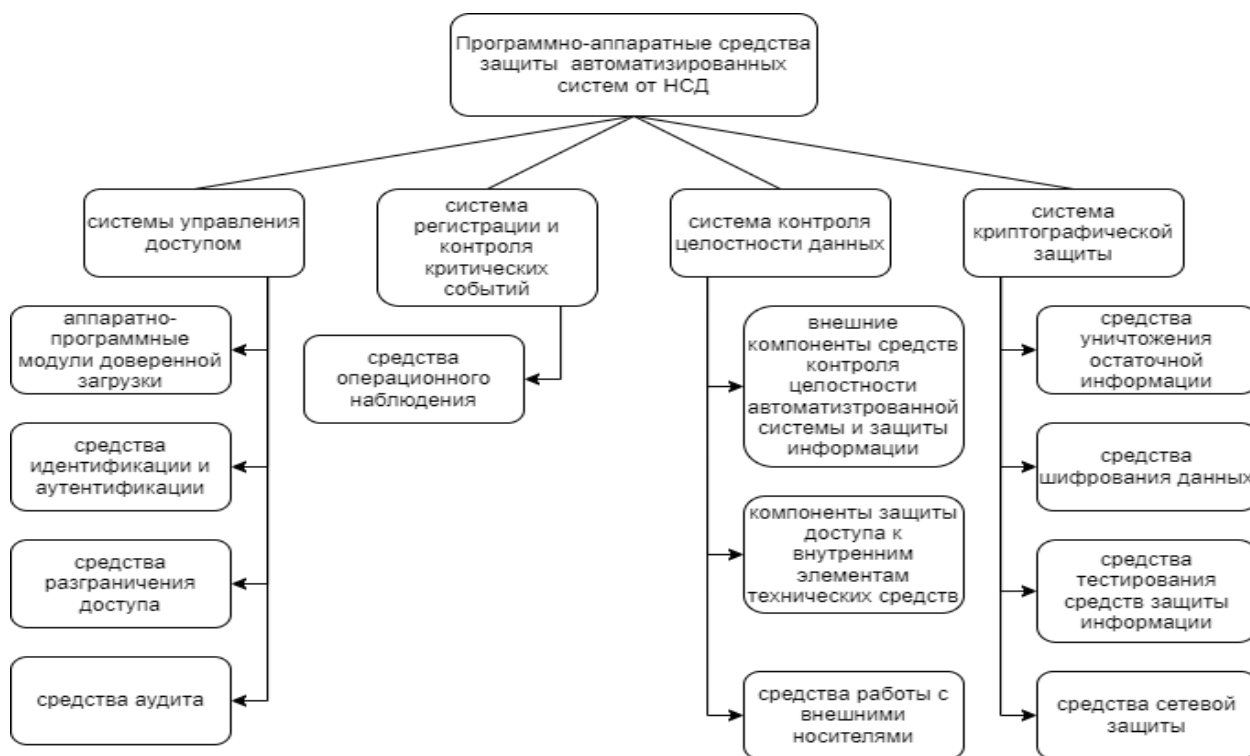


Рис. Программно-аппаратные средства защиты компьютерной системы от несанкционированного доступа

Аутентификация играет ключевую роль в подтверждении личности пользователя или устройства, стремящихся получить доступ к системе. В этом процессе используются различные методы, такие как пароли, биометрические данные и аппаратные ключи [4]. Важно уметь выбирать и интегрировать эти методы, чтобы обеспечить высокий уровень защиты.

Также не менее важно управление доступом, которое определяет, кто или что может взаимодействовать с определёнными ресурсами внутри системы. Внедрение политик безопасности, установление правил и ролей, а также использование механизмов контроля доступа, включая шифрование и списки контроля доступа, играют здесь центральную роль.

Как же не упомянуть о шифровании данных? Это ещё один крайне важный аспект защиты компьютерных систем. Шифрование трансформирует чувствительные данные в формат, который можно безопасно хранить и передавать. Симметричное и асимметричное шифрование стоят во главе угла среди методов обеспечения конфиденциальности информации.

Обнаружение и предотвращение инцидентов безопасности, конечно же, не остаются без внимания. Системы мониторинга и аналитики в это тоже вовлечены, отслеживая атаки и необычные действия пользователей

или устройств. Благодаря их реактивности возможно оперативно реагировать на возникающие угрозы.

И напоследок, обновление системы – ну, это просто необходимо для поддержания её защищённости. Злоумышленники могут эксплуатировать любые уязвимости, если не проводить регулярные обновления и установку патчей. Важно всегда оставаться на чеку и обновлять систему без промедления.

Технологические проблемы, связанные с защитой компьютерных систем от криптографической атаки (НСД), требуют комплексного подхода и постоянного развития [5]. С помощью новейших методов и технологий можно построить надежную систему защиты, способную противостоять различным угрозам и атакам. Для обеспечения безопасности системы также важно проводить регулярное обучение персонала и аудит.

Резервное копирование данных является важной частью защиты компьютерной системы. Регулярное создание резервных копий позволяет восстановить данные в случае их утраты из-за сбоя в системе, атаки вредоносного ПО или других непредвиденных ситуаций. Резервные копии следует хранить в надежных, защищенных местах, таких как облачные хранилища или внешние накопители.

Защита от вредоносного программного обеспечения также имеет решающее значение. Установка и регулярное обновление антивирусных программ, использование антишпионского ПО и проведение систематических сканирований помогают предотвращать и устранять угрозы от вирусов, троянов, программ-вымогателей и других видов вредоносного программного обеспечения.

Внедрение принципа минимальных привилегий и контроль за безопасностью приложений также важны для защиты системы. Приложения должны иметь как можно меньше прав, чтобы не злоупотреблять ими в случае компрометации.

СПИСОК ЛИТЕРАТУРЫ

1. Рогозин Д. Ю. Информационная безопасность организации: учебное пособие / Д. Ю. Рогозин. – Москва : Проспект, 2016. – 288 с.
2. Синегубов С. В. Моделирование систем и сетей телекоммуникаций : учебное пособие. – Воронежский институт МВД России, 2016. – 300 с.
3. ГОСТ Р ИСО/МЭК 7498-1-2014. Информационная технология. Системы и средства обработки информации. Термины, определения и обозначения. Часть 1. Основные термины. Введ. 2015-01-01. – Москва : Издательство стандартов, 2014. – 18 с.
4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [утверждена зам. Директора ФСТЭК России 14 февраля 2008 г.]

[Электронный ресурс]. – URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakhpersonalnykh-dannykh-fstek-rossii-2008-god> (дата обращения: 20.10.2024).

5. Е. К. Баранова Информационная безопасность и защита : учебное пособие / Е. К. Баранова, А. В. Бабаш. – Москва : Инфра-М, 2016 – 324 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Авсентьев Александр Олегович.

Доцент кафедры компьютерной безопасности и технической экспертизы.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: aoaao8787@mail.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Avsentiev Alexander Olegovich.

Associate Professor of the chair of Computer Security and Technical Expertise.

Candidate of Technical Sciences.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: aoaao8787@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: компьютерная система; угроза; сеть; несанкционированный доступ.

Keywords: computer system; threat; network; unauthorized access.

УДК 004.056:519.1

**ПРОГРАММНЫЙ МОДУЛЬ «ВРАЖЕСКИЙ БПЛА»
В ПРОЦЕССЕ ПОДГОТОВКИ СОТРУДНИКОВ,
НЕСУЩИХ СЛУЖБУ В ОСОБЫХ УСЛОВИЯХ**

**SOFTWARE MODULE «ENEMY UAV»
IN THE PROCESS OF TRAINING EMPLOYEES
PERFORMING SERVICE IN SPECIAL CONDITIONS**

Статья посвящена перспективам применения технологии программно-определяемого радио в системах радиосвязи специального назначения.

В качестве первого варианта применения автором предложено применение технологии SDR для диагностики и проверки правильности настройки радиооборудования сетей радиосвязи специального назначения. Второй вариант использования подразумевает собой реализацию метода противодействия деструктивным воздействиям за счет переноса спектра информационного сигнала в другой частотный диапазон.

The article is devoted to the prospects of using software-defined radio technology in special-purpose radio communication systems. As the first option, the author suggests using SDR technology for diagnostics and checking the correctness of the radio equipment settings of special-purpose radio communication networks. The second option involves the implementation of a method for counteracting destructive effects by transferring the spectrum of the information signal to another frequency range.

Применение БВС сотрудниками ОВД на службе в особых условиях охватывает широкий спектр задач, от разведки и наблюдения до непосредственной поддержки наземных войск и нанесения ударов по противнику. БВС выполняет сбор информации о расположении и действиях противника на командные пункты в режиме реального времени, позволяя лучше понимать обстановку, корректировать огонь ракетных войск. Эксплуатация БВС в качестве средства боевой атаки представляет собой одну из наиболее значимых и эффективных тактик, применяемых на службе в особых условиях. Она позволяет наносить удары по противнику с высокой точностью и минимальными рисками для личного состава. Также активно применяются БВС для выполнения задач по поддержке снабжения. Дроны доставляют боеприпасы, медикаменты и другие необходимые ресурсы в удаленные или опасные районы, что существенно повышает мобильность и эффективность сотрудников ОВД [1-2].

Сотрудникам полиции, привлекаемым к несению службы в особых условиях, необходимо уметь пользоваться средствами связи, телекоммуникационными устройствами, навигационным оборудованием, специаль-

ной техникой, знать классификацию, функциональные возможности, тактико-технические характеристики БЛА, специальные средства противодействия им, а также частоты работы БЛА и частоты подавления их информационных каналов [3].

В связи с этим, авторами был разработан программный комплекс «Вражеский БПЛА» (рис.) который содержит в себе частоты работы и передачи данных, спектры каналов управления, видеозаписи, изображения БПЛА и техническую документацию. На основании данных параметров осуществляется выработка рекомендаций по подавлению БПЛА. Имеющиеся в базе данных материалы возможно дополнять и редактировать при появлении новой информации.



Рис. Интерфейс программного обеспечения

На основании рекомендаций по подавлению БПЛА выбирается техническое средство воздействия, а также частотный диапазон и тип помехи [4].

Реализация предложенного программного обеспечения позволит оптимизировать процесс получения сведений о вражеских БЛА, которые используются в противоправных действиях, и выработке рекомендаций по их радиоэлектронному подавлению. Разработанное программное обеспечение планируется к внедрению в центры информационных технологий, связи и защиты информации, а также сводные отряды полиции, привлекаемые к службе в особых условиях.

СПИСОК ЛИТЕРАТУРЫ

1. Об утверждении Порядка принятия решения о пресечении функционирования беспилотных воздушных, подводных и надводных судов и аппаратов, беспилотных транспортных средств и иных автоматизированных беспилотных комплексов в целях защиты жизни, здоровья и имущества граждан, сотрудников органов внутренних дел, в том числе в месте проведения публичного (массового) мероприятия и прилегающей к нему территории, проведения неотложных следственных действий и оперативно-розыскных мероприятий и Перечня должностных лиц полиции, уполномоченных на принятие такого решения : приказ МВД России от 16.11.2023 № 865. – URL: <http://www.consultant.ru> (дата обращения: 20.11.2024).

2. Макаренко С. И. Противодействие беспилотным летательным аппаратам : монография. – Санкт-Петербург : Наукоемкие технологии, 2020. – 204 с.

3. Методические рекомендации по организации проведения дополнительных занятий в системе профессиональной служебной и физической подготовки с сотрудниками органов, организаций, подразделений МВД России, привлекаемыми к несению службы по охране общественного порядка и обеспечению общественной безопасности в особых условиях – Москва : ГУРЛС МВД России, 2023. – 116 с.

4. Беспилотные авиационные системы МВД России : обзор / сост. А. А. Морев. – ФКУ НПО «СТиС» МВД России, 2024. – 45 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Гилев Игорь Владимирович.

Преподаватель кафедры инфокоммуникационных систем и технологий.

Воронежский институт МВД России.

E-mail: gileviv@bk.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Ртищев Роман Владимирович.

Слушатель 5 курса радиотехнического факультета.

Воронежский институт МВД России.

E-mail: rtishchev48.r@yandex.ru

Россия, 394065, Воронеж, проспект Патриотов, 53.

Gilev Igor Vladimirovich.

Lecturer of the Department of Infocommunication Systems and Technologies.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: gileviv@bk.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Rtishchev Roman Vladimirovich.
5th year student of the radio engineering faculty.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: rtishchev48.r@yandex.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: особые условия; беспилотные летательные аппараты; подавление; спектр сигналов.

Keywords: special conditions; unmanned aerial vehicles; suppression; signal spectrum.

УДК 004.891.3

В. И. Кудряш

ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ СРЕДСТВ ЭЛЕКТРОПИТАНИЯ СИСТЕМ БЕЗОПАСНОСТИ И СВЯЗИ

PROSPECTS FOR IMPROVING THE POWER SUPPLY OF SECURITY AND COMMUNICATION SYSTEMS

Рассмотрение ключевых направлений совершенствования средств электропитания, а также их влияние на эффективность и надежность систем безопасности и связи.

Consideration of key areas for improving power supplies, as well as their impact on the efficiency and reliability of security and communication systems.

Системы безопасности и связи играют ключевую роль в современном обществе, обеспечивая защиту жизненно важных объектов и передачу информации. Учитывая растущие угрозы, такие как кибератаки, террористические акты и природные катастрофы, надежность этих систем становится критически важной. Одним из основных аспектов их функционирования является электропитание. В данной статье рассматриваются перспективы совершенствования средств электропитания для систем безопасности и связи, включая новые технологии, подходы и интеграцию с современными решениями.

В последние годы наблюдается стремительное развитие технологий, которые могут значительно повысить эффективность и надежность электропитания для систем безопасности и связи. Инновационные решения, такие как возобновляемые источники энергии, новые аккумуляторные технологии, интеллектуальные системы управления энергией и интеграция с интернетом вещей (IoT), открывают новые горизонты для обеспечения бесперебойной работы этих систем.

Одним из наиболее перспективных направлений в области электропитания является использование возобновляемых источников энергии (ВИЭ). Солнечные панели и ветряные установки становятся все более доступными и эффективными. По данным исследования [1], интеграция солнечных батарей в системы видеонаблюдения позволяет значительно снизить затраты на электроэнергию и повысить автономность работы устройств. Важно отметить, что ВИЭ могут быть особенно полезны для удаленных объектов, где подключение к централизованной сети невозможно. В качестве примера можно привести проекты по установке солнечных панелей на крышах зданий с системами безопасности. Это решение не только обеспечивает бесперебойное питание, но и способствует снижению углеродного следа, что соответствует современным экологическим стандартам [2].

Традиционные литий-ионные аккумуляторы постепенно уступают место более современным решениям, таким как твердотельные батареи и аккумуляторы на основе графена. Эти новые технологии обеспечивают большую плотность энергии и безопасность эксплуатации [3]. Твердотельные батареи, например, имеют меньшую вероятность возгорания по сравнению с литий-ионными аналогами и могут значительно увеличить срок службы устройств. Твердотельные аккумуляторы уже активно исследуются для применения в системах безопасности. Они могут обеспечить более длительное время работы без подзарядки и снизить необходимость в частом обслуживании. Это особенно важно для автономных систем, таких как датчики движения и камеры наблюдения.

Оптимизация энергопотребления является важным направлением в совершенствовании средств электропитания. Использование энергоэффективных компонентов, таких как светодиоды и низко потребляющие датчики, помогает снизить общее потребление энергии. Например, применение датчиков движения для включения освещения только при необходимости может существенно сократить расход электроэнергии. Современные системы видеонаблюдения уже интегрируют технологии анализа видео с целью определения активности и включения записи только в случае необходимости. Это не только экономит энергию, но и увеличивает срок службы оборудования.

Интеллектуальные системы управления энергией способны адаптироваться к изменяющимся условиям и автоматически регулировать потребление энергии в зависимости от времени суток или наличия резервных источников питания. Это обеспечивает более эффективное использование ресурсов и повышает надежность работы систем безопасности. Примером такой системы может служить умное освещение, которое использует данные о внешней освещенности для автоматической регулировки яркости ламп. Это позволяет не только экономить электроэнергию, но и продлить срок службы оборудования.

Беспроводная зарядка представляет собой инновацию, которая может упростить процесс обслуживания систем безопасности и связи. Такие технологии позволяют избежать использования проводов и разъемов, что особенно важно для устройств, расположенных в труднодоступных местах. Беспроводные зарядные станции могут быть интегрированы в инфраструктуру, обеспечивая постоянное питание для устройств без необходимости их физического подключения. Внедрение беспроводной зарядки в системы видеонаблюдения может значительно упростить их установку и обслуживание. Это особенно актуально для уличных камер, которые часто подвержены воздействию внешней среды.

Интеграция систем безопасности с интернетом вещей (IoT) требует разработки решений для бесперебойного электропитания устройств, которые могут работать в режиме реального времени. Использование IoT позволяет создать более умные и адаптивные системы, способные реагировать на изменения в окружающей среде и обеспечивать высокий уровень безопасности. Примером такой интеграции может служить система умного дома, где устройства безопасности взаимодействуют друг с другом через облачные сервисы. Это позволяет не только повысить уровень защиты, но и оптимизировать энергопотребление всей системы [4].

Совершенствование систем резервного питания, таких как генераторы и источники бесперебойного питания (ИБП), критически важно для обеспечения надежной работы систем безопасности в случае отключения электроэнергии. Разработка более компактных и эффективных решений позволит сократить затраты на обслуживание и повысить уровень защиты. Современные ИБП уже используют литий-ионные аккумуляторы вместо традиционных свинцово-кислотных, что позволяет значительно уменьшить вес и размеры устройств, а также повысить их эффективность.

Перспективы совершенствования средств электропитания систем безопасности и связи охватывают широкий спектр технологий и подходов. Инновации в области возобновляемых источников энергии, аккумуляторов, интеллектуальных систем управления и интеграции с IoT создают новые возможности для повышения надежности и эффективности этих систем.

Важно продолжать исследовать и развивать эти направления, чтобы обеспечить безопасность и стабильность в условиях постоянно меняющегося мира.

СПИСОК ЛИТЕРАТУРЫ

1. Кузнецов В. А. Использование возобновляемых источников энергии в системах безопасности // Энергетика и безопасность. 2021. – С. 45–50.
2. Петров С. А. Энергоэффективные решения для систем безопасности // Журнал электротехники. 2020. – С. 112–118.

3. Смирнов И. П. Новые технологии аккумуляторов для систем связи // Научный вестник. 2019. – С. 78–83.

4. Лебедев Е. С. Интеграция IoT в системы безопасности: вызовы и решения // Информационные технологии. – 2021. – С. 56-62.

СВЕДЕНИЯ ОБ АВТОРЕ

Кудряш Владлен Иванович.
Доцент кафедры физики и радиоэлектроники.
Кандидат физико-математических наук.
Воронежский институт МВД России.
E-mail: Kudrjashvi@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Kudryash Vladlen Ivanovich.
Associate Professor of the Department of Physics and Radioelectronics.
Candidate of Physical and Mathematical Sciences.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: Kudrjashvi@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: электропитание; надежность; безопасность.

Keywords: power supply; reliability; safety.

УДК 629.064.5

А. Н. Лукьянова

ПОРОГОВЫЕ ЗНАЧЕНИЯ ДЛЯ ВЕЙВЛЕТ-ФИЛЬТРАЦИИ ИССЛЕДУЕМОГО СИГНАЛА

THRESHOLD VALUES FOR WAVELET FILTERING OF THE STUDIED SIGNAL

Математические и инженерные области проявляют большой интерес к разработке новой теории и метода, касающихся вейвлетов и их применения. Подавление шума в сигналах является одной из важных исследовательских тем в области анализа сигналов. Исследуя сигнал, представлено сравнение и оптимальная способность к снижению уровня шума при мягком и жестком выборе двух правил пороговых значений, а именно Sqtwolog и Minimax на программной платформе MATLAB.

Mathematical and engineering fields are showing great interest in developing a new theory and method concerning wavelets and their applications. Noise

reduction in signals is one of the important research topics in the field of signal analysis. Examining the signal, a comparison and optimal ability to reduce noise levels are presented with a soft and hard choice of two threshold rules, namely Sqtwolog and Minimax on the MATLAB software platform.

Подавление шума в сигналах является одной из важных исследовательских тем в области анализа сигналов. В настоящее время существует метод вейвлет-анализа, в котором используются разные шумы и сигналы с выбором подходящих параметров для шумоподавления. На практике спектр сигнала и спектр шума перекрываются, традиционный метод фильтрации не может обеспечить эффективное удаление шума, и извлечь полезный сигнал.

Вейвлет-преобразования (ВП) – это особый набор ортогональных базисных функций, специально сформированных для фильтрации и прогнозирования тенденций в сигналах. Одним из ключевых преимуществ ВП является то, что он позволяет одновременно учитывать как временное, так и спектральное представление компонентов сигнала [3]. Является специальным математическим инструментом для преобразования данных в информативные вейвлет-коэффициенты таким образом, чтобы каждый коэффициент при определенном разрешении соответствовал своему масштабу.

Важнейшее свойство ВП заключается в том, что оно позволяет анализировать данные в различных масштабах или разрешениях. Таким образом, вейвлеты могут быть выражены вейвлет-функцией $\psi(t)$ и масштабирующей функцией $\phi(t)$ во временной области [1].

Волновая функция и функция масштабирования также называются материнским и отцовским вейвлетами соответственно. Рассмотрим вейвлет-преобразование реального сигнала $p(t)$; выражение $p(t)$ относительно базисной функции $\psi(t)$ вейвлета представлена (1):

$$P(b, a) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} \psi^l\left(\frac{t-b}{a}\right) p(t) dt \quad (1)$$

В уравнении (1) ψ^l обозначает комплексное сопряжение ψ , a – называется параметром масштаба, b – параметром положения.

Если мы определим $\psi a, b(t)$, как:

$$\psi(a, b) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right), \quad (2)$$

что подразумевает сдвиг на b и масштабирование на a , то выражение в уравнении (1) может быть записано как скалярное произведение сигнала $p(t)$ с функцией $\psi a, b(t)$ в виде:

$$P(b, a) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} \psi'_{a,b}(t) p(t) dt. \quad (3)$$

Метод коэффициента вейвлет-разделения – это процедура для удаления шума путем сокращения вейвлет-коэффициентов в домене вейвлета. Метод основан на пороговом сигнале, что каждый вейвлет-коэффициент сигнала сравнивается с заданным порогом. Если коэффициент меньше порога, то он устанавливается на ноль, в противном случае он сохраняется или слегка уменьшается по амплитуде. Мягкое и жесткое пороговое значение используются для удаления искажений сигналов. Использование вейвлетов для удаления шума из сигнала требует идентификации, какие компоненты содержат шум, а затем восстановления сигнала без этих компонентов [2].

Подавление шума сигнала с помощью ВП включает в себя три этапа, а именно декомпозицию, установление порогового значения и реконструкцию. Для декомпозиции и реконструкции сигнала мы используем программную платформу MATLAB. Для устранения помех в информативном сигнале на рисунке 1 представлен 3-й уровень вейвлет-декомпозиции. В MATLAB wavelet toolbox существует несколько семейств вейвлетов. В статье рассмотрена модификация вейвлета Добеши – так называемая Symlets, по той причине, что это семейство вейвлетов обеспечивает плавную и надежную реконструкцию сигнала.

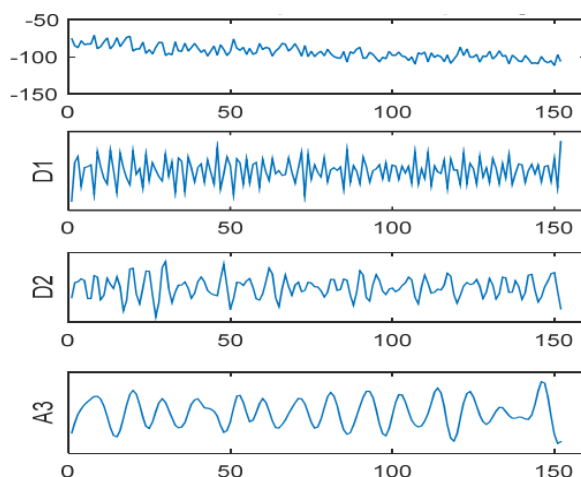


Рис.1. Уровень вейвлет-декомпозиции разложения входного сигнала

Определение порога – имеет дело с выделением исходного сигнала из зашумленной формы сигнала с использованием методов устранения шума. Представлены ниже два наиболее распространенных метода определения порога сигнала, которые являются жестким порогом и мягким поро-

гом; их краткое описание приведено в функциях (4), (5) и на рисунке 2 с помощью MATLAB wavelet toolbox:

$$T_{\lambda}(\tilde{d}; \lambda) = \begin{cases} 0, \text{если } |\tilde{d}| \leq \lambda \\ \tilde{d}, \text{если } |\tilde{d}| > \lambda \end{cases} \quad (4)$$

$$T_M(\tilde{d}; \lambda) = \begin{cases} 0, \text{если } |\tilde{d}| \leq \lambda \\ \text{sign}(\tilde{d}) \cdot \left(|\tilde{d}| - \lambda \right), \text{если } |\tilde{d}| > \lambda, \end{cases} \quad (5)$$

где λ – величина порога, $\tilde{d}$ – обрабатываемый коэффициент разложения (детализирующие коэффициенты, относительная погрешность которых на порядок и более выше, чем у аппроксимирующих коэффициентов).

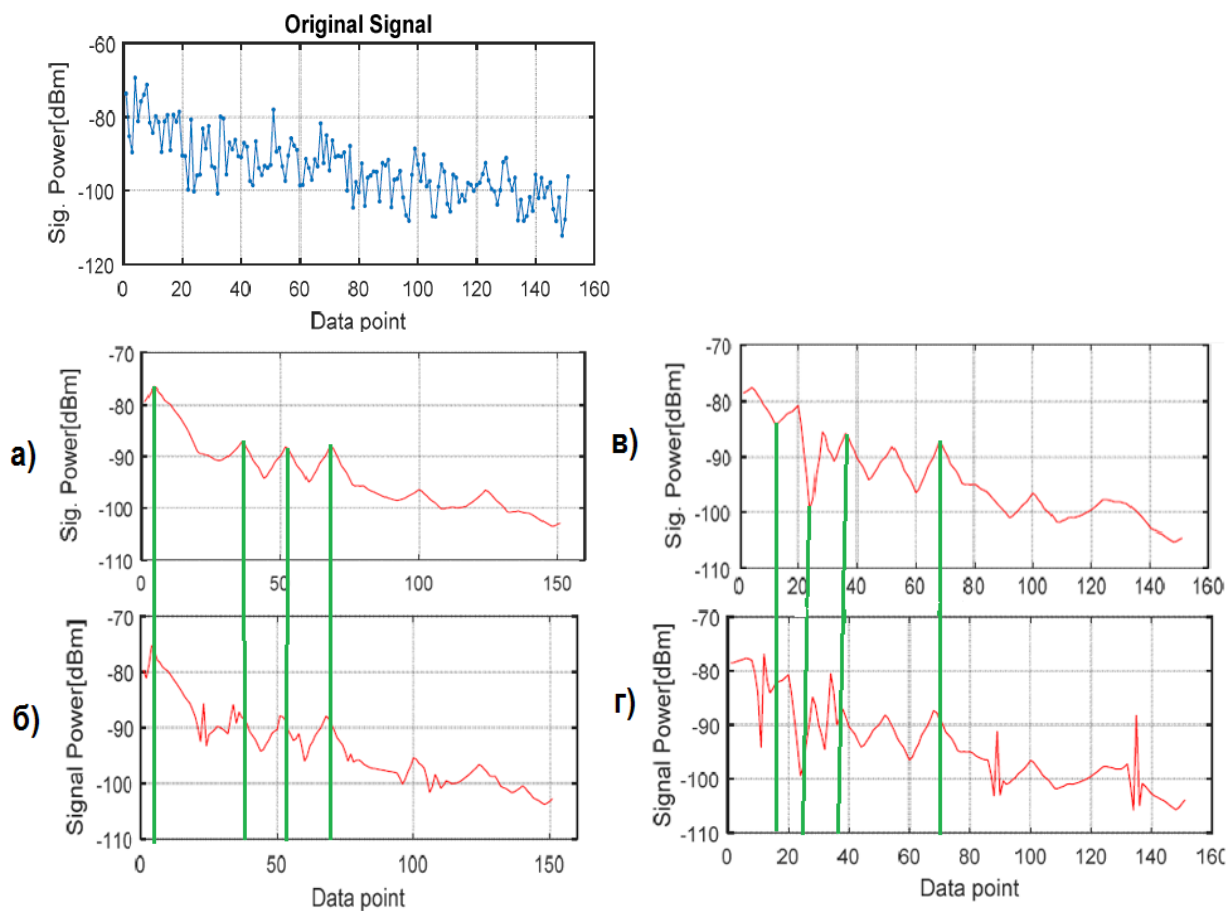


Рис.2. Исследуемый шумовой сигнал и его исходный сигнал с низким уровнем шума с помощью правил установлении пороговых значений для применения к вейвлет-разложению сигнала: Sqtwolog (а,в) и Minimax (б,г)

Ключевой задачей является определение наилучшего порогового значения (λ), которое помогает оценить уровень шума на основе звукового сигнала или данных. В этой работе рассматриваются два правила выбора пороговых значения для применения к вейвлет-разложению сигнала: Sqtwolog и Minimax на программной платформе MATLAB. На графиках рисунка 2 отображены: исследуемый шумовой сигнал и его исходный сигнал с низким уровнем шума с помощью Sqtwolog при плавном (а) и жестком (в) установлении порога, и соответственно исходный сигнал с низким уровнем шума с помощью Minimax при мягком (б) и жестком (г) пороговом значении.

Однако ключевой проблемой при использовании ВП для оптимальной обработки сигналов является определение правильного порогового значения, которое позволяет оценить уровень шума в искаженном сигнале. Если выбранное пороговое значение слишком велико, то некоторые важные компоненты сигнала могут быть отфильтрованы. С другой стороны, если выбранное пороговое значение слишком мало, то в данных все равно будет присутствовать значительное количество шума.

С помощью программной платформы MATLAB выбран 3-й уровень вейвлет-декомпозиции, выполнены вычисления для устранения помех в исследуемом сигнале, представлено сравнение графиков и оптимальный способ снижения уровня шума при мягком и жестком установлении порога из двух правил выбора пороговых значения для применения к вейвлет-разложению сигнала.

СПИСОК ЛИТЕРАТУРЫ

1. Астафьева Н. М. Вейвлет-анализ: основы теории и примеры применения / Успехи физических наук. Обзоры актуальных проблем. – 1996. – Т. 166. – № 11. – С. 1145–1170.
2. Дьяконов В. П. Вейвлеты. От теории к практике. – Москва : СОЛОН-Р. – 2002. – 448 с.
3. Лукьянова А. Н. Вейвлет-преобразование искажений радиосигналов с амплитудно-фазовой модуляцией в квадратурном формирователе // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сборник материалов Всероссийской научно-практической конференции. – Воронеж : Воронежский институт МВД России. – 2020. – С. 17–19.

СВЕДЕНИЯ ОБ АВТОРЕ

Лукьянова Анна Николаевна.
Преподаватель кафедры физики и радиоэлектроники.
Воронежский институт МВД России.
E-mail: annaburavcova@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Lukyanova Anna Nikolaevna.
Voronezh Institute of the Ministry of the Interior of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: анализ сигнала; модулирующий сигнал; шумоподавление; Вейвлет-преобразования.

Keywords: signal analysis; modulating signal; noise reduction; Wavelet transformations.

УДК 621.3

А. С. Лукьянов

ВОЗМОЖНОСТИ ЦИФРОВОЙ СИСТЕМЫ РАДИОСВЯЗИ НА БАЗЕ МНОГОФУНКЦИОНАЛЬНОЙ ПРИВЯЗНОЙ ВЫСОТНОЙ ПЛАТФОРМЫ

THE CAPABILITIES OF A DIGITAL RADIO COMMUNICATION SYSTEM BASED ON A MULTIFUNCTIONAL TETHERED HIGH-RISE PLATFORM

В материале предложены возможности цифровой системы радиосвязи с технологией дистанционного беспроводного энергоснабжения, которая позволяет увеличить время полета БПЛА с цифровыми mesh-ретрансляторами, а также получить высокую эффективность тракта передачи энергии.

The article suggests the possibilities of a digital radio communication system with remote wireless power supply technology, which allows you to increase the flight time of a UAV with digital mesh repeaters, as well as to obtain high efficiency of the energy transmission path.

В настоящее время одним из перспективных технологических направлений является создание систем дифракции быстрых электронов (ДБЭ) беспилотных летательных аппаратов (БПЛА), при размещении на них полезной нагрузки в виде ретрансляторов для систем радиосвязи. Оптимальной транспортной средой для дистанционной передачи электрической энергии является лазерное излучение, представляющее собой узконаправленный пучок монохроматического инфракрасного излучения. Лазер способен передавать энергию как для летящих, так и зависающих беспилотных аппаратов, что даёт им возможность неограниченное время находиться в воздухе и выполнять функции радио ретрансляторов [3].

Стандарт цифровой радиосвязи DMR предназначен для работы в рамках существующих лицензируемых частотных диапазонов с разносом частотных каналов 12,5 кГц, используемых в сухопутной подвижной ра-

диосвязи. DMR обеспечивает передачу голоса, данных и других дополнительных услуг.

Стандарт DMR подразделяется на несколько направлений:

«Tier I» – маломощные коммерческие рации;

«Tier II» – оборудование профессиональных конвенциональных систем радиосвязи;

«Tier III» – профессиональные системы цифровой транкинговой радиосвязи.

Для размещения на БПЛА рассмотрим mesh-ретранслятор компании Hitera E-pack100.

Ретрансляторы Hytera E-pack имеют возможность размещения на базе БПЛА, благодаря конструктивному исполнению в виде пыле- и влагозащитного корпуса (IP67), невысокой мощности передатчика (от 5 Вт до 20 Вт), низкому потреблению электроэнергии и малому весу (от 1,5 до 3,6 кг с встроенным аккумулятором в зависимости от исполнения).

E-pack 100 – переносной цифровой автономный приемопередающий модуль, который можно использовать независимо, не полагаясь на другие внешние средства, такие как системы электропитания и IP-сети. Ретранслятор разработан в виде интеллектуальной коммуникационной платформы, предлагающий максимальную универсальность для подключения различных систем и обеспечения их бесперебойного взаимодействия.

Парк абонентских радиостанций выполнен в виде компактной, легкой, с обтекаемой формой, обладают совместимостью с классом защиты IP67, выдерживают погружение на глубину до 1 м на 30 минут и более.

Рассмотрим случай подъема нагрузки весом 500 г на высоту 25-30 м с потреблением по питанию около 20-30 Вт (видеокамера, ретранслятор, модем). Критерием для выбора номинала питающего напряжения является типовое бортовое питание коптера около 12 В (3S), при токах около 20-25 А, которое используется в коптерах с полетным весом от 1,2 до 1,5 кг. С учетом дополнительной бортовой нагрузки задаем максимальный ток потребления до 30 А, т.е. мощность наземной станции должна быть не менее 360 Вт. В то же время, подавать на полетную платформу постоянное напряжение номиналом 12 В недопустимо, т.к. в этом случае толщина и соответственно масса питающих кабелей будут неприемлемо высокими. С учетом оптимального сочетания ток/вес/удельное сопротивление/потери можно выбрать витую пару МГТФ сечением 0,35-0,5 мм².

Так, например, витая пара МГТФ-0,5 имеет удельный вес 6,25 г/м, и удельное сопротивление 0,039 Ом/м. При высоте подъема 30 м (общая длина кабеля составит 60 м) сопротивление кабеля составит 2,4 Ома, а вес – 675 г.

Допустимый ток по МГТФ-0,5 в обдуваемой витой паре может быть до 6-7 А. То есть, если подавать с наземной питающей станции напряжение

номиналом 60 В с током 6-7 А, то на бортовой преобразователь дойдет постоянное напряжение (за вычетом потерь) около 45 В.

На рисунке представлена принципиальная схема наземной станции питания и бортового конвертера (преобразователя) напряжения.

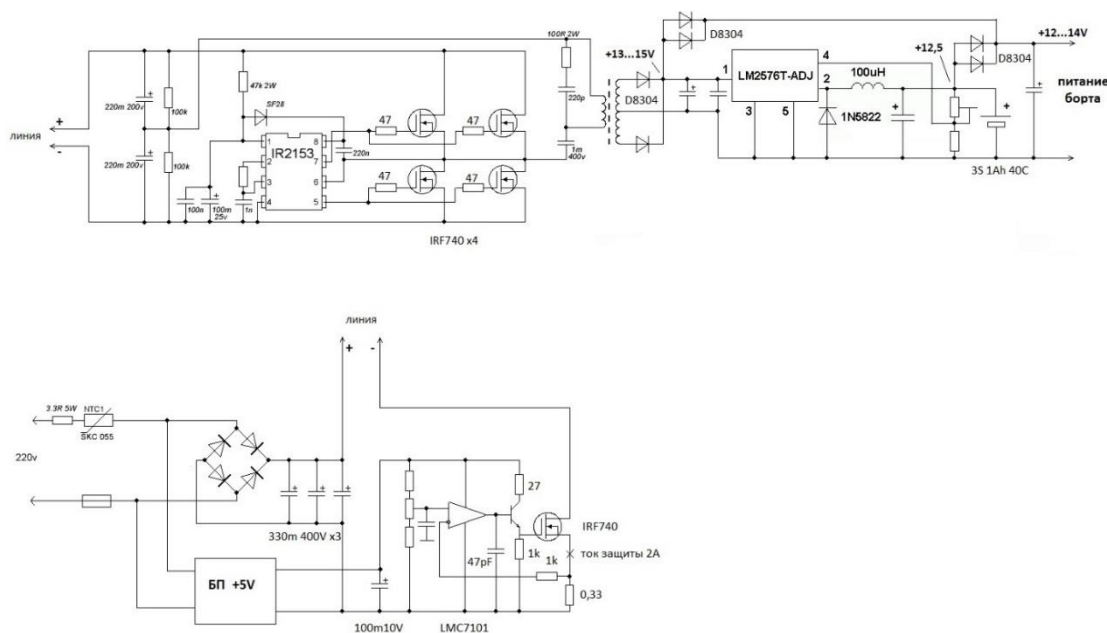


Рис. 1. Принципиальная схема наземной станции питания и бортового конвертера (преобразователя) напряжения

На наземной станции питания реализована токовая отсечка на 2 А. На коптер подается напряжение номиналом 300-320 В с током около 1 А. Кабель сечением 0,35 мм² допускает прохождение длительного тока до 4 А. Основная емкость 1000 мкФ на наземной станции. На коптере (в левой половине схемы вверху) размещен стандартный конвертор. Несмотря на хорошее охлаждение транзисторов, при их длительной работе возможен перегрев кристаллов, поэтому применено их параллельное включение.

На выходе преобразователя формируется нестабилизированное напряжение от 13 до 16 В, что допустимо для бортовых регуляторов оборотов. Для зарядки литиевого аккумулятора реализован отдельный стабилизатор на микросхеме LM2576 строго на 12,5 В. Аккумулятор будет включаться в работу в случае пропадания или больших скачков напряжения бортового питания. Развязка по выходному питанию осуществляется через быстродействующие мощные диоды Шотки D8304 [1].

Номинальный режим работы коптера обеспечивается после 2 минут работы от наземной станции питания. В этом режиме питанием обеспечиваются все узлы полетной платформы и навесного оборудования, включая ретрансляторы стандарта DMR. Также обеспечивается заряд резервной аккумуляторной батареи.

При решении задач радиосвязи с помощью БПЛА учитываются основные полетные характеристики: грузоподъемность (в пределах 0,1-7 кг), время полета и управляемость взлетом, посадкой и нахождением в точке зависания. Предлагаемая технология дистанционного беспроводного энергоснабжения позволит увеличить время полета БПЛА, работающих от аккумуляторов, вплоть до круглосуточного нахождения в воздухе без посадки, что позволит повысить эффективность использования БПЛА для системы радиосвязи.

В состав структурной схемы входят следующие элементы:

- БПЛА квадрокоптерного типа, дополнительно оснащенный: цифровым mesh-ретранслятором стандарта DMR с приемо-передающей антенной; основным и резервным аккумуляторными блоками; Ethernet-модемом передачи данных; приемником-преобразователем лазерного излучения; резервным GSM-модемом;

- комплекс лазерного питания БПЛА, включающий в себя: первичный источник питания, источник питания и охлаждения лазера, лазер, лучевую станцию, систему наведения лазерного луча на приемник-преобразователь БПЛА, высокоскоростную цифровую видеокамеру с оптико-механическим объективом;

- ведущий наземный mesh-ретранслятор стандарта DMR;

- 4 группы цифровых абонентских радиостанций стандарта DMR;

- радиосервер управления стандартом DMR;

- радиодиспетчер стандарта DMR.

Принцип действия структурной схемы заключается в следующем. Квадрокоптер с дополнительно установленным оборудованием за счет штатных аккумуляторных блоков поднимается на высоту от 20 до 100 метров относительно земной поверхности и фиксируется в точке зависания с помощью бортовой системы позиционирования. Допускается отклонение от исходной точки в пределах нескольких метров в зависимости от силы бокового ветра.

В процессе работы квадрокоптера происходит естественный процесс разряда аккумуляторных батарей, который с учетом веса дополнительно установленного оборудования ограничивает его полетное время. С целью поддержания полетного режима квадрокоптера вместо привязного питания может использоваться наземная система дистанционного энергоснабжения, в которой монохроматическое излучение источника формируется в малорасходящийся пучок, наводимый с помощью высокоскоростной цифровой видеокамеры с оптико-механическим объективом на приемник-преобразователь, закрепленный на летательном аппарате и подключенный к аккумуляторному блоку для его зарядки. Существует два типа дистанционного энергоснабжения – непрерывный и периодический.

Данная технология дистанционного беспроводного энергоснабжения позволит увеличить время полета БПЛА с цифровыми mesh-

ретрансляторами, работающих от аккумуляторов, вплоть до нахождения в воздухе 24 часа в сутки без посадки. Основные преимущества – высокая эффективность тракта передачи энергии (до 40%), возможность использования небольших по размерам приемников (до 100 мм в диаметре), масса которых не превышает 0,1 кг.

Основными характеристиками системы лазерного питания, состоящей из полупроводниковых лазеров и фотоэлектрических преобразователей, являются: КПД, коэффициент отражения и коэффициент пропускания оптических компонентов системы формирования пучка.

Следовательно, на расстояниях порядка 1 км пятно излучения будет порядка $D_{1\text{км}}=40$ см. В ближней зоне (менее 500 метров) возможно уменьшение пятна путем фокусировки до 3-10 см без потери эффективности, что дает возможность использовать такую оптическую систему для дистанционного снабжения БПЛА, а небольшое фокусное расстояние позволяет сделать компактную систему.

Таким образом, при расстоянии от станции лазерного питания до квадрокоптера, равном 100 метрам, пятно излучения будет порядка $D_{100\text{м}}=2$ см без потери эффективности питающего аккумулятор излучения. В сочетании с применением LiFePO₄-аккумуляторов очевиден экономический выигрыш.

СПИСОК ЛИТЕРАТУРЫ

1. T-motor Flame 60A ESC. – URL: <https://www.foxtechfpv.com/t-motor-flame-60a-esc.html> (дата обращения 17.10.2024).
2. Айхлер Ю. Лазеры. Исполнение, управление, применение / Ю. Айхлер, Г. И. Айхлер. – Москва : Техносфера, 2008. – 440 с.
3. Шрёдер Г. Техническая оптика / Г. Шрёдер, Х. Трайбер. – Москва : Техносфера, 2006. – 424 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Лукиянов Александр Сергеевич.

Старший преподаватель кафедры инфокоммуникационных систем и технологий.

Кандидат технических наук.

Воронежский институт МВД России.

E-mail: las92@yandex.ru

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

Lukyanov Alexander Sergeyevich.

Senior teacher of department of infocommunication systems and technologies.

Candidate of Technical Sciences.

E-mail: las92@yandex.ru
Voronezh Institute of the Ministry of the Interior of Russia.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: беспилотный летательный аппарат; радиосвязь; питание.

Keywords: unmanned aerial vehicle; radio communication; nutrition.

УДК 623.746

Р. М. Ляшко, В. А. Николаев, Н. В. Талышев

**ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ
ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ**

**PROMISING AREAS OF APPLICATION OF ARTIFICIAL
INTELLIGENCE TECHNOLOGIES IN THE ACTIVITIES
OF LAW ENFORCEMENT AGENCIES**

В статье рассмотрены направления применения технологий искусственного интеллекта в деятельности правоохранительных органов Российской Федерации, отмечены основные проблемы внедрения технологий нормативно-технического характера и пути их решения.

The article examines the areas of application of artificial intelligence technologies in the activities of law enforcement agencies of the Russian Federation, highlights the main problems of implementing technologies of a regulatory and technical nature and ways to solve them.

В последние годы совершенствование элементной базы, развитие технологий и алгоритмов обработки данных (в том числе «больших данных») предопределили интенсивное проникновение технологий искусственного интеллекта (далее – ИИ) во все сферы функционирования государств, гражданского общества, бизнеса и жизнедеятельности каждого человека.

В Российской Федерации основные направления развития технологий ИИ определены в Национальной стратегии развития искусственного интеллекта на период до 2030 года [1]. В документе одной из целей развития искусственного интеллекта определено «обеспечение национальной безопасности и правопорядка», реализуемое, в том числе через массовое внедрение наиболее эффективных технологических решений.

Проводимые в ФКУ «НИЦ «Охрана» Росгвардии исследования, позволяют выделить следующие перспективные направления применения технологий ИИ:

Первое направление – это распознавание человека по биометрическим признакам, в частности по лицу. Это сложное и неоднозначное с точки зрения нормативно-правового регулирования направление, которое имеет огромное значение для обеспечения общественной безопасности и повышения эффективности функционирования систем охраны объектов.

Технология распознавания по лицу осуществляется на основе сравнения характерных точек на идентифицируемом лице с имеющейся базой облаков точек, поставленных в соответствие конкретному человеку. Применение искусственного интеллекта в процессе аналитической выборки совокупности точек в условиях внешних динамических или преднамеренно создаваемых маскирующих шумов позволяет значительно увеличить вероятность распознавания объекта контроля и повысить эффективность принятия системой обоснованного решения.

В перспективе такие решения будут все шире внедряться в различные технические средства и системы, используемые правоохранительными органами – от систем обеспечения безопасности охраняемых объектов и средств противодействия проникновению до носимых видеорегистраторов.

В условиях возрастания криминогенности обстановки и уровня террористической опасности становится важным выявление на самых ранних стадиях явных или преднамеренно скрываемых признаков возникновения угрозы охраняемому объекту, а также физическим лицам, находящимся на его территории. Для решения указанной задачи получили свое развитие два взаимосвязанных направления технологий искусственного интеллекта – это ситуационная аудио- и видеоаналитика.

Проводимые в настоящее время исследования и результаты испытаний ряда из присутствующих на рынке систем показывают невозможность их применения в качестве основных технических систем охраны из-за значительного количества ложных срабатываний (как ложноположительных, так и ложноотрицательных ошибок), достигающих 20%. Это связано преимущественно с рядом нерешенных на сегодняшний день вопросов.

Так, например, одним из основных проблемных вопросов применения аудиоаналитики для выявления выстрелов является сложность формирования обучающих наборов данных для нейросети, исходными элементами для которых являются аудиозаписи выстрелов. Это связано с разнообразием огнестрельного оружия, зависимостью аудиозаписей от качества микрофонов и акустической аппаратуры, различной акустической обстановкой на объектах и имеющимися переотражениями звука.

Анализ речи на предмет выявления контрольных фраз для регистрации тревожных событий также на порядок сложнее решённых в телефонных помощниках как в силу уже указанных причин, так и в связи с

необходимостью исключения хулиганских действий, направленных на срыв работы объекта охраны.

Схожие проблемы возникают и при реализации видеоаналитики. Например, в ходе тестирования модулей видеоаналитики разных производителей на предмет выявления оружия установлено, что на качество распознавания влияют даже тени, блики и погодные условия.

Указанные проблемы пока не позволяют автоматически формировать извещения о тревоге без дополнительного контроля человеком, однако их применение в дополнение к традиционным средствам обнаружения и тревожной сигнализации является перспективным по ряду направлений – от подтверждения тревожных ситуаций до распознавания перемещения нарушителя с оружием, выявления выстрелов, контроля преднамеренно оставленных предметов и т.п. Их применение позволит повысить вероятность обнаружения нарушителя, уйти от пресловутого человеческого фактора при работе тревожной сигнализации и минимизировать количество ложных тревог, снизив нагрузку на группы задержания (патрули, наряды).

Следующим перспективным направлением является внедрение технологий ИИ в системы поддержки принятия решений (далее – СППР).

На примере практической деятельности сотрудников дежурных смен подразделений вневедомственной охраны, осуществляющих оперативное управление нарядами, следует отметить, что такая деятельность сопряжена с необходимостью быстрого принятия эффективных решений в условиях повышенных информационных нагрузок и внешних отвлекающих факторов. Применение ИИ в перспективных системах поддержки принятия решений позволит на основе анализа всей совокупности сложившихся условий осуществлять просчет их влияния на вероятность успешного решения поставленных задач и в автоматическом режиме предлагать дежурному наиболее эффективные алгоритмы действий (сколько и какие экипажи задействовать при тревоге, траектории их движения с учетом складывающейся оперативной и дорожной обстановки и другие).

Применение искусственного интеллекта в этой сфере в перспективе позволит снизить время реакции сил охраны на тревожные события, повысить эффективность обеспечения безопасности объектов, а также снизит нагрузку на операторов локальных систем охраны и пультов централизованного наблюдения за счет представления подготовленных сценариев действий, а в дальнейшем и за счет полной автоматизации некоторых сценариев.

Следующим направлением, перспективным с точки зрения применения современных технологий, является оптимизация затрат рабочего времени сотрудников и работников правоохранительных органов за счет автоматизации рутинных задач. По многим аспектам деятельности данное направление увязано с необходимостью проведения анализа существующих процессов и принятия организационных решений по их предварительной оптимизации, однако существуют и мероприятия, не требующие такой

подготовки. К таким, например, относится применение интеллектуальных голосовых помощников, интегрированных в комплекс средств автоматизации пунктов централизованной охраны. Внедрение данной технологии в перспективе позволит повысить автоматизацию проверки технических средств охранной сигнализации на объекте, значительно снизив нагрузку на операторов пультов централизованного наблюдения в пиковые часы нагрузки, а также позволит снять часть организационных задач с сотрудников подразделений вневедомственной охраны.

Ситуационное моделирование на основе цифровых двойников – еще одно направление, наибольшая практическая польза от которого возможна только с применением технологий искусственного интеллекта. Для создания цифрового двойника охраняемого объекта проводится его оцифровка, то есть представление данного объекта, размещенных на нем систем безопасности и окружающей его обстановки, сил и средств обеспечения безопасности и нарушителя, а также персонала и возможных посетителей, в виде облаков точек, каждой из которых поставлен в соответствие характеризующий её набор данных. Кроме того, облака точек в зависимости от вариантов их действий или реакций на воздействия динамически меняют свою пространственную конфигурацию, а как следствие изменяются и наборы данных, соответствующие им [2].

Компиляция совокупности цифровых двойников в прикладное программное обеспечение трехмерной визуализации предоставляет возможность осуществления многовариантного ситуационного моделирования (десятки и сотни тысяч ситуаций), которое на основе сравнительного анализа при различных начальных условиях позволяет автоматизированным способом оценить вероятность эффективности предлагаемых решений и выбрать наиболее оптимальное из них [3].

Для реализации этого направления, в ФКУ «НИЦ «Охрана» Росгвардии планируются к проведению исследования по созданию единого программно-аппаратного комплекса, состоящего из средств сбора информации (лидар, средство фотофиксации, беспилотные авиационные системы), обработки и преобразования информации в унифицированный формат данных (цифровых моделей). При этом предполагается, что данный комплекс должен будет максимально обеспечивать автоматизацию каждого из этапов занесения, интерпретации и обработки информации, иметь подробную базу данных типовых элементарных объектов, их реакций и средства ее редактирования.

Реализация такого подхода позволит обеспечить достоверность решения по обоснованности заключения об устойчивости объекта к угрозам, реализуемым моделями нарушителей, предусмотренными паспортом безопасности объекта. Особенно это касается подготовленных высоко мотивированных нарушителей, имеющих гибкий алгоритм действий при совершении актов незаконного вмешательства.

Кроме приведенных выше направлений, технологии искусственного интеллекта могут применяться в технических средствах и системах обнаружения, сопровождения и наблюдения нарушителя на охраняемых объектах большой площади или прилегающей акватории.

В настоящее время уже есть практические решения по их использованию:

- в радиолокационных и тепловизионных средствах обнаружения, для защиты больших территорий охраняемых объектов;
- в перспективных гидроакустических средствах обнаружения для защиты акваторий объектов, в том числе от угроз применения беспилотных аппаратов;
- в комплексах технических средств для обнаружения пролетов беспилотных воздушных судов в зоне расположения охраняемых объектов;
- в волоконно-оптических средствах обнаружения для защиты протяженных периметров охраняемых объектов.

Внедрение технологий искусственного интеллекта в технические решения при создании систем безопасности позволяет обеспечить защиту охраняемых объектов от новых типов угроз (например, воздушных или морских беспилотных аппаратов) или уменьшить количество технических средств охраны с сохранением требуемого уровня защиты вероятному воздействию угроз и снижением рисков ошибочных действий, обусловленных человеческим фактором.

Вместе с тем, для подобных систем остро стоит проблема поиска непредвзятого решения, требующего репрезентативный, релевантный и корректно размеченный набор данных. Другими словами, для обучения таких систем остро стоит вопрос формирования больших массивов данных (датасетов).

Для применения в связке с такими средствами обнаружения перспективно применение беспилотных систем, предназначенных для видеоподтверждения тревоги и наблюдения за нарушителем.

В рамках уже проведенных ФКУ «НИЦ «Охрана» Росгвардии исследований определены ряд направлений применения беспилотных систем в деятельности правоохранительных органов:

- осуществление видеоподтверждения при извещении о тревоге от периметральных средств обнаружения, не оборудованных телевизионной охранной системой,
- наблюдение за нарушителем при его передвижении по объекту большой площади или его территории с протяженным периметром, а также попытке скрыться с места правонарушения;
- проведение предварительного осмотра места правонарушения при поступлении извещений о тревоге (например, проникновении на объект);
- наблюдение обстановки при обеспечении безопасности массовых мероприятий;

– осмотр собственных объектов при проведении мероприятий по антитеррористической защищенности, в том числе для задач контроля радиационной опасности.

Использование беспилотных систем в комплексных системах охраны объектов позволит повысить оперативность и эффективность действий за счет большей информации сотрудников о нарушителях, их действиях, числе, составе, вооружении, транспортном оснащении. Кроме того, скоростные характеристики беспилотных систем позволяют в несколько раз увеличить производительность поиска.

При этом применение беспилотных систем способно снизить угрозу жизни и здоровью сотрудников правоохранительных органов от внезапного нападения, а также при контакте с взрывчатыми веществами и взрывными устройствами, объектами радиационной, химической и биологической опасности.

Таким образом внедрение искусственного интеллекта в деятельность сотрудников правоохранительных органов является одним из самых перспективных векторов развития информационных технологий.

Вместе с тем их применение в области обеспечения безопасности объектов связано с рядом насущных взаимосвязанных проблем, к основным из которых относятся:

- отсутствие методических рекомендаций по разработке технических решений и применению готовых изделий, имеющих свою специфику;
- низкий технический уровень ряда имеющихся на рынке решений;
- сложности сбора данных для создания обучающего датасета для нейросети, особенно специфической направленности, а также при необходимости дообучения на объекте;
- отсутствие доверия специалистов в области охраны к техническим решениям, реализуемым с применением технологий ИИ;
- высокая стоимость сторонней разработки и конечных решений в области ИИ;
- отсутствие достаточной нормативно-технической базы в области терминологии, технических требований и методов испытаний технических средств и комплексов с ИИ.

На проблеме формирования национальной нормативно-технической базы стоит остановиться чуть подробнее, так как несмотря на активизацию деятельности по указанному направлению, такая деятельность в ряде случаев неоптимальна по следующим причинам:

1) далеко не всегда оправданной разработки национальных нормативно-технических документов, основанной на непосредственном использовании текстов международных стандартов (применение «метода обложки»). С одной стороны опора на мировой опыт является залогом зрелости и полноты Российской системы стандартизации, однако не следует забывать, что российские ГОСТы включают в себя конкретные требования к

продукции, процессам производства, методикам контроля, нередко они содержат подробные технические спецификации и методы испытаний. В свою очередь в международных стандартах обычно отражены общие принципы и подходы и в целом они носят более общий характер, очерчивая рамки, но оставляя свободу для адаптации под условия каждого из участников их разработки, а их практическая составляющая во многом вынесена на уровень ниже и реализуется на национальном уровне каждой из стран. Таким образом, активное применение «метода обложки» при формировании национальной нормативно-технической базы приводит к недостаточной практичности вновь разрабатываемых документов;

2) второй причиной является нередкое игнорирование мероприятий по регистрации официальных переводов зарубежных нормативно-технических документов, принимаемых за основу для разработки национальных стандартов с целью исключения возможных случаев некорректного перевода, усложняющего восприятие текстов и/или вовсе искажающего смысл положений исходных документов.

3) третья причина – большое количество одновременно разрабатываемых документов, что нередко превышает возможности экспертов по их детальной проработке.

В результате, к сожалению, иногда количество превалирует над качеством и в предлагаемых на рассмотрение проектах документов нередко встречается:

- наличие общих (неподкрепленных фактами) оценочных суждений, характерных для зарубежных нормативно-технических документов, но нецелесообразных в национальных;

- излишнее применение англицизмов в случаях, когда зарубежному термину или выражению есть самодостаточный синоним, широко применяемый в России;

- недостаточная проработка предлагаемого к стандартизации терминологического аппарата, например, дублирование уже существующих терминологических статей, которые по смыслу изложения, присутствующему в принятых на национальном уровне документах по стандартизации не требуют уточнения.

- неполное раскрытие предметной области предлагаемого на рассмотрение проекта стандарта даже при условии наличия подобных по объекту и предмету стандартизации и принятых на национальном уровне нормативно-технических документов в смежных областях;

4) в качестве четвертой причины хотелось бы отметить несбалансированность и незавершенность работ в области разработки национальных стандартов. В частности, разрабатывается и планируется к разработке достаточно много национальных стандартов регламентирующих общие положения, термины и определения, однако до разработки технических требований, а главное методов испытаний – дело доходит редко.

Указанные проблемы не являются новыми. Организациями-разработчиками технологий и их потенциальными заказчиками проводится работа по каждой из представленных выше проблем и в обозримом будущем они найдут свое решение, однако более качественное и скорейшее решение указанных проблемных вопросов возможно посредством:

- расширения межведомственного взаимодействия в области подготовки и обмена исходными данными специфической направленности для обучения нейросетей;

- расширения межведомственного информационного обмена в части разработанных решений, технологий, средств, использования единых или адаптированных решений для решения смежных задач других ведомств;

- расширения межведомственного научно-практического взаимодействия для выработки единых подходов к созданию нормативно-технических документов и проведения единой технической политики в области технических средств безопасности, использующих технологии искусственного интеллекта;

- более тщательного планирования мероприятий по развитию национальной стандартизации, которые должны обеспечивать возможность более качественной проработки документов и быть в большей степени направлены на достижение целей стандартизации Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ

1. О развитии искусственного интеллекта в Российской Федерации : указ Президента Российской Федерации от 10 октября 2019 г. № 490.

2. Николаев В. А., Прошутинский Д. А., Талышев Н. В. Перспективы создания программно-аппаратного комплекса средств цифрового моделирования для повышения эффективности служебной деятельности правоохранительных органов / Информатизация и информационная безопасность правоохранительных органов : сборник трудов Международной научно-практической конференции / под общ. ред. А. В. Бецкова [и др.]. – Москва : Академия управления МВД России, 2024. – С. 216–221.

3. Программное обеспечение для имитационного моделирования и анализа эффективности системы безопасности. – URL: https://iter.ru/model_sfz.html (дата обращения: 10.10.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Ляшко Роман Михайлович.

Научный сотрудник развития инновационных решений, цифровых технологий и программного обеспечения.

ФКУ «НИЦ «Охрана» Росгвардии

E-mail: lyashkorm@rosgvard.ru

Россия, 111539, г. Москва, ул. Реутовская, д. 12Б.

Николаев Владимир Анатольевич.
Начальник отдела развития инновационных решений, цифровых технологий и программного обеспечения.

ФКУ «НИЦ «Охрана» Росгвардии.

E-mail: nikolaevva@rosgvard.ru

Россия, 111539, г. Москва, ул. Реутовская, д. 12Б.

Талышев Николай Васильевич.

Главный научный сотрудник отдела развития инновационных решений, цифровых технологий и программного обеспечения.

Кандидат технических наук, доцент.

ФКУ «НИЦ «Охрана» Росгвардии.

E-mail: talishevnv@rosgvard.ru

Россия, 111539, г. Москва, ул. Реутовская, д. 12Б.

Lyashko Roman Mikhailovich.

Researcher at the Department of Development of Innovative Solutions, Digital Technologies and Software.

Federal state institution «Scientific Research Center «Protection» of Rosgvardiya.

E-mail: lyashkorm@rosgvard.ru

Russia, 115539, Moscow, Reutovskaya Str., 12B.

Nikolaev Vladimir Anatolyevich.

Head of the Department of Development of Innovative Solutions, Digital Technologies and Software.

Federal state institution «Scientific Research Center «Protection» of Rosgvardiya.

E-mail: nikolaevva@rosgvard.ru

Russia, 115539, Moscow, Reutovskaya Str., 12B.

Talyshev Nikolay Vasilyevich.

Chief Researcher of the Department of Development of Innovative Solutions, Digital Technologies and Software.

Candidate of Technical Sciences, Associate Professor,

Federal state institution «Scientific Research Center «Protection» of Rosgvardiya.

E-mail: talishevnv@rosgvard.ru

Russia, 115539, Moscow, Reutovskaya Str., 12B.

Ключевые слова: искусственный интеллект; видеоаналитика; аудиоаналитика; поддержка принятия решений; голосовой помощник; ситуационное моделирование.

Keywords: artificial intelligence; video analytics; audio analytics; decision support; voice assistant; situational modeling.

УДК 004.93:519.816:519.876.6.

Е. В. Прокофьева, П. С. Порываева

**ВИРТУАЛЬНЫЕ ТЕХНОЛОГИИ
И ТЕХНОЛОГИИ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ
ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ МВД РОССИИ**

**VIRTUAL TECHNOLOGIES
AND AUGMENTED REALITY TECHNOLOGIES
IN THE TRAINING OF SPECIALISTS
OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA**

Перспективы применения новейших технологий виртуальной и дополненной реальностей в сфере инновационного образования обусловлены стремительным развитием и внедрением информационно-коммуникационных технологий [1]. Изучаемые технологии рассматриваются в поле практического применения при подготовке специалистов системы МВД России.

The prospects for the application of the latest technologies of virtual and augmented reality in the field of innovative education are determined by the rapid development and implementation of information and communication technologies [1]. The technologies studied are considered in the field of practical application in the training of specialists of the Russian Ministry of Internal Affairs system.

Современное состояние науки и техники, стремительное развитие новых технологий не могло не оказать влияние на образовательный процесс. Технологии виртуальной и дополненной реальностей не являются новыми, однако в образовании реализуются относительно недавно.

В контексте изучаемого вопроса, виртуальная реальность понимается искусственно созданным программными средствами пространством на основании компьютерных технологий, через имитацию реального мира посредством компьютерной графики. На сегодняшний день к виртуальным технологиям в основном относят технологии виртуальной и дополненной (VR, AR).

Технология виртуальной реальности создает техническими средствами виртуальный мир, воспринимаемый человеком через ощущения, путем полного погружения в него. Достижение эффекта погружения (иммерсивности) требует применения специальных устройств – VR-очков, шлемов, перчаток, наушников, обеспечивающих максимальный эффект присутствия [2].

Известны успешные примеры применения VR технологий в образовательной деятельности, с 2018 года запущен целый ряд крупных образовательных VR-программ: «Образование-2024»; «Цифровая школа»; «Со-

временная цифровая образовательная среда»; «Цифровая экономика Российской Федерации» и др.

В основе обучения с применением виртуальной реальности лежат иммерсивные технологии реализуемые посредством виртуального расширения реальности, позволяющие воспринимать и понимать окружающую действительность в превалентном виде, с полным погружением в заданную событийную среду.

Преимуществом иммерсивного подхода является: наглядность, позволяющая детально рассмотреть объекты и процессы, которые невозможно или очень сложно проследить в реальном мире; сосредоточенность, исключая в виртуальном мире внешнее воздействие на обучающегося, обеспечивая сконцентрированность на материале и лучшем его усвоении; вовлечение, реализующее обучение с высокой точностью запрограммированности и контроля; а также безопасность и эффективность [3].

Сегодня создаются платформы виртуальной реальности для реализации образовательного процесса. Мобильный класс виртуальной реальности «PolyVR» [4] позволяет организовывать образовательный процесс в динамичной форме, создавая эффект погружения в изучаемую проблематику, развивает эмоциональную сферу и воображение обучающихся, открывая возможности для творчества с 3D-моделированием, повышая мотивацию и вовлеченность обучающихся, расширяя их кругозор.

Имеются примеры реализации VR-технологий и в вузах системы МВД России. В Волгоградской академии МВД России используются современные VR-технологии в рамках образовательного процесса для закрепления навыков применения технико-криминалистических средств в заданных условиях [5]. В своей работе Р. А. Грязнов [6] отмечает целесообразность и эффективность использования технологий виртуальной реальности при подготовке сотрудников правоохранительных органов, реализуя наиболее эффективный способ передачи информации.

Отличие технологии дополненной реальности от описанной выше, заключается в дополнении реального мира виртуальными объектами посредством применения AR-очков, AR-шлемов, смартфонов и планшетов [2]. Камера устройства фиксирует кадр из реального мира, после чего программа AR добавляет к ней виртуальные объекты, в результате на экране устройства визуализируется реальность с изменёнными параметрами. Как справедливо отмечает в своей работе Е. Г. Бижанов [7], технологии дополненной реальности позволяют обучающимся быть вовлеченным в явления, которые трудно реализуемы или опасны в реальном мире. Посредством современной технологии возможно визуализировать сложные пространственные решения и абстрактные концепции, а также отрабатывать необходимые практики и навыки с расширенными возможностями обучения. AR-технологии обеспечивают повсеместное, совместное и дистанционное

обучение, ощущение присутствия, непосредственности и погружения обучающихся [7].

В образовательном процессе вузов системы МВД России применение технологий дополненной реальности проходит стадию активного внедрения с целью интеграции в образовательный процесс современных технологий, обеспечивающих высокоэффективную подготовку специалистов для реализации задач ОВД, через трансформацию полученного теоретического знания в практический опыт. В работе И. Н. Горбулинской и И. В. Трущенко [8] сообщается о возможности использования технологий дополненной реальности в целях визуализации криминалистических объектов и обучении криминалистике.

VR- и AR-технологии позволяют реализовать полное погружение обучающихся в искусственно созданный мир в рамках образовательного процесса с целью эффективного изучения материала и отработки полученных навыков в моделируемых ситуациях [9].

Актуальные тенденции свидетельствуют о том, что со временем технологии виртуальной и дополненной реальности повсеместно будут внедрены в образование с целью подготовки специалистов МВД России [4].

СПИСОК ЛИТЕРАТУРЫ

1. Набокова Л. С., Загидуллина Ф. Р. Перспективы внедрения технологий дополненной и виртуальной реальности в сферу образовательного процесса высшей школы // Профессиональное образование в современном мире. – 2019. – Т. 9. – № 2. – С. 2710–2717.
2. Виртуальные технологии. Краткий обзор. – URL: <https://svega-computer.ru/news/340/?ysclid=m1z1ysxs3w385321428> (дата обращения: 02.10.2024).
3. Виртуальная реальность в образовании. – URL : <https://hsbi.hse.ru/articles/virtualnaya-realnost-v-obrazovanii/?ysclid=m1sxjwo8dq261785768> (дата обращения: 02.10.2024).
4. PolyVR – мобильный класс виртуальной реальности. – URL : <https://polymedia.ru> (дата обращения: 05.10.2024).
5. На кафедре предварительного расследования Волгоградской академии МВД России проведено открытое практическое занятие с применением VR-технологий. – URL : <https://ва.мвд.пф/Press-sluzhba/Novosti/item/43047008>
6. Грязнов С. А. Использование технологии виртуальной реальности при подготовке сотрудников правоохранительных органов // Вестник Самарского юридического института. – 2021. – №1 (42). – С. 101–105.
7. Бижанов Е. Г. Технологии дополненной реальности в образовательной сфере (обзор) // Молодой ученый. – 2020. – № 31 (321). – С. 10–12. – URL: <https://moluch.ru/archive/321/72914/> (дата обращения: 5.10.2024).
8. Горбулинская И. Н., Трущенко И. В. Технологии искусственного интеллекта и дополненной реальности в экспертно-криминалистической

деятельности органов внутренних дел // ADVANCES IN LAW STUDIES. – 2022. – Т. 10. – № 4. – URL : <https://naukaru.ru/ru/nauka/article/55383/view> (дата обращения: 02.10.2024)

9. Дополненная реальность: что такое AR, описание технологии, перспективы развития. – URL : <https://skillbox.ru/media/management/kak-rabotaet-tekhnologiya-dopolnennoy-realnosti-ar-i-chem-ona-polezna-biznesu/?ysclid=m1sxs9i6n1564751358> (дата обращения: 02.10.2024)

СВЕДЕНИЯ ОБ АВТОРАХ

Прокофьева Елена Васильевна.

Доцент кафедры криминалистической техники учебно-научного комплекса экспертно-криминалистической деятельности.

Кандидат физико-математических наук, доцент.

Волгоградская академия МВД России.

E-mail: olenyonok83@mail.ru

Россия, 400023, г. Волгоград, ул. Майская, 55.

Порываева Полина Сергеевна.

Преподаватель кафедры криминалистической техники учебно-научного комплекса экспертно-криминалистической деятельности.

Волгоградская академия МВД России.

E-mail: 01081998poli@gmail.com

Россия, 400023, г. Волгоград, ул. Майская, 55.

Prokofieva Elena Vasilievna.

Associate Professor of the Department of Forensic Technology of the Educational and Scientific Complex of Expert-Forensic Activity.

Candidate of Physical and Mathematical Sciences, Associate Professor.

Volgograd Academy of the Ministry of Internal Affairs of Russia.

E-mail: olenyonok83@mail.ru

Russia, 400023, Volgograd, Mayskaya St., 55.

Poryvaeva Polina Sergeevna.

Lecturer of the Department of Forensic Technology of the Educational and Scientific Complex of Expert-Forensic Activity.

Volgograd Academy of the Ministry of Internal Affairs of Russia.

E-mail: 01081998poli@gmail.com

Russia, 400023, Volgograd, Mayskaya St., 55.

Ключевые слова: виртуальная реальность; сфера инновационного образования; информационно-коммуникационные технологии.

Keywords: virtual reality; sphere of innovative education; information and communication technologies.

УДК 623.746

ПРИКЛАДНЫЕ АСПЕКТЫ ПРЕПОДАВАНИЯ КУРСОВ ФИЗИКИ И МАТЕМАТИЧЕСКИХ ДИСЦИПЛИН

APPLIED ASPECTS OF TEACHING PHYSICS AND MATHEMATICS COURSES

В статье рассмотрены практические аспекты преподавания курсов физики и математических дисциплин.

The article discusses the practical aspects of teaching physics and mathematics courses.

Центральным понятием современного высшего образования является понятие компетенции.

Изучение дисциплин «Физика» и «Математика» обеспечивает овладение следующими общепрофессиональными компетенциями [1]:

- способность выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения;
- способность использовать положения, законы и методы естественных наук и математики для решения задач инженерной деятельности;
- способность использовать в профессиональной деятельности основные законы естественнонаучных дисциплин, применять методы математического анализа и моделирования, теоретического и экспериментального исследований, приобретать новые математические и естественнонаучные знания, используя современные образовательные и информационные технологии.

Даже из этого краткого перечисления ясно, какую важную роль в успешном решении стоящих перед профессиональным техническим образованием задач играют вопросы преподавания базовых общеобразовательных дисциплин – в первую очередь, физики и математики. Базовые учебные дисциплины (физика, математика, информатика), с изучения которых курсанты начинают учебу в вузе обеспечивают дальнейшее успешное изучение общепрофессиональных и специальных дисциплин. Однако первые занятия по базовым дисциплинам выполняют не только образовательную функцию : именно на них у курсантов должны быть выработаны общие подходы к учебному процессу, курсанты должны изучить виды учебных занятий и единые для вуза требования, связанные с их проведением. Курсантам должны быть привиты навыки самостоятельной работы и работы с литературными источниками. Компетенции, приобретаемые в процессе освоения базовых дисциплин, не должны быть привязаны к изучению

только конкретной учебной дисциплины, а обязательно должны носить универсальный характер.

Прикладная направленность курсов физики и математических дисциплин предполагает рассмотрение как физических явлений, так и разделов математики в контексте технических и междисциплинарных проблем. Деятельность инженера всегда носит разноплановый характер, поэтому будущий инженер должен уметь комплексно применять знания различных дисциплин в профессиональной деятельности. В системе профессионального образования междисциплинарные связи имеют особое значение, так как учебный процесс должен строиться в тесной связи с общеобразовательными, общепрофессиональными и специальными дисциплинами. Именно прикладные задачи помогают реализовать межпредметные связи курсов математики и физики с последующими техническими дисциплинами. Они формируют математическую базу для познания процессов, протекающих в природе и технике, служат моделями для изучения явлений. Вместе с тем, при решении прикладных задач обучающиеся упражняются и тренируются в практическом применении знаний, навыков и умений, которые они получают на занятиях, что способствует сознательному усвоению и закреплению программного материала по математике и физике.

Большое влияние на формирование интересов курсантов оказывают формы организации учебной деятельности. Четкая постановка познавательных задач занятия, доказательное объяснение материала, выверенная структура занятия, использование в учебном процессе разнообразных демонстраций – все это является мощным средством развития познавательного интереса. Обучающиеся при такой организации учебного процесса переживают ряд положительных эмоций, которые способствуют поддержанию и развитию их интереса к дисциплине. Преподаватель при проведении опыта не только иллюстрирует какое-либо явление, но и противопоставляет новые факты и наблюдения сложившейся системе знаний. В этом случае активная поисковая деятельность обучающихся поддерживается непосредственным, глубоким, внутренним интересом. Л. Н. Толстой по этому поводу говорил: «Чем труднее учителю, тем легче ученику, и, чем легче учителю, тем труднее ученику».

Одним из методов, способствующих активизации познавательной деятельности, пробуждения и воспитания интереса к изучаемым предметам, является их практическая и профессиональная направленность, учитывающая будущую специальность, по которой ведется обучение. При этом возможно выделение прикладных элементов знаний для соответствующей специальности практически в каждой дисциплине учебной программы, и, конечно, при изучении курсов физики и математических дисциплин. Особенно наглядно это можно сделать в лабораторном практикуме.

При разработке лабораторного практикума для будущих технических специалистов можно сформулировать следующие задачи.

Первая – практикум должен отвечать всем требованиям федерального государственного образовательного стандарта.

Вторая – привить курсантам навыки работы с физическими (измерительными) приборами, научить приемам математической обработки результатов и оценке их погрешности, работать с прикладными математическими программами.

Третья – с целью повышения уровня знаний курсантов и их подготовки к изучению специальных дисциплин, развития интереса к предмету показать значение изучаемых явлений и закономерностей для обеспечения работы систем связи и безопасности, функционирования радиотехнических систем.

Такой подход к организации лабораторного практикума, имеющего профессиональную направленность, развивает и поддерживает интерес курсантов к изучению курсов физики и математики, повышает уровень их восприятия, способствует формированию профессиональных компетенций.

Реализация комплекса мероприятий, направленных на повышение эффективности преподавания физики и математических дисциплин, способствует повышению прикладного значения этих дисциплин, обеспечивает овладение общепрофессиональными инженерными компетенциями [2]:

- способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения;
- способностью к профессиональной эксплуатации современного оборудования и приборов;
- способностью осуществлять подбор, изучение, анализ и обобщение научно-технической информации.

СПИСОК ЛИТЕРАТУРЫ

1. Белоусова О. Е., Шерстяков А. П., Черевко А. Г. Методика оценивания уровня сформированности необходимых компетенций при изучении физики. В сборнике: Качество высшего и среднего профессионального образования в условиях перехода на федеральные государственные образовательные стандарты нового поколения. – 2019. – С. 10–20.

2. Логинов В. А., Иванова О. М., Ключникова И. Д. Реализация принципа профессиональной направленности учебного процесса на лабораторных работах по физике. В сборнике: Проблемы и современные пути развития образования в области аэронавигации. – 2020. С. 382–385.

СВЕДЕНИЯ ОБ АВТОРЕ

Сычев Игорь Валерьевич.

Начальник кафедры математики и моделирования систем.

Кандидат физико-математических наук, доцент.

Воронежский институт МВД России.

E-mail: mail.r.1964@mail.ru

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

Sychev Igor Valeryevich.

Head of the Department of Mathematics and Systems Modeling.

Candidate of Physical and Mathematical Sciences, Associate Professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: mail.r.1964@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: инженерные компетенции; естественнонаучные дисциплины; повышение эффективности; научно-техническая информация.

Keywords: engineering competencies; natural sciences; efficiency improvement; scientific and technical information.

УДК 378.1

ВСЕРОССИЙСКИЙ СЕМИНАР

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

М. А. Алексюк

АНАЛИЗ РЕЗУЛЬТАТОВ ЧИСЛЕННОГО ЭКСПЕРИМЕНТА С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ ПРЯМОЙ ПЕРЕДАЧИ СИГНАЛА, РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ ЭКСПЕРТИЗЫ

ANALYSIS OF THE RESULTS OF A NUMERICAL EXPERIMENT USING A FEEDFORWARD NEURAL NETWORK FOR SOLVING THE INVERSE PROBLEM OF EXPERTISE

Данная работа посвящена исследованию возможности использования нейронных сетей прямой передачи сигнала для решения задач обратной экспертизы. В работе будет рассмотрен численный эксперимент, результаты которого будут анализироваться с использованием нейронной сети. Основной целью исследования является определение эффективности такого подхода к решению задач экспертизы и его применимости в реальных условиях.

This work is dedicated to investigating the possibility of using direct signal transmission neural networks to solve problems of reverse expertise. The work will consider a numerical experiment, the results of which will be analyzed using a neural network. The main goal of the research is to determine the effectiveness of such an approach to solving expertise problems and its applicability in real conditions.

Нейронная сеть прямого распространения сигнала. Нейронная сеть прямого распространения сигнала имеет много преимуществ, таких как высокая точность и способность обрабатывать большие объемы данных. Это позволяет использовать ее в различных отраслях. Однако, чтобы достичь оптимальных результатов, необходимо правильно подготовить обучающий набор данных и настроить параметры нейронной сети. Под сетью прямого распространения сигнала понимается нейронная сеть, не имеющая обратных связей по выходным сигналам любого слоя. Попытаемся далее применить ее к решению задачи калибровки модели (определению множества весов и смещений) при подаче на ее вход векторов-строк матрицы референтных данных X , соответствующих разным объектам экспертизы (образцам).

В частности, процесс обучения нейрона – это как частный случай адаптивной фильтрации [5]. Нейронная модель, описываемая таким обра-

зом, получила название *адаптивного фильтра* или *адаптивного линейного сумматора* [4, 7].

Многомерная калибровка с помощью нейронной сети. Это метод, используемый для определения зависимостей между несколькими переменными, с целью создания моделей, которые могут предсказывать значения для одной или нескольких переменных, на основе значений других переменных. Этот метод широко применяется в научных и промышленных областях, чтобы повысить точность и надежность предсказания результатов экспериментов или процессов.

Представим процедуру многомерной калибровки в виде двух этапов (рис. 1).

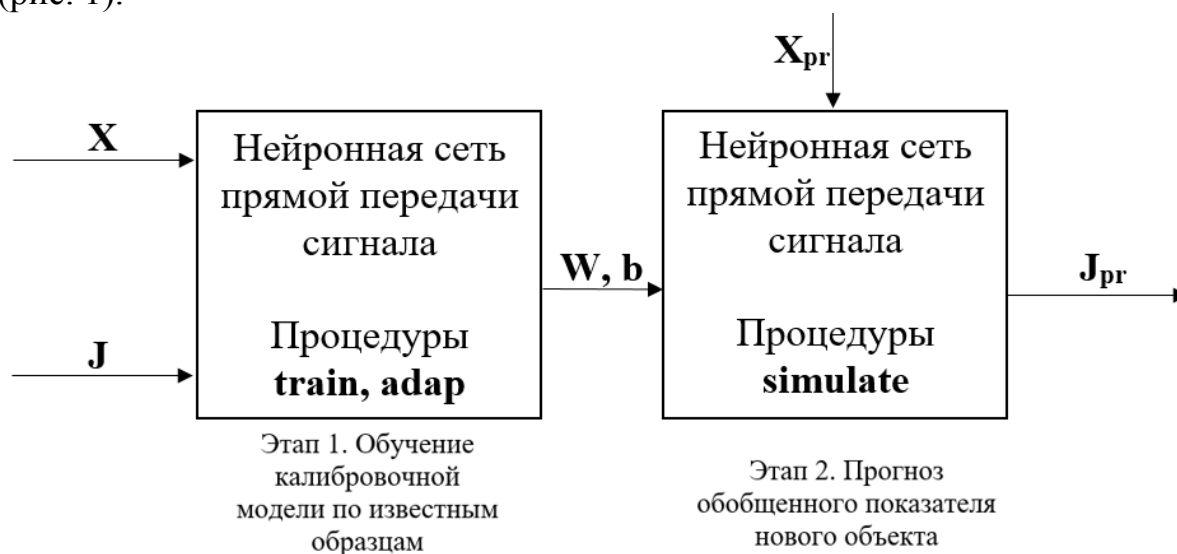


Рис. 1. Решение обратной задачи экспертизы методом многомерной калибровки на основе нейронной сети

В данном случае (рис. 1) под калибровкой модели понимается нахождение матрицы весовых коэффициентов W и вектора смещений b нейронной сети, получаемых в результате итеративной процедуры обучения.

Как видим, использование нейронной сети прямого распространения сигнала (ППС) для решения обратной задачи экспертизы представляется вполне возможным. Практическим средством решения данной задачи может служить использование пакета `nntool` языка `MATLAB` [1, 2]. В данном пакете используются два варианта настройки сети: с использованием встроенной функции `train` (обучение) и встроенной функции `adapt` (адаптация). Для прогнозирования значений J_{pr} нового образца можно использовать функцию моделирования `sim` (см. рис. 1).

При использовании команды `nntool` открывается возможность создания и обучения нейронной сети `Feed-forward backprop` (прямого распространения сигнала с обратным распространением ошибки). При этом применяется достаточно сложный метод «обратного распространения ошибки», существо которого состоит в том, что при обучении многослойной сети способом кор-

рекции ошибок нейроны настраиваются последовательно в обратном порядке – от последнего слоя к первому слою [4].

Нелинейное и нечетко-множественное моделирование. Необходимость нечетко-множественного моделирования возникает, когда система, которую необходимо описать, содержит нечёткую информацию. Данное моделирование основано на нечетких множествах и языке нечеткой логики. Нечеткое множество не описывает точное значение, а определяет степень принадлежности к некоторому понятию.

Нелинейное и нечетко-множественное моделирование имеет ряд преимуществ по сравнению с традиционными методами моделирования. Они позволяют решать более сложные задачи и учитывать неопределенность в данных. Кроме того, они могут использоваться для создания более реалистичных и точных моделей, которые являются более адекватными для сложных систем.

Очевидно, что нейронные сети с нелинейными функциями активации являются естественным средством решения нелинейных задач экспертизы, но такие сети пригодны и для решения актуальных нечетко-множественных экспертных задач.

Результаты численного эксперимента, проведенного с использованием нейронной сети прямой передачи сигнала, могут быть использованы для решения обратной задачи экспертизы. Два варианта решения этой задачи: метод наименьших квадратов и метод максимального правдоподобия. Метод наименьших квадратов позволяет определить наилучшие значения параметров, которые привели к определенным результатам, используя матричную алгебру. Метод максимального правдоподобия используется для определения наиболее вероятных значений параметров, которые привели к определенным результатам, на основе статистической оценки.

Принимая во внимание два вышеупомянутых метода, результаты численного эксперимента также могут быть анализированы с использованием понятия ошибки. Ошибки могут быть выявлены и использованы для улучшения процесса анализа данных в будущем. Эта информация может быть полезной для принятия решений при решении сложных задач.

На рисунке 2 изображена двухуровневая модель нейронной сети с прямым потоком информации и механизмом обратного распространения ошибки.

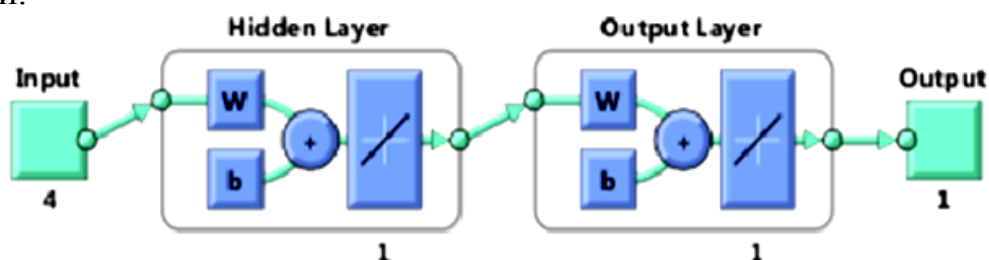


Рис. 2. Представление двухслойной нейронной сети в символической форме

Данная нейронная сеть содержит скрытый и выходной слои, а также матрицы весов для первого и второго слоя ($W^{1,2}$), и константные сигналы смещений для обоих слоев ($b^{1,2}$) [8].

Обучение с учителем (train) заключается в том, что нейронная модель обучается на заданных данных, где для каждого входного образца известен желаемый выход. В процессе обучения модель настраивает свои веса и параметры таким образом, чтобы минимизировать ошибку между желаемым и реальным выходом на каждом образце.

Последовательная адаптация (adapt) используется для обновления нейронной модели на новых данных или при изменении условий работы модели. В процессе адаптации модель натренирована на некотором наборе данных, и она должна быстро адаптироваться к новым условиям. В отличие от полного обучения, где модель обучается на всем наборе данных заново, при адаптации модель обновляется только на новых данных, сохраняя ранее полученные знания.

Архитектура нейронных сетей позволяет учитывать нечетко-множественные признаки объекта экспертизы более естественным образом. Принцип разделения признаков позволяет для каждой из групп признаков использовать в качестве функций активации соответствующие функции принадлежности.

Также архитектура нейронных сетей позволяет автоматически выделять наиболее релевантные признаки и производить классификацию объектов на основе этих признаков. Это делает процесс экспертизы быстрее и более точным. Кроме того, в нейронных сетях можно использовать различные алгоритмы обучения, чтобы улучшить качество и точность вычислений. В целом, архитектура нейронных сетей позволяет создавать более гибкие и адаптивные системы, которые могут использоваться в различных областях.

СПИСОК ЛИТЕРАТУРЫ

1. Круглов В. В. Нечеткая логика и искусственные нейронные сети / В. В. Круглов, М. И. Дли, М. И. Голунов. – Москва : Горячая линия-Телеком, 2004. – 225 с.
2. Медведев В. С. Нейронные сети. Matlab 6 / В. С. Медведев, В. Г. Потемкин. – Москва : ДИАЛОГ–МИФИ, 2002. – 496 с.
3. Миркес Е. М. Нейрокомпьютер. Проект стандарта / Е. М. Миркес. – Новосибирск : Наука. Сибирская издательская фирма РАН, 1998. – 188 с.
4. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Пер. с польск. / Д. Рутковская, М. Пилиньский, Л. Рутковский. – Москва : Горячая линия-Телеком, 2006. – 385 с.
5. Тихонов А. Н. Методы решения некорректных задач / А. Н. Тихонов, В. Я. Арсенин. – 3-е изд., испр. – Москва : Наука, 1986. – 299 с.

6. Уидроу Б. Адаптивная обработка сигналов / Б. Уидроу, С. Стирнз / Пер. с англ. – Москва : Радио и связь, 1989. – 440 с.
7. Хайкин С. Нейронные сети: полный курс / С. Хайкин : Пер. с англ. – 2-ое изд. – Москва – Санкт-Петербург. – Киев : Вильямс, 2006. – 1104 с.
8. Бухарин С. В. Методы теории нейронных сетей в экспертизе технических и экономических объектов: монография / С. В. Бухарин, В. В. Навоев. – Воронеж : Научная книга, 2015. – 255 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Алексюк Милена Александровна.
Адъюнкт кафедры автоматизированных информационных систем органов внутренних дел.
Воронежский институт МВД России.
E-mail: WowMilena01@yandex.ru
Россия, 394065, Воронеж, проспект Патриотов, 53.

Aleksyuk Milena Aleksandrovna.
Adjunct of the Department of Automated Information Systems of Internal Affairs Bodies.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: WowMilena01@yandex.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: нейронная сеть; прямая передача сигнала; решение обратной задачи; анализ результатов; моделирование.

Keywords: neural network; forward signal transmissio; inverse problem solving; analysis of results; modeling.

УДК 004.052

**СПЕЦИФИКА РЕАЛИЗАЦИИ СУПЕРСЕРВИСА
«ПРАВОСУДИЕ ОНЛАЙН»
ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ
СУДЕБНОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**THE SPECIFICS OF THE IMPLEMENTATION
OF THE JUSTICE ONLINE SUPERSERVICE
TO IMPROVE THE EFFICIENCY
OF THE JUDICIAL SYSTEM OF THE RUSSIAN FEDERATION**

В статье проводится анализ специфики реализации суперсервиса «Правосудие онлайн», разрабатываемого для повышения эффективности деятельности судебной системы Российской Федерации, исследуется понятие «суперсервис» и рассматриваются принципы интеграции суперсервиса в государственную телекоммуникационную инфраструктуру.

The article analyzes the specifics of the implementation of the Justice Online superservice, which is being developed to improve the efficiency of the judicial system of the Russian Federation, explores the concept of "superservice" and examines the principles of integrating a superservice into the state telecommunications infrastructure.

В условиях современного общества, характеризующегося стремительным развитием информационных технологий и цифровизацией многих сфер жизни, особое значение приобретает повышение эффективности деятельности судебной системы. Одним из инструментов, способствующих решению этой задачи, является внедрение в инфокоммуникационную инфраструктуру судебной системы Российской Федерации суперсервиса «Правосудие онлайн».

Актуальность темы обусловлена необходимостью модернизации судебной системы страны с целью обеспечения более быстрого, доступного и справедливого правосудия. Внедрение современных информационных технологий в деятельность судов может способствовать повышению их открытости, прозрачности и эффективности работы.

Понятие «суперсервис» можно описать как комплексный государственный сервис, предоставляющий гражданам и бизнесу широкий спектр услуг в режиме «одного окна» с использованием современных информационных технологий.

В условиях цифровизации общества суперсервисы становятся важным инструментом повышения эффективности деятельности государственных органов, включая суды Российской Федерации. Они позволяют

автоматизировать рутинные процессы, упростить взаимодействие граждан и бизнеса с судебной системой, а также обеспечить более быстрое и справедливое правосудие.

Как показал проведённый анализ, роль суперсервисов в повышении эффективности судов заключается в ряде важных моментов.

Суперсервисы предоставляют гражданам доступ к актуальным данным о судебных делах, что позволяет им лучше ориентироваться в процессе и принимать обоснованные решения. Также они могут автоматизировать такие задачи, как подача заявлений, оплата госпошлин и получение уведомлений о ходе рассмотрения дел. Это освобождает сотрудников судов от выполнения этих функций и позволяет им сосредоточиться на более сложных задачах. Отдельным положительным аспектом использования суперсервисов можно обозначить обеспечение доступа к информации о деятельности судов, что способствует повышению доверия граждан к судебной системе. Так, как показывает практика, автоматизация процессов и предоставление гражданам возможности решать некоторые вопросы самостоятельно (например, через подачу электронных документов) позволяет снизить нагрузку на суды и ускорить рассмотрение дел. Более того, суперсервисы позволяют гражданам получать услуги в удобное для них время и месте, что повышает их удовлетворённость работой судов.

Таким образом, можно сделать вывод, что внедрение суперсервиса «Правосудие онлайн» может стать важным шагом на пути к модернизации судебной системы Российской Федерации и повышению её эффективности.

Что касается реализуемого в настоящее время суперсервиса «Правосудие онлайн», то он призван быть основанным на следующих принципах:

- быть интуитивно понятным и простым в использовании, чтобы граждане могли легко получить доступ к необходимым услугам;
- быть доступен для всех граждан, независимо от их местонахождения или уровня технической подготовки;
- обеспечивать защиту персональных данных и конфиденциальной информации граждан;
- предоставлять услуги в режиме реального времени или с минимальным ожиданием;
- интегрироваться с другими государственными сервисами, чтобы обеспечить гражданам доступ ко всем необходимым услугам в одном месте.

Что касается существующих проблем, которые должен решить разрабатываемый суперсервис «Правосудие онлайн», то одной из таких является то, что граждане часто сталкиваются с трудностями при получении информации о судебных делах, статусе рассмотрения их заявлений и обращений, дате и месте проведения заседаний и вынесенных решениях. Суперсервис позволит гражданам получать эту информацию в режиме реального времени. Также, судебные процессы могут затягиваться на длительное время, что приводит к нарушению прав граждан на справедливое и

быстрое правосудие – и здесь можно ускорить рассмотрение дел за счёт автоматизации рутинных процессов и предоставления гражданам возможности решать некоторые вопросы самостоятельно. Более того, суды используют различные информационные системы и базы данных, что затрудняет обмен информацией между ними – и в этом случае суперсервис позволит приблизиться к созданию единой информационной платформы, объединяющей все суды Российской Федерации.

Уже сейчас становится понятным, что внедрение суперсервиса «Правосудие онлайн» окажет значительное влияние на эффективность судебной системы Российской Федерации и должно привести к следующим результатам:

- суперсервис позволит гражданам получать услуги в удобное для них время и месте, что повысит их удовлетворённость работой судов;
- автоматизация рутинных процессов и предоставление гражданам возможности решать некоторые вопросы самостоятельно (например, через подачу электронных документов) позволит снизить нагрузку на суды и ускорить рассмотрение дел;
- суперсервис обеспечит более быстрое и эффективное взаимодействие между гражданами и судами, что приведёт к повышению качества предоставляемых услуг;
- автоматизация процессов и использование современных технологий позволят сократить расходы на содержание судов и оплату труда сотрудников;
- предоставление гражданам доступа к информации о деятельности судов и возможность получения услуг в удалённом формате повысят доверие граждан к судебной власти;
- объединение всех судов Российской Федерации в единую информационную систему позволит обеспечить более эффективное управление ресурсами и координацию работы судов;
- внедрение суперсервиса потребует модернизации оборудования, программного обеспечения и каналов связи в судах, что улучшит качество предоставляемых услуг и повысит эффективность работы судов;
- интеграция суперсервиса с другими государственными сервисами, такими как портал «Госуслуги», позволит гражданам получить доступ ко всем необходимым услугам в одном месте;
- внедрение суперсервиса будет способствовать развитию электронного документооборота в судебной системе Российской Федерации, что ускорит процесс рассмотрения дел и снизит затраты на обработку бумажных документов.

Таким образом, в результате было выявлено, что внедрение суперсервиса может стать важным шагом на пути к модернизации судебной системы Российской Федерации и повышению её эффективности. Суперсер-

вис позволит упростить доступ граждан к информации о работе судов, автоматизировать рутинные процессы, повысить прозрачность работы судов и снизить нагрузку на них.

Для успешного внедрения суперсервиса «Правосудие онлайн» проводится тщательная подготовка: происходит непрерывный анализ текущего состояния судебной системы, дополняется и уточняется концепция суперсервиса, проводится тестирование и доработка его функциональных элементов, а также выстраивается система обеспечения безопасности данных и интеграция с другими государственными системами и сервисами.

Подводя общий итог, стоит отметить, что внедрение суперсервиса «Правосудие онлайн» должно привести к повышению доступности правосудия, сокращению сроков рассмотрения дел, улучшению качества обслуживания, снижению затрат на судебные процессы, увеличению доверия граждан к судебной системе Российской Федерации, созданию единой информационной платформы, модернизации инфраструктуры судов, интеграции с другими сервисами и развитию электронного документооборота.

СПИСОК ЛИТЕРАТУРЫ

1. О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти : Федеральный закон от 23 июня 2016 г. № 220-ФЗ // СПС «КонсультантПлюс».
2. Об утверждении Положения о суперсервисе «Правосудие онлайн» : постановление Правительства РФ от 24 октября 2022 г. № 1890// СПС «КонсультантПлюс».
3. Об утверждении Концепции развития информатизации судов до 2030 года : распоряжение Правительства РФ от 20 февраля 2021 г. № 431-р // СПС «КонсультантПлюс».
4. Информатизация судебной системы России: генезис содержание и будущее : монография / под. ред. Р. А. Шарифуллина – Москва : Проспект, 2023. – 270 с.
5. Грешонков А. М. Информационные системы судопроизводства: лекционный курс : учебное пособие / А. М. Грешонков, М. А. Шибачев. – Москва : ИНФРА-М, 2023. – 73 с.
6. Гаспарян Д. Э. Прикладные проблемы внедрения этики искусственного интеллекта в России. Отраслевой анализ и судебная система : монография / Д. Э. Гаспарян, Е. М. Стырин ; Нац. исслед. ун-т «Высшая школа экономики». – 2-е изд. – Москва : Изд. дом Высшей школы экономики, 2021. – 112 с.
7. Андрюшечкина И. Н. Судебная статистика : учебное пособие / И. Н. Андрюшечкина. – Москва : РГУП, 2022. – 291 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Зарубин Сергей Владимирович.

Доцент кафедры правовой информатики, информационного права и естественнонаучных дисциплин.

Кандидат технических наук.

Центральный филиал Российского государственного университета.

E-mail: zarubin_rgup@mail.ru

Россия, 394006 г. Воронеж, ул. 20-летия Октября, 95.

Zarubin Sergey Vladimirovich.

Associate Professor of the Department of Legal Informatics, Information Law and Natural Sciences.

Candidate of Technical Sciences.

Central Branch of the Russian State University.

E-mail: zarubin_rgup@mail.ru

Russia, 394006, Voronezh, 20th Anniversary of October str. 95.

Ключевые слова: суперсервис; телекоммуникационная инфраструктура; правосудие; суд; автоматизация; Госуслуги.

Keywords: super service; telecommunication infrastructure; justice; court; automation; public services.

УДК 004.77

А. В. Мельников

К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

ON THE QUESTION OF ENSURING THE INTEGRITY OF INFORMATION IN ELECTRONIC DOCUMENT MANAGEMENT OF STATE AUTHORITIES

В статье предложено для организации электронного документооборота (ЭДО) органов государственной власти, использовать технологию распределенных реестров, которая предполагает хранение журналов входящей и исходящей корреспонденции, учета состава и содержания сопроводительных документов всеми операторами узлов распределённого реестра блокчейн и создание механизмов управления сетью системы. Предложена концептуальная модель ЭДО с использованием технологии блокчейн и распределённых реестров, построенных на основе централизованного консенсуса.

The article proposes to use distributed registry technology for organizing electronic document management (EDM) of government bodies, which involves storing incoming and outgoing correspondence logs, accounting for the composition and content of accompanying documents by all operators of the blockchain distributed registry nodes and creating mechanisms for managing the system network. A conceptual model of EDM using blockchain technology and distributed registries built on the basis of centralized consensus is proposed.

Одним из перспективных направлений в разработке систем ЭДО является применение технологии распределённых реестров (Distributed Ledger Technology, DLT). DLT базируется на закодированной и распределённой базе данных, где хранятся записи о транзакциях.

Существуют три типа консенсуса в DLT:

Централизованный – узлы должны получать разрешение центрального органа для доступа к данным или внесения изменений в сеть.

Децентрализованный – отсутствует центральный орган для проверки транзакций. Узлы коллективно отвечают за проверку транзакций с использованием predetermined алгоритмов и механизмов консенсуса.

Гибридный – сочетает элементы централизованного и децентрализованного принятия решений по разрешённым транзакциям.

В сентябре 2023 года ФНС России создала хранилище для машиночитаемых доверенностей (МЧД) на базе технологии распределённого реестра (блокчейн). Цифровая платформа ФНС России на основе блокчейна позволяет создать единую цифровую среду доверия для всех участников электронного документооборота.

Для интеграции этой технологии в системы ЭДО организаций необходимо обратиться к любому участнику реестра, который является оператором узла распределённого реестра блокчейн. Это позволит организациям автоматически обмениваться машиночитаемыми доверенностями и проверять полномочия без участия человека. Операторами узлов распределённого реестра блокчейн являются: Федеральное Казначейство, Федеральная нотариальная палата, Федеральная служба по контролю за алкогольным и табачным рынками, Федеральная таможенная служба, Центральный банк Российской Федерации.

Успешное внедрение технологии распределённого реестра ФНС России для использования единой формы машиночитаемой доверенности (МЧД) подтвердили крупнейшие разработчики программного обеспечения и операторы государственных информационных систем и электронного документооборота.

В условиях сложной геополитической обстановки необходима консолидация усилий всех органов государственной власти для обеспечения целостности информации в государственных информационных системах на основе технологии распределённых реестров, создания бесшовной си-

системы межведомственного электронного взаимодействия и развития сектора государственных услуг с передачей информации по защищённым каналам.

Организация электронного документооборота органов государственной власти, с использованием технологии распределённых реестров, предполагает хранение журналов входящей и исходящей корреспонденции, учета состава и содержания сопроводительных документов всеми операторами узлов распределённого реестра блокчейн и создание механизмов управления сетью системы электронного документооборота органов государственной власти (СЭДООГВ).

Для хранения транзакций СЭДООГВ предлагается использовать технологию блокчейн, т.е. хранить квитанции в виде цепочки блоков, где каждый блок создает уникальный хеш, который может быть использован в качестве доказательства правильности транзакций. У каждого узла есть копия «бухгалтерской книги» (базы данных транзакций), что делает ее более прозрачной.

Бухгалтерская книга в технологии блокчейн – это цифровая база данных, которая ведется распределенной сетью компьютеров и узлов. Эта книга служит для хранения записей обо всех транзакциях, когда-либо совершенных в сети блокчейн. Каждая транзакция проверяется несколькими узлами сети перед тем, как быть добавленной в книгу. После успешной проверки, транзакции группируются в блоки, которые затем добавляются в существующую цепочку блоков, что и дало название технологии – блокчейн.

Смарт-контракт – это компьютерный алгоритм, предназначенный для автоматизации выполнения условий договора между двумя или более сторонами. Он основан на принципах безопасности и прозрачности, присущих технологии блокчейн, и выполняется непосредственно в распределенном реестре блоков транзакций.

Блокчейн – это основа для работы смарт-контрактов. Он обеспечивает децентрализованное и неизменное хранение всех транзакций. Это гарантирует автоматическое выполнение условий смарт-контракта без вмешательства третьей стороны. Процесс становится безопасным и надёжным. Выполнение смарт-контракта на блокчейне не требует доверия к какой-либо стороне. Код смарт-контракта и данные транзакций хранятся в распределённой сети и проверяются всеми участниками. Это позволяет избежать посредников и снижает риски мошенничества.

Таким образом, смарт-контракты и блокчейн образуют взаимодополняющую пару, где блокчейн обеспечивает безопасность и прозрачность, а смарт-контракты автоматизируют выполнение условий договоров, делая процесс более эффективным и экономичным. В контексте смарт-контрактов на блокчейне оракул играет ключевую роль в преодолении разрыва между децентрализованными сетями и внешним миром. Он служит мостом, который позволяет смарт-контрактам взаимодействовать с собы-

тиями и информацией реального мира, что значительно расширяет их функциональность и применимость. Основные цели использования оракулов включают: интеграция с реальным миром, расширение функциональности смарт-контрактов, обеспечение безопасности и надёжности данных, поддержка децентрализации.

Для решения задачи по созданию модели СЭДООГВ проведем ее декомпозицию и выделим несколько уровней иерархии – концептуальная модель, системная (логическая) модель, технологическая (физическая) модель, а также отдельные модели, характеризующие детали реализации.

Концептуальная модель СЭДООГВ с использованием технологии блокчейн содержит следующие элементы: распределённая блокчейн-сеть, участники (звенья) ЭДО (доверенные и базовые узлы), цифровые соглашения (смарт-контракты), информация о МЧД и ЭП.

Основой модели является распределённая блокчейн-сеть, состоящая из узлов (нод), каждый из которых хранит копию всей истории транзакций (мастернода, полная нода) (рис.).

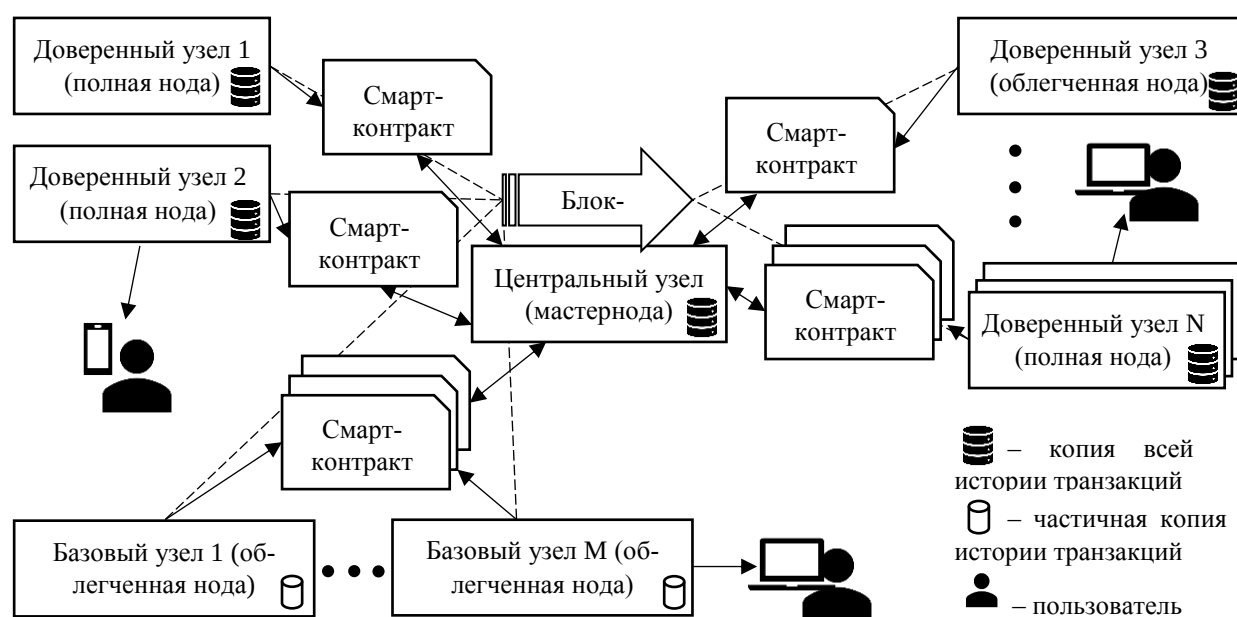


Рис. – Концептуальная модель информационной системы

Все доверенные узлы выполняют функции узла-валидатора, который проверяет и утверждает транзакции. В случае обнаружения ошибки, узел может отклонить операцию. Возможные причины включают неправильное форматирование, ошибки алгоритмов, дублирование или манипуляции с записями.

Полная нода содержит всю информацию о транзакциях и блоках с момента запуска сети до текущего времени.

Мастернода аналогична полной ноде, но также выполняет дополнительные функции. Она хранит всю информацию из блокчейна и синхронизируется с ним, действуя как оракул – узел, передающий информацию из

внешних систем в блокчейн. Например, она может предоставлять актуальные данные о требованиях ГОСТ к строительным материалам. Скрипты преобразуют эту информацию в формат, понятный для смарт-контрактов, настраивая их под условия и требования рынка.

Организация, владеющая мастернодой (например, государственный орган или предприятие), является центральным узлом и представляет интересы всех участников сети. Она формирует и поддерживает смарт-контракты в актуальном состоянии. Центральный узел выполняет функции управляющего контура, распределяя вычислительные ресурсы и права доступа к ресурсам системы.

Для управления системой электронного документооборота достаточно одного управляющего центра и нескольких доверенных узлов, которые будут верифицировать транзакции и вносить изменения в цепочку блоков.

С технической точки зрения, цифровая экосистема представляет собой одноранговую сеть, где доверенные узлы обработки данных (ЦОДы) выполняют роль узлов. Каждый узел содержит полную копию блокчейна и формирует блоки поочередно с периодом не более секунды. Для поддержания работоспособности экосистемы достаточно одного узла. Доверенные узлы обеспечивают бесперебойную работу сети и защиту от несанкционированных изменений.

Если система развернута в пределах одного государства, она является закрытой – доступ к ресурсам сети имеют только пользователи с приватными ключами. Однако это не исключает возможности последующего включения государственной сети в международную.

Облегченная нода загружает весь блокчейн при первом запуске и синхронизирует его только при необходимости. Далее она автоматически подгружает новые блоки и удаляет старые при достижении определенного объема памяти, например, 20 Гбайт.

Таким образом, использование технологии распределённых реестров в системах электронного документооборота обеспечивает высокий уровень безопасности, надёжности и эффективности, способствуя развитию государственных услуг и межведомственного взаимодействия.

СПИСОК ЛИТЕРАТУРЫ

1. Болдачев А. Цифровая экосистема eGaaS / А. Болдачев // Habr Blockchain Publishing LTD. – URL: <https://habr.com/ru/articles/325986/> (дата обращения 30.09.2024).
2. Лойко А. И. Философия цифровой экономики учебное пособие / А. И. Лойко/ – Минск : Белорусский национальный технический университет, 2023. – 196 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Мельников Александр Владимирович.
Профессор кафедры автоматизированных информационных систем ОВД.
Доктор технических наук, профессор.
Воронежский институт МВД России.
E-mail: meln78@mail.ru
Россия, 394065, г. Воронеж, просп. Патриотов, 53.

Melnikov Alexander Vladimirovich.
Professor of the chair of Automatic Information Systems.
Doctor of technical sciences, Professor.
Voronezh Institute of the Ministry of Internal Affairs of Russia.
E-mail: meln78@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: электронный документооборот органов государственной власти; технологии распределённого реестра; блокчейн.

Keywords: Electronic document management of government bodies; distributed ledger technologies; blockchain.

УДК 004.05

В. В. Меньших, А. В. Подольских

ТЕОРЕТИКО-ГРАФОВАЯ МОДЕЛЬ ОБУЧЕНИЯ ГЕТЕРОГЕННОЙ ГРУППЫ СПЕЦИАЛИСТОВ ДЕЙСТВИЯМ В КРИЗИСНЫХ СИТУАЦИЯХ

THEORETICAL AND GRAPHICAL MODEL OF TRAINING A HETEROGENEOUS GROUP OF SPECIALISTS TO ACT IN CRISIS SITUATIONS

Представлена теоретико-графовая модель, позволяющая эффективно организовать обучение гетерогенной группы специалистов действиям в кризисных ситуациях. Учитываются разнообразие компетенций специалистов и курсов обучения образовательных организаций. Предложенная модель основывается на графовой структуре, где вершины представляют собой курсы обучения, а дуги – зависимости между ними.

A graph-theoretic model is presented, which allows to effectively organize training of a heterogeneous group of specialists to act in crisis situations. The diversity of competencies of specialists and training courses of educational organizations is taken into account. The proposed model is based on a graph structure, where vertices represent training courses and arcs represent dependencies between them.

Кризисные ситуации, такие как природные бедствия, социальные волнения или экономические кризисы требуют от специалистов быстро принимать решения, эффективно взаимодействовать и координировать свои действия [1,2]. Гетерогенные группы, состоящие из представителей различных компетенций, могут существенно повысить эффективность реагирования в таких условиях [3-5].

В качестве примера рассмотрим кризисную ситуацию стихийного бедствия, приведшего к разрушению инфраструктуры и человеческим жертвами в некотором населённом пункте.

В этом случае должна быть сформирована гетерогенная группа, состоящая из:

- сотрудников МЧС (аварийно-спасательные работы);
- медицинских работников (оказание первой помощи и лечение пострадавших);
- социальных работников (оказание психологической помощи);
- специалистов по логистике (обеспечение доставки помощи и материалов);
- сотрудников силовых ведомств (обеспечение безопасности).

Для моделирования процессов организации совместного обучения специалистов гетерогенных групп в интересах улучшения взаимодействия между ними могут быть использованы методы теории графов [6, 7].

В теоретико-графовой модели обучения специалистов гетерогенных групп курсы обучения представлены в виде вершин U , а причинно-следственные связи между ними – в виде дуг E , веса вершин T отражают длительность обучения на каждом курсе [8, 9].

Примеры графов, моделирующих процессы обучения трёх специалистов гетерогенной группы, приведены на рисунке 1.

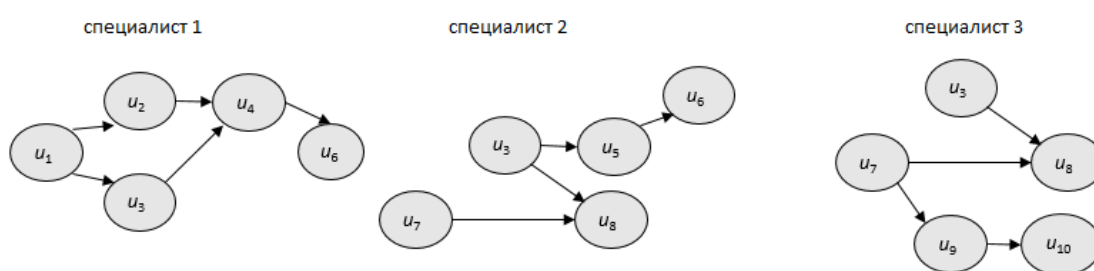


Рис. 1. Примеры графовых моделей обучения специалистов гетерогенной группы

Графовая модель обучения всей гетерогенной группы представляет собой объединение [6] графовых моделей специалистов этой группы. Пример приведён на рисунке 2.

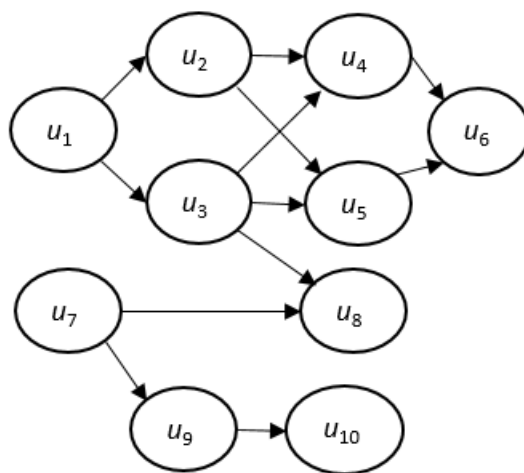


Рис. 2. Пример графовой модели обучения гетерогенной группы

Используя теоретико-графовую модель, можно:

- настраивать образовательную траекторию для каждого специалиста так, чтобы выполнить требования к подготовке специалистов [10, 11] Например, составлять расписание, позволяющее минимизировать общее время подготовки всей группы;
- осуществлять выбор образовательной организации [12, 13] для подготовки группы и решения ряда других задач.

СПИСОК ЛИТЕРАТУРЫ

1. Семенова В. Н. Классификация кризисных ситуаций и особенности их формирования / В. Н. Семенова // Научный вестник Московского государственного технического университета гражданской авиации. – 2013. – № 190. – С. 97–100.
2. Моделирование коллективных действий сотрудников органов внутренних дел / В. В. Меньших, А. Ф. Самороковский, Е. Н. Середа, В. В. Горлов. – Воронеж : Воронежский институт МВД РФ, 2017. – 236 с.
3. Математическое моделирование действий органов внутренних дел в чрезвычайных обстоятельствах / В. В. Меньших, А. Ф. Самороковский, В. В. Горлов [и др.]. – Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2016. – 187 с.
4. Никитенко А. Н. Описание типов равновесий в теоретико-игровых моделях при принятии управленческих решений / А. Н. Никитенко, Т. В. Меньших // Актуальные проблемы деятельности подразделений уголовно-исполнительной системы : сборник материалов Всероссийской научно-практической конференции, Воронеж, 19 октября 2023 года. – Воронеж : Научная книга, ФКОУ ВО Воронежский институт ФСИН России., 2023. – С. 372–374.

5. Меньших В. В. Использование ситуационных центров для обучения действиям в кризисных ситуациях / В. В. Меньших, О. В. Пьянков, А. Ф. Самороковский // Информационная безопасность регионов. – 2011. – № 2(9). – С. 104–107.
6. Дискретная математика : учебник : Рекомендовано ЮгРОУМО вузов по образованию в области информационной безопасности для студентов высших учебных заведений, обучающихся по УГС НП 10.00.00 «Информационная безопасность» / В. В. Меньших, А. Н. Копылов, В. А. Кучер, С. А. Телкова. – Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2016. – 228 с.
7. Дровникова И. Г. Графовая модель процесса эксплуатации уязвимостей в программном обеспечении автоматизированных систем органов внутренних дел / И. Г. Дровникова, А. Д. Попова // Вестник Воронежского института ФСИН России. – 2023. – № 4. – С. 40–46.
8. Меньших В. В. Модель определения состава курсов обучения по нескольким направлениям / В. В. Меньших, А. В. Лихобабаина // Информатика: проблемы, методы, технологии : Материалы XXIV Международной научно-практической конференции им. Э. К. Алгазинова, Воронеж, 14–15 февраля 2024 года. – Воронеж : Воронежский государственный университет, 2024. – С. 1116–1122.
9. Menshikh, V. V. A model and a numerical method for optimizing the choice of a training trajectory for heterogeneous groups of specialists / V.V. Menshikh, A.V. Podolskikh // Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software. – 2024. – Vol. 17.– № 4. – P. 32–41.
10. Lihobabina, A. Model and Numerical Method of Optimization of Selection of Training Programs for Specialists / A. Lihobabina, V. Menshikh // Proceedings – 2023 5th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency, SUMMA 2023. – P. 447–450.
11. Меньших В. В. Моделирование процессов оптимизации выбора программ подготовки и переподготовки специалистов с использованием генетического алгоритма / В. В. Меньших, А. В. Лихобабаина // Автоматизация и моделирование в проектировании и управлении. – 2024. – № 1(23). – С. 42–48.
12. Меньших, В. В. Модель выбора направлений группового обучения специалистов в условиях ограниченных ресурсов образовательной организации / В. В. Меньших, А. В. Лихобабаина // Техника и безопасность объектов уголовно-исполнительной системы : сборник материалов Международной научно-практической конференции, Воронеж, 22–23 мая 2024 года. – Воронеж : Строки, 2024. – С. 185–187.

13. Лихобаба А. В. Генетический алгоритм формирования групп специалистов, проходящих обучение в образовательной организации / А. В. Лихобаба // Техника и безопасность объектов уголовно-исполнительной системы : сборник материалов Международной научно-практической конференции, Воронеж, 22–23 мая 2024 года. – Воронеж : Строки, 2024. – С. 171–173.

СВЕДЕНИЯ ОБ АВТОРАХ

Меньших Валерий Владимирович.
Профессор кафедры математики и моделирования систем.
Доктор физико-математических наук, профессор.
Воронежский институт МВД России.
E-mail: menshikh@list.ru.
Россия, 394065 г. Воронеж, проспект Патриотов, 53.

Подольских Анна Викторовна. Адъюнкт.
Воронежский институт МВД России.
E-mail: podolskihanna@mail.ru.
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Menshikh Valeriy Vladimirovich.
Professor of the chair of Mathematics and Systems Modeling.
Doctor of Physical and Mathematical Sciences, Professor.
Voronezh Institute of the Russian interior Ministry.
E-mail: menshikh@list.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Podolskikh Anna Viktorovna. Adjunct.
Voronezh Institute Ministry of the interior of Russian.
E-mail: podolskihanna@mail.ru.
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: гетерогенная группа специалистов; кризисные ситуации; компетенции специалистов; курсы обучения образовательные организации.

Keywords: heterogeneous group of specialists; crisis situations; competencies of specialists; training courses educational organizations.

УДК 004.94

ПОДХОДЫ К КЛАССИФИКАЦИИ УСЛОВИЙ ФУНКЦИОНИРОВАНИЯ МУЛЬТИАГЕНТНЫХ СИСТЕМ

APPROACHES TO CLASSIFICATION OF OPERATING CONDITIONS FOR MULTI-AGENT SYSTEMS

В данной работе рассмотрены основные подходы к классификации условий функционирования мультиагентных систем как перспективного направления в области искусственного интеллекта, обладающего значительным потенциалом для использования таких систем подразделениями органов внутренних дел.

This paper considers the main approaches to classifying the conditions of functioning of multi-agent systems as a promising direction in the field of artificial intelligence, which has a significant potential for the use of such systems by divisions of the internal affairs bodies of the Russian Federation.

Современные технологии активно развиваются в сторону автоматизации и автономности, что привело к широкому распространению различных решений на основе искусственного интеллекта, в том числе такое направление области искусственного интеллекта, как мультиагентные системы (МАС). МАС позволяют решать задачи, требующие коллективных действий и распределенного принятия решений, особенно в условиях сложной и меняющейся среды. МАС – это система, состоящая из нескольких взаимодействующих между собой и окружающей средой агентов. Агент в свою очередь – это то, что можно рассматривать как имеющее способность воспринимать окружающую среду с помощью датчиков (сенсоров) и воздействовать на эту среду с помощью исполнительных механизмов [1,2]. Действия агента в ответ на восприятие зависит от программы агента, которая обрабатывает информацию, полученную агентом, в соответствии с заданной логикой.

МАС находят применение в различных сферах, причем каждая из них обладает уникальными особенностями, специально разработанными для решения определенных задач.

Далее приведены примеры возможных областей использования мультиагентных систем:

- 1) построение распределенных систем управления в экономике, на объектах оборонно-промышленного комплекса, объектах силовых ведомств;
- 2) робототехника, беспилотные аппараты и комплексы;
- 3) построение систем дистанционного обучения;
- 4) разработка компьютерных игр;
- 5) разработка симуляторов действий объектов в виртуальной реальности, в том числе для подготовки (переподготовки) сотрудников к действиям в реальных условиях;
- 6) логистика и так далее.

При создании агента и организации функционирования мультиагентных систем важным аспектом является рассмотрение характеристик среды их функционирования с наибольшей возможной полнотой, поскольку построение программы каждого агента основывается на алгоритмах, предпосылками создания которых является анализ факторов, которые могут повлиять на самого агента, а также на его действия.

В [3] представлен перечень факторов и характеристик, по которым можно классифицировать среду функционирования как отдельного агента, так и мультиагентной системы. Рассмотрим данную классификацию.

1. Классификация среды по её наблюдаемости.

Среда может быть **ненаблюдаемой**. В таком случае у агента будут отсутствовать датчики восприятия информации об окружающей его обстановке в конкретный момент времени.

Среда может быть **частично наблюдаемой**, например, ввиду отсутствия каких-либо датчиков восприятия, либо по причине их неисправной работы.

Например, робот-пылесос, в котором не предусмотрено наличие камер, не может в полной мере получать информацию о среде его функционирования по средством её визуализации, однако, для выполнения его функций в соответствии с заданной программой это не является критичной необходимостью. Или, наоборот, могут возникать ситуации, когда для агента наличие того или иного датчика будет являться необходимостью, а выход его из строя приведет к возникновению некоторых последствий, которые по возможности тоже нужно учитывать.

Если датчики агента в полной мере обеспечивают ему доступ к информации о состоянии среды, релевантной для принятия решения о дей-

ствии агента в ответ на это восприятие в каждый момент времени, то такая среда является **наблюдаемой**. Наблюдаемая среда является очень удобной с точки зрения проектирования агента, однако, чаще всего это идеальный случай, потому что в реальности будут возникать обстоятельства, которые сделают среду частично наблюдаемой.

2. По виду взаимодействия агентов. Среда может быть **конкурентной**. В такой среде взаимодействие агентов строится на отношениях соперничества, каждый агент будет пытаться максимизировать только свои показатели в ущерб показателям другого агента. Среда также может быть **кооперативной**, в такой среде агенты будут действовать согласованно, будет присутствовать внутригрупповая коммуникация. Также может существовать среда, совмещающая в себе элементы конкуренции и кооперации.

3. Детерминированность среды. Если последующее состояние среды будет определяться текущим состоянием среды и действием агента системы в определенный момент времени, то такая среда является детерминированной. В противном случае система является недетерминированной. В реальных условиях ситуации могут быть настолько сложными, что невозможно отследить все аспекты, в таком случае целесообразно рассматривать среду, как недетерминированную.

4. Статистическая или динамическая среда. Если среда может измениться за время принятия агентом решения на то или иное действие, то среда является **динамической** для данной мультиагентной системы. В противном случае она является **статической**.

5. Дискретная и непрерывная среда. **Дискретная среда** характеризуется конечным набором четко определенных состояний и действий. Здесь пространство состояний делится на отдельные элементы, что ограничивает перемещения и взаимодействия агентов. **Непрерывная среда** имеет бесконечное множество состояний и действий, позволяя агентам свободно перемещаться и взаимодействовать в рамках заданных диапазонов значений. Дискретные среды упрощают моделирование и анализ, но могут ограничивать гибкость агентов в динамичных условиях. Непрерывные среды, несмотря на сложность, предлагают большую адаптивность и точность, что может быть критично для задач, требующих быстрого реагирования на протекающие в среде изменения.

6. Известная и неизвестная среда. Строго говоря, данный аспект касается не самой среды, а состояния знаний агента (или его разработчика) об этой среде. Если среда **известна**, результаты в ней определены для каж-

дого действия агента на заранее известное возможное событие. Если среда **неизвестна**, то агенту необходимо будет анализировать, как она функционирует для принятия решения о последующих действиях.

Обратимся к рассмотрению вопроса об использовании мультиагентных систем силовыми ведомствами.

В Федеральном законе «О полиции» [4] указано, что «полиция в своей деятельности использует достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру». Таким образом, необходимо сосредоточить внимание на вопросах оптимизации использования в целях обеспечения общественной безопасности, защиты жизни и здоровья граждан беспилотных аппаратов и комплексов, робототехнических комплексов, которые можно рассматривать как мультиагентные системы. В условиях современных вызовов, с которыми сталкивается полиция, таких как необходимость оперативного реагирования на происшествия и поддержания общественной безопасности, становится очевидным, что внедрение мультиагентных систем может существенно повысить эффективность работы правоохранительных органов. Беспилотные летательные аппараты (БПЛА) и робототехнические комплексы, рассматриваемые как мультиагентные системы, могут быть задействованы в различных аспектах деятельности подразделений при решении задач органов внутренних дел. Например, БПЛА могут использоваться для мониторинга больших территорий, сбора информации о правонарушениях и быстрого реагирования на чрезвычайные ситуации, позволяя принимать обоснованные решения на основе актуальных данных [5,6].

Робототехнические комплексы могут выполнять задачи, связанные с обеспечением безопасности на массовых мероприятиях, а также помогать в ситуациях, требующих особой осторожности, таких как операции по обезвреживанию взрывных устройств. Эти системы способны взаимодействовать друг с другом, обмениваться данными и координировать свои действия, что значительно повышает общую эффективность операций, а также может предотвратить потери личного состава при выполнении таких опасных для жизни и здоровья операций.

Ещё одним перспективным направлением использования МАС является разработка систем частичного подыгрыша оперативной обстановки в зоне возникновения чрезвычайного обстоятельства, что может быть использовано при проведении учений [7] или при подготовке групп специалистов к действиям в зоне возникновения чрезвычайного обстоятельства [8 – 10].

В тексте были рассмотрены МАС как перспективное направление в области искусственного интеллекта, обладающее значительным потенциалом для использования таких систем подразделениями органов внутренних дел. Учитывая современные вызовы, с которыми сталкиваются правоохрани-

нительные органы, внедрение МАС может существенно повысить эффективность их функционирования. Важно продолжать исследование данных технологий с целью их интеграции в деятельность органов внутренних дел с учетом возможных ограничений.

СПИСОК ЛИТЕРАТУРЫ

1. Wooldridge M. An introduction to Multiagent Systems. – Chichester, West Sussex, England: JOHN WILEY & SONS, LTD, 2002. – P. 492.

2. Тарасов В. Б. Нетрадиционные и гибридные логики в моделировании интеллектуальных агентов. I. Искусственные деятели, интернациональные характеристики и пути моделирования // Известия РАН. Теория и системы управления. – 2000. – № 5. – С. 5–17.

3. Рассел С., Норвиг П. Искусственный интеллект: современный подход, 4-е изд., том 1. Решение проблем: знания и рассуждения / пер. с английского. – Санкт-Петербург : Диалектика, 2021. – 704 с.

4. О полиции : Федеральный закон от 07.02.2011 №3-ФЗ (ред. от 08.08.2024) // СПС «КонсультантПлюс» (дата обращения: 08.10.2024).

5. Никитенко А. Н. Подход к разработке теоретико-игровой модели обслуживания объектов беспилотными летательными аппаратами // IV научно-педагогические чтения молодых ученых имени профессора С.В. Познышева : Сборник материалов Всероссийской научно-практической конференции курсантов и студентов, Воронеж, 17 апреля 2024 года. – Воронеж : Воронежский институт ФСИН России, 2024. – С. 6–9.

6. Никитенко А. Н., Меньших Т. В. Описание типов равновесий в теоретико-игровых моделях при принятии управленческих решений // Актуальные проблемы деятельности подразделений уголовно-исполнительной системы : сборник материалов Всероссийской научно-практической конференции, Воронеж, 19 октября 2023 года. – Воронеж : Научная книга, ФКОУ ВО Воронежский институт ФСИН России., 2023. – С. 372–374.

7. Меньших В. В., Пьянков О. В. Самороковский А. Ф. Использование ситуационных центров для обучения действиям в кризисных ситуациях // Информационная безопасность регионов. – 2011. – № 2(9). – С. 104–107.

8. Lihobabina, A. Model and Numerical Method of Optimization of Selection of Training Programs for Specialists / A. Lihobabina, V. Menshikh // IEEE Proceedings of 5th International Conference on Control Systems, Mathe-

mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, 08–10 ноября 2023 года. – Lipetsk: Lipetsk State Technical University, 2023. – P. 447–450.

9. Меньших В. В., Лихобаба А. В. Моделирование процессов оптимизации выбора программ подготовки и переподготовки специалистов с использованием генетического алгоритма // Автоматизация и моделирование в проектировании и управлении. – 2024. – № 1(23). – С. 42–48.

10. Menshikh, V. V. A model and a numerical method for optimizing the choice of a training trajectory for heterogeneous groups of specialists / V.V. Menshikh, A.V. Podolskikh // Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software. – 2024. – Vol. 17, No. 4. – P. 32–41.

СВЕДЕНИЯ ОБ АВТОРЕ

Никитенко Анастасия Николаевна.
Адъюнкт кафедры математики и моделирования систем.
Воронежский институт МВД России.
E-mail: nikitenkoan27@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.

Nikitenko Anastasia Nikolaevna.
Post-graduate student of the chair of mathematics and modeling systems.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: nikitenkoan27@mail.ru
Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: интеллектуальный агент; мультиагентные системы; среда функционирования; дискретная среда; наблюдаемая среда.

Keywords: intelligent agent; multi-agent systems; operating environment; discrete environment; observable environment.

УДК 004.94

**К ВОПРОСУ ОБ ИССЛЕДОВАНИИ
ВРЕМЕННЫХ ХАРАКТЕРИСТИК УЯЗВИМОСТЕЙ
ПРИ ПОДГОТОВКЕ К ИХ ЭКСПЛУАТАЦИИ
В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ**

**ON THE ISSUE OF STUDYING
THE TEMPORAL CHARACTERISTICS OF VULNERABILITIES
IN PREPARATION FOR THEIR EXPLOITATION IN THE SOFTWARE
OF INFORMATIZATION FACILITIES
OF INTERNAL AFFAIRS BODIES**

В статье предложена методика исследования текущих уязвимостей в процессе подготовки к их эксплуатации в программном обеспечении (ПО) автоматизированных систем (АС) органов внутренних дел (ОВД), позволяющая определять временные характеристики уязвимостей. Описаны основные этапы методики и представлены результаты ее реализации на примере версий пакета программ LibreOffice. Практическое использование предложенной методики позволит проводить количественную оценку уровня защищенности ПО в режиме реального времени и выбирать его наиболее защищенную версию для эксплуатации на объектах информатизации ОВД.

The article proposes a methodology for investigating current vulnerabilities in the process of preparing for their operation in the software of automated systems of internal affairs agencies, which allows determining the temporary characteristics of vulnerabilities. The main stages of the methodology are described and the results of its implementation are presented using the example of versions of the LibreOffice software package. The practical use of the proposed methodology will allow for a quantitative assessment of the level of security of the software in real time and select its most secure version for operation at the facilities of informatization of internal affairs bodies.

В соответствии с требованиями действующей нормативной правовой документации обеспечение информационной безопасности (ИБ) объектов информатизации ОВД напрямую связано с решением задачи проведения количественной оценки защищенности используемого ПО. Это предполагает применение адекватных показателей защищенности, и, в первую очередь, показателя временной защищенности ПО, позволяющего оценивать изменение его эксплуатационной ИБ (ЭИБ) в процессе жизненного цикла в АС ОВД [1].

В [2, 3] обосновано, что при оценивании реальной защищенности ПО

АС ОВД в качестве простейшего элемента его ЭИБ целесообразно рассматривать текущую уязвимость (текущие уязвимости определенного типа), при этом решающее влияние на защищенность ПО оказывают уязвимости высокого и критического уровней критичности.

В [4, 5] представлены разработанные математические модели, используемые для определения показателя временной защищенности ПО в отношении уязвимости ($V_{вз\ у}(t)$):

- графовая модель процесса эксплуатации уязвимости в ПО злоумышленником;
- аналитическая динамическая непрерывная модель, построенная на основе математического аппарата полумарковских процессов.

Проведение расчета $V_{вз\ у}(t)$ с помощью программного комплекса, реализующего представленные модели, требует определения временных характеристик текущей уязвимости (τ_{ij}) в процессе подготовки к ее эксплуатации в используемом ПО в соответствии с разработанной графовой моделью (i, j – состояния графовой модели), как представлено в таблице 1.

Таблица 1

Описание действий злоумышленника в процессе подготовки к эксплуатации текущей уязвимости в ПО АС ОВД

№ состояния	Характеристика состояния	τ_{ij} , с
0	Штатный режим функционирования ПО	–
1	Обнаружение уязвимости в ПО	τ_{01}
2	Поиск обнаруженной уязвимости в ПО среди уязвимостей, представленных в стандартных базах данных (БД)	τ_{12}
3	Получение информации об уровне критичности найденной уязвимости в ПО	τ_{23}
4	Самостоятельный расчет уровня критичности уязвимости в ПО	τ_{24}
5	Для уязвимости в ПО высокого и критического уровней критичности поиск эксплойта	τ_{35}
6	Для уязвимости в ПО высокого и критического уровней критичности самостоятельная разработка эксплойта	τ_{46}, τ_{56}
7	Запуск эксплойта	τ_{57}, τ_{67}

В таблице 2 описана методика определения временных характеристик текущей уязвимости в ПО АС ОВД, указанных в таблице 1, в виде последовательности поэтапных действий злоумышленника.

Таблица 2

Методика определения временных характеристик текущей уязвимости
в процессе подготовки к ее эксплуатации в ПО АС ОВД

Номер этапа	τ_{ij}	Характеристика этапа
1	τ_{01}	Выявление уязвимостей в ПО с помощью автоматизированного статического анализа программного кода на основе применения SAST-анализатора SonarQube [6, 7]. Для сканирования уязвимостей с помощью SonarQube используется плагин Dependency Check Maven, а для генерации отчета об уязвимостях – плагин OWASP dependency-check Maven. Фиксация времени сканирования. Определение среднего времени сканирования в расчете на 1-ну уязвимость
2	τ_{12}	Поиск информации о нахождении выявленных уязвимостей в ПО в National Vulnerabilities Database (NVD) на основе выполнения SQL-запроса. Фиксация времени поиска. Определение среднего времени поиска в расчете на 1-ну уязвимость
3	τ_{23}	В соответствии с полученной из NVD информацией об уровнях опасности выявленных уязвимостей в ПО выбор из них уязвимостей высокого и критического уровней. При осуществлении выбора предполагается, что влияние уязвимости в ПО на процесс функционирования АС ОВД, использующей данное ПО, максимально, следовательно, согласно [8] уровень опасности уязвимости (I_{cvssy}) равен уровню ее критичности ($V_{кpy}$). Фиксация времени выбора. Определение среднего времени выбора в расчете на 1-ну уязвимость
4	τ_{24}	Расчет уровней критичности уязвимостей в ПО, не обнаруженных при статическом анализе с использованием SonarQube (уязвимостей нулевого дня), по методике Common Vulnerability Scoring System (CVSS) v.4.0 [9] с последующим отбором уязвимостей высокого и критического уровней критичности в соответствии с таблицей, представленной в [1]. Фиксация времени расчета и отбора. Фиксация среднего времени расчета и отбора в расчете на 1-ну уязвимость
5	τ_{35}	Поиск эксплойтов для выявленных уязвимостей в ПО высокого и критического уровней критичности в БД эксплойтов ExploitDB [10, 11]. Фиксация времени поиска. Определение среднего времени поиска в расчете на 1-ну уязвимость
6	$\tau_{46} = \tau_{56}$	Для уязвимостей в ПО высокого и критического уровня критичности, эксплойты которых не найдены, самостоятельная разработка тестов на проникновение (пентестов) на основе макросов или вредоносных документов. Фиксация времени разработки. Фиксация среднего времени разработки в расчете на 1-ну уязвимость
7	$\tau_{57} = \tau_{67}$	Запуск эксплойтов, обнаруженных в БД эксплойтов ExploitDB или самостоятельно разработанных. Фиксация времени запуска. Определение среднего времени запуска в расчете на 1-ну уязвимость

В таблице 3 представлены средние значения временных характеристик текущих уязвимостей в процессе подготовки к их эксплуатации в ПО ($\tau_{01} - \tau_{67}$), рассчитанные в соответствии с описанной выше методикой для ряда версий пакета офисных программ LibreOffice, широко используемого на объектах информатизации ОВД.

Таблица 3

Результаты расчета временных характеристик текущих уязвимостей
при подготовке к их эксплуатации в ПО АС ОВД

Версии ПО	Количество уязвимостей в ПО	Количество уязвимостей высокого и критического уровней кри- тичности	Временные характеристики уязвимостей в ПО, с								
			τ_{01}	τ_{12}	τ_{23}	τ_{24}	τ_{35}	τ_{46}	τ_{56}	τ_{57}	τ_{67}
Версия LO № 6.4	21	7	31,37	1,57	120	1200	1	1200	1200	2	2
Версия LO № 7.0	15	3	35,02	1,6	130	1200	1,2	1200	1200	2,15	2,15
Версия LO № 7.1	22	5	36,73	1,74	150	1200	1,24	1200	1200	2,34	2,34
Версия LO № 7.2	17	3	37,14	1,87	155	1200	1,3	1200	1200	2,5	2,5
Версия LO № 7.3	24	3	38	1,91	162	1200	1,5	1200	1200	2,46	2,46
Версия LO № 7.4	20	6	40	2	169	1200	1,55	1200	1200	2,51	2,51
Версия LO № 7.5	19	3	41	2,1	172	1200	1,75	1200	1200	2,87	2,87
Версия LO № 7.6	25	5	42	2,17	180	1200	1,75	1200	1200	3,0	3,0
Версия LO № 24.2	10	3	45	2,3	200	1200	1,9	1200	1200	3,5	3,5

Таким образом, анализ текущих уязвимостей на этапе подготовки к их эксплуатации в ПО позволяет выявлять потенциально возможные уязвимости, которые будут актуальными в процессе жизненного цикла ПО в АС ОВД (к ним относятся текущие уязвимости высокого и критического уровней критичности, имеющие действующие эксплойты), и определять их временные характеристики.

Дальнейшее проведение расчетов $V_{вз\ y}(t)$ с помощью программного комплекса анализа и оценки защищенности ПО с учетом указанных временных характеристик позволит выбирать наиболее защищенную версию используемого ПО для эксплуатации на объектах информатизации ОВД.

СПИСОК ЛИТЕРАТУРЫ

1. Дровникова И. Г. Показатели защищенности программного обеспечения, используемого на объектах информатизации органов внутренних дел / И. Г. Дровникова, А. Д. Попова // Вестник Воронежского института МВД России. – 2024. – № 1. – С. 50–59.
2. Щеглов К. А. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / К. А. Щеглов, А. Ю. Щеглов. – Санкт-Петербург : СПбГУ ИТМО, 2014. – 83 с.
3. Ефимов А. О. Об осуществлении управления уязвимостями автоматизированных систем / А. О. Ефимов // Вестник Воронежского института МВД России. – 2023. – № 3. – С. 186–196.
4. Дровникова И. Г. Графовая модель процесса эксплуатации уязвимостей в программном обеспечении автоматизированных систем органов внутренних дел / И. Г. Дровникова, А. Д. Попова // Вестник Воронежского института ФСИН России. – 2023. – № 4. – С. 40–46.
5. Дровникова И. Г. Аналитические модели расчета показателей защищенности программного обеспечения автоматизированных систем органов внутренних дел / И. Г. Дровникова, А. Д. Попова // Вестник Воронежского института МВД России. – 2024. – № 2. – С. 22–33.
6. Static Application Security Testing (SAST). – URL: https://docs.gitlab.com/ee/user/application_security/sast/ (дата обращения: 19.09.2024).
7. Зуев П. Анализ и измерение качества программного кода с помощью SonarQube / П. Зуев. – URL: <https://o2k.ru/blog/analiz-kachestva-koda-s-pomoshchyu-sonarqube/> (дата обращения: 19.09.2024).
8. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств: методический документ от 28 октября 2022 г. // ФСТЭК России. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2> (дата обращения: 18.10.2024).
9. Common Vulnerability Scoring System version 4.0: User Guide–e. – URL: <https://www.first.org/cvss/v4.0/user-guide> (дата обращения: 18.10.2024).
10. Поиск эксплойтов для любой уязвимости. – URL: <https://www.itsecforu.ru/2022/02/21/поиск-эксплойтов-для-любой-уязвимости> (дата обращения: 05.11.2024).
11. Top 10 Exploit Databases or Finding Vulnerabilities. – URL: <https://www.how-to/top-10-exploit-databases-for-finding-vulnerabilities-0189314/> (дата обращения: 05.11.2024).

СВЕДЕНИЯ ОБ АВТОРАХ

Попова Арина Дмитриевна.

Адъюнкт кафедры автоматизированных информационных систем ОВД.
Воронежский институт МВД России.

E-mail: arnpva@mail.ru

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

Дровникова Ирина Григорьевна.

Профессор кафедры автоматизированных информационных систем ОВД.
Доктор технических наук, профессор.

Воронежский институт МВД России.

E-mail: idrovnikova@mail.ru

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

Popova Arina Dmitrievna.

Post-graduate student of the chair of information systems in interior affairs department.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: arnpva@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Drovnikova Irina Grigoryevna.

Professor of the chair of Automatic Information Systems.

Doctor of technical sciences, professor.

Voronezh Institute of the Ministry of the Interior of Russia.

E-mail: idrovnikova@mail.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: уязвимость в программном обеспечении; временные характеристики уязвимости; уровень критичности уязвимости; SAST-анализатор; SonarQube.

Keywords: vulnerability in software; time characteristics of vulnerability; vulnerability severity level; SAST analyzer, SonarQube.

УДК 004.056

**ВЛИЯНИЕ СИСТЕМЫ «ЧЕЛОВЕК-МАШИНА-СРЕДА»
НА НАДЕЖНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**THE INFLUENCE OF THE MAN-MACHINE-ENVIRONMENT SYSTEM
ON THE RELIABILITY OF AUTOMATED SYSTEMS
OF THE INTERNAL AFFAIRS BODIES OF THE RUSSIAN FEDERATION**

В статье рассмотрено влияние системы «человек-машина-среда» (Далее – «ЧМС») на надежность автоматизированных систем (Далее – АС) органов внутренних дел Российской Федерации (Далее – ОВД РФ). Исследование проведено на основе анализа возможных человеческих и технических факторов, а также факторов окружающей среды, влияющих на надежность АС, различных источников научной литературы и публикаций. Отмечена важность системы «ЧМС» при расчете надежности АС ОВД РФ, отражены основные факторы, влияющие на надежность АС, предложен вариант расчета вероятности правильного и своевременного выполнения задачи оператором.

The article examines the impact of the man-machine-environment system (hereinafter - CHMS) on the reliability of automated systems (hereinafter - AS) of the internal affairs bodies of the Russian Federation (hereinafter - the Ministry of Internal Affairs of the Russian Federation). The study was conducted on the basis of an analysis of possible human and technical factors, as well as environmental factors affecting the reliability of nuclear power plants, various sources of scientific literature and publications. The author noted the importance of the CHMS system in calculating the reliability of the automated control system of the Russian Federation, reflected the main factors affecting the reliability of the automated control system, and proposed a variant for calculating the probability of correct and timely task completion by the operator.

С необходимостью вычисления надёжности технических устройств и систем столкнулось человечество с момента их внедрения. Так, в начале XX века возникла потребность в заправке газовых фонарей. Чтобы вычислить время их заправки, требовались знания среднего времени горения. Позднее методику вычисления среднего времени работы электронной лампы разработал шведский учёный В. Вейбулл. В дальнейшем она стала более известна как распределение Вейбулла [1].

Одними из первых советских исследований в области оценки надёжности стали работы профессора В. И. Сифорова и инженера Б. М. Якуба. В исследованиях расчет надежности систем определялся как произведение

надёжности отдельных элементов с последовательным соединением компонентов [2].

С развитием технологий одной из важных задач становится оценка надежности АС. Это обусловлено ростом требований к сложности продукции и ее качеству. В результате сбоев или отказа техники, а также различных устройств и приборов в неподходящий момент могут возникнуть самые серьезные последствия, включая возможную гибель людей, что не может оправдываться никакими экономическими показателями. Поэтому первоочередными задачами для производителей в последнее время становится уменьшение затрат на обслуживание технических средств, их ремонт, продление срока службы выпускаемой продукции и повышение ее надёжности.

Вопросы влияния системы «ЧМС» на надежность ранее рассматривались в таких исследованиях как [3,4,5].

Применение АС с высокими показателями надежности в ОВД позволяет:

1. обеспечивать непрерывную работу и отслеживание всех происходящих событий, что способствует оперативному реагированию на возможные угрозы и предотвращению различных инцидентов [6];

2. оперативно анализировать информацию и принимать решения – это способствует оптимизации работы сотрудников и повысить общую эффективность работы ОВД;

3. обеспечить доверие к АС, тогда пользователи, могут быть уверены, что система не подведет их в критических ситуациях и будет работать стабильно;

4. сократить время на обработку информации и уменьшить нагрузку на сотрудников, что способствует экономии ресурсов и повышению производительности.

Надежность АС и ее элементов является важным свойством, определяющим качество тех операций, для которых эти АС предназначены. Рост количества технических и технологических отказов приводит к снижению надежности систем.

Часто это возникает в связи с нарушением согласованности между отдельными составляющими системы «человек-машина-среда» (далее – «ЧМС»). Машины управляются и обслуживаются человеком-оператором, и поэтому оператор рассматривается как важный компонент, от которого зависит надежность всей системы «ЧМС» [3]. Современные АС характеризуются требовательностью как к оборудованию и технологий, так и к человеку, который является элементом системы «ЧМС». Но человек не просто элемент системы, а самый важный элемент.

Надежность АС в значительной степени зависит от взаимодействия человека, машины и окружающей среды. Изучение этого взаимодействия позволит лучше понять и предсказывать возникновение отказов, связанных с ошибками оператора или неблагоприятными условиями среды.

Результаты исследования системы «ЧМС» помогут оптимизировать интерфейсы между человеком и машиной, улучшить процессы обучения персонала. Это в свою очередь позволит повысить надежность, безопасность и эффективность функционирования АС.

Система «ЧМС» применима в различных сферах, таких как авиация, энергетика, промышленность, транспорт. Исследования в этом направлении имеют высокую практическую значимость для многих отраслей.

Изучение системы «ЧМС» требует объединения знаний из таких областей, как эргономика, психология, инженерия, информатика. Это делает данное направление интересным и перспективным с точки зрения развития междисциплинарного научного подхода.

В целом, исследование влияния системы «ЧМС» на надежность АС ОВД РФ является актуальным и многообещающим направлением, способным внести значительный вклад в повышение безопасности и эффективности современных технических систем.

СПИСОК ЛИТЕРАТУРЫ

1. Распределение Вейбулла: история и современность / С. Я. Гродзенский // Нелинейный мир. – 2023. – Т. 21, № 3. – С. 54-65. – DOI 10.18127/j20700970-202303-06. – EDN HNVPDQ.

2. Анализ структурных схем с помощью сигнатур. Вычисление сигнатуры сложной структуры / В. А. Чепурко, А. Н. Черняев // Надежность. – 2022. – Т. 22, № 2. – С. 10-21. – DOI 10.21683/1729-2646-2022-22-2-10-21. – EDN HCFFFB.

3. Оптимизация системы «человек-машина-среда»: оценка надежности человека-оператора / В. И. Швецова // Системы контроля окружающей среды. – 2021. – № 1(43). – С. 147-153. – DOI 10.33075/2220-5861-2021-1-147-153. – EDN NQYFBT.

4. Анализ человеко-машинных систем по воздействию факторов на безопасность и работоспособность оператора / А. А. Кузнецов // Проблемы энергообеспечения, информатизации и автоматизации, безопасности и природопользования в АПК: Международная научно-техническая конференция, Брянск, 12–14 сентября 2012 года. – Брянск : Издательство Брянской ГСХА, 2012. – С. 69-78. – EDN TVZJAZ.

5. Психология труда : учебное пособие для бакалавров / В. А. Шамис, Г. Г. Левкин. – Москва : Ай Пи Ар Медиа, 2023. – 130 с. – ISBN 978-5-4497-1828-0. – EDN SJLLZO.

6. К вопросу использования новой информационной технологии, связанной с дополнительной аутентификацией субъектов доступа по клавиатурному почерку, в системах защиты информации от несанкционированного доступа на объектах информатизации органов внутренних дел / А. В. Бацких, И. Г. Дровникова, Е. А. Рогозин // Вестник

Воронежского института МВД России. – 2020. – № 2. – С. 21–33. – EDN DDVYPU.

СВЕДЕНИЯ ОБ АВТОРЕ

Романова Виктория Романовна.

Адъюнкт кафедры автоматизированных информационных систем ОВД.
Воронежский институт МВД России.

E-mail: romanovna_vika@inbox.ru

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

Romanova Victoria Romanovna.

Adjunct of the Department of Automated Information Systems of the Internal Affairs Directorate.

Voronezh Institute of the Ministry of Internal Affairs of Russia.

E-mail: romanovna_vika@inbox.ru

Russia, 394065, Voronezh, Prospect Patriotov, 53.

Ключевые слова: надежность; автоматизированная система; факторы надежности; факторы среды; «человек-машина-среда».

Keywords: security assessment; security requirements; data bank of information security threats; security indicator; security criteria; operating system; automated calculation system.

УДК 004.052

Научное издание

НАУЧНЫЙ БЮЛЛЕТЕНЬ
ВОРОНЕЖСКОГО ИНСТИТУТА МВД РОССИИ

*Сборник материалов
научно-представительских мероприятий*

Выпуск 4

В авторской редакции

Компьютерная верстка Н. В. Крючковой

Объем 3,5 Мб

Воронежский институт МВД России,
394065, Воронеж, просп. Патриотов, 53