БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ ИМЕНИ И.Д. ПУТИЛИНА

Проблемы информационного обеспечения деятельности правоохранительных органов

Сборник статей
4-й Международной научно-практической конференции
13 октября 2017 года

Белгород
Белгородский юридический институт МВД России имени И.Д. Путилина
2018

УДК 351.74:002
ББК 67.401.114
П 78

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России имени
И.Д. Путилина

Выпускается с 2015 года.

П 78 Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 4-й Международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2018. – 242 с.
ISBN 978-5-91776-224-1

Редакционная коллегия:

Амельчаков И.Ф. – начальник Белгородского юридического института МВД России имени И.Д. Путилина, кандидат юридических наук, доцент (председатель);

Озеров И.Н. – заместитель начальника института по научной работе, кандидат юридических наук, доцент (зам. председателя);

Прокопенко А.Н. – начальник кафедры информационно-компьютерных технологий в деятельности ОВД, кандидат технических наук, доцент;

Насонова В.А. – профессор кафедры информационно-компьютерных технологий в деятельности ОВД, кандидат физико-математических наук, доцент;

Акапьев В.Л. – доцент кафедры информационно-компьютерных технологий в деятельности ОВД, кандидат педагогических наук (отв. секретарь).

В сборнике представлены научные статьи, в которых исследуются проблемы противодействия компьютерным преступлениям и обеспечения информационной безопасности.

Предназначен для курсантов, слушателей, адъюнктов, профессорско-преподавательского состава образовательных организаций системы МВД России, сотрудников органов внутренних дел.

УДК 351.74:002
ББК 67.401.114

ISBN 978-5-91776-224-1

© РИО Белгородского юридического
института МВД России имени
И.Д. Путилина, 2018

СЕКЦИЯ № 1.
ТЕОРЕТИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ВЕДОМСТВЕННОГО ОБРАЗОВАНИЯ НА СОВРЕМЕННОМ ЭТАПЕ (НА ПРИМЕРЕ БЕЛ ЮИ МВД РОССИИ ИМЕНИ И.Д. ПУТИЛИНА)

USE OF INFORMATION TECHNOLOGIES IN THE SYSTEM OF DEPARTMENTAL EDUCATION AT THE PRESENT STAGE (ON AN EXAMPLE BELGOROD LAW INSTITUTE OF MIA OF RUSSIA NAMED AFTER I.D. PUTILIN)

Жукова Полина Николаевна,
Прокопенко Алексей Николаевич,
Гуржий Алексей Александрович
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Zhukova Polina Nikolaevna,
Prokopenko Alexey Nikolaevich,
Gurzhy Alexey Aleksandrovich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin)

Аннотация: рассматриваются вопросы применения информационных технологий в учебном процессе как инструмента в рамках педагогических технологий, изучения технических средств или программного обеспечения, которые используются для решения оперативно-служебных задач, создания на основе технических средств и программного обеспечения специализированной учебной модели или имитационных курсов. Анализируются направления использования информационных технологий для организации учебного процесса как для планирования учебного процесса в целом, так и для учета работы педагогического состава.

Ключевые слова: информационные технологии в образовании, электронная информационно-образовательная среда, специализированное программное обеспечение.

Annotation: questions of application of information technologies in educational process as tool within pedagogical technologies, a study of technical means or the software which are used for the decision of the operational and official tasks, creation on the basis of technical means and the software of a specialized training model or imitative courses are

considered. The directions of use of information technologies for the organization of educational process, both for planning of educational process in general, and for accounting of operation of teaching staff are analyzed.

Key words: information technologies in education, the electronic information and education environment, the specialized software.

Создание и совершенствование технических средств и программного обеспечения привело к созданию новых технологий в различных сферах научной и практической деятельности. Одной из таких сфер стало образование – процесс передачи систематизированных знаний, навыков и умений от одного поколения к другому. Являясь само по себе мощной информационной сферой, образование быстро откликнулось на возможности современной техники. В процессе педагогической работы применяются различные новаторские приемы, направленные на интенсификацию учебного процесса.

Повышения качества образования можно достичь с помощью индивидуализации учебного процесса, внедрения новых, более информативных и наглядных методов обучения. Необходимо отметить, что индивидуализация образования в первую очередь должна происходить через воспитание у подрастающего поколения информационной культуры, навыков самостоятельной работы с информацией, потребности к самообразованию. Данная проблема является глобальной для всей системы высшего образования в стране и непосредственно касается системы образования МВД России. Сотрудники правоохранительных органов должны обладать не только компьютерной грамотностью, но и иметь навыки использования информационных и сетевых технологий для решения служебных задач и постоянного самообразования. Вообще, с увеличением количества информации на первый план выходит задача не научить обучающегося, а научить его учиться самостоятельно, что позволит ему в течение всей последующей деятельности оставаться способным к самосовершенствованию и переподготовке.

Информационные технологии в системе образования в последние годы применяются для решения двух глобальных задач:

1. Использование информационных технологий непосредственно в учебном процессе.

2. Использование информационных технологий для организации учебного процесса.

Информационные технологии в учебном процессе используются по трем направлениям.

1. *Использование технических средств и программного обеспечения как инструмента в рамках педагогических технологий*.

Здесь можно говорить о том, что компьютерная техника в первую очередь и различные технические средства визуализации – во вторую используются для индивидуализации, иллюстрирования, оживления учебного материала.

Основным педагогическим инструментом является специализированное программное обеспечение, предназначенное для осуществления учебного процесса. К нему относятся программные среды для обучения и программные продукты для обучающихся, которые облегчают им изучение учебных дисциплин.

В Бел ЮИ МВД России имени И.Д. Путилина используется электронная информационно-образовательная среда (далее – ЭИОС), электронный УМК и электронная библиотека. Указанные системы позволяют обучающемуся самостоятельно получать доступ к различным образовательным ресурсам.

В нашем институте создана ЭИОС на базе программной среды Moodle, в которой осуществляется размещение материалов для обучающихся, контрольное тестирование курсантов и слушателей, дистанционное обучение отдельных категорий обучающихся. Функционал использования ЭИОС постоянно расширяется. В частности, в ЭИОС организовано проведение теоретических занятий по правовой, служебной, огневой и морально-психологической подготовке. В прошлом учебном году занятия в рамках эксперимента проводились в ЭИОС только для 3 учебной группы. В этом году эксперимент распространен на все учебные группы по профессиональной служебной подготовке и морально-психологической подготовке.

ЭИОС является доступной как через Интернет с сайта института под названием «Образовательный портал института», так и в локальной сети института. Материалы дополнительных профессиональных программ доступны посредством интегрированной мультисервисной телекоммуникационной сети МВД России. Таким образом, обучающиеся имеют фактически неограниченный доступ к системе.

Следующим педагогическим инструментом является программное обеспечение, используемое для обеспечения и контроля учебного процесса профессорско-преподавательским составом.

К ним относятся программы контроля знаний, программы учета оценок обучающихся, программы визуализации информации и т.п. В нашем институте используются программа тестирования My Test, тесты в рамках ЭИОС, электронный журнал для учета оценок, полученных обучающимися, база выпускных квалификационных работ.

Еще одним педагогическим инструментом являются технические средства визуализации.

В основном применяется сочетание компьютера и проектора с экраном. В качестве второго варианта используется компьютер и интерактивная доска. Оба комплекта могут быть оснащены аудиосистемой или быть без нее. Кроме того, может использоваться комплект в виде телевизора и передающего устройства (видеодвойка, TV с DVD и т.д.). Демонстрируемые материалы – это видео или презентации, созданные в MS Power Point.

Анализ использования информационных технологий как педагогических инструментов в Бел ЮИ МВД России имени И.Д. Путилина позволяет сделать следующие выводы и предложения:

а) представляется излишним дублирование двух систем: ЭИОС и электронного УМК, которые решают аналогичные задачи. В этой связи можно отказаться от электронного УМК в пользу более эффективной и функциональной ЭИОС;

б) считаем, что необходимо, не отказываясь в общем от My Test, более активно использовать для тестирования в рамках самостоятельной работы обучающихся возможности ЭИОС;

в) следует более активно использовать возможности электронной информационно-образовательной среды при обучении слушателей факультета заочного обучения. Необходимо отметить, что наиболее эффективно ЭИОС используется в рамках заочной формы обучения и дистанционного образования. Использование электронных сред при очном образовании менее популярно, но также выполняет функцию индивидуализации обучения. Опыт других образовательных организаций показал, что материалы для самостоятельной работы слушателей ФЗО в межсессионный период должны включать в себя:

– текст рабочей программы учебной дисциплины;

– методические указания слушателю по изучению учебных материалов и выполнению заданий;

– тексты теоретического материала: учебники, учебные пособия, лекции, фондовые лекции, хрестоматии и т.д.;

– иллюстративные материалы: фотографии, видео, презентации, схемы и т.д.;

– вопросы к семинарским и практическим занятиям;

– вопросы к зачету или экзамену;

– перечень нормативных правовых актов или выдержки из них (можно, например, тексты приказов МВД России);

– задачи для самостоятельного решения;

– тесты по темам или разделам учебной дисциплины.

Таким образом, к началу итоговой сессии слушатель должен будет изучить учебный материал, решить задачи, поставленные преподавателем, и ответить на вопросы теста.

В настоящий момент по подавляющему числу учебных дисциплин предусмотрена контрольная работа, которая сдается в виде компьютерного теста на итоговой сессии. Представляется, что данные контрольные работы должны состоять из одного или нескольких тестов, практических задач или материалов эссе. Выполняться они должны в ЭИОС в межсессионный период, а в ходе итоговой сессии осуществляется только защита результатов выполнения данной контрольной работы.

2. *Изучение технических средств или программного обеспечения, которые используются для решения оперативно-служебных задач*.

В этом случае, обучающиеся изучают технику или программные продукты с целью наработки навыков работы с ними в своей дельнейшей учебной или профессиональной деятельности. В рамках данного направления использования информационных технологий можно выделить:

1) специализированное программное обеспечение, которое используют органы внутренних дел в своей деятельности.

В Бел ЮИ МВД России имени И.Д. Путилина изучаются «КонсультантПлюс», «ГАРАНТ», СТРАС «Юрист», программы для составления субъективных портретов, сервисы ИСОД МВД России. Причем в рамках учебной дисциплины «Информатика и информационные технологии в профессиональной деятельности» справочные правовые системы и «Фоторобот» изучаются для приобретения навыков их использования. А в ходе изучения последующих учебных дисциплин указанные программы используются для решения конкретных задач – поиска документов, составления портретов и т.д.;

2) технические средства и оборудование, которое используют органы внутренних дел в своей деятельности.

К ним относятся специализированные криминалистические, досмотровые, транспортные технические средства и оборудование, а также технические средства и оборудование специальной техники. В нашем институте данное направление в последние годы активно развивается, особенно на кафедрах криминалистики и обеспечения безопасности на объектах транспорта.

Анализ данного направления использования информационных технологий показывает, что по мере приобретения или централизованной поставки оборудования, технических средств и программного обеспечения осуществляется их изучение. Существует проблема с изучением служебных сервисов ИСОД МВД России по профилю обучающихся, доступ к которым не открыт для образовательных организаций МВД России. Предполагается, что указанная проблема будет решена после централизованной разработки сервиса, который будет включать в себя учебные модули, имитирующие реальные служебные сервисы ИСОД МВД России.

3. *Создание на основе технических средств и программного обеспечения специализированной учебной модели или имитационных курсов*.

В рамках данного использования информационных технологий обучающиеся изучают особенности оперативно-служебной деятельности при работе не на реальном устройстве или с реальным программным обеспечением, а при работе с учебным устройством или программным обеспечением. Можно выделить следующие имитационные модели и курсы.

Обучающие тренажёры.

К ним относятся тренажёры отдельных технических средств, которые полностью или частично имитируют работу реальных устройств с использованием специализированного программного обеспечения. В качестве примера используемых в Бел ЮИ МВД России имени И.Д. Путилина обучающих тренажёров можно привести:

– интерактивный стрелковый тренажер «Рубин»;

– учебную систему видеонаблюдения и видеоаналитики;

– обучающий тренажер – магнито-оптический прибор для идентификации и выявления фальсификаций номеров агрегатов транспортных средств «Регула 7505М»;

– обучающий тренажер – портативный рентгенофлуоресцентный анализатор «МетЭксперт»;

– обучающий тренажер – детектор взрывчатых веществ и наркотических средств «SABRE 4000» и другие.

Обучающее программное обеспечение и имитационные информационные системы.

Данное программное обеспечение позволяет создать условия для изучения учебного материала в ситуации, приближенной к реальной. В качестве примера можно привести автоматизированное рабочее место следователя (дознавателя), которое имитирует оперативно-служебную деятельность, предоставляя дополнительный учебный и практический материал.

Учебные полигоны.

В нашем институте учебные полигоны расположены преимущественно на кафедрах криминалистики и обеспечения безопасности на объектах транспорта:

– макет железнодорожного пассажирского вагона;

– макет гражданского воздушного судна «Як-40»;

– ситуационный полигон «Квартира»;

– ситуационный полигон «Участок местности»;

– полигон «Подпольная нарколаборатория»;

– полигон «Криминалистической техники и музейной экспозиции»;

– полигон осмотра мест происшествий по фактам краж из помещений финансово-кредитных организаций (банков);

– полигон «Автомобиль» и другие.

Анализ использования в институте имитационных моделей и курсов позволяет сделать следующие выводы и предложения:

а) наиболее развитым направлением можно признать изучаемые технические средства и оборудование, а также созданные на их основе учебные полигоны. Однако по направлению «специальная техника» требуется существенное обновление оборудования;

б) основной проблемой является малое количество обучающего программного обеспечения и имитационных информационных систем. Их небольшое количество объясняется значительной ценой программного обеспечения и почти полным отсутствием учебных версий программного обеспечения, используемого в МВД России. Для устранения данной проблемы в ближайшие два года запланирована разработка межкафедрального электронного обучающего комплекса раскрытия и расследования отдельных видов преступлений.

Таким образом, можно констатировать, что использование информационных технологий непосредственно в учебном процессе носит в институте системный характер. Дальнейшее поступательное развитие в данном направлении должно быть сконцентрировано по направлению расширения использования ЭИОС института и созданию специализированного обучающего программного обеспечения.

Информационные технологии для организации учебного процесса применяются по двум направлениям.

1. Организация образовательной деятельности в целом.

В данном направлении речь идет о планировании учебного процесса, составлении расписания, учете учебных занятий, расчете учебной нагрузки, отчете об исполнении учебной нагрузки и т.д. Образовательными организациями создается или закупается программное обеспечение для составления учебных планов, расписания занятий, учета успеваемости.

Анализ данного направления показывает, что в Бел ЮИ МВД России имени И.Д. Путилина указанное программное обеспечение используется только по отдельным направлениям. Причем используемое программное обеспечение не адаптировано под особенности учебного процесса в образовательной организации МВД России и не интегрировано между собой. В результате возникает дублирование по одним направлениям и недостаточное использование возможностей информационных технологий по другим направлениям.

Для создания единого информационного пространства Бел ЮИ МВД России имени И.Д. Путилина необходимы разработка и внедрение интегрированной системы управления учебным процессом.

Предполагается, что на первом этапе интегрированная система управления учебным процессом будет состоять из трех блоков.

Первый блок – **«Блок планирования учебного процесса»**. Он будет включать в себя:

1. Учебные планы для каждого взвода (специализации). В настоящий момент учебные планы составляются в другой программе, приобретенной институтом. На первом этапе составленные учебные планы будут в готовом виде переноситься в интегрированную систему. Внесение учебных планов будет осуществляться учебным отделом (для очной формы обучения), факультетом заочного обучения (для заочной формы обучения), адъюнктурой (для адъюнктов). На втором этапе предполагается разработка собственного модуля для составления учебных планов.

2. Образовательные программы профессиональной подготовки, переподготовки и повышения квалификации. Внесение программ будет осуществляться факультетом переподготовки и повышения квалификации и учебным отделом (для профессиональной подготовки).

3. Закрепление за кафедрами учебных дисциплин и модулей – каждая учебная дисциплина или учебный модуль за все время обучения должны быть закреплены за конкретной кафедрой. Если учебная дисциплина преподается на нескольких кафедрах, то производится закрепление за кафедрами конкретных часов. Закрепление осуществляется теми подразделениями, которые вносят в систему учебные планы и образовательные программы.

4. Количество обучающихся в каждом взводе вносится учебным отделом, ФЗО, ФПП и ФПиПК.

5. Тематические планы по каждой учебной дисциплине или модулю. Темпланы вносятся кафедрой с одновременной проверкой системой соответствия тематического плана учебному плану.

6. Структура кафедр и закрепление профессорско-преподавательского состава за кафедрами в системе (вносится отделом кадров).

7. Расстановка преподавателей, которые запланированы для проведения занятий, приема зачетов и экзаменов, проверки практикумов или курсовых работ (вносится кафедрами).

На основании всех внесенных данных система автоматически составляет план учебной нагрузки кафедры.

В случае изменения учебных планов или образовательных программ возможно внесение оперативных изменений в систему с одновременным пересчетом планируемой нагрузки.

Второй блок – **«Блок отчета о выполнении учебного процесса»**. Он будет включать в себя:

1. Расписание учебных занятий. В настоящий момент расписание составляется в специализированной программе для составления расписания, приобретенной институтом. На первом этапе составленное расписание будет в готовом виде переноситься в интегрированную систему учебным отделом. На втором этапе предполагается разработка собственного модуля составления расписания.

2. Изменения расписания учебных занятий на основании рапортов на замену (вносятся учебным отделом).

3. Электронный журнал учебных занятий. Сами учебные занятия вносятся в журнал автоматически на основании расписания. Преподаватель вносит оценки и отмечает отсутствующих, заполнение журнала проверяется факультетами.

4. Отчет за месяц о выполнении учебной нагрузки преподавателя. Отчет составляется системой автоматически на основании данных электронного журнала, а также внесенной преподавателем информации о проведении практик и работе с дипломниками.

5. Отчет за месяц о выполнении учебной нагрузки кафедры. Отчет составляется автоматически на основании отчетов преподавателей.

6. Отчет за учебный год о выполнении учебной нагрузки кафедры. Отчет составляется автоматически на основании отчетов за месяц.

7. Информация о текущей успеваемости обучающихся на основании данных электронного журнала.

Каждый следующий элемент системы должен быть связан с предыдущим, а проверка правильности его заполнения осуществляется системой. Предлагаемая интегрированная информационная система позволит ликвидировать ошибки при составлении тематических планов, расписания, отчетов о выполненной нагрузке преподавателей и кафедр, а также при планировании учебной нагрузки. Одновременно она позволит не составлять в бумажном виде тематические планы и отчеты о нагрузке преподавателей за месяц.

2. Учет работы профессорско-преподавательского состава.

Деятельность профессорско-преподавательского состава включает в себя учебную, методическую, научную и воспитательную работу, а также другие виды работ. Планирование деятельности преподавателя осуществляется в соответствии с индивидуальным планом преподавателя.

В Бел ЮИ МВД России имени И.Д. Путилина отчеты о работе преподавателя осуществляются путем заполнения индивидуального плана, а также отдельно по разным направлениям. Так, отдельно учитывается учебная нагрузка, отдельно считаются публикационная активность и издательская деятельность, отдельно учитывается работа куратора и т.д. Кроме того, преподавателями осуществляется большое количество незапланированных работ, особенно методических, которые для того, чтобы не путать отчетность, не записываются в индивидуальный план.

В результате складывается ситуация, что реальную комплексную оценку деятельности профессорско-преподавательского состава осуществить сложно. Для исправления сложившейся ситуации на базе имеющейся в институте системы рейтинговой оценки ППС (Мотивация) будет создан третий блок интегрированной системы – **«Блок учета работы профессорско-преподавательского состава»**, который будет включать в себя:

1. Отчет о выполненной учебной нагрузке. Вносится автоматически по данным электронного журнала и подтверждается учебным отделом.

2. Сведения о проделанной методической работе. Предполагается засчитывать в качестве данных сведений материалы, утвержденные методическим советом института и внесенные в ЭИОС. К ним могут относиться рабочие программы учебных дисциплин, образовательные программы профессиональной подготовки, переподготовки и повышения квалификации, частные методики, практикумы и т.д. Методические материалы подтверждаются начальником кафедры и учебным отделом.

3. Сведения о научных работах, публикациях, участии в конференциях, конкурсах. В случае если научные работы и публикации осуществлялись, а конференции и конкурсы проводились в Бел ЮИ МВД России имени И.Д. Путилина, то они вносятся в систему научно-исследовательским отделом и редакционно-издательским отделом. В случае если публикации (участие в конференциях и конкурсах) осуществлялись за пределами института, то они вносятся преподавателем, а подтверждаются начальником кафедры и РИО на основании сведений РИНЦ.

4. Звания и повышение квалификации. Вносятся преподавателем, подтверждаются начальником кафедры и отделом кадров.

5. Сведения о кадровой работе и работе по морально-психологическому обеспечению служебной деятельности. Вносятся преподавателем, отделом кадров и отделом морально-психологического обеспечения, подтверждаются начальником кафедры и отделом кадров или ОМПО.

6. Работа с иностранными слушателями и международное сотрудничество. Вносятся преподавателем, подтверждаются начальником кафедры и учебным отделом.

Данные в систему должны вноситься преподавателем и отделами, а подтверждаться начальником кафедры и соответствующими подразделениями. Предложенные изменения позволят осуществлять системный учет деятельности профессорско-преподавательского состава в постоянном режиме. В перспективе возможен перевод индивидуальных планов работы преподавателей в электронную

форму с заполнением в интегрированной системе. На втором этапе разработки интегрированной системы, как отмечалось выше, предполагается создание собственных модулей разработки учебных планов и составления расписания.

Самым важным итогом второго этапа разработки системы представляется создание своеобразного портфолио каждого преподавателя в рамках третьего блока. На основе портфолио будут формироваться индивидуальные планы преподавателей, отчеты об их деятельности, рейтинг профессорско-преподавательского состава, отчеты о работе кафедр в общем и по отдельным направлениям, а также сведения по институту в целом по разным направлениям деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Страхов А.А., Анисимова Т.В. Организация обучения по дисциплинам информатики основных и дополнительных профессиональных образовательных программ нового поколения // Вестник Московского университета МВД России. 2015. № 12. С. 221-225.

2. Булгаков О.М., Гривенная Е.Н., Старостенко И.Н. К вопросу о математической модели рейтинговой оценки педагогической деятельности преподавателей образовательной организации МВД России // Вестник Воронежского института МВД России. 2017. № 1. С. 24-34.

ПРАВОВЫЕ ИНТЕРНЕТ-РЕСУРСЫ РЕСПУБЛИКИ КАЗАХСТАН И ИХ РОЛЬ В ПОСТРОЕНИИ ПРАВОВОГО ГОСУДАРСТВА

JUDICIAL INTERNET RESOURCES OF THE REPUBLIC OF KAZAKHSTAN AND THEIR ROLE IN THE DEVELOPMENT OF THE STATE OF LAW

Молбасин Сагынган Игенович
(Научно-исследовательский институт Карагандинской академии МВД Республики Казахстан имени Баримбека Бейсенова)

Molbassin Sagyngan Igenovich
(Karaganda Academy of the MIA of the Republic of Kazakhstan named after Barimbek Beisenov)

Аннотация: статья посвящена изучению роли правовых интернет-ресурсов в повышении правовой культуры, правосознания граждан и снижении уровня преступности в обществе. Автор исследует правовые интернет-ресурсы, функционирующие в Республике Казахстан.

Ключевые слова: Интернет, правовые интернет-ресурсы, правовой сайт, правовой интернет-портал, правовая поисковая система, правовое государство, правосознание.

Annotation: the given considers the role of the judicial Internet resources in increase of legal culture, legal awareness of citizens and crime reduction. The author studies the judicial Internet resources that occur and function within the Republic of Kazakhstan.

Key words: Internet, judicial Internet resources, judicial website, judicial web portal, judicial search engine, a state of law, legal awareness.

Построение правового государства требует создания эффективных механизмов использования правовой информации во всех сферах общественной жизни. Наличие эффективной системы распространения правовой информации является одним из ключевых условий развития любой страны как цивилизованного правового государства [1, с. 47]. Доступность правовой информации и ее распространенность напрямую влияют на повышение уровня основных показателей правового государства – правовой культуры, правового воспитания и правосознания граждан. Как отмечает Г.Э. Адыгезалова, усиление роли правового воспитания и образования, развитие правовой культуры и правосознания, повышение правовой информированности – это те условия, при которых возможен рост социально активного поведения граждан, стремящихся соблюдать, исполнять, использовать право, отстаивать свои интересы посредством права и бороться за свои права [2, с. 245-247]. Кроме того, повышение уровня правового воспитания, правовой культуры и правосознания оказывает непосредственное влияние на уровень преступности в обществе. По мнению С.А. Тимко, правосознание – неотъемлемый элемент правовой культуры, характеризующий осознание социальной действительности в правовых категориях и предполагающий знание законодательства, правильное к нему отношение, понимание, использование, применение и «…определяющий деятельность людей в государственно-правовой сфере…». Подобные знание и отношение в совокупности с активной жизненной позицией – залог низкой криминализации населения и успешного противодействия преступности [3, с. 92]. Таким образом, посредством правового информирования граждан можно качественно повлиять на уровень их правовой грамотности, а также воздействовать на уровень преступности в обществе.

Одним из эффективных способов правового информирования является передача информации посредством электронных средств. Данный вопрос все больше приобретает актуальность с развитием интернет-технологий во всем мире. Электронная передача информации дает возможность охватить широкие массы населения. По последним данным, на современном этапе более 40% населения планеты имеет доступ к Интернету, и почти в каждых 7 из 10 домохозяйств есть мобильный телефон. Цифровые технологии дали ряд преимуществ – упрощение доступа населения и бизнеса к государственным услугам, ускорение обмена информацией, появление новых возможностей для ведения бизнеса, создание новых цифровых продуктов и т.д. [4]. Таким образом, интернет-технологии и интернет-ресурсы на сегодняшний день являются мощным «ору-

дием» в сфере правового информирования населения и повышения уровня правового воспитания, правовой культуры и правосознания граждан.

Как и в других странах в Республике Казахстан ведутся активные работы по развитию интернет-технологий. На современном этапе в стране сформирована достаточно развитая инфраструктура предоставления интернет-услуг. Разработана Государственная программа «Цифровой Казахстан», одной из целей которой является переход на проактивное государство – усовершенствование системы электронного и мобильного правительства, оптимизация сферы предоставления государственных услуг. Безусловно, для выполнения задач в рамках программы будет проводиться работа по дальнейшему развитию правовых интернет-ресурсов в республике. В этой связи считаем необходимым изучить действующую систему правовых ресурсов Интернет в Республике Казахстан. Прежде чем подробнее рассмотреть правовые интернет-ресурсы, функционирующие в Казахстане, необходимо разъяснить само понятие «интернет-ресурс». Согласно распространенному в интернет-словарях определению, интернет-ресурсом (синонимы «веб-ресурс, веб-сайт, веб-сервис, сайт») является совокупность интегрированных средств технического и программно-аппаратного характера, а также информации, предназначенной для публикации во Всемирной паутине. В законодательстве Республики Казахстан также дается определение данному понятию. Так, в п. 46 ст. 1 Закона Республики Казахстан от 24 ноября 2015 г. № 418-V «Об информатизации» закреплено, что интернет-ресурс – электронный информационный ресурс, отображаемый в текстовом, графическом, аудиовизуальном или ином виде, размещаемый на аппаратно-программном комплексе, имеющий уникальный сетевой адрес и (или) доменное имя и функционирующий в Интернете [5]. Анализируя вышеприведенные определения, приходим к выводу о том, что основным предназначением интернет-ресурсов являются размещение или передача информации. В зависимости от сферы деятельности интернет-ресурсы могут содержать в себе информацию разных отраслей жизнедеятельности общества, в том числе и правовую.

К интернет-ресурсам принято относить сайты, порталы и поисковые системы. Сайтом или веб-сайтом (от англ. website: web – «паутина, сеть» и site – «место», буквально «место, сегмент, часть в сети») является совокупность логически связанных между собой веб-страниц, а также место расположения контента сервера. Обычно сайт в Интернете представляет собой массив связанных данных, имеющий уникальный адрес и воспринимаемый пользователем как единое целое [6, с. 432]. Интернет-порталом же является многофункциональный сайт, который позволяет пользоваться различными нужными ресурсами и помогает получать актуальную и полную информацию по нескольким или одному направлению. Интернет-портал, как многие считают, это не только сайт обо всем. Он также может иметь узкий профиль, поэтому имеются отличия узкотематического интернет-портала от обычного информационного сайта. Поисковая система – это аппаратно-программный комплекс, который предназначен для осуществления функции поиска в интернете и реагирующий на пользовательский запрос, который обычно задают в виде какой-либо текстовой фразы (или точнее поискового запроса), выдачей ссылочного списка на информационные

источники, осуществляющейся по релевантности (например, к распространенным системам поиска относятся Google, Bing, Yahoo, Baidu. В Рунете – Яндекс, Mail.Ru, Рамблер). Правовыми являются те интернет-ресурсы (сайты, порталы и поисковые системы), которые содержат информацию правового характера.

В науке информацию правового характера принято подразделять на виды. Так, А.М. Волков правовую информацию разделяет на официальную; индивидуально-правового характера, имеющую юридическое значение; неофициальную. По мнению автора, официальная правовая информация исходит от полномочных государственных органов, имеет юридическое значение и направлена на регулирование общественных отношений. Официальная правовая информация, в свою очередь, подразделяется на нормативную и иную официальную правовую информацию. Нормативная часть правовой информации представляет собой совокупность нормативных правовых актов во всем их многообразии и динамике. Индивидуально-правовой характер, по мнению А.М. Волкова, имеет информация, обладающая юридическим значением. Она предоставляется различными субъектами права и предназначена для создания, изменения и прекращения конкретных правоотношений (договоры, сделки, заявления, жалобы). Данные субъекты права не имеют властных полномочий. Неофициальная правовая информация – материалы и сведения о законодательстве и практике его осуществления (применения), не влекущие правовых последствий и обеспечивающие эффективную реализацию правовых норм [7, с. 84]. Таким образом, критерием для классификации правовой информации могут служить субъекты, её предоставляющие, или её предназначение. О.А. Манохина и В.И. Кленина по схожему критерию приводят классификацию правовых ресурсов Интернет, согласно которому правовые интернет-ресурсы могут подразделяться на сайты, принадлежащие органам государственной власти; информационно-правовые базы данных; правовые СМИ в сети Интернет; виртуальные правовые клубы и правовые форумы; правозащитные организации и юридические фирмы; WWW-страницы известных юристов [8, с. 122-123]. Считаем, что к отдельному виду правовых ресурсов Интернет (правовых сайтов, правовых порталов и правовых поисковых систем) можно отнести научные и научно-юридические сайты, а также сайты учебных заведений, осуществляющих подготовку специалистов юридической направленности.

В соответствии с приведенной выше классификацией правовые интернет-ресурсы в Республике Казахстан можно группировать следующим образом:

1) сайты, принадлежащие органам государственной власти. В Республике Казахстан функционируют официальные сайты таких государственных органов и должностных лиц, как Президент РК (http://www.akorda.kz/ru), Верховный Суд РК (http://sud.gov.kz/rus), Парламент РК (http://www.parlam.kz/ru), Правительство РК (http://www.government.kz/ru/), Конституционный Совет РК (http://ksrk.gov.kz/), Генеральная Прокуратура РК (http://prokuror.gov.kz/rus), Комитет национальной безопасности РК (http://www.knb.kz/), Агентство РК по делам государственной службы и противодействию коррупции (http://kyzmet.gov.kz/ru), Национальное бюро по противодействию коррупции Агентства РК по делам государственной службы и противодействию коррупции (Антикоррупционная служба) (http://anticorruption.gov.kz/), Служба экономических расследований Комитета

государственных доходов Министерства финансов РК (http://kgd.gov.kz/ru), Министерство внутренних дел РК (http://mvd.gov.kz/portal/page/portal/mvd/MVD); Министерство юстиции РК (http://www.adilet.gov.kz/ru) и т.д. На перечисленных сайтах собраны официальная информация и сведения о деятельности рассматриваемых властных институтов.

2) информационно-правовые базы данных – основные правовые базы данных, присутствующие в казахстанском сегменте Интернет. Эти базы данных созданы как государственными (Информационный сервис Комитета по правовой статистике и специальным учетам Генеральной прокуратуры РК (http://qamqor.gov.kz/)), так и частными (Информационно-правовая система «Параграф-WWW» (http://online.zakon.kz/)), Информационно-правовая система НПА Республики Казахстан «Әділет» (http://adilet.zan.kz/) структурами и содержат самую актуальную и полную информацию о законодательстве Республики Казахстан.

Хотелось бы подробнее рассказать об информационном сервисе Комитета по правовой статистике и специальным учетам ГП РК. Комитет (аналог Главного информационно-аналитического центра МВД России), будучи включен в структуру Генеральной Прокуратуры РК, является межотраслевой службой, которая централизованно обеспечивает правоохранительные органы правовой информацией. Статус органов прокуратуры как надзорного и в определенной степени надведомственного органа, координирующего деятельность всех правоохранительных органов, стал ключевым фактором в определении прокуратуры оператором системы формирования правовой статистики в Республике Казахстан. На сегодняшний день Комитетом создана система информационного обмена правоохранительных и специальных органов (СИО ПСО), которая представляет собой окно доступа к 64 интегрированным базам данных государственных органов [9, с. 97]. Благодаря интеграции базы данных в информационном сервисе граждане имеют возможность подать заявление или проверить уже поданное заявление в полицию, проверить своё обращение в государственные органы, просмотреть информацию о розыске алиментщиков, уточнить законность проверки своего бизнеса (Бизнес тірегі), получить правовую статистику, просмотреть информацию об эффективности частного судебного исполнителя, проверить автотранспорт на ДТП, узнать о своих штрафах. Кроме этого, в информационном сервисе функционируют Геокарта (карта преступности по республике), публичный сектор Единого реестра досудебных расследований, проверка справок, розыск преступников, должников, без вести пропавших [9, с. 97]. Вся необходимая информация размещается на сайте и является доступной, как для рядовых граждан, так и для сотрудников правоохранительных и иных государственных органов. Также необходимо отметить, что данный сервис удобен в работе субъектов научной деятельности, так как в сервисе свободно можно, не направляя официальные запросы в правоохранительные органы, получить правовую информацию и статистику, имеющую научную ценность.

3) правовые СМИ в сети Интернет – в Казнете широко представлены различные виды СМИ, в том числе правового характера. Часть из них является интернет-версией официальных бумажных изданий, другая часть появляется и существует независимо от них и исключительно только в электронном виде. К

правовым интернет-изданиям можно отнести журнал «Право и государство» университета КАЗГЮУ (http://km.kazguu.kz/), специализированный ежемесячный журнал «ЮРИСТ» (https://journal.zakon.kz/journal/9143/) и т.д.;

4) виртуальные правовые клубы и правовые форумы – интернет-площадки, созданные и ведомые группами профессиональных юристов. Здесь ведутся обсуждения различных вопросов, возникающих в связи с применением законодательства в целом и разрешением конкретных ситуаций в частности. Например, в качестве правовых форумов можно назвать сайты Казахстанского юридического форума (http://forum.zakon.kz/), Юридического и бухгалтерского форума Казахстана (http://kodeksy-kz.com/forum/viewforum.php?f=2), Форума ОО «Общество содействия автомобилистам» (http://forum.oo-osa.org/) и т.д.

5) сайты правозащитных организаций и юридических фирм – представлены как сайты, созданные различными общественными правозащитными структурами и организациями, так и сайты крупных и известных юридических фирм. Например, среди сайтов правозащитных организаций Казахстана можно выделить сайты Казахстанского международного бюро по правам человека и соблюдению законности (https://bureau.kz/), Международного фонда защиты свободы слова «Адил соз» (http://www.adilsoz.kz/), Центра исследования правовой политики (LPRC) (http://lprc.kz/ru), Казахстанского центра правовой защиты (www.centerkorgau.kz) и т.д. На данных сайтах собраны материалы, посвященные различным правовым вопросам, с учетом специализации организации. Среди ведущих юридических фирм Казахстана, имеющих собственные сайты, можно выделить следующие: «Алматинская юридическая корпорация» (http://www.almatylegalcorporation.com), «Юридическая фирма «Зангер» (www.zangerlf.com), «Muratov Company» (www.muratov.kz) и т.д. [10].

6) WWW-страницы или личные страницы в социальных сетях известных юристов – представлены веб-страницы или личные страницы в социальных сетях ряда известных казахстанских юристов, где выложены биографические данные, материалы об их профессиональной деятельности и области их специализации. Например, это сайты таких известных юристов, как государственный деятель К. Мами (http://blog.sud.kz/ru), адвокат Д. Утебеков (https://ru-ru.facebook.com/people/Jokhar-Utebekov/100007447955436) или общественный деятель Р. Лазута (https://vk.com/rusik70) и т.д. Анализ казахстанского сегмента Интернет показал, что в республике практика ведения личных сайтов известными юристами, государственными и общественными деятелями, правозащитниками широко не распространена. Как показало исследование, в основном в Казахстане данная категория лиц ограничивается ведением личных страниц в общеизвестных социальных страницах или в рамках сайтов организаций, где они осуществляют свою юридическую деятельность.

Как отмечалось ранее, кроме перечисленных к правовым интернет-ресурсам можно отнести научные и научно-юридические сайты, а также сайты учебных заведений, осуществляющих подготовку специалистов юридической направленности. К таковым относятся:

а) научные и научно-юридические правовые интернет-ресурсы (правовые сайты, правовые порталы и правовые поисковые системы): Национальный

научный портал Республики Казахстан (http://www.nauka.kz/), Наука в Казахстане (http://www.naukakaz.kz/), Наука и жизнь Казахстана (http://nauka-zan.kz/) и т.д.;

б) сайты учебных заведений, осуществляющих подготовку специалистов юридической направленности и организаций, осуществляющих научные исследования в области права: Казахский национальный университет имени аль-Фараби (КазНУ, г. Алматы, http://www.kaznu.kz/), Казахский Гуманитарно-юридический университет (КазГЮУ, г. Астана, http://kazguu.kz/ru/), Карагандинская академия МВД Республики Казахстан имени Б. Бейсенова (http://www.kzi.kz/), Академия правоохранительных органов при ГП РК (г. Астана, http://academygp.kz/) и т.д.

Анализируя правовые интернет-ресурсы, функционирующие в Республике Казахстан, приходим к выводу о том, что в республике достаточно динамично развивается система предоставления интернет-услуг в правовой сфере. Информация, размещенная в перечисленных правовых интернет-ресурсах, дает возможность найти материалы и сведения правового характера, необходимые в повседневной жизни простых граждан, в деятельности сотрудников правоохранительных и иных государственных органов, а также в исследовательской деятельности научных коллективов или ученых. Развивая инфраструктуру предоставления электронной правовой информации и обеспечивая свободный доступ к ней, можно достигнуть всеобщего правового информирования населения и тем самым повышения уровня правового воспитания, правовой культуры и правосознания граждан. Кроме того, размещение правовой информации на сайтах государственных органов позволяет осуществлять общественный контроль за деятельностью органов власти, что повышает уровень «прозрачности» их работы. Несомненно, перечисленные факторы положительно воздействуют на процесс построения правового государства в Республике Казахстан.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Литвинов А.А. Обеспечение правовой информацией как основа формирования правового государства // Вестник ТГУ. 2003. № 2 (3). С. 47-50.
2. Адыгезалова Г.Э. Правовое информирование общества как условие построения правового государства // Система ценностей современного общества: сборник материалов XVII Междунар. науч-практ. конф.: в 2 ч. – Новосибирск: НГТУ, 2011. Ч. 1.
3. Тимко С.А. Формирование правосознания и правовой активности личности посредством современного российского законодательства, направленного на противодействие преступности // Юридическая наука и правоохранительная практика. 2017, № 1 (39). С. 92-99.
4. Государственная программа «Цифровой Казахстан» [Электронный ресурс]. – Режим доступа: https://zerde.gov.kz/activity/management-programs/digital-kazakhstan/
5. Закон Республики Казахстан от 24 ноября 2015 г. № 418-V «Об информатизации» (с изменениями от 28.12.2016 г.) Казахстан» [Электронный ресурс]. – Режим доступа: http://online.zakon.kz/document/?doc_id=33885902.

6. Воройский Ф.С. Информатика. Энциклопедический систематизированный словарь-справочник. – М.: Физматлит, 2006. – 945 с.

7. Волков А.М. Правовая информация и практика использования справочных правовых систем при подготовке специалистов в МГГРУ // Известия высших учебных заведений. Серия геология и разведка. 2003. № 5. С. 84-87.

8. Манохина О.А., Кленина В.И. Правовые информационные ресурсы в сети интернет // Ученые записки: Социальное управление, экономика и право. 2010. № 11. С. 118-123.

9. Абаев Е.М. Система правовой статистики в Республике Казахстан: опыт реформирования // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 2 (52). С. 95-98.

10. Лица, оказывающие юридические услуги в Казахстане (организации, коллегии, адвокатские конторы) (2017). [Электронный ресурс]. – Режим доступа: http://online.zakon.kz/Document/?doc.

РАЗВИТИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ МВД РОССИИ

DEVELOPMENT OF INFORMATION RESOURCES OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Акапьев Виктор Львович,
Дрога Андрей Анатольевич,
Савотченко Сергей Евгеньевич
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Akapyev Viktor Lvovich,
Droga Andrey Anatolyevich,
Savotchenko Sergey Evgenyevich
(Belgorod Law Institute of MIA of Russia named after I.D. Putilin)

Аннотация: проведен анализ совокупности значимых общественных отношений в области информационных технологий МВД России, их становления, развития, эффективности действия, а также обеспечения их защиты. Рассмотрены юридические нормы, регулирующие конституционно-правовую обстановку и законность при использовании информационных ресурсов МВД России на современном этапе.

Ключевые слова: информационные ресурсы, информационная безопасность, компьютерные сети, Интернет.

Annotation: the analysis of a set of significant public relations in the field of information technologies of the Ministry of Internal Affairs of Russia, their formation, development, effectiveness of action, as well as ensuring their protection is derived. Norms regulat-

ing the constitutional legal environment and legality are considered using information resources of MIA of Russia.

Key words: information resources, information security, computer networks, Internet.

Информационные ресурсы являются неотъемлемой составной частью знаний человечества и движущей силой информационного общества. С началом активного внедрения информационных технологий во все области жизнедеятельности человека в конце XX века информационные ресурсы оформились как отдельный класс объектов информационной сферы.

Информационные ресурсы органов внутренних дел включают, прежде всего, данные о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах. В ходе модернизации информационного обеспечения органов внутренних дел при помощи информационных ресурсов МВД характеризуется как способ оптимизации и совершенствования деятельности правоохранительных органов в современном Российском государстве; рассматриваются особенности их использования на современном этапе и проблемы, возникающие при осуществлении внутриведомственного и межведомственного взаимодействия.

Организация управления органами внутренних дел МВД России напрямую отражается в осуществлении руководства ресурсами ОВД, которые целесообразно делятся на макро- (в масштабах всего государства или конкретного региона) и микро- (в рамках определенного подразделения) уровни.

Количество ресурсов, с помощью которых осуществляет свою деятельность Министерство внутренних дел России, несоизмеримо велико, к ним стоит отнести такие как: экономические, правовые, кадровые, материально-технические, финансовые, информационные [1]. В ходе рассмотрения темы будет обращено внимание на такой важный составной элемент ресурсов органов внутренних дел, как информационные ресурсы. Стоит пояснить, что информационные ресурсы – это организованная и структурированная документированная информация, содержащаяся в библиотеках, архивах, фондах, банках данных, информационных системах [2].

Их значимость определена современным этапом в развитии общества, вступившего в эпоху информационных технологий, где самым ценным и востребованным ресурсом является информация, а также средства ее накопления, обработки и использования.

В первую очередь необходимо отметить два основных вида информационных ресурсов, которые используются в деятельности органов внутренних дел:

- первый – это сама информация, требующаяся для функционирования подразделений органов внутренних дел;

- второй – это средства получения, накопления, хранения, обработки и передачи информации.

Часть указанных ресурсов по своей сущности – материально-технические средства, однако их применение в целях хранения, обработки и передачи информации делает возможным считать их информационными.

Экономическая безопасность как одна из составляющих обеспечения национальной безопасности страны занимает ведущую позицию среди инфор-

мационных ресурсов органов внутренних дел. Важнейшим ресурсом МВД России внешнего пользования является «Реестр дисквалифицированных лиц». Данный информационный ресурс имеет существенные минусы при использовании: доступ пользования является закрытым и предоставление соответствующей информации из Реестра происходит только на платной основе.

Это связано, прежде всего, с тем, что размещение в открытом доступе дисквалифицированных лиц на сайте, будет способствовать снижению уровня экономической безопасности, что приведет к предупреждению преступности в рамках осведомления информационного сообщества, в потребности соблюдения мер осторожности при вступлении в экономические отношения с дисквалифицированными лицами, а также с позиций разработки дополнительной неформальной санкции для нарушителя.

В настоящее время руководство МВД России уделяет много внимания вопросу прогрессивного развития информационных ресурсов второго типа – средств получения, накопления, хранения, обработки и передачи информации. Так, на данный момент уже созданы и активно используются интегрированные базы данных федерального («ИБД-Ф») и регионального уровней («ИБД-Регион») [3], которые охватывают информацию о лицах, судимых и находящихся в розыске, утерянном, украденном огнестрельном оружии, автомототранспорте, антиквариате, драгоценных вещах, средств сотовой связи и других субъектов учета, что в результате позволяет осуществлять качественное оперативное раскрытие преступлений.

В развитии информационных технологий, несомненно, наблюдаются успехи в области осуществления правоохранительной деятельности, однако наличие большого количества актуальной информации в базах федерального и территориального компонентов системы позволяет констатировать, что существует проблема разобщенности актуальной информации (в т.ч. и по различным ведомствам), отсутствии единой аналитической надстроечной системы над информационными ресурсами, которые бы в дальнейшем координировались, дополнялись, что в конечном счете не позволяет в полной мере использовать их потенциальные возможности [4].

Информационный ресурс, во-первых, должен был обеспечить доступ всех подразделений органов внутренних дел ко всем существующим федеральным и региональным базам данных МВД России, а во-вторых, создать единую электронную систему управления органами внутренних дел в режиме реального времени. Такой ресурс не только будет способствовать повышению качества расследования преступлений путем оперативного получения сотрудниками органов внутренних дел в режиме реального времени точной и достоверной оперативно-справочной, разыскной и криминалистической информации, а также позволяет уменьшить часть расходов органов внутренних дел.

В соответствии с поручением Президента Российской Федерации в Министерстве внутренних дел в настоящее время ведется создание единой системы информационно-аналитического обеспечения деятельности МВД России.

Непосредственное руководство по созданию единой системы информационно-аналитического обеспечения деятельности МВД России осуществляет

Совет, образованный приказом Министра внутренних дел Российской Федерации от 24 октября 2011 г. № 1097. Также указанный совет создан в целях оптимизации процесса управления в области информационных технологий, внедрения в системе МВД России современных информационно-телекоммуникационных технологий, выработки общей стратегии по созданию и развитию единой системы информатизации Министерства, подготовки рекомендаций по решению важнейших научно-технических проблем в области информатизации, связи и защиты информации. В его состав вошли представители не только МВД России, но и Правительства Российской Федерации и федеральных органов исполнительной власти.

Однако сосредоточение разнородных информационных ресурсов в единой системе, безусловно, относится к сложным организационно-техническим задачам и предполагает затраты времени, интеллектуального труда и материальных ресурсов [5].

Особое внимание стоит уделить использованию информационных ресурсов в оперативной и служебной деятельности правоохранительных органов Российской Федерации. В общей сложности оперативно-справочные и разыскные информационные ресурсы МВД России содержат информацию миллиардов объектов учета и ежедневно пополняются миллионами документов. Ключевым для формирования и использования данного вида информационных ресурсов является то, что большая их часть – базовая для всех правоохранительных органов России и стран СНГ. Именно МВД России ведет межгосударственный банк данных и предоставляет информацию всем заинтересованным ведомствам [6].

Отдельно необходимо выделить криминалистические информационные ресурсы Министерства, которые содержат информацию о всех проводимых экспертизах и формируются экспертно-криминалистическими подразделениями.

Для целей анализа и учета формируются статистические информационные ресурсы, которые также являются базовыми для всех правоохранительных ведомств (под контролем прокуратуры) [7].

Национальное центральное бюро Интерпола также является подразделением МВД России и предоставляет доступ всем заинтересованным ведомствам.

Часть информационных ресурсов формируется правоохранительными органами совместно, например, Правоохранительный портал. Однако ведущая роль органов внутренних дел при формировании информационных ресурсов правоохранительного характера неоспорима.

Для удобства пользователей и возможности работы в реальном масштабе времени в последние десять лет в Министерстве созданы своя компьютерная распределенная сеть и защищенные механизмы обмена информацией. Информационные ресурсы объединены по видам в составе специализированных информационных систем. Организован сквозной поиск по всей стране.

Также необходимо отметить наметившиеся тенденции использования мобильных, носимых устройств, которые позволяют осуществлять доступ к информационным ресурсам не только из дежурной части, но и непосредственно с места происшествия.

Однако в последние годы, с увеличением количества объединяемой информации, сформировались и некоторые проблемы. Сопровождение информационных ресурсов органов внутренних дел также связано с рядом проблем, которые, прежде всего, обусловлены необходимостью обеспечения технической защиты информации. Ведь закрытые базы данных МВД России в случае несанкционированного доступа к ним могут быть использованы не для борьбы с преступностью, а, наоборот, для совершения преступлений и их сокрытия.

В этой связи обработка и хранение информации ограниченного доступа разрешается только на аттестованных по требованиям безопасности объектах информатизации, т.е. только в тех подразделениях органов внутренних дел, где в полном объеме проведен комплекс мероприятий в области технической защиты информации, включая выдачу аттестата соответствия объекта информатизации требованиям безопасности информации.

Проблема МВД России заключается как раз в том, что Министерство в настоящее время имеет недостаточное количество защищенных по требованиям безопасности информации объектов информатизации – аттестованных подразделений органов внутренних дел. Несмотря на то, что техническая оснащенность подразделения может фактически соответствовать требованиям информационной безопасности, однако без прохождения необходимой аттестации сотрудников оно не может считаться защищенным объектом информатизации, а следовательно, и использовать имеющиеся в распоряжении современные информационные ресурсы.

К сожалению, данная проблема актуализируется недостатком финансовых средств, которые не позволяют, во-первых, обеспечить потребность органов внутренних дел в современных, отвечающих соответственным критериям безопасности информационно-технических ресурсах, во-вторых – пройти аттестацию подразделения на соответствие требованиям безопасности, что показывает невозможность решения первого вопроса и образует замкнутый круг в этом вопросе.

И, конечно же, стоит сказать, что использование современных информационных технологий связано с потребностью государства в высококвалифицированных работниках, недостаток которых может привести к несоответствующему использованию дорогостоящей техники, что опять же приведет к повышению стоимости оказания правоохранительной услуги, но никак не улучшит её качество.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Литвиненко А.Н. Ресурсы МВД России в системе обеспечения экономической безопасности страны // Экономические науки. 2010. № 8. С. 69-74.

2. Занина Т.М., Караваев А.А., Рыдченко К.Д. Правовые основы информационной безопасности в органах внутренних дел: курс лекций. – Воронеж: ВИ МВД России, 2013. – 183 с.

3. Интернет-интервью с генерал-лейтенантом внутренней службы М.Л. Тюркиным [Электронный ресурс]. – Режим доступа: http://www.garant.ru/.

4. Каримов В.Х. Возможности реализации государством комплекса мер по предотвращению террористических угроз // Российский следователь. 2016. № 16. С. 38-41.

5. Арбузов П.В., Гуде С.В., Карпика А.Г. Вопросы интеграции информационных ресурсов вузов МВД России в ИСОД // Юристъ-Правоведъ. 2014. № 2. С. 17-20.

6. Прокопенко А.Н. Правовое регулирование информационных ресурсов МВД России: монография. – Белгород: Бел ЮИ МВД России, 2010. – 160 с.

7. Сметанин М.В. Развитие интернет-ресурсов МВД России в 2016 году // Архив тематического сборника «Информационные технологии, связь и защита информации МВД России – 2016». 2016. № 1. С. 32-33.

ОБЕСПЕЧЕНИЕ ИНФОРМИРОВАНИЯ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ СИСТЕМЫ МВД РОССИИ

PROVISION OF INFORMATION IN THE EDUCATIONAL ORGANIZATIONS OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Печенкова Елена Анатольевна,
Корень Алена Игоревна
(Московский университет МВД России имени В.Я. Кикотя)

Pecinkova Elena Anatolivna,
Koren Alena Igorevna
(Moscow University of the MIA of Russia named after V.Ya. Kikot)

Аннотация: в статье приводятся данные об информировании постоянного и переменного состава в образовательных организациях системы МВД России. Акцент сделан на особенностях подачи информации личному составу.

Ключевые слова: информирование постоянного и переменного состава, субъективная информация, профилактическая деятельность, образовательные организации, информационные ресурсы, информационные потребности, компьютерная этика, открытие образовательного общества.

Annotation: the article provides information on informing the permanent and variable composition in the educational organizations of the MIA of Russia. The emphasis is on the specifics of information delivery to the personnel.

Key words: informing of permanent and variable composition, subjective information, preventive activity, educational institutions, information resources, information needs, computer ethics, opening of the educational society.

В настоящее время происходит значительное усиление информационного компонента обучения, осознание фундаментальной роли информатизации общественной деятельности. Одной из проблем обеспечения всестороннего развития образовательного пространства является адаптация к открытому информационному взаимодействию субъектов начально-воспитательного процесса.

Создание открытого образовательного пространства (сетевой обмен информацией между учебными заведениями, библиотеками, организациями, предприятиями, государственными учреждениями), внедрение различных информационных продуктов, коммуникационных и мультимедийных средств, создание значительных массивов электронной информации (электронные энциклопедии и учебники, авторские электронные курсы изучения дисциплин, электронные каталоги), популяризация и обеспечение доступности электронной информации требуют от субъектов учебно-воспитательного процесса специфических качеств.

Таким образом, информационный компонент образовательного пространства формирует новые требования к субъектам, которые осуществляют образовательную деятельность. На современном уровне развития информационного компонента образовательного пространства актуальны информационная культура (поиска, разработки новой информации), коммуникативная культура (построения отношений в электронной сети на разных уровнях) [2, с. 407-417].

Современное образовательное пространство нуждается в субъектах, которые способны:

– совместно использовать информацию;
– презентовать свои информационные потребности;
– предлагать информацию в доступной форме;
– осуществлять информационный обмен;
– действовать с учетом требований «компьютерной этики» [4].

Компьютерная этика как составляющая информационной культуры предусматривает регулирование отношений между людьми, сложившихся в процессе информационного обмена в соответствии с определенной совокупностью моральных принципов и норм.

Обучение в информационной среде имеет ряд особенностей, которые существенно отличают его от традиционных форм. К особенностям нового формата образовательного пространства можно отнести то, что субъекты образовательного пространства достаточно часто сотрудничают в интерактивном режиме, оперируют значительными массивами противоречивой информации, активно применяют мультимедиа. Однако сегодня, несмотря на все положительные черты информатизации образования, есть проблемы, которые значительно уменьшают положительный эффект информационного компонента [3].

Ощутимым является деление на активных потребителей электронных услуг (посетителей сайтов и т.д.) и тех, кто не имеет такой возможности (недостаточное финансирование, отсутствие информационной культуры, отсутствие мотивации). В связи с возникновением информационного общества, информатизацией деятельности сформировались условия для развития открытого образовательного пространства, которое дает шанс каждому субъекту учебно-

воспитательного процесса продуктивно использовать информационный компонент [5, с. 448].

Итак, информационный компонент является самым важным на сегодня в процессе трансформации образования. Оптимальные условия взаимодействия субъектов образовательного пространства способны обеспечить методы кооперативного и глобального обучения (стандартизированные тесты, дистанционное обучение, электронные лекции, медиаконференции) [1, с. 358-368].

Таким образом, обеспечивая образовательные организации информационными ресурсами, мы добьемся процветания образовательного процесса и облегчим понимание и усвоение материала, с помощью дополнительных ресурсов, которые предоставляются начальствующим и преподавательским составами университета, профессорами и докторами наук, ведомственными и вневедомственными учреждениями; ускорим и повысим качество выполнения служебной деятельности, а также расширим возможности саморазвития для постоянного и переменного состава.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кирилова Г.И. Развитие и саморазвитие информационной образовательной среды профессионального образования // Образовательные технологии и общество (Educational Technology & Society). 2012. Т. 15. № 3. С. 358-368.

2. Кирилова Г.И., Власова В.К. Моделирование регионально-профессиональной инфраструктуры информационной среды профессионального образования // Образовательные технологии и общество (Educational Technology & Society). 2011. Т. 14. № 1. С. 407-417.

3. Кирилова Г.И. Оптимизация содержания информационно-компьютерной подготовки в средней профессиональной школе: дис. … д-ра пед. наук. – Казань, 2001.

4. Волик О.Н. Проектирование и реализация конкурса компьютерного творчества учащейся молодежи: дис. … канд. пед. наук. – Казань, 2005.

5. Волик О.Н. Алгоритмы информационно-средового взаимодействия субъектов в системе образования // Образовательные технологии и общество (Educational Technology & Society). 2011. Т. 15. № 4. С. 448.

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ АНАЛИЗА И МОДЕЛИРОВАНИЯ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

THE POSSIBILITIES OF APPLYING THE INFORMATION SYSTEMS FOR ANALYSIS AND MODELING IN LAW ENFORCEMENT

Савотченко Сергей Евгеньевич
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Наджаджра Мухаммед Хасан Наджи
(Университет Аль-Истикляль, г. Иерихон, Палестина)

Savotchenko Sergey Evgenyevich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin);
Nadzhadzhra Muhammed Hasan Nadzhi
(University of Al-Istiklal, Jericho, Palestine)

Аннотация: проведен анализ информационных систем, применимых для анализа и моделирования процессов. Описаны основные типы таких информационных систем. Детализирована структура информационно-аналитической системы.
Ключевые слова: информационные системы, информационно-аналитические системы, системы поддержки принятия решений.

Annotation: the analysis of information systems applicable for analysis and modeling of processes is carried out. The basic types of such information systems are described. The structure of the information-analytical system is detailed.
Key words: information systems, data mining systems, decision support system.

Обеспечение максимальной эффективности анализа и оценки оперативной обстановки для принятия управленческих решений в сфере охраны общественного порядка, общественной безопасности и борьбы с преступностью невозможно в современном высокотехнологическом обществе без использования соответствующих информационных систем [1].

На рынке информационных технологий существует множество информационных систем, специализирующихся на анализе, моделировании и поддержке принятий решений.

Вся проблема аналитической подготовки принятия решений имеет три аспекта: сбор и хранение необходимой для принятия решений информации; собственно анализ, в том числе оперативный и интеллектуальный; подготовка результатов оперативного и интеллектуального анализа для эффективного их восприятия потребителями и принятия на ее основе адекватных решений.

Аспект, касающийся сбора и хранения информации с сопутствующей доработкой, оформился в концепцию информационных хранилищ (Data Warehouse).

В связи с большим объемом и сложностью аспект проблемы собственно анализа имеет два направления – оперативный анализ данных (информации), широко распространена англоязычная аббревиатура названия - On - Line Analytical Processing - OLAP. Основной задачей оперативного или OLAP-анализа является быстрое (в пределах секунд) извлечение необходимой аналитику или ЛПР для обоснования или принятия решения информации.

Интеллектуальный анализ информации (Data mining) предназначен для фундаментального исследования проблем в той или иной предметной области. Жестких границ между OLAP и интеллектуальным анализом нет, но при решении сложных задач приходится использовать весьма мощные специальные программные средства или, как говорят, инструменты.

Средства автоматизации анализа представлены в различных видах. Имеются комплексные информационно-аналитические системы, выполняющие в той или иной степени функции в соответствии с рассмотренными аспектами.

Представлены на рынке программных продуктов и целевые программные системы, выполняющие в увеличенном объеме, расширенном составе и повышенной сложности какие-либо функции, например, оперативного или интеллектуального анализа. ИАС информационно подпитывают системы поддержки принятия решений (СППР), в литературе также применяют аббревиатуру DSS (Decision support system).

Модули, предназначенные для выполнения функций OLAP-анализа, входят также и в состав интегрированных информационных систем (ИИС) (системы, выполняющие весь комплекс автоматизации работ в информационном пространстве экономического или какого-либо другого объекта). Наиболее развитые ИИС выполняют функции и оперативного, и интеллектуального анализа.

Современный уровень развития аппаратных и программных средств с некоторых пор сделал возможным повсеместное ведение баз данных оперативной информации на разных уровнях управления.

Очень часто информационно-аналитические системы, создаваемые в расчете на непосредственное использование лицами, принимающими решения, оказываются просты в применении, но жестко ограничены в функциональности. Такие статические системы называются в литературе Информационными системами руководителя (ИСР), или Executive Information Systems (EIS). Результатом работы такой системы, как правило, являются многостраничные отчеты, после тщательного изучения которых у аналитика появляется новая серия вопросов.

Полная структура информационно-аналитической системы, построенной на основе хранилища данных, приведена на рисунке 1 (см. рис. 1).

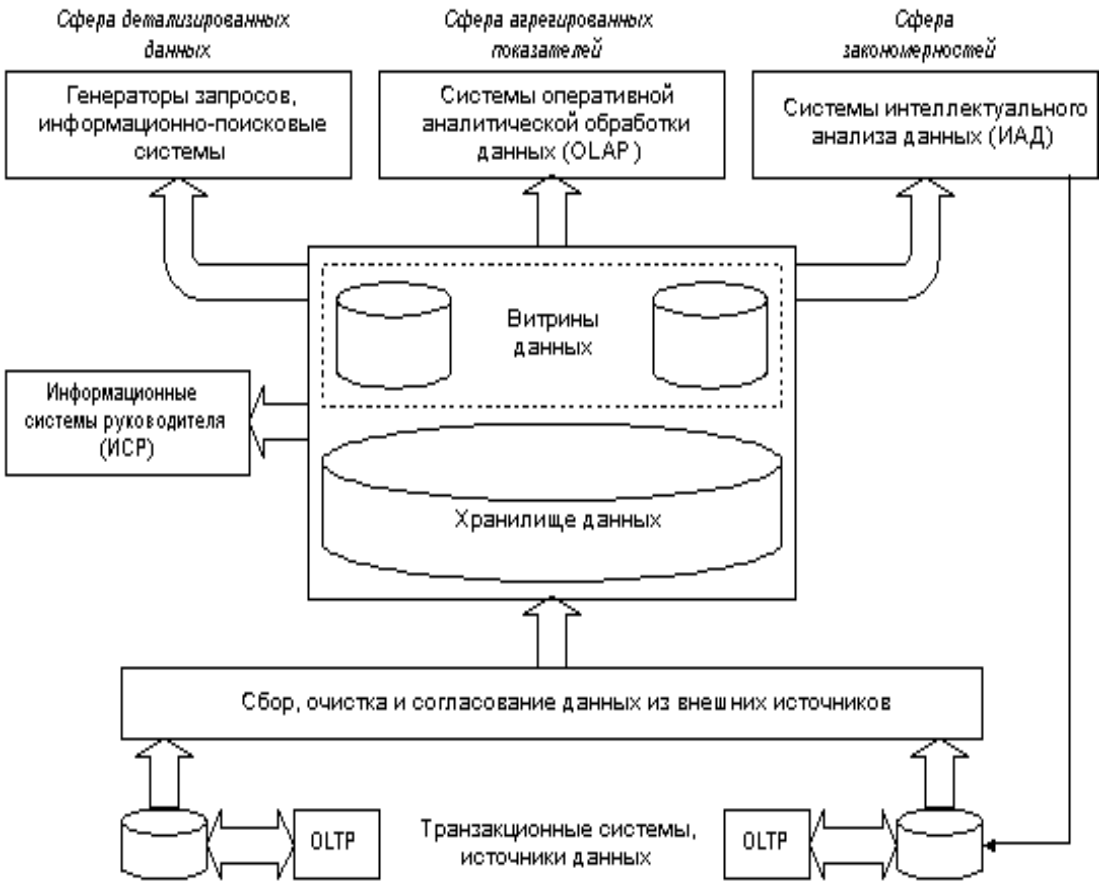


Рис. 1. Общая структура информационно-аналитической системы.

В конкретных реализациях отдельные компоненты этой схемы часто отсутствуют. В настоящее время на рынке присутствует большое количество продуктов, которые в той или иной степени обеспечивают функциональность OLAP.

Помимо OLAP-систем, широкое распространение получил интеллектуальный анализ данных – это процесс поддержки принятия решений, основанный на поиске в данных скрытых закономерностей (шаблонов информации). При этом накопленные сведения автоматически обобщаются до информации, которая может быть охарактеризована как знания.

В последние годы отмечается использование автоматизированных систем, построенных на принципах интеграции OLAP и ИАД. Большинство систем OLAP заостряет внимание только на обеспечении доступа к многомерным данным, а большинство средств ИАД, работающих в сфере закономерностей, имеют дело с одномерными перспективами данных.

Эти два вида анализа должны быть тесно объединены, то есть системы OLAP должны фокусироваться не только на доступе, но и на поиске закономерностей. K. Parsaye вводит составной термин «OLAP Data Mining» (многомерный интеллектуальный анализ) для обозначения такого объединения (см. рис. 2).

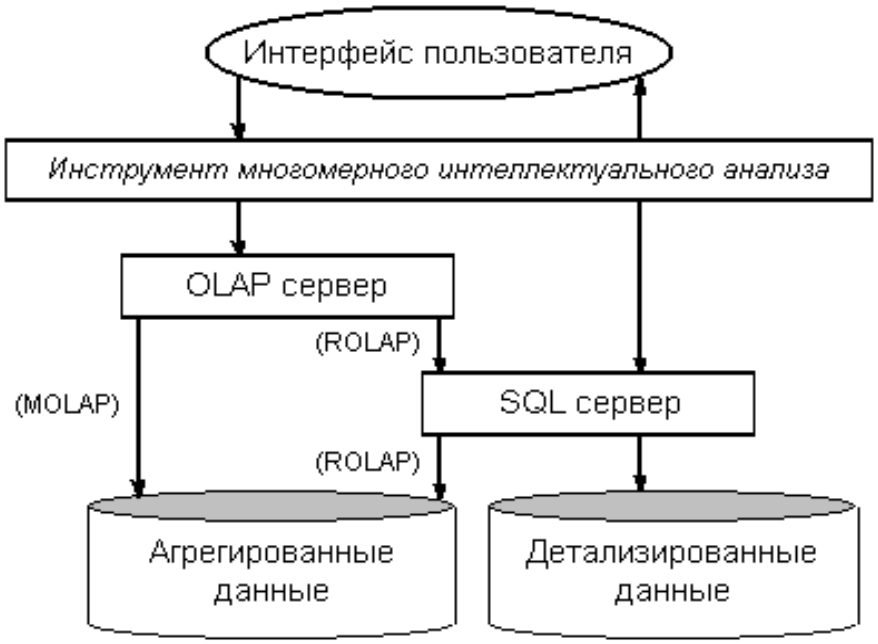


Рис. 2. Архитектура системы многомерного интеллектуального анализа данных.

В то же время, несмотря на успехи в разработке такого вида информационных систем, остаются неразрешенными целый ряд проблем, связанных с нормативным и законодательным регулированием их использования в правоохранительной деятельности, особенно в случае возникновения международных взаимодействий [2, 3, 4].

Следует отметить, что большинство информационных систем анализа и моделирования, используемого в правоохранительной деятельности, сделаны российскими разработчиками, что в полной мере отражает современные тенденции последнего времени по импортозамещению в сфере программного обеспечения и информационных технологий [5].

Таким образом, можно утверждать, что активное использование информационных систем анализа и моделирования в процессе расследования преступлений, а также при подготовке профессиональных кадров не может не отразиться благоприятно на положительной динамике уменьшения преступности и повышении безопасности личности в обществе в целом.

Применение информационных систем анализа и моделирования можно считать одним из основных факторов для достижения наибольшей эффективности правоохранительной деятельности, позволяющим существенно упростить и ускорить процедуру раскрытия преступления, повысить безопасность охраняемых объектов на основе разработанных современных систем с высоким уровнем надежности и безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Акапьев В.Л., Дрога А.А., Савотченко С.Е. Возможности применения современных средств компьютерного моделирования в правоохранительной деятельности / Математические методы и информационно-технические средства: материалы XII Всероссийской научно-практической конференции. – Краснодар: Краснодарский университет МВД России, 2016. С. 9-12.
2. Вихляев А.О. Применение информационно-коммуникационных технологий в обеспечении безопасности государств – членов Евразийского экономического союза // Международное публичное и частное право. 2014. № 6. С. 62-70.
3. Шипилов В.В. Международный опыт организации информационного обеспечения оперативно-розыскной деятельности // Российский следователь. 2013. № 22. С. 102-110.
4. Никишкин И.К. Развитие правовой базы информационного обеспечения полицейского сотрудничества государств – членов Евразийского экономического союза // Административное право и процесс. 2015. № 10. С. 54-60.
5. Акапьев В.Л., Савотченко С.Е. Актуальные проблемы импортозамещения программного обеспечения образовательных организаций в контексте информационной безопасности // Дистанционное и виртуальное обучение. 2015. № 11 (101). С. 113-125.

ИСПОЛЬЗОВАНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННОЙ ИНСПЕКЦИИ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ

USE OF MOTOR-FREE FLYERS IN THE ACTIVITY OF STATE ROAD TRAFFIC SAFETY INSPECTION

Кирюшин Иван Иванович,
Коваленко Дарья Николаевна
(Барнаульский юридический институт МВД России)

Kiryushin Ivan Ivanovich,
Kovalenko Daria Nikolaevna
(Barnaul Law Institute of the MIA of Russia)

Аннотация: в настоящее время средства ведомственной авиации достаточно широко используются в современных подразделениях полиции при патрулировании дорог совместно с экипажами ГИБДД, осуществлении поиска пропавших лиц в лесистой местности, реализации разведки местности. Однако единая методика использования возможностей и порядка интеграции беспилотных летательных аппаратов (БПЛА) в общее аэронавигационное пространство при решении повседневных задач полиции в МВД России пока не сформирована.

Ключевые слова: государственная инспекция безопасности дорожного движения, беспилотные летательные аппараты, транспорт, безопасность дорожного движения.

Annotation: at present, the means of aviation are widely used in modern police units: when patrolling roads together with the traffic police crews, searching for missing persons in forest belts, realizing reconnaissance of the terrain. However, a unified methodology for using the capabilities and order of integrating unmanned aerial vehicles (UAVs) into the common air navigation space while solving routine police tasks in the Russian Ministry of Internal Affairs has not yet been formed.

Key words: state road safety inspectorate, unmanned aerial vehicles, transport, road safety.

В Государственной инспекции безопасности дорожного движения России (далее – ГИБДД) широко применяются современные полицейские радары и камеры фото-, видеофиксации, которые могут в автоматическом режиме фиксировать превышение установленной скорости движения, осуществлять фиксацию выезда на полосу движения общественного транспорта, нарушения правил остановки и стоянки, проезда на запрещающий сигнал светофора и другие виды нарушений правил дорожного движения.

В последнее время ГИБДД внедряет в работу и новые технологии. Одна из них – беспилотный летательный аппарат (далее – БПЛА), построенный на базе радиоуправляемой модели самолёта или вертолета и оснащенный средствами видеофиксации. БПЛА – это сложный высокотехнологичный комплекс, сочетающий в себе системы управления полетом, системы связи, системы обнаружения (тепловизоры, оптические и радиометрические датчики), системы захвата и сопровождения объекта наблюдения [2].

Производство беспилотных летательных аппаратов в настоящее время является одним из перспективных направлений развития техники. Применение БПЛА в деятельности ГИБДД весьма эффективно экономически и часто позволяет выполнить задачу лучше и быстрее, чем с применением «большой» авиации.

В данной статье рассмотрены технические проблемы БПЛА, а также анализ ситуаций, в которых могут быть использованы БПЛА в деятельности ГИБДД.

Летательные аппараты предоставляют ГИБДД и службам дорожной инфраструктуры информацию, благодаря которой эксперты оценивают общее состояние дорог, проводят регулярный мониторинг эксплуатационного состояния дорог, контролируют проводимые на дорогах ремонтные работы, наблюдают за придорожной обстановкой. Используя БПЛА в деятельности ГИБДД, можно осуществлять мониторинг дорожно-транспортной обстановки в режиме реального времени и соблюдения правил дорожного движения его участниками. В случае обнаружения правонарушителей БПЛА следят за ними в автоматическом режиме и распознают номера автомобилей, совершают оперативную разведку с места ДТП, аварии или катастрофы на дороге или объекте транспортной инфраструктуры, позволяя сотрудникам полиции принимать наиболее эффективные управленческие решения в кратчайшие сроки.

Для получения аналитических данных о состоянии дорожно-транспортной структуры и придорожной обстановки целесообразно использовать БПЛА самолетного типа класса «Е» – ZALA 421-16E или ZALA 421-16EM. Если необходимо осуществить оперативный мониторинг участка дороги на малом удалении или на локальном участке с получением точных данных целесообразно применять самолет малого класса – ZALA 421-08 или вертолеты – ZALA 421-21, ZALA 421-22.

Подобные устройства давно используются во многих подразделениях МВД, но в ГИБДД пока разрабатываются методики их использования в ходе проводимых полётов. Применение БПЛА в ГИБДД используется для поиска угнанных транспортных средств, в том числе спрятанных на закрытой территории, куда нет доступа сотрудникам правоохранительных органов. Сотрудники ГИБДД предполагают, что БПЛА можно будет эффективно использовать и при преследовании автомобиля, скрывающегося с места преступления или ДТП, например, после наезда на пешехода, ведь в этих случаях чаще всего сразу объявляется план «Перехват».

Заметим, что при всей фантастической манёвренности летательных аппаратов они всё-таки имеют определённую инерцию. И даже опытный оператор не мгновенно сориентирует аппарат так, чтобы номерной знак автомобиля попал в поле зрения бортовой видеокамеры. Если ориентироваться только по изображению на мониторе или видеоочках, то на это потребуется одна-две минуты. Это к вопросу об эффективности БПЛА: много ли можно «просканировать» объектов на одном заряде аккумуляторной батареи, учитывая, что БПЛА ещё должен вернуться к месту старта.

Другая ситуация: преследование угонщика или нарушителя. Как ни странно, здесь мини-вертолёт будет более полезен. Нет нужды запускать БПЛА в преследование, гораздо больше пользы можно получить от запуска беспилотника на определенную высоту, с которой он позволяет просматривать большую площадь. Пара БПЛА способна скоординировать действия полицейских экипажей вплоть до того, что будет транслировать картинку с воздуха прямо на автомобильные мониторы. Помогут они и тогда, когда угнанный автомобиль укрывается за насыпью или иным препятствием.

Ещё одно применение БПЛА – оперативный мониторинг автотранспорта в системе «Поток». В настоящее время это выглядит малореальным, так как для такого мониторинга нужна специальная оптическая система высокого разрешения, которая для установки на БПЛА пока не разработана [5-6].

Беспилотные летательные аппараты обладают и отдельными недостатками:

- требование наличия благоприятной рабочей температуры. В некоторых регионах существенно ограничивается период возможного использования БПЛА в течение года (Алтайский край);
- отсутствие возможности использования комплекса при превышении скорости ветра у поверхности земли более 15 м/с, в условиях лесостепной и степной зон, а также в предгорных районах;
- недопустимость использования комплекса при низкой облачности, ливневых осадках, снегопаде, тумане, видимости менее 200 метров.

Наряду с этим применение БПЛА в деятельности ГИБДД является перспективным, поскольку:

- значительно уменьшаются экономические затраты при подготовке и обучении экипажа, подготовке и обслуживании пилотируемых летательных аппаратов – вертолетов и их непосредственном использовании путем делегирования некоторых задач на беспилотные летательные аппараты;
- часть задач, выполняемых вертолетами, перейдет на БПЛА, тем самым повысится общая эффективность эксплуатации пилотируемых летательных аппаратов;
- ускорится быстрота реагирования из-за малого времени подготовки БПЛА к полету (в отличие от крупной авиации);
- обеспечится возможность мобильного использования БПЛА при решении задач, стоящих перед ГИБДД МВД России [6].

В ГИБДД России беспилотники появились на вооружении более 5 лет назад. Используют их в разных регионах. Например, в Государственной инспекции безопасности дорожного движения по Красноярскому краю БПЛА поставлены на вооружение в 2014 году. В Алтайском крае беспилотники начали использовать весной 2015 года для патрулирования оживлённых трасс [7]. В 2016 году с помощью беспилотника в крае зафиксировано более 200 нарушений правил дорожного движения – запрещённые обгоны и выезды на полосу встречного движения. По словам представителей ГИБДД, в те дни, когда на дорогах дежурит беспилотник, наблюдается уменьшения нарушений ПДД, а также снижается аварийность. Беспилотник вылетает на трассы, где наблюдается активный поток машин. Он оснащен видео- и фотокамерами, картинку с которых контролирует инспектор ГИБДД в режиме реального времени. В случае нарушения правил дорожного движения, информация передается ближайшему экипажу ДПС. Устройство работает с помощью GPS/ГЛОНАСС, то есть летает по координатам, которые ему задаются с компьютера [7]. Радиус действия сигнала аппарата – до 40 км. Почти всё лето беспилотник дежурил на трассе М-52 и следил за потоком машин в сторону Республики Алтай. У алтайской полиции пока лишь один экземпляр техники – подобный беспилотник стоит от 2 миллионов рублей.

Говоря о применении данной системы в ГИБДД, необходимо отметить то, что она является эффективной в борьбе с правонарушениями, так как большинство водителей, нарушая ПДД, даже не догадываются о том, что за ними следят с воздуха. Новый метод позволяет обнаружить гораздо большее количество нарушителей.

В будущем применение систем автоматического контроля поможет повысить эффективность выявления правонарушений и их профилактики на дорогах страны, освободить человеческий «ресурс» и создать условия для более экономного использования беспилотных летательных аппаратов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Eskov A., Svistula A., Dolmatov A. Parameters of fuel jet extraction in video. Transport. 2005. Т. 20. № 2. С. 62-65.

2. JustMedia-новости [Электронный ресурс]. – Режим доступа: http://www.justmedia.ru/news/society/.

3. Автоновости Алтайского края [Электронный ресурс]. – Режим доступа: http://auto.altapress.ru/story/.

4. Беспилотники - dxdt.ru: занимательный интернет-журнал [Электронный ресурс]. – Режим доступа: https://dxdt.ru/category/uav.

5. Готовы выжить. Беспилотники (БПЛА). [Электронный ресурс]. – Режим доступа: http://xn--b1aabok6aa5af0gbp.xn--p1ai/index.php/.

6. Кирюшин И.И., Иванов Н.А. Об использовании беспилотных летательных аппаратов в МВД России // Вестник Барнаульского юридического института МВД России. 2015. № 1 (28). С. 109-112.

7. Сабикенова С.А., Кирюшин И.И. К вопросу об ответственности в сфере управления беспилотными транспортными средствами // Альтернативные источники энергии в транспортно-технологическом комплексе: проблемы и перспективы рационального использования. 2016. Т. 3. № 2. С. 359-362.

ПРИМЕНЕНИЕ WEB-РАСШИРЕНИЯ ДЛЯ ДОСТУПА К ФУНКЦИОНАЛЬНЫМ ИНТЕРФЕЙСАМ ИНФОРМАЦИОННЫХ СИСТЕМ

APPLICATION OF THE WEB-EXTENSION FOR ACCESS TO THE FUNCTIONAL INTERFACES OF INFORMATION SYSTEMS

Тимакина Юлия Анатольевна
(Ростовский юридический институт МВД России)

Timakina Julia Anatolievna
(Rostov law Institute of MIA Russia)

Аннотация: в статье исследуются и анализируются процессы перехода от работы на стационарных устройствах к работе на мобильных устройствах с помощью WEB-расширения для доступа к функциональным интерфейсам информационных систем.

Ключевые слова: многоплатформеность, Web-технологии, облачные технологии, гипермедиа структуры, интерфейс.

Annotation: the article examines and analyses the processes of transition from working on stationary devices to mobile devices via WEB extensions for the access to the functional interfaces of information systems.

Key words: multiplatform, Web technologies, cloud computing, hypermedia structure interface.

В современных условиях одним из важнейших факторов улучшения информационного обеспечения деятельности правоохранительных органов и одним из перспективных инструментов повышения производительности труда в данной сфере является применение информационных технологий (ИТ).

В настоящее время происходит активный переход от работы на стационарных устройствах к работе на мобильных устройствах. Благодаря развитию информационных технологий стала осуществимой интеграция приложений, обеспечивающая быстрый доступ к базам данных на отдалённом расстоянии. Современные гаджеты (планшеты, смартфоны) дают новые возможности, но в России не очень активно происходит освоение всех потенциалов систем управления.

Системы, привязанные к компьютеру и работе через сеть, не могут гарантировать своим пользователям комфорт, мобильность и быстродействие, которые так ценятся в современном мире. Web-расширения предоставляют открытые инструменты для обработки информации и интеграции с корпоративными базами данных.

Web-интерфейс обеспечивает взаимодействие пользователя с ресурсами сети Интернет и сети, является результатом совместной работы дизайнеров, художников-графиков, IT-специалистов, программистов. Изначально ориентированный не на работу с данными в ее базовом понимании (ввод – обработка – вывод), а на поиск информации в сети Интернет, просмотр на экране компьютера, web-интерфейс должен быть привлекательным, т.е. его содержание должно быть интересным и довольно часто обновляться, вызывая дальнейший интерес к нему.

Выделим следующие требования к интернет-развитию управленческих информационных систем:

- выбор платформы, которая осуществляет интеграцию в Интернет;
- платформонезависимость и работа с различными операционными системами на любом типе современного компьютерного оборудования;
- получение доступа к одним и тем же функциям системы с помощью любого интерфейса (web-браузера, терминального подключения, традиционного Windows-интерфейса, мобильного устройства с WAP-доступом);
- гибкий графический интерфейс управления информацией;
- высокое качество линий связи и передачи данных [2, с. 56].

Целый комплекс свойств, таких как: многоплатформенность, распределенность, широкая поддержка общепринятых стандартов, возможность взаимодействия с другими системами, требуется от информационных систем, способных обеспечивать эти преимущества. Такие свойства более полно, эффективно и с меньшими затратами реализуются в условиях универсализации и стандартизации платформ, на которых базируются ИС. В настоящее время процесс универсализации систем активно протекает в мировой индустрии информационных технологий.

Создание и развитие web-технологии, ставшей одним из главных факторов, подвергнувших бурному развитию и колоссальной популярности Интернет

как глобальной информационной системы, сыграло решающую роль в плане построения и интеллектуализации пользовательских интерфейсов. В целом в области web-интерфейсов был создан и приведен к реализации унифицированный способ построения сетевых информационных систем, не зависящих от платформ; использование браузеров-программ, обеспечивающих доступ пользователю к ресурсам Интернет, в качестве элемента интерфейсов пользователей значительно упростило доступ к данным и позволило унифицировать работу с данными [3, с. 89].

Особенности информационных систем, построенных на основе использования web-технологий следующие:

1) база знаний, реализуемая в виде гипермедиа структур (гипермедиа является обобщением гипертекста – нелинейного текста, что обеспечивает возможность его просмотра в произвольных направлениях в соответствии с гипертекстовыми ссылками);

2) развитый и совершенствуемый интерфейс «Общение» пользователя с системой на понятном ему языке (браузер – в качестве диалогового монитора, сценарии диалога – на языке разметки гипертекстов HTML – HyperTextMarkupLanguage);

3) наличие средств автоматизированного пополнения и модификации гипертекстовых структур [3, с. 68].

В настоящее время наряду с развитием возможностей языка HTML, используемого при создании гипермедиа структур в web-системах, активно развиваются технологии, основанные на ExtensibleMarkupLanguage (XML), языке, спецификации которого недавно получили статус стандарта W3C (WorldWideWebConsortium) [1, с. 29].

В современном мире все чаще приходится слышать такой термин, как «облачные технологии», которые за последнее десятилетие приобрели колоссальную популярность. Многочисленные пользователи перешли от десктопных приложений к web-приложениям Gmail, Yahoo или Mail.ru. Важно отметить, что многие из них не имеют полного представления о том, что их данные, переписка, документы и многое другое могут храниться не только в пределах глобальной сети. Однако даже разбирающиеся пользователи доверили свои вышеперечисленные личные ресурсы облачным технологиям.

Развитие облачных хранилищ провоцируется стремительным размещением большого объема самых разных типов данных в самых различных форматах. Термин «облачные технологии» в узком смысле – это предоставление виртуального сервиса через Интернет. В широком смысле – это потребление спектра продуктов в межсетевом экране, то есть в облаке. Однозначным является то, что облачные технологии представляют собой новейший способ предоставления IT-ресурсов в виде сервиса, при этом пользователю не нужно покупать лицензионное программное обеспечение, так как сервисы работают благодаря оплате услуги, которой пользуется пользователь в конкретное, реальное время через Интернет. В зависимости от потребностей пользователей существует несколько моделей их обслуживания со стороны поставщика облачных вычислительных услуг:

предоставление облачной инфраструктуры (IaaS), предоставление облачной платформы (PaaS) и предоставление программного обеспечения (SaaS).

Облачные технологии, как и все остальные технологии, имеют как положительные характеристики – достоинства, так и отрицательные – недостатки. Прежде всего, к главным преимуществам относятся:

- доступность облака. Данная характеристика описывается тем, что размещенная клиентом информация на облаке, доступна ему в любой точке мира, где есть Интернет, а также с любого устройства;

- неограниченность вычислительных ресурсов. Высокий уровень вычислительной мощности, предоставленной в облаке, имеет открытый доступ для пользователей;

- низкая себестоимость. Сокращение издержек на обслуживание сервиса, фактическая оплата за пользование ресурсами облака.

Однако стоит рассмотреть и недостатки облачных технологий, которые представлены следующими характеристиками:

- зависимость от Интернета. Только подключение к сети может предоставить пользователю возможность работы с облаком;

- программное обеспечение. На облаке доступно определенное программное обеспечение, кроме того, существуют ограничения, выраженные в том, что пользователь не имеет возможности настройки приложения согласно своим персональным требованиям;

- конфиденциальность информации. Выкладывая персональную информацию на облако, пользователь должен понимать, что на данном этапе развития нет технологии, которая смогла бы обеспечить полную конфиденциальность.

Применение облачных технологий актуально во многих областях, что обуславливается широким спросом на данный тип технологий. Так, например, их стремительное развитие достигло почтовых клиентов. До недавнего времени пользователи устанавливали почтовый клиент, через который осуществлялись прием, отправка и обработка электронной почты. На данном этапе перечисленные функции выполняют Gmail, Yahoomail, Webmail, Hotmail и другие. Другим примером являются офисные пакеты, так как ZohoWriter или Документы Google обладают таким же функционалом, что и стандартные офисные пакеты. Более того, онлайн-редакторы способны импортировать и экспортировать документы в другие форматы. Следует отметить, что существует такая область, в которой использование облачных технологий однозначно принесет колоссальную пользу. Это область образовательных услуг.

Подводя итог, стоит отметить, что облачные технологии: представляют широкий спектр возможностей благодаря развитым сервисам для пользователей; обеспечивают новые рабочие места для IT-специалистов, которые принимают прямое участие в настраивании облаков; имеют большие возможности для развития и дальнейшего применения в самых различных областях жизни.

Таким образом, web-технологии помогают пользователю из правоохранительных органов решить ряд важных проблем, с которыми он сталкивается в процессе автоматизации своей деятельности. Интеграция между системами ин-

формационных систем в настоящее время необходима правовой сфере для ее дальнейшего успешного развития.

Web-расширение позволяет встраивать доступ к данным основной программы в существующие web-сайты и web-приложения и создавать готовые web-приложения, использующие информационную базу системы. Благодаря web-расширению разработчик может быстро построить пользовательский web-интерфейс, по стилю работы схожий с интерфейсом основного продукта, и легко адаптировать web-приложение к изменениям прикладного решения.

Современный этап развития систем пользования ЭВМ характеризуется тем, что имеет место массовое внедрение сетей вычислительных машин во все сферы человеческой деятельности, работы и учебы, включая и правоохранительные органы. При этом информационные системы, построенные на основе использования web-технологий и гипермедиа, осуществляют приближение пользователей к сетевым ресурсам за счет применения интерфейсов, которые можно отнести к разряду интеллектуальных.

Проанализировав все аспекты развития интерфейсов, можно сделать вывод, что информационные системы, построенные на основе использования web-технологий и гипермедиа структур, можно рассматривать как особую разновидность интеллектуальных комплексов нового направления – систем, доставляющих знания (KnowledgeDeliverySystems).

Развитие web-интерфейса в первую очередь связано с добавлением в базу данных ЕИС учетов в органах внутренних дел новых данных, таких как механизмы и данные пользовательского вида. Также развитие и усовершенствования связаны с увеличением числа постоянных пользователей, которые будут предлагать различные нововведения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Браун И. Веб-разработка с применением Node и Express. Полноценное использование стека JavaScript. – М.: Питер, 2017. – 336 с.

2. Макушкин В.А., Володичев Д.С. Интеграция приложений на основе WebSphereMQ: курс лекций. – М.: ИНТУИТ, 2016.

3. Мандел Т. Разработка пользовательского интерфейса. – М.: ДМК Пресс, 2009. – 416 с.

4. Попов А., Ануфриева Н. Интерфейсы информационных систем: учебное пособие. – Бийск: Алт. гос. техн. ун-т, 2015. – 51 с.

5. Akiko Hoshikawa, Bart Steegmans, Cristian Molaro, Kaitlin E. Murray. IBM Db2 12 for z/OS Performance Topics // Acn IBM Redbooks publication. 2017.

6. Configuring your Browser for trusted HTTPS Connections to IBM Content Navigator and Box // An IBM Redbooks publication. 2017.

ОПЫТ ВНЕДРЕНИЯ И ЭКСПЛУАТАЦИИ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ВЕДОМСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ (НА ПРИМЕРЕ БЕЛ ЮИ МВД РОССИИ ИМЕНИ И.Д. ПУТИЛИНА)

THE EXPERIENCE OF IMPLEMENTING AND OPERATING ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS IN WESTON EDUCATIONAL ORGANIZATIONS (ON AN EXAMPLE BELGOROD LAW INSTITUTE OF THE MIA OF RUSSIA NAMED AFTER I.D. PUTILIN)

Тримасов Евгений Анатольевич,
Колтунов Николай Леонидович
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Колтунова Татьяна Владимировна
(НИУ «БелГУ»)

Trimasov Evgeniy Anatolevich,
Koltunov Nikolay Leonidovich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin);
Koltunova Tatiana Vladimirovna
(NIU «BelSU»)

Аннотация: в статье описаны основные этапы внедрения системы электронного документооборота, основанные на опыте Белгородского юридического института МВД России имени И.Д. Путилина, рассмотрены плюсы и минусы данного вида автоматизации.

Ключевые слова: система электронного документооборота, СЭД, электронная почта, электронная подпись, внедрение, система управления инфраструктурой, Бел ЮИ МВД России имени И.Д. Путилина.

Annotation: the article describes the main stages of the implementation of the electronic document management system based on the experience of the Belgorod Law Institute of the MIA of Russia named after I.D. Putilin, considered the pros and cons of this type of automation.

Key words: electronic document management system, SED, e-mail, electronic signature, implementation, infrastructure management system, Bel LI of the MIA of Russia named after I.D. Putilin.

Система электронного документооборота (далее – СЭД) – это система (компьютерная программа, программное обеспечение), которая позволяет организовать и автоматизировать работу с электронными документами, поддерживается с помощью информационно-коммуникационных технологий на компьютерах, объединенных в сетевую структуру. При этом не исключается использо-

вание «бумажных» документов. Основной функционал СЭД включает в себя возможность создания, изменения, хранения и маршрутизации документов, а также ряда сервисных возможностей, таких как поиск, классификация и пр.

Кроме того, СЭД предназначена для организации и автоматизации процессов взаимодействия между сотрудниками (передачи документов, выдачи заданий, отправки уведомлений и т.п.).

Документооборот существует очень давно, и опыт работы с «бумажными» документами позволяет говорить о том, что все основные проблемы здесь решены.

Электронный документооборот внедряется в нашу повседневную деятельность сравнительно недавно.

Любая технология имеет свои плюсы и минусы.

К основным достоинствам СЭД можно отнести:

1. Ускорение процессов документооборота за счет передачи информации по каналам связи с большой скоростью, вне зависимости от расстояния до получателя.

2. В современном мире документы в абсолютном большинстве случаев создаются в электронном виде. Использование СЭД позволяет значительно сократить время на их редактирование, размножение и распространение.

3. При использовании встроенных поисковых систем, даже при наличии неполной информации, значительно сокращается время на поиск необходимых документов.

4. Использование функционала СЭД позволяет повысить контроль за сроками исполнения документов.

5. Экономию бумаги тоже можно отнести к плюсам.

Как у любой технологии, у электронного документооборота есть свои недостатки, которые необходимо учитывать при отказе от «бумажных» документов. Вот некоторые из них:

1. С широким распространением электронных документов и средств их обработки особо актуальной становится проблема установления подлинности и авторства таких документов.

В конце «бумажного» письма или документа исполнитель (ответственное лицо) ставит свою подпись, тем самым достигая двух целей. Во-первых, получатель имеет возможность убедиться в истинности документа, сравнив подпись с имеющимся у него образцом. Во-вторых, личная подпись является юридическим гарантом авторства документа.

Существует электронная подпись (далее – ЭП), которая призвана заменить собственноручную подпись.

ЭП отчуждаема от своего владельца, а вот подпись под «бумажным» документом неотделима от человека, и никто другой не может подделать ее так, чтобы это не было обнаружено криминалистической экспертизой. С электронной же подписью нельзя быть столь же категоричным. Злоумышленник, завладевший секретным ключом электронной подписи, сможет воспользоваться ею так же, как и законный владелец, что влечет за собой принятие дополнительных мер по обеспечению ее сохранности.

2. Наиболее актуальной является проблема обеспечения сохранности электронных документов.

Технологии обеспечения сохранности «бумажных» документов давно известны, хорошо отработаны и достаточно эффективно применяются в документоведении.

Электронные документы представляют собой информацию, хранящуюся на различных носителях средств вычислительной техники. Электронные носители информации, даже с однократной записью, недолговечны. CD и DVD-диски разрушаются, магнитная лента осыпается и размагничивается. Все электронные носители информации требуют специальных программно-аппаратных комплексов для воспроизведения, которые могут быть повреждены из-за технического сбоя, поломки, ошибки обслуживающего персонала, а также из-за ограниченного срока службы.

И если нарушение правил сохранности в традиционном «бумажном» архиве может повлечь за собой уничтожение одного или нескольких документов, то сбой в компьютерной системе может повлечь потерю всего массива информации.

В связи с этим возникает необходимость обеспечить сохранность как самой информации, так и ее носителей. Это, в свою очередь, требует проведения целого комплекса мероприятий по созданию материально-технической базы, надлежащей организации и оптимальных условий хранения электронных документов, которые исключали бы утрату электронных носителей и обеспечивали бы поддержание их в должном физическом и техническом состоянии, а также воспроизведение электронных документов.

Система электронного документооборота должна быть внедрена на всех автоматизированных рабочих местах, на которых создается, редактируется либо хранится информация, в ином случае эффективность от ее функционирования будет минимальной. Такая позиция в первую очередь выявляет одну из основных проблем внедрения: в любой организации есть люди, не желающие использовать в своей повседневной деятельности что-либо новое. Консерватизм сотрудников обычно связан с нежеланием обучаться и повышать свой профессиональный уровень, а также зачастую с низкой образованностью.

Как поступить в этой ситуации? Работа с людьми – это всегда политика на уровне всей организации и психология на уровне конкретных людей. В большинстве случаев нужен индивидуальный подход к каждому сотруднику, учет его возрастных, профессиональных и личных особенностей. Необходимо понимать, что люди на протяжении многих лет привыкали к одному способу работы, а им предлагается кардинально переключиться на другой, абсолютно им непривычный, при этом не снижая нагрузку. Что можно сделать, чтобы облегчить работникам этот переход?

Во-первых, переход необходимо делать поэтапным. Первым этапом внедрить только электронную почту. Принципы работы электронной почты вполне понятны, и люди легко к ним привыкают. Следующим этапом – построить интернет-систему и постепенно приучать сотрудников искать нужные им справочные материалы (даты, повестки и протоколы совещаний, распоряжения,

приказы и другие нормативные документы, номера внутренних телефонов и т.п.) на внутреннем информационном портале. Благодаря этому люди понемногу привыкнут работать с электронными образами документов и распечатывать только то, что нужно. Данный подход, безусловно, сократит тиражирование бумажных документов и облегчит их обновление. При этом желательно, чтобы система электронной почты и доступа к информации посредством интернет-портала изначально предполагалась как составляющая единой системы документооборота в будущем.

Во-вторых, при подготовке внедрения неплохо было бы найти сторонников-энтузиастов, которые помогали бы «отстающим» сотрудникам вникать в новую для них безбумажную технологию работы. Это должны быть неконфликтные, сдержанные и дружелюбные люди, у которых есть желание помочь другим в освоении того, что сами они уже знают. В соответствии с принципом взаимопомощи должны быть организованы курсы обучения. Важно, чтобы первоначально данные курсы были практически добровольными. Сотрудники, обучающиеся по своему желанию, при правильном подходе к организации обучения будут увлечены и впоследствии станут сторонниками развития. Но уже при массовом внедрении курсы должны стать обязательными, однако к тому времени у людей возникнет интерес и появится определенная информация, которую они получили от тех, кто первым прошел обучение.

Участие руководства – самый важный фактор. Отсутствие принципиальной позиции руководителей организации может привести к негативным последствиям разного уровня тяжести.

Одной из причин неоднозначного отношения к внедрению СЭД руководителей разных уровней в организации является боязнь прозрачности собственной деятельности, которая возникает вследствие внедрения данной системы.

Как решить данную проблему? Убедить руководителя. Подобрать аргументы, которые помогут сделать руководителя сторонником внедрения СЭД.

Основная цель СЭД – не искоренение «бумажных» документов, а создание функциональной и эффективной возможности управления и работы организации. Кроме того, к значительному снижению объема «бумажных» документов приведет тот факт, что распечатывать придется только конечный результат работы – конкретный, полностью подготовленный «бумажный» документ и только в одном «правоустанавливающем» экземпляре.

Чтобы «бумажные» документы могли попасть из внешнего мира во внутреннюю систему электронного документооборота, нужно получить их электронные образы. Для этого используют сканеры.

Распознавание текста документа, а также его хранение вместе с изображением не является необходимым. Однако при наличии распознанного текста появляется возможность использовать одни и те же механизмы полнотекстового поиска.

Этап перевода документов из бумажной формы в электронную является, как правило, одним из самых опасных. Если он не проработан тщательно, есть

риск появления проблем, способных перечеркнуть всю предыдущую работу и провалить весь проект.

В государственных органах при внедрении СЭД нужно учитывать повышенные требования к обеспечению безопасности данных и ограничения доступа.

Слабый кадровый состав, а также вышеупомянутый консерватизм сотрудников особенно характерны для государственных органов. Решение этой проблемы будет возможно посредством реализации перспективных программ повышения квалификации сотрудников государственных органов.

Несмотря на указанные основные недостатки, системы электронного документооборота все более активно внедряются в нашу повседневную деятельность и в перспективе неизбежно заменят старые «бумажные» технологии.

В настоящее время в Бел ЮИ МВД России имени И.Д. Путилина функционирует несколько систем электронного документооборота.

1. Система электронного документооборота Федерального казначейства России. Участниками этой СЭД являются должностные лица института, наделенные полномочиями финансовой подписи распорядителей бюджетных средств.

2. Введена в эксплуатацию система внутреннего электронного документооборота на основе внутренней компьютерной сети.

Пользователями системы являются сотрудники (работники) структурных подразделений и служб института, назначенные их руководителями для непосредственной работы с документами. Участники электронного документооборота выполняют технологические функций по созданию документов и введению данных о них (реквизитов, сроков исполнения, ответственных исполнителей и т.п.).

Система внутреннего электронного документооборота состоит из двух подсистем:

– подсистема внутреннего автоматизированного контроля исполнения документов и поручений;

– подсистема внутренней электронной почты.

Подсистему внутреннего автоматизированного контроля исполнения документов и поручений целесообразно использовать для документального контроля сроков и этапов реализации поручений и мероприятий системы управления инфраструктурой образовательной организации, внося в подсистему пункты планов и поручений с указанием промежуточных и окончательных сроков исполнения конкретным должностным лицам.

Подсистема внутренней электронной почты предназначена для пересылки и получения электронных сообщений, не требующих обязательной регистрации (периодических изданий: газет, журналов, сборников, плакатов, рекламных извещений, проспектов, поздравительных писем и телеграмм, сообщений о заседаниях, совещаниях, занятиях).

В настоящее время (после перевода компьютерной сети института на новый доменный сервер) внутренней электронной почтой обеспечиваются 100% пользователей, работающих на компьютерах в локальной сети института.

Программное обеспечение внутренней СЭД института установлено на серверной части сети института, что позволяет обеспечить сохранность (целостность) электронных документов. Доступ к СЭД института организован че-

рез веб-интерфейс, что значительно снижает нагрузку на автоматизированные рабочие места пользователей.

3. Одной из систем, получивших развитие в последние годы и функционирующих в институте, является Сервис электронного документооборота Единой системы информационно-аналитического обеспечения деятельности органов внутренних дел Российской Федерации (далее – ИСОД МВД России).

Сервис электронного документооборота предназначен для автоматизации деятельности сотрудников федеральных государственных гражданских служащих и работников, сотрудников и работников МВД России, территориальных органов МВД России, а также иных организаций и подразделений.

В отделении делопроизводства и режима института организовано и настроено автоматизированное рабочее место делопроизводителя, укомплектованное персональным компьютером, а также специализированной организационной техникой, поставленной централизованным порядком по нашей заявке. Поточный сканер, принтер и сканер штрих-кода позволяют сотрудникам отделения вести полноценный электронный документооборот и работать не только с электронными документами, но и переводить документы из бумажных носителей в электронный вид.

Сотрудниками ОИТО УП института были осуществлены мероприятия по оснащению структурных подразделений института средствами вычислительной техники для подключения к ИСОД МВД России, осуществлена настройка специализированного программного обеспечения информационной безопасности.

Для подключения к СЭД МВД России участникам электронного документооборота необходимо создать учетную запись системы управления доступом к информационным системам (далее – СУДИС) ИСОД МВД России. Учетные записи СУДИС ИСОД МВД России в настоящее время имеют более 100 сотрудников и работников института, из них 50 обеспечены электронной подписью для работы в сервисах ИСОД МВД России, выданных удостоверяющим центром МВД России. В институте организовано 60 автоматизированных рабочих мест, подключенных к ИСОД МВД России. Для структурных подразделений, не оборудованных доступом в ИСОД МВД России, в служебном помещении ОИТО УП и кабинете педагогического мастерства организованы рабочие места.

Проведенные мероприятия по программно-техническому обеспечению сервиса электронного документооборота МВД России в институте позволяют сотрудникам и работникам института использовать возможности Сервиса в необходимом объеме.

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ СЕТЕЙ СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

THE POSSIBILITY OF USING SOCIAL NETWORKING BY LAW ENFORCEMENT OFFICIALS

Семенов Евгений Юрьевич,
Пузикова Ирина Юрьевна
(Орловский юридический институт МВД России имени В.В. Лукьянова)

Semenov Evgeni Yurevich,
Puzikova Irina Yurevna
(Orel Law Institute of the MIA of Russia named after V.V. Luk'anov)

Аннотация: в статье рассмотрены возможности использования социальных сетей сотрудниками правоохранительных органов.

Ключевые слова: безопасность общества, мониторинг социальных сетей, противозаконная деятельности в сети, сетевые информационные технологии, социальные сети.

Annotation: the article considers possibilities of the use of social media by law enforcement officials.

Key words: public safety, social monitoring, illegal activities in the network, network information technology, social networking.

Использование передовых достижений науки и техники, современных информационно-телекоммуникационных сетей общего и ограниченного доступа, доступа к разнообразным базам данных играет важную роль в интенсификации процесса передачи, обмена и получения информации в ходе предупреждения, пресечения и раскрытия преступлений и в дальнейшем будет только усиливать свое влияние и значимость в оперативно-служебной деятельности ОВД и иных правоохранительных органов Российской Федерации.

В современных условиях важная роль в обеспечении безопасности общества, защиты жизни, здоровья, прав и свобод человека отводится оперативно-техническим подразделениям МВД России, в обязанности которых входит своевременное реагирование на информацию, поступающую от граждан о происшествиях и преступлениях [4, с. 146].

Основополагающим направлением в данной области стала реализация требований Указа Президента Российской Федерации от 7 мая 2012 г. «Об основных направлениях совершенствования системы государственного управления» [1].

В последнее время сотрудники правоохранительных органов все чаще производят мониторинг социальных сетей с целью поиска преступников, установления обстоятельств преступного деяния, розыска возможных свидетелей и

очевидцев. В соответствии с действующим законодательством основными направлениями противодействия террористической и экстремистской деятельности являются: принятие профилактических мер, направленных на предупреждение террористической и экстремистской деятельности, в том числе на выявление и последующее устранение причин и условий, способствующих осуществлению террористической и экстремистской деятельности; выявление, предупреждение и пресечение террористической и экстремистской деятельности общественных и религиозных объединений, иных организаций, физических лиц. Однако не стоит забывать, что поиск преступников с помощью социальных сетей является второстепенным методом работы для сотрудников правоохранительных органов.

В силу широкого использования информационных технологий сети Интернет диапазон правонарушений, которые можно обнаружить с помощью исследования электронных сетей, достаточно велик. Маловероятно, что злоумышленник станет обсуждать в социальных сетях заказное убийство или ограбление банка. Но распитие алкоголя несовершеннолетними или акт вандализма вполне может иметь свидетельства в социальной сети, и иногда подобные действия сотрудникам полиции удается предотвратить [2].

Каждый подключенный к сети Интернет персональный компьютер имеет уникальный сетевой IP-адрес. Одновременно в сети не может находиться два компьютера с одинаковым адресом, что позволяет определить, с какого компьютера осуществлялась противоправная деятельность. Некоторые сервисы сразу выдают и данные о местонахождении компьютера, в качестве примера можно привести российский сервис 2ip.ru. Данный ресурс позволяет в считанные секунды получить достаточно полный объем информации, но определение местоположения компьютера довольно часто оказывается ошибочным.

Человек, занимающийся в Интернете противозаконной деятельностью, зачастую предпринимает меры по скрытию своего реального IP-адреса, поэтому большая вероятность, что даже если обычному пользователю удается определить реальный сетевой адрес компьютера, то он не сможет узнать данные его владельца, так как провайдеры предоставляют такие сведения только по запросу правоохранительных органов.

Борьбу с преступлениями в сфере информационных технологий осуществляет бюро специальных технических мероприятий (БСТМ) МВД, получившее название в структуре подразделений криминальной полиции «отдел "К"». В процессе своей служебной деятельности сотрудники МВД в рамках материалов проверки, а также при возбужденном уголовном деле обращаются к «отделу "К"» для получения информации в рамках решаемых задач отдела. В задачи БСТМ входят:

- борьба с нарушением авторских и смежных прав, выявление незаконного проникновения в компьютерную сеть;
- борьба с распространителями вредоносных программ;
- выявление нарушений правил эксплуатации ЭВМ;
- выявление использования подложных банковских карт;
- борьба с распространением порнографии посредством сети Интернет и компакт-дисков;

- выявление незаконного подключения к телефонным линиям;

- борьба с незаконным оборотом радиоэлектронных и специальных технических средств, противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей [3].

В настоящее время широкое распространение получили отечественные социальные сети «Вконтакте» и «Одноклассники». Основное предназначение использования данных сетей в повседневной жизни человека – общение и обмен фотографиями с другими пользователями данных социальных сетей. Не исключен факт, что правонарушитель, объявленный в розыск, может быть зарегистрирован и иметь личную страничку с фотографиями в социальной сети. В этом случае становится актуальным определение местонахождения такого человека по IP-адресу компьютера, с которого он выходит в социальную сеть.

Кроме того, при регистрации в социальных сетях зачастую пользователи указывают свои контактные сотовые телефоны. IP-адрес и номер сотового телефона пользователя социальной сети можно узнать только по официальному запросу правоохранительных органов, направив его непосредственно в административный офис социальной сети, адрес которого можно узнать через службу технической поддержки сети.

Запрос в ООО «Вконтакте» может быть направлен по адресу: 191040, г. Санкт-петербург, Лиговский проезд, д. 61, литер А.; а запрос в ООО «Одноклассники»: 125167, г. Москва, Ленинградский проспект, д. 39, строение 79, БЦ «SkyLight» на имя генерального директора управляющей организации ООО «Интернет-компания Мэйл.Ру» Багудиной Е.Г.

В ответном письме ООО «Одноклассники» и ООО «Вконтакте» предоставляют сведения о номере телефона запрашиваемого лица, его e-mail-адрес и даты входа в социальную сеть с указанием IP-адреса компьютера [4, с. 147-148].

Анализ возможностей социальных сетей в получении информации показывает возможные направления их использования следователем. Во-первых, социальные сети позволяют быстро получать разнообразную справочно-вспомогательную информацию по расследуемому уголовному делу. Во-вторых, проводя тщательный анализ имеющейся в социальных сетях информации о лице или лицах, имеющих отношение к расследуемому уголовному делу, можно получать данные о них самих, их связях, увлечениях, отношении к чему-либо и подобном, также можно определить их местоположение. Отличным примером для подобной ситуации будет являться сайт «Одноклассники». В профиле видны не только друзья самого пользователя, но и друзья друзей, а это является достаточно полным спектром связей фигуранта. В-третьих, социальные сети могут давать возможность прямого контакта с интересующими следователя лицами посредством видеосвязи или использования различного рода сообщений. При этом не имеет значения, представился ли следователь своим именем или использовал какую-нибудь легенду.

Использовать информацию из социальных сетей как основную в процессе раскрытия и расследования преступлений нельзя, так как наличие каких-либо данных, полученных из сети Интернет, без уголовно-процессуальной составляющей доказательствами не считаются [5, с. 426]. Поэтому поиск преступни-

ков с помощью социальных сетей является второстепенным методом работы для сотрудников правоохранительных органов, т.к. человек может зарегистрироваться под чужими ФИО и не размещать на своей странице собственное фото. Это может навести следователя или оперуполномоченного на ложный след. Однако игнорировать подобный способ собирания оперативной информации нельзя.

К сожалению, социальные сети можно считать криминогенной средой. Комфортные условия для распространения преступности всевозможных форм и видов приводят к появлению в данных сетях многочисленных зон общения между преступными элементами. Посредством этих сетей преступники могут собирать информацию о своих жертвах, так как данная информация, как правило, находится в абсолютно свободном доступе. Также в социальных сетях в последние годы происходит увеличение разнообразных информационных ресурсов, которые имеют явную экстремистскую направленность.

Наряду с использованием некоторых радио- и телепрограмм, в сети Интернет создаются соответствующие сайты, а в социальных сетях группы и сообщества, которые организованы преступными элементами и могут использоваться не только для обмена информацией, но и для распространения и популяризации своих националистических, экстремистских идей и образа поведения. И это лишь малая часть возможностей социальных сетей и Интернета, которыми пользуются преступники. Широкое распространение информации о местах сбыта наркотических веществ, рекомендаций по их изготовлению и потреблению, торговле оружием, распространению всевозможной литературы экстремистской направленности, с призывами к разжиганию межнациональной розни, пропаганды разврата и т.п. – все это стало возможным с помощью сети Интернет. Нередко стало в последнее время распространение на таких знаменитых ресурсах, как Youtube и Вконтакте, разнообразного видео, снятого на камеру мобильных телефонов, с избиением случайных прохожих или несовершеннолетних детей.

Таким образом, использование социальных сетей для получения информации о криминальном событии российскими правоохранительными органами в силу стремительного развития информационных технологий становится более актуальным и требует дальнейшего развития и изучения. Кроме того, использование таких систем службами собственной безопасности правоохранительных органов может помочь выявлению нарушений среди личного состава сотрудников.

Можно прийти к выводу, что мониторинг социальных сетей сотрудниками правоохранительных органов – очень эффективная деятельность по сбору криминалистически значимой информации. Однако большие объемы усложняют процедуру сбора и могут затруднять работу следователя в ходе расследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 7 мая 2012 г. № 601 «Об основных направлениях совершенствования системы государственного управления» // СЗ РФ. 2012. № 19. Ст. 2338.

2. Полиция в социальной сети. Newsland [Электронный ресурс]. – Режим доступа: http://newsland.com/.

3. Управление «К» [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Управление К.

4. Михед А.Д., Безгубова А.А. Использование правоохранительными органами Интернета и телекоммуникационных систем для получения информации о криминальном событии // Известия Тульского государственного университета. Экономические и юридические науки. 2015. № 3.

5. Цимбал Н.Г., Цимбал В.Н. Использование информации социальных сетей Интернет в ходе предварительного расследования // Теория и практика общественного развития. 2013. № 10.

ИНФОРМАТИЗАЦИЯ МИГРАЦИОННОЙ СИСТЕМЫ РОССИИ – ВАЖНЕЙШАЯ СОСТАВЛЯЮЩАЯ МИГРАЦИОННОГО УЧЕТА

COMPUTERIZATION OF THE IMMIGRATION SYSTEM IN RUSSIA – HE MOST IMPORTANT COMPONENT OF MIGRATION REGISTRATION

Кочеткова Наталья Дмитриевна
(Орловский юридический институт МВД России имени В.В. Лукьянова)

Kotchetkova Natalia Dmitrievna
(Orel Law Institute of the MIA of Russia named after V.V. Luk'anov)

Аннотация: в статье рассмотрены проблемы информатизации миграционной системы России как важнейшей составляющей миграционного учета.

Ключевые слова: миграционные процессы, миграционная служба, регистрационный учет, информационно-аналитическая система, иностранные граждане, информационный обмен.

Annotation: the article considers the problems of informatization of the migration system of Russia as a major component of migration control.

Key words: migration processes, the migration service, registration, information-analytical system, foreign citizens, exchange of information.

Наличие полной и достоверной информации о состоянии миграционных процессов необходимо государству для выработки и реализации эффективной государственной миграционной политики, включая предотвращение негативных тенденций развития миграционной и демографической ситуации. Данные миграционного учета (эффективная система накопления, обработки и последующего анализа учетной информации) обеспечивают решение ряда практических задач в области управления в кризисных ситуациях, планирования развития территорий и рационального распределения трудовых ресурсов в Российской Федерации.

В соответствии с Указом Президента Российской Федерации от 5 апреля 2016 г. № 156 «О совершенствовании государственного управления в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров и в сфере миграции» [1] упразднена Федеральная миграционная служба России, а ее функции и полномочия переданы МВД России. Основными функциями и полномочиями, возложенными на Министерство внутренних дел Российской Федерации в рассматриваемой сфере, являются выработка и реализация государственной политики и нормативно-правовое регулирование, а также правоприменительные функции по федеральному государственному контролю и надзору в сфере миграции.

Главное управление по вопросам миграции Министерства внутренних дел Российской Федерации – подразделение МВД России, являющееся самостоятельным структурным оперативным подразделением центрального аппарата Министерства внутренних дел, на которое возложена реализация государственной политики в сфере миграции (эмиграции, иммиграции). Оно осуществляет правоприменительные функции, функции по оказанию государственных услуг в сфере миграции, гражданства, регистрации физических лиц, беженцев и иных категорий мигрантов, предусмотренных законодательством. Занимается борьбой с незаконной иммиграцией.

Основными задачами являются также правоприменение нормативно-правовых актов в сфере регистрационного учёта, выдачи и замены основных документов, удостоверяющих личность гражданина России, в том числе за пределами территории Российской Федерации, приобретения гражданства Российской Федерации и отказа от него, контроля за пребыванием на территории стране иностранных граждан и лиц без гражданства. И в этой связи государству просто необходима информатизация миграционной системы.

Информационно-аналитическая система Российской Федерации представляет собой центральный банк данных по учету иностранных граждан. Так, в соответствии с Положением о создании, ведении и использовании центрального банка данных по учету иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации, утвержденным Постановлением Правительства Российской Федерации от 6 апреля 2005 г. № 186 [2], центральный банк данных – это специализированная межведомственная автоматизированная информационная подсистема, содержащая информацию об иностранных гражданах и лицах без гражданства, въезжающих в Российскую Федерацию, временно пребывающих и временно или постоянно

проживающих в Российской Федерации и выезжающих из Российской Федерации. Федеральные органы исполнительной власти Российской Федерации совместно пополняют данный банк и используют в своей деятельности необходимую им информацию в целях осуществления контроля за миграционной ситуацией в Российской Федерации.

Центральный банк данных является федеральным информационным ресурсом и находится в ведении МВД России. Ведение центрального банка данных осуществляется с применением стандартизированных технических и программных средств, прошедших соответствующую проверку и сертификацию, а также унифицированных информационных ресурсов на основе использования единых форматов и классификаторов учетных данных, стандартных протоколов и регламентов обмена информацией.

В центральном банке данных накапливается информация об иностранных гражданах, поступающая от федеральных органов исполнительной власти и организаций, оформляющих въездные-выездные документы иностранных граждан, осуществляющих их регистрацию при пересечении государственной границы Российской Федерации и по месту пребывания или проживания, а также определяющих регламент пребывания.

Сведения об иностранных гражданах, находящихся на территории Российской Федерации, направляются органами исполнительной власти субъектов Российской Федерации в федеральные органы исполнительной власти, осуществляющие учет иностранных граждан, где они проходят обработку и затем передаются в центральный банк данных, где полученная информация обрабатывается и накапливается.

Как справедливо указывает Л.Д. Матросова, территориальным органам внутренних дел необходимо шире использовать имеющиеся у них автоматизированные рабочие места в целях ведения статистической работы в рассматриваемой сфере общественных отношений [4].

В соответствии с Федеральным законом «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» Правительство Российской Федерации утвердило Положение о государственной информационной системе миграционного учета [3], которое определяет порядок формирования и обеспечения функционирования государственной информационной системы миграционного учета, внесения изменений в сведения (информацию) об иностранных гражданах и лицах без гражданства, содержащиеся в информационной системе, порядок и срок их хранения, порядок доступа к сведениям, порядок их предоставления, использования и защиты, а также порядок взаимодействия органов миграционного учета с иными федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации и органами местного самоуправления в целях эффективного использования и защиты сведений.

Государственная информационная система миграционного учета – это межведомственная автоматизированная система, функционирование которой осуществляется путем применения стандартизированных технических и программных средств, прошедших соответствующую проверку и сертификацию,

единых форматов, классификаторов учетных данных, словарей, справочников и стандартных протоколов в порядке, определяемом нормативными правовыми актами, принятыми совместно с заинтересованными федеральными органами исполнительной власти.

Доступ участников информационного обмена к сведениям осуществляется с учетом требований Положения о государственной информационной системе миграционного учета, утвержденного Постановлением Правительства РФ от 14 февраля 2007 г. № 94 «О государственной информационной системе миграционного учета» [3], а также установленных законодательством Российской Федерации ограничений по использованию сведений и при условии применения программно-технических средств, позволяющих идентифицировать лицо, осуществляющее доступ к сведениям.

В территориальных органах МВД России выделяются подразделения, на которые возлагается ответственность за организацию информационного обмена сведениями, а также иной информацией об иностранных гражданах, содержащейся в их информационных системах и подлежащей включению в информационную систему.

Так, во исполнение Указа Президента России от 5 апреля 2016 г. № 156, за счет упразднения территориальных подразделений ФМС России в структуре Управления МВД России по Орловской области сформировано Управление по вопросам миграции, а также территориальные подразделения на районных уровнях.

Сотрудники Управления по вопросам миграции УМВД России по Орловской области постоянно проводят комплексные профилактические операции по проверке соблюдения гражданами, иностранными гражданами и лицами без гражданства, должностными лицами установленных паспортно-регистрационных правил, а также осуществляют целевые проверки соблюдения указанными лицами паспортно-регистрационных правил на территории отдельных объектов, предприятиях, организациях.

На МВД России возложена ответственность за ведение центрального банка данных. При выявлении правонарушений в области обеспечения режима пребывания иностранных граждан и лиц без гражданства на территории Российской Федерации, как справедливо указывает О.В. Катаева, виновные привлекаются к административной ответственности [5].

Значимое внимание органами внутренних дел уделяется вопросам противодействия экстремизму, обеспечения надлежащего контроля за миграционной ситуацией, профилактике межнациональных и межрелигиозных конфликтов. В целях недопущения совершения преступлений террористического и экстремистского характера совместно с УФСБ России по Орловской области осуществлен комплекс дополнительных оперативно-разыскных мероприятий.

Сотрудниками УМВД России по Орловской области за 2016 год проведено 667 контрольно-надзорных мероприятий по выявлению фактов нарушений миграционного законодательства, в ходе которых было проверено 54 объекта в сфере торговли, 20 – в строительстве, 7 промышленных предприятий, 99 мест компактного пребывания (проживания) иностранных граждан. Также осуществлено

113 проверок соблюдения гражданами Российской Федерации и должностными лицами Правил регистрации. По выявленным нарушениям по 140 материалам районными судами приняты решения о применении наказания в виде административного выдворения иностранных граждан за пределы Российской Федерации, 99 таких решений исполнены. УВМ УМВД России по Орловской области вынесено 119 решений о депортации иностранных граждан, из которых исполнено 110 [6].

При осуществлении контроля за соблюдением миграционного законодательства выявлено 4 213 административных правонарушений, в т.ч. 592 – по ст. 18.8 КоАП РФ, 120 – по ст. 18.9 КоАП РФ, 33 – по ст. 18.10 КоАП РФ, 85 – по ст. 18.15 КоАП РФ, 3 333 – в сфере регистрационного и паспортного режима [6].

Таким образом, в настоящее время самостоятельное осуществление функций Главного управления по вопросам миграции МВД России по осуществлению контроля и надзора за соблюдением правил въезда, выезда, пребывания и транзитного проезда иностранных граждан через территорию России не представляется возможным. Это связано с недостаточно развитой нормативно-правовой, организационной и материально-технической базой службы. При этом следует указать на широкий круг полномочий сотрудников полиции в сфере предупреждения, выявления и пресечения, применения мер принуждения, а также возбуждения дел об административных правонарушениях и обеспечения режима пребывания иностранных граждан или лиц без гражданства на территории Российской Федерации, а также исполнения административных наказаний вплоть до реализации административного выдворения.

В целом можно сделать вывод о том, что в настоящее время в рамках проведенной реформы 2016 года в сфере совершенствования государственного управления в сфере миграции и политико-правовых и организационных последствий существует широкий круг полномочий сотрудников полиции в сфере предупреждения, выявления и пресечения, применения мер государственного принуждения, а также возбуждения дел об административных правонарушениях в миграционной сфере.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента Российской Федерации от 5 апреля 2016 г. № 156 «О совершенствовании государственного управления в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров и в сфере миграции» // СЗ РФ. 2016. № 15. Ст. 2071.

2. Постановление Правительства Российской Федерации от 6 апреля 2005 г. № 186 «Об утверждении Положения о создании, ведении и использовании центрального банка данных по учету иностранных граждан, временно пребывающих и временно или постоянно проживающих в Российской Федерации, в том числе участников Государственной программы по оказанию содействия добровольному переселению в Российскую Федерацию соотечественников, проживающих за рубежом» (в ред. от 7 декабря 2011 г.) // СЗ РФ. 2005. № 15. Ст. 1348.

3. Постановление Правительства Российской Федерации от 14 февраля 2007 г. № 94 «О государственной информационной системе миграционного учета» (в ред. от 30 ноября 2016 г.) // СЗ РФ. 2007. № 8. Ст. 1012.

4. Матросова Л.Д. Перспективные возможности использования автоматизированных рабочих мест в статистической работе правоохранительных органов // Наука и практика. 2014. № 1 (58). С 170.

5. Катаева О.В. Административная ответственность за нарушения в области обеспечения режима пребывания иностранных граждан и лиц без гражданства на территории Российской Федерации: дис. … канд. юрид. наук. – Воронеж, 2007. – 186 с.

6. Информационно-аналитическая записка «О деятельности подразделений полиции УМВД России по Орловской области за 2016 год» [Электронный ресурс]. – Режим доступа: https://57.мвд.рф/slujba/action/item/.

ВОПРОСЫ РАЗВИТИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В РОССИЙСКОЙ ФЕДЕРАЦИИ

ISSUES OF ELECTRONIC GOVERNMENT DEVELOPMENT IN RUSSIAN FEDERATION

Линьков Вадим Вячеславович
(Орловский юридический институт МВД России имени В.В. Лукьянова)

Lin'kov Vadim Vyacheslavovich
(Orel Law Institute of MIA of Russia named after V.V. Luk'anov)

Аннотация: в статье рассматриваются особенности формирования информационного общества и принципы построения электронного правительства в Российской Федерации.

Ключевые слова: информационно-коммуникационные технологии, электронное правительство, развитие информационного общества, электронная подпись, образовательная среда.

Annotation: in the article features of formation of an information society and principles of construction of electronic government in the Russian Federation are considered.

Key words: information and communication technologies, electronic government, information society development, electronic signature, educational environment.

Внедрение электронного правительства предполагает построение общегосударственной распределенной системы общественного управления, реализующей решение полного спектра задач, связанных с управлением документами и процессами их обработки. Электронное правительство не является дополнением или аналогом традиционного правительства, а лишь определяет новый способ взаимодействия на основе активного использования информационно-

коммуникационных технологий в целях повышения эффективности и качества предоставления государственных услуг.

Развитие технологии web 2.0 укрепит эту тенденцию. Данная технология обеспечит новую интеграцию государства и граждан.

Основными целями электронного правительства являются:

– оптимизация порядка предоставления государственных услуг;

– увеличение степени участия всех избирателей в процессах руководства и управления страной;

– рост технологической осведомленности и информационной культуры граждан;

– снижение влияния фактора географического местоположения за счет использования распределенных систем [1].

Практическая реализация Стратегии развития информационного общества в России является актуальной и важной задачей в настоящее время. Ее реализация способствует созданию новых возможностей развития рынка труда и решения проблем занятости населения, экономии энергии и материалов, повышения производительности труда, эффективности информационных коммуникаций и качества управления [2].

Ключевыми элементами национальной инфраструктуры электронного правительства являются:

1. Единый портал государственных и муниципальных услуг (ЕПГУ).

2. Федеральный реестр государственных услуг (ФРГУ).

3. Единая система нормативно-справочной информации (ЕСНСИ).

4. Единая система межведомственного электронного взаимодействия (СМЭВ).

5. Единая система идентификации и аутентификации (ЕСИА).

6. Единое пространство доверия (ЕПД).

7. Государственная информационная система о государственных и муниципальных платежах (ГИС ГМП).

Однако становление электронного правительства в Российской Федерации еще не завершено. В ближайшем будущем преобразования коснутся избирательной системы. Они будут связаны с внедрением такой формы взаимодействия, как электронная демократия.

Повсеместное использование электронной подписи в системах документооборота государственных органов является одним из приоритетных направлений реформирования системы управления, и этот процесс уже реализуется.

Для Российской Федерации, учитывая ее территориальную распределенность, важным аспектом является ликвидация цифрового неравенства, которое выражается в несопоставимых уровнях развития информационных инфраструктур в различных регионах страны.

Для повышения доступности к информационным ресурсам и исполнителям государственных услуг одной из перспективных задач является внедрение бесплатных Wi-Fi точек доступа к сети Интернет по всей территории Российской Федерации.

Немаловажным этапом развития системы электронного правительства также является формирование образовательной среды для массового обучения граждан в сфере информационных технологий. Реализация этого процесса повысит вовлеченность населения в деятельность электронного правительства.

Таким образом, реализация концепции электронного правительства в Российской Федерации позволяет снизить административные барьеры для граждан и организаций; сократить коррупционные риски и значительно уменьшить сроки предоставления государственных услуг за внедрения современных информационных технологий в деятельность органов исполнительной власти.

В настоящее время идет активное внедрение основных положений концепции электронного правительства. Многие задачи этого направления уже решены. В перспективе еще предстоит обеспечить повсеместное использование электронной подписи, внедрить систему электронной демократии и сформировать условия для большего вовлечения населения в государственную деятельность за счет эффективного использования информационных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011-2020 годы)» // СЗ РФ. 2014. № 18 (ч. II).

2. Исаева И.В. Инновационная стратегия развития вертикально-интегрированных предприятий в регионах России // Бизнес. Инновации. Образование. 2015. № 9.

К ВОПРОСУ СОВЕРШЕНСТВОВАНИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ГОСАВТОИНСПЕКЦИИ С ЦЕЛЬЮ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ

TO IMPROVING MANAGEMENT AND TECHNICAL SUPPORT ACTIVITIES OF THE STATE TRAFFIC INSPECTORATE WITH THE AIM OF IMPROVING THE EFFICIENCY OF ROAD SAFETY

Матросова Лидия Дмитриевна
(Орловский юридический институт МВД России имени В.В. Лукьянова)

Matrosova Lidia Dmitrievna
(Orel Law Institute of the MIA of Russia named after V.V. Luk’anov)

Аннотация: в статье раскрывается проблема совершенствования управления информационно-технического обеспечения деятельности Госавтоинспекции с целью повышения эффективности безопасности дорожного движения.

Ключевые слова: единое информационное пространство, информационное обеспечение, федеральная информационная система.

Annotation: the article reveals the problem of improving management and technical support activities of the state traffic Inspectorate with the aim of improving the efficiency of road safety.

Key words: common information space, information security, Federal information system.

В целях обеспечения деятельности подразделений Госавтоинспекции МВД России, а также их взаимодействия с соответствующими органами государственной власти Российской Федерации разработано специальное программное обеспечение федеральной информационной системы Госавтоинспекции (ФИС ГИБДД-М). Она является одной из систем обеспечения оперативно-служебной деятельности органов внутренних дел, размещенных в центре обработки данных Единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России), функционирует круглосуточно на федеральном уровне [1, с. 161].

ФИС ГИБДД-М создана для организации единого централизованного информационного пространства Госавтоинспекции, обеспечения эффективной информационной поддержки деятельности подразделений Госавтоинспекции, а также информационного обмена с заинтересованными органами в целях предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций.

Можно выделить основные достоинства данной системы. Прежде всего, это обеспечение подразделений органов внутренних дел Российской Федерации информацией о юридически значимых действиях, относящихся к компетенции Госавтоинспекции, обеспечение подразделений Госавтоинспекции сведениями, содержащимися в централизованных учетах ФКУ «ГИАЦ МВД России» (о разыскиваемых транспортных средствах и о лицах, объявленных в федеральный розыск), прикладных сервисах обеспечения повседневной деятельности подразделений МВД России, информационных системах МВД России, а также информационных ресурсах заинтересованных органов, необходимых для деятельности подразделений Госавтоинспекции.

Немаловажным, на наш взгляд, является и обеспечение подразделений Госавтоинспекции функциональными возможностями по исполнению административных регламентов и процессов, включая мероприятия по информационному взаимодействию с подразделениями органов внутренних дел Российской Федерации, заинтересованными органами, а также гражданами в рамках предоставления государственных и муниципальных услуг.

Отметим, что ФИС ГИБДД-М состоит из подсистем, обеспечивающих автоматизацию проведения регистрационных действий с транспортными средствами, автоматизацию функций Госавтоинспекции по учету сведений о выданных российских национальных и международных водительских удостоверениях, лицах, получивших водительское удостоверение, а также для обеспечения

предоставления подразделениями Госавтоинспекции государственной услуги по проведению экзаменов на право управления транспортными средствами и выдаче водительских удостоверений, включая межведомственное информационное взаимодействие в ходе предоставления государственной услуги.

Данная система позволяет вести учет административных правонарушений, по которым сотрудники Госавтоинспекции уполномочены составлять протоколы об административном правонарушении, и автоматизации процесса производства по ним, а также информационного обеспечения оказания подразделениями Госавтоинспекции государственной услуги по предоставлению сведений об административных правонарушениях в области дорожного движения. Разработаны подсистемы для учета распределенной в подразделения Госавтоинспекции, утраченной, похищенной, уничтоженной специальной продукции, необходимой для допуска транспортных средств и водителей к участию в дорожном движении, имеется возможность обеспечения взаимодействия ФИС ГИБДД-М с прикладными сервисами ИСОД МВД России, информационными системами МВД России, а также с информационными ресурсами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, предоставляющих государственные или муниципальные услуги и исполняющих государственные или муниципальные функции, а также организаций, в которых размещается государственное задание (заказ) или муниципальное задание (заказ) на предоставление таких услуг.

Сведения, содержащиеся в базовых ресурсах, включенных в ФИС ГИБДД-М, предоставляются гражданам, юридическим лицам, а также заинтересованным органам в случаях и в порядке, которые предусмотрены законодательством Российской Федерации.

Доступ заинтересованного органа к базовым ресурсам в электронном виде обеспечивается с помощью федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

Информационное обеспечение оперативно-служебной деятельности Госавтоинспекции по субъектам Российской Федерации осуществляет и координирует отделение обслуживания технических средств и защиты информации ЦАФАП ГИБДД УМВД России. В рамках оперативно-служебной деятельности осуществляется использование таких федеральных информационных ресурсов, как Федеральная информационная адресная система (ФИАС), Многопараметрическая информационно-аналитическая система прогнозирования и моделирования ситуации в области обеспечения безопасности дорожного движения (МИАС ГИБДД), Автоматизированная информационно-управляющая система Госавтоинспекции (АИУС ДПС), Автоматизированная система учета дорожно-транспортных происшествий (АС УДТП). Одновременно с указанными информационными банками данных на региональном уровне используются возможности информационных ресурсов УМВД России по субъектам: информацион-

ной базы данных «ИБД-Регион», справочно-правовых систем, сервисов активации лицензионных программных продуктов.

С 2015 года во всех подразделениях Госавтоинспекции УМВД России на региональном уровне проведены практические мероприятия по развертыванию и внедрению в промышленную эксплуатацию информационной системы «ФИС ГИБДД-М», запущены в эксплуатацию и успешно используются программно-аппаратные комплексы «Экзаменационный класс» для принятия теоретических экзаменов на получение водительского удостоверения.

В 2016 году в соответствии с приказом МВД России от 5 февраля 2016 г. № 60 во всех территориальных органах МВД России на районном уровне, проведены практические мероприятия по подключению сотрудников дежурных частей к специальному программному обеспечению федеральной информационной системы Госавтоинспекции «ФИС ГИБДД-М» [2].

Но, учитывая, непродолжительный срок эксплуатации данной системы, однозначные выводы относительно как достоинств, так и недостатков делать рано. Система разработана, введена в эксплуатацию, разработчиками продолжаются работы по ее совершенствованию. Все технические и эксплуатационные вопросы регулярно озвучиваются сотрудниками региональных отделений информационного обеспечения, регистрационных, экзаменационных подразделений и сотрудниками подразделений по исполнению административного законодательства в ходе проводимых сеансов ВКС.

С 2016 года реализуются мероприятия подпрограммы «Автомобильные дороги» федеральной целевой программы «Развитие транспортной системы России (2010-2020 гг.)», введена в эксплуатацию информационная система персональных данных – Центр автоматизированной фиксации административных правонарушений в области дорожного движения (ЦАФАП ОДД) ГИБДД УМВД России по Красноярскому краю, Приморскому краю, Хабаровскому краю, Чукотскому автономному округу [3]. Созданы Информационные системы персональных данных (ИСПД), представляющие собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. ИСПД позволяет обрабатывать данные о нарушениях правил дорожного движения (ПДД), выявленных комплексами автоматической фото-, видеофиксации, при обработке нарушений система автоматически обращается к сведениям, содержащимся в ФИАС ГИБДД, формирует административные материалы в отношении собственников транспортных средств, совершивших административные правонарушения, начиная от составления материала и заканчивая его фактическим исполнением. Данная информационная система имеет дополнительную функцию формирования банка данных обо всех транспортных средствах, зафиксированных комплексами фото- и видеофиксации, полученная информация эффективно применяется службами УМВД России при раскрытии преступлений, совершаемых с использованием транспортных средств.

Конечно, могут возникать проблемы при эксплуатации ФИС ГИБДД-М, в частности, это частые сбои при работе модулей, небольшое количество различных отчетов и выборок, а также отсутствие специальных мобильных аппаратных комплексов (например, АПК «БАРС») для удаленной работы подразделений отдельного батальона дорожно-патрульной службы на обслуживаемой территории.

В настоящее время в России насчитывается более 42 млн автотранспортных средств, существенная часть граждан нашей страны (43%) имеет водительские права. До недавнего времени вся информация о зарегистрированных транспортных средствах, выданных водительских удостоверениях, административных нарушениях содержалась и обрабатывалась в нескольких слабосвязанных информационных системах Госавтоинспекции регионального и федерального уровней, что приводило к постоянным сбоям и задержкам в работе подразделений ГИБДД. Кроме того, при таком уровне связей было проблематично оказание в электронном виде государственных услуг, связанных с деятельностью ГИБДД, таких как выдача прав, регистрация автотранспорта и другие. Поэтому для ускоренного решения этих задач, а также для общего повышения качества работы Госавтоинспекции была создана единая централизованная система «ФИС ГИБДД-М», которая позволяет автоматизировать деятельность регистрационно-экзаменационных и строевых подразделений Госавтоинспекции, а также процессы поиска и закрытия информации об участниках дорожного движения и их транспортных средствах. Стал доступен обмен данными между подразделениями Госавтоинспекции в режиме реального времени: информация о регистрации автомобиля, лишении права на управление транспортным средством, информация об административных правонарушениях – все эти и многие другие данные стали мгновенно доступны в любом подразделении. Для граждан сократилось время оказания государственных услуг и получения информации о штрафах за совершение административных правонарушений (на портале государственных услуг и сайте ГИБДД), а также информации об их оплате.

На данный момент к ФИС ГИБДД-М уже подключено более 18400 пользователей в 12 регионах Российской Федерации (в том числе Ставропольский край, Нижегородская область, Республика Тыва). Система позволяет еженедельно проводить регистрационные действия с 25 000 транспортных средств и обеспечивает выдачу более 11 700 водительских прав. Кроме того, каждую неделю через систему проходит информация о 162 200 административных правонарушений (в том числе зафиксированных видеокамерами).

Таким образом, существующие на сегодняшний день модули сервиса ФИС ГИБДД-М достаточно разнообразны, что позволяет грамотно и быстро выполнять служебные обязанности сотрудников ГИБДД МВД России.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Семенов Е.Ю. Федеральная информационная система Госавтоинспекции МВД России (ФИС ГИБДД-М) // Наука и практика. 2016. № 3 (68).

2. Приказ МВД России «О порядке эксплуатации специализированного программного обеспечения федеральной информационной системы Госавтоинспекции» от 5 февраля 2016 г. № 60. Документ опубликован не был // СПС «КонсультантПлюс».

3. Федеральный закон «О федеральном бюджете на 2017 год и на плановый период 2018 и 2019 годов» от 19 декабря 2016 г. № 415-ФЗ (ред. от 01.07.2017) // СЗ РФ. 2016. № 52 (ч. V). Ст. 7464.

4. Федеральный закон Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (ред. от 15.02.2016) // СПС «КонсультантПлюс».

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВИДЕОТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

THE FEATURES OF THE TECHNICAL EXAMINATION

Росоха Анастасия Юрьевна
(НИУ «БелГУ»)

Rosokha Anastasia Yuryevna
(NIU «BelSU»)

Аннотация: в работе рассмотрены основания и методы проведения видеотехнической экспертизы в рамках судебного разбирательства.

Ключевые слова: видеозапись, видеоаппаратура, видеотехническая экспертиза.

Abstract: the article is devoted to the grounds and methods of conducting video technical expertise within the framework of the trial.

Key words: video recording, video equipment, video technical expertise.

В настоящее время видеозаписи часто используются в качестве доказательств в ходе разнообразных судебных разбирательств. В таких случаях подлинность записей имеет решающее значение. Для изучения видеоматериалов, установления видеоаппаратуры, на которую производилась запись, определения подлинности видеозаписей и других задач, так или иначе связанных с процессом видеозаписи и его результатами, проводят видеотехническую экспертизу.

В зависимости от поставленных задач, видеотехническая экспертиза осуществляется по четырем основным направлениям:

1. Установление подлинности и аутентичности видеозаписи (выявление признаков монтажа).

Производится для определения фактов произвольного воздействия на запись с целью искажения ее содержимого. Подлинность видеозаписи понимается как отсутствие признаков монтажа или иных воздействий на запись после того, как она была произведена.

Монтаж – мощный прием воздействия на запись, позволяющий исказить ее содержание, а подчас и превратить смысл происходящего в полностью противоположный. Выявление признаков монтажа базируется на основных принципах обработки видеозаписей. Видеомонтаж бывает линейным и нелинейным. Линейный монтаж чаще всего осуществляется в реальном времени, когда видеосигнал поступает сразу из нескольких источников: видеомагнитофонов, камер и т.д. Нелинейный же монтаж уже предполагает наличие какого-то отснятого материала. Этот видеоматериал делится на определенные отрезки, расставляется так, как того требует сюжет (то есть в определенной последовательности), совмещается со звуком (накладываются эффекты и т.д.), а потом все это выводится в один цельный файл.

Под аутентичностью видеозаписи подразумевают полное соответствие ее содержания происходящим событиям. Основными признаками аутентичности видеозаписи считаются следующие показатели: сохранность звукового компонента в процессе хранения видеозаписи и в ходе ее последующего воспроизведения; непрерывность видеозаписи на протяжении всей ее продолжительности; четкость видеозаписи, то есть достаточный уровень качества записи, позволяющий однозначно идентифицировать запечатленные на ней объекты; полнота видеозаписи – отсутствие фрагментов записи, на которых наблюдается существенная потеря изображения или звукового компонента.

2. Установление содержания видеозаписи.

Это один из разделов видеотехнической экспертизы, предназначенный для определения объектов и процессов, запечатленных на записи, и последующего описания выявленных данных посредством вербальных средств. Установление содержания видеозаписи – длительный, трудоемкий процесс, для производства которого требуются специальные знания, а также опыт выполнения подобных процедур. В результате проведения данного вида анализа видеозаписи можно выявить условия, в которых была сделана запись, идентифицировать лица, их действия и дословное содержание их разговоров. Также анализируются и фиксируются все происходящие на записи события – жесты людей, движения людей, животных и предметов, по возможности – особенности мимики и так далее. Установление содержания видеозаписи, кроме расшифровки происходящих процессов, также способствует определению дополнительных свойств записи, как то: наличие следов монтажа, признаков копирования, фальсификации, особенности оборудования, на которое производилась запись. Установление содержания видеозаписи может иметь решающее значение при определении относимости доказательства – в данном случае по результатам экспертизы определяют, является ли искомая видеозапись доказательством по данному делу, то есть будет ли она входить в доказательную базу одной из сторон. Также данное исследование способствует определению подлинности записи.

3. Идентификация видеозаписывающего устройства.

Это один из видов видеотехнической экспертизы, предназначенный для определения характерных особенностей устройства (или устройств), на котором производилась видеозапись, а также для ответа на вопрос, была ли осуществлена исследуемая видеозапись на данном конкретном устройстве. Этот

вид анализа позволяет определить общее количество использованных в процессе записи устройств – была ли запись произведена на одном устройстве, или было задействовано несколько устройств. Ответы на подобные вопросы имеют большое значение при определении следов монтажа или иного преднамеренного искажения (фальсификации) записи. Установление устройства, на котором была сделана та или иная запись, используется для идентификации самой записи, доказательства ее подлинности, соответствия событиям, о которых идет речь в ходе судебных разбирательств, и так далее.

Идентификация видеозаписывающего устройства производится по характерным особенностям самого устройства, которые непосредственным образом отражаются на свойствах полученных видеоматериалов. На сегодняшний день видеозапись выполняется на традиционных (аналоговых) устройствах, цифровых устройствах, а также на записывающих механизмах гибридного типа.

4. Установление соответствия или несоответствия звукоряда видеоряду.

Относится к роду сложных комплексных экспертиз. Данное исследование сочетает в себе мероприятия фоноскопической и видеотехнической экспертиз. Видеофонограмма является записью одновременно видеоинформации и звуковой дорожки. Установление соответствия или несоответствия звукоряда видеоряду сопоставляет изображение и звуковую дорожку, определяет совпадение событий, отображенных на видео, и звуков, которыми эти события сопровождаются. Подобный анализ в большинстве случаев производится для определения подлинности записи, установления признаков позднего внесения изменений, фактов фальсификации, а также наложения звука поверх записанного видео с целью скрыть фальсификацию записи. Для установления соответствия звуковой записи и видео проводится установление содержания видеозаписи и фонограммы, а затем проводится хронологическое сравнение этих двух документов.

Под звукорядом принято понимать определенную последовательность фонетических единиц, записанных на том или ином носителе. Задача эксперта – максимально подробно воспроизвести на бумаге (или в формате электронного текстового документа) это самое чередование звуков. Записи подлежит не только речь, но также и все звуки, которые специалист может идентифицировать. Звуки, природу которых не удается определить при прослушивании, заносятся в документ как звуки невыясненной природы с указанием характеристик, продолжительности звучания и очередности появления в течение звукоряда. Под видеорядом понимают последовательность кадров, содержащих визуальные образы. Экспертом описывается содержимое кадра и все события, которые осуществляются в кадре. То есть эксперт подробно описывает, что происходит в записи, смену места съемки, движение, лица, их речь и действия.

После завершения работ специалист приступает к формированию экспертного заключения – основного документа, имеющего доказательную силу в суде. В заключение вносятся все изученные материалы по делу (копии), описание всех выполненных процедур с указанием полученного результата. Также в заключение вносятся ответы на включенные в договор вопросы. Если специалист считает необходимым, он вносит в бумаги свои рекомендации или комментарии относительно своего исследования.

Таким образом, видеотехническая экспертиза решает следующие задачи:

1. Определение режима и формата записи, а также системы цветопередачи исследуемых материалов.

2. Установление фактов видеомонтажа и иных способов изменения записей. Определение типа монтажа.

3. Определение оригинальности исследуемой видеозаписи (является ли она оригиналом или копией).

4. Установление номера копии видеозаписи.

5. Определение устройства, на которое производилась анализируемая запись.

6. Установление характерных признаков несоответствия записей, находящихся на различных носителях.

7. Установление соответствия записи предоставленным для анализа записывающим устройствам.

8. Исследование объектов, находящихся в кадре, и определение их параметров.

СЕКЦИЯ № 2.
ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОПИСАНИЕ ДУАЛЬНОГО ПОДХОДА УПРАВЛЕНИЯ ОХРАННЫМИ ОРГАНИЗАЦИЯМИ

DESCRIPTION OF THE DUAL APPROACH OF MANAGEMENT OF SECURITY ORGANIZATIONS

Сумин Виктор Иванович,
Исаев Олег Викторович,
Душкин Александр Викторович,
Кочедыков Сергей Сергеевич,
Иванов Сергей Владимирович
(Воронежский институт ФСИН России)

Sumin Viktor Ivanovich,
Isaev Oleg Victorovich,
Dushkin Alexander Viktorovich,
Kochedykov Sergey Sergeevich,
Ivanov Sergey Vladimirovich
(Voronezh Institute of the Russian Federal Penitentiary Service)

Аннотация: в данной статье рассматривается проблема разработки дуального подхода управления охранными организациями. Определяется функционирование охранных организаций. Формируется концепция разработки охранных организаций с определением целей и задач этой организации.

Ключевые слова: охранные организации, информационные технологии, охраняемые объекты, концепция разработки охранных систем.

Annotation: this article deals with the problem of developing a dual approach to managing security organizations. The functioning of security organizations is determined. A concept for the development of security organizations is formed with the definition of the goals and objectives of this organization.

Key words: security organizations, information technology, protected objects, the concept of developing security systems.

В настоящее время человечество приступило к практической реализации задачи перевода информационных процессов в охранных организациях (ОО) на новые информационные технологии (ИТ) преимущественно на безбумажной основе. Однако разработка систем управления (СУ) ОО, как и в других отраслях человеческой деятельности, имеет целый ряд сложных проблем, решение которых является обязательным условием эффективного функционирования этих систем. Для эффективной разработки СУОО, как и для любой большой системы, необходимо создать научно-методологическую базу. Такой поход до настоящего времени не разработан, и эти работы ПО осуществляются стихийно и не на высоком научном уровне. Все это ведет к дополнительным расходам из-за совершенных краж из охраняемых объектов.

Формирование научно-методологической базы сопряжено со значительными трудностями как общего процесса функционирования системы охраны, так и специфики, обусловленной особенностями проблемы. Характерной особенностью является повышение подверженности процессов функционирования охранных систем (ОС) влиянию случайных факторов (например, отказы, сбои и ошибки работы охранно-пожарной организации (ОПС) или сотрудников подразделений ОО) и прежде всего таких, как злоумышленные действия преступников, которые являются не только случайными, но и вообще непредсказуемыми или в лучшем случае трудно предсказуемыми.

В связи с этим методы моделирования, разработанные в рамках традиционной теории систем, не позволяют адекватно описывать процессы ОС и осуществлять повышение эффективности их функционирования. Необходимо расширить использование традиционных методов на основе методологии проектирования организационных и технических подсистем, причинного анализа и т.д. Поэтому проблема проектирования и повышения эффективности функционирования ОС должна быть комплексной и решаться в рамках единой концепции и т.д.

Все вышеизложенное подводит к выводу: для эффективного решения этой проблемы необходима не просто научно-методологическая база, а обоснованная теория проектирования и управления ОС.

Для разработки общий теории проектирования и управления ОС осуществим общий анализ этой проблемы.

Определение 1. Под функционированием ОС понимается регулярное использование средств и методов, принятие мер и осуществление мероприятий для обеспечения требуемой эффективности и надежности охраны материальных ценностей на охраняемых объектах.

Требуемая эффективность и надежность охраны материальных ценностей на охраняемых объектах (ОО) может быть обеспечена за счет целенаправленного управления подразделениями ОО по основным направлениям функционирования ОО:

– осуществление охраны имущества собственника;

– систематизация и совершенствование охраны материальных ценностей;

– приведение функционирования ОО к единой технической политике.

Цели функционирования ОО и определили задачи.

Основными задачами функционирования ОО являются:

– осуществление охраны имущества собственников на основе договора;

– реализация мер по упорядочению и совершенствованию охраны материальных ценностей;

– приведение функционирования ОО к единой технической политике в области разработки средств охранных систем, контроля за качеством, повышения тактики использования ОС, внедрения и эксплуатационного обслуживания.

Основное направление функционирования ОО и определяет цели ОО (см. рис. 1).



Рис. 1. Цели функционирования ОО.

Основные задачи функционирования ОО и определяют их функциональный аспект (предмет).

Определение 2. Предметом функционирования ОО является охрана имущества собственников, участие в разработках и реализации мер по упорядочению и совершенствованию охраны материальных ценностей и проведению единой технической политики.

Структура функционирования ОО определяет его предмет и разбивается на предмет функционирования ОО управления субъекта федерации и районного отдела.

Предметом функционирования ОО управления субъекта федерации являются стандартные функции управляющего субъекта организационной системы, поэтому детально не рассматриваются.

В отличие от управления субъекта федерации, функционирование районного отдела необходимо рассмотреть более детально.

Структура функционирование районного отдела представлена на рис. 2 (см. рис. 2).

Предмет функционирования районного отдела разбивается на два основных направления: охрану объектов всех форм собственности, а также предоставление услуг и проведение различных работ с элементами системы охраны.

ОО структурно представляют из себя помещения, здания с прилегающей территорией, автотранспорт, охраняемые отдельные строения (коттеджи и гаражи). Работы с системами охраны представляют следующее: установка, ремонт, техническое обслуживание, поставка тревожной сигнализации. Предоставляемые услуги – это перевозка ценностей на автотранспорте, борьба с хищениями, контроль за несением службы, дополнительные услуги.

Управленческое звено районного отдела выполняет функции, аналогичные функциям сотрудников управления субъекта федерации.

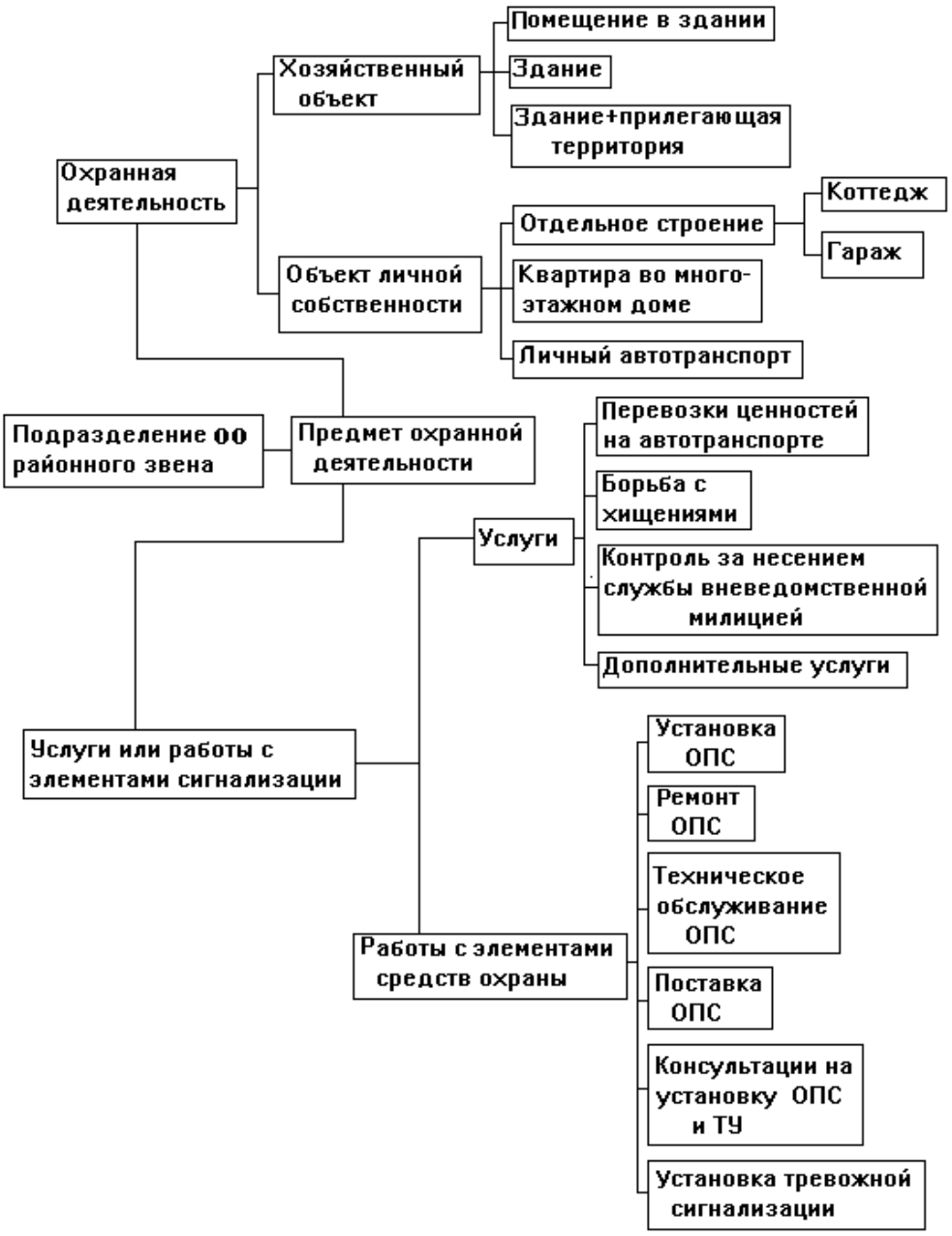


Рис. 2. Структура функционирования районного отдела.

Ранее при разработке больших систем использовался позадачный подход и такой подход необходимо коренным образом изменить. Необходимо объединить на системном уровне управление и автоматизированную обработку информации в ОС на основе дуального подхода. Это позволит создать интегрированную технологию автоматизированного управления, в которой средства и методы управления используются сотрудниками ОО в повседневной деятельности, а не для решения отдельных задач.

В наше время сильно возрастает уязвимость информации от различных дестабилизирующих факторов. Так как в настоящее время снижена надежность информации, защита информации объективно приобретает характер задачи повышенной актуальности.

Основу методологии формирования ОС составляет дуальный подход.

Сущность дуального подхода при разработке ОС заключается в трех теоретических посылках:

1) системном анализе исследуемой или разрабатываемой проблемы;

2) разработке полной и непротиворечивой концепции решения проблемы;

3) системном анализе методов моделирования.

Такой подход к проектированию ОС позволит:

– проводить разработку ОС с единой методологической позиции;

– системно решать все вопросы разработки ОС;

– осуществить непрерывную работу по модернизации и совершенствованию ОС;

– обеспечить единство в организации работы по управлению подразделениями ОО;

– определить единую концепцию разработки ОС.

Для разработки эффективной ОС должна быть создана регулярная система, одним из главных признаков должно являться наличие управления. Причем в основу регулярности ОС должен быть положен принцип дуального управления.

Проведем обоснование структуры и содержания дуального подхода.

Структура функционирования районного отдела представлена на рис. 3:



Рис. 3. Структура функционирования районного отдела.

Определение 3. Под дуальным подходом будем понимать все множество взглядов, положений и решений, необходимых и достаточных для решения всех задач и проблем разработки и повышения эффективности функционирования ОС.

Исходя из общетеоретических и отраслевых требований, систему требований к формированию дуального подхода управления и разработки ОС можно представить в виде общетеоретических, прикладных и отраслевых требований.

Система общетеоретических требований представляется в виде: полнота; непротиворечивость; стройность. Система прикладных требований: унифицированность; реализуемость; перспективность.

Общее содержание посылок приведено на рис. 4:

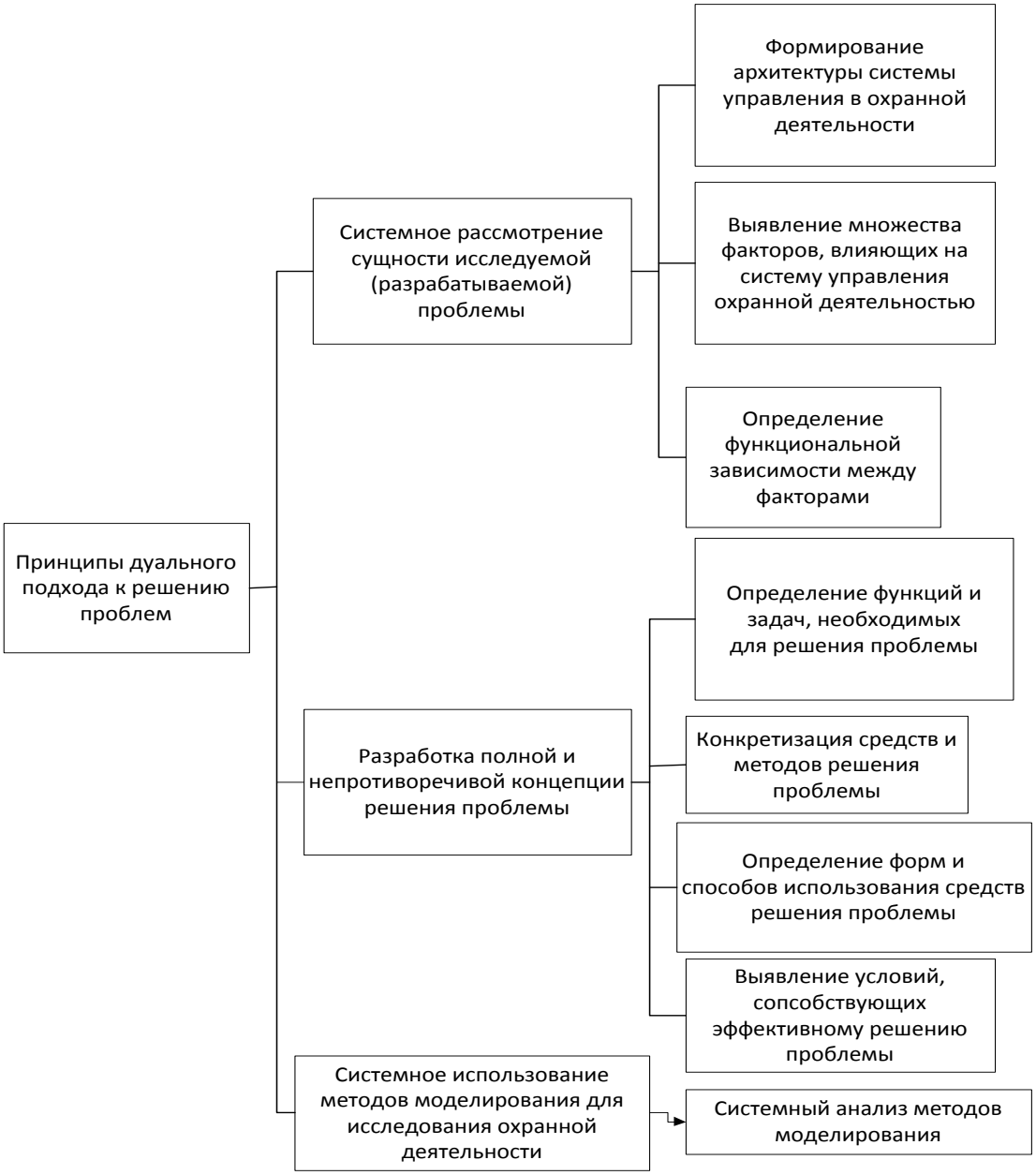


Рис. 4. Классификация принципов дуального подхода по управлению и разработке ОС.

Структура дуального подхода приведена на рис. 5.

На основе системного анализа базисных концепций и целей ОС должны быть определены объекты и элементы ОС и с учетом этого определена система факторов, влияющих на функционирование ОС.

Элементами разработки ОС являются функции, задачи и средства ОС. Эти элементы определяются следующим образом:

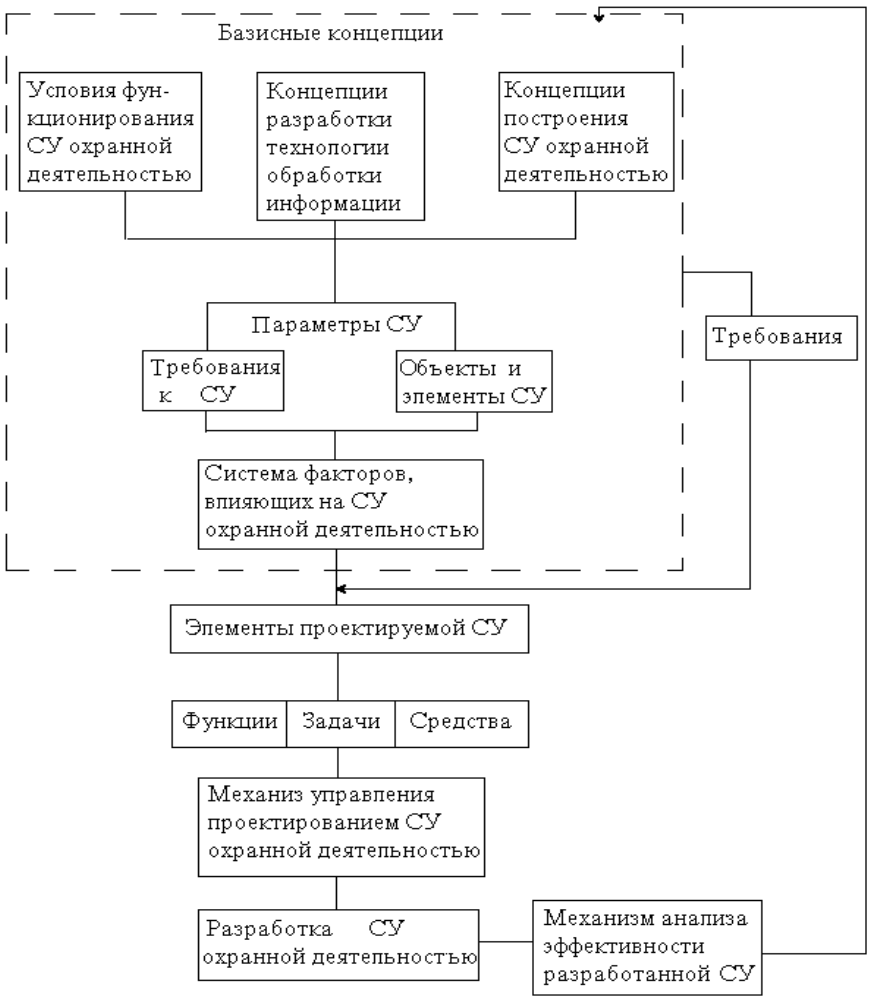


Рис. 5. Структура дуального подхода разработки и управления ОС.

Определение 4. Функции ОС – это совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в ОС с целью создания, поддержания и обеспечения условий, объективно необходимых для эффективного функционирования ОС.

Определение 5. Задачи ОС – это организованные возможности средств, методов и мероприятий, реализуемых в ОС с целью реализации функций ОС.

Определение 6. Средства ОС – это устройства, программы и мероприятия, предназначенные для решения в ОС задач ОС.

Перечисленные элементы дуального подхода определяют необходимую последовательность решений, реализация которых и создает реальную основу для эффективного функционирования ОС.

Объекты и элементы ОС. Функционирование ОС может быть эффективным только в том случае, если это функционирование будет надежным на всех объектах и во всех элементах системы. Следовательно, необходимо иметь однозначное и полное определение перечня объектов и элементов с целью организации управленческого цикла.

Определение 7. Объект ОС – это структурный компонент, в котором находится информация, подлежащая обработке.

Объект ОС должен отвечать следующим условиям:

– принадлежность к одному и тому же компоненту ОС;

– осуществление одних и тех же функций.

Такой объект будем называть типовым структурным объектом.

Под элементом ОС будем понимать находящуюся в ОС совокупность данных и процедур обработки. Элементы ОС выделяются по следующим условиям:

– нахождение в одном и том же объекте ОС;

– локализируемость с точки зрения носителя информации и процедуры ее обработки;

– однородность в смысле воздействия факторов, влияющих на ОС.

Одним из основных методологических принципов, гарантирующих соблюдение требований дуального подхода, является принцип типизации, модульности, необходимых и достаточных для решения всех задач, возникающих в процессе исследования различных аспектов проблемы разработки ОС. Другой принцип – системное использование методов моделирования для анализа ОС, который должен обеспечить рациональный выбор методов решения задач, возникающих при исследованиях и разработках ОС.

Принцип системного рассмотрения сущности исследуемой (разрабатываемой) проблемы на основе анализа рассматриваемых проблем можно представить как системную классификацию существенно значимых особенностей (см. рис. 6).

Соблюдение принципа системного использования методов разработки ОС требует более детального рассмотрения.

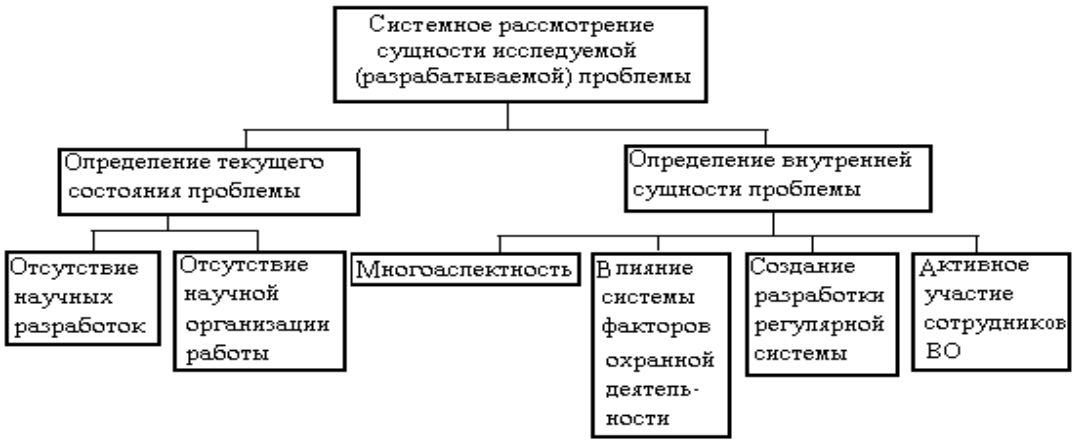


Рис. 6. Системная классификация системного рассмотрения сущности исследования (разработки) проблемы ОС.

РАЗРАБОТКА ДИНАМИЧЕСКИХ МОДЕЛЕЙ ПРОЦЕССОВ ПРИНЯТИЯ ДИАГНОСТИЧЕСКИХ РЕШЕНИЙ О РАБОТОСПОСОБНОСТИ ПРОГРАММНЫХ КОМПОНЕНТОВ АВТОМАТИЗИРОВАННЫХ УПРАВЛЯЮЩИХ СИСТЕМ КРИТИЧЕСКОГО НАЗНАЧЕНИЯ

DEVELOPMENT OF DYNAMIC MODELS OF DIAGNOSTIC DECISION-MAKING PROCESSES ON THE OPERABILITY OF SOFTWARE COMPONENTS OF AUTOMATED CONTROL SYSTEMS OF CRITICAL PURPOSE

Кочедыков Сергей Сергеевич,
Душкин Александр Викторович,
Сумин Виктор Иванович,
Иванов Сергей Владимирович
(Воронежский институт ФСИН России)

Kochedykov Sergey Sergeevich,
Dushkin Alexander Viktorovich,
Sumin Viktor Ivanovich,
Ivanov Sergey Vladimirovich
(Voronezh institute of the Russian Federal Penitentiary Service)

Аннотация: в данной работе предлагается комплекс динамических моделей процессов принятия диагностических решений о работоспособности программных компонентов исполнительных устройств автоматизированной системы управления, описываемых сетью Петри-Маркова, который позволяет предложить методику принятия диагностических решений, определить показатель функциональности диагностических решений, выяснить уровень работоспособности и получить диагностическое заключение, а также оценить риски работоспособности с учетом факторов риска, исправности компонентов и перечня ассоциированных неисправностей автоматизированной системы управления.

Ключевые слова: автоматизированная система управления, исполнительное устройство, диагностика, конфликт, процесс управления, ресурс, математическая модель.

Annotation: In this paper, a complex of dynamic models for the processes of making diagnostic decisions about the operability of software components of executive devices of an automated control system described by the Petri-Markov network is proposed. Which allows to propose a method for making diagnostic decisions, to determine the diagnostic functionality, to determine the level of efficiency and to receive a diagnostic conclusion, and to assess the risks of working capacity, taking into account the risk factors, component health and the list of associated faults of the automated control system.

Key words: automated control system, executive device, diagnostics, conflict, management process, resource, mathematical model.

На основе результатов построения алгоритма диагностирования работоспособности программных компонентов (ПК) программного обеспечения (ПО) АСУ, применяя технологию IDEF, строится динамическая модель (ДМ).

Целью создания ДМ является описание причинно-следственных связей между АСУ во времени и пространстве.

Моделирование динамики функционирования АСУ отражается сетью Петри-Маркова [1, 2], задаваемой структурно-параметрической парой

$$M_d = \{\Psi, \Omega\}. \quad (1)$$

Сеть Петри Ψ определяет структуру процесса диагностики

$$Z, \quad (2)$$

где A – конечное множество позиций; Z – конечное множество переходов; I – конечное множество входов системы; O – конечное множество выходов системы.

Случайный процесс Ω определяет вероятностные характеристики процесса диагностики ПО:

$$\Omega = \{P, f(p), \Lambda\}, \quad (3)$$

где P – матрица вероятностей; $f(p)$ – матрица функции распределения вероятностей; Λ – матрица логических условий:

$$\lambda_i(a,z) = \begin{cases} \{0,1\}, если\ O(Z_i) \cap a_i = a_i \\ 0, если\ O(Z_i) \cap a_i = \varnothing. \end{cases}; \quad (4)$$

На рисунке 1 представлен алгоритм диагностики ПО и оценки рисков работоспособности системы [2], отражающий моделирование динамики функционирования системы (см. рис. 1).

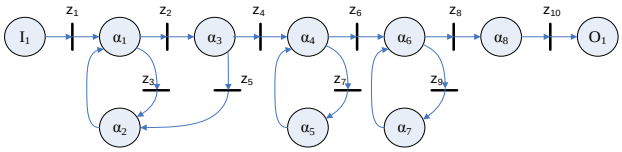


Рис. 1. Динамическая модель принятия диагностических решений.

Вершины графа отражают этапы диагностического процесса:

a_1 – получение диагностических данных;

a_2 – дополнительные тесты;

a_3 – определение функциональных диагностических показателей;

a_4 – формирование паттерна данных;

a_5 – применение альтернативного метода формирования паттерна данных;

a_6 – классификация состояния ПО АСУ;

a_7 – применение альтернативного метода классификации состояния ПО АСУ;

a_8 – интерпретация результатов классификации.

Получение диагностических данных α_1 производится в процессе прохождения АСУ диагностических тестов, подробно описанных в алгоритме процесса диагностики ПО. Переход z_1 определяет инициализацию процесса диагностики, когда на вход системы поступает входная информация I_1. Переходы z_2 и z_3

моделируют условие проверки корректности и целостности данных на этом этапе. Они срабатывают асинхронно, то есть если не срабатывает переход z_2 (данные не удовлетворяют требованиям корректности), то срабатывает переход z_3, переводя систему в режим сбора информации во время выполнения дополнительных диагностических тестов a_2.

На основании полученных данных производится определение функциональных диагностических показателей a_3 – уровня ПО, определение неработающих компонентов. Далее диагностический процесс распараллеливается на определение стадии нарушения работоспособности ПО и определение уровня работоспособности. Поскольку алгоритмы обработки данных и принятия решения на этих этапах идентичны, на рисунке 1 они представлены как единая ветвь анализа. Функциональные диагностические показатели являются определяющими для всего диагностического процесса, следовательно, проверка условия корректности и целостности данных на этом этапе крайне важна и моделируется асинхронными переходами z_4 и z_5. Если данные корректны и получены в необходимом объеме, то срабатывает переход z_4, иначе срабатывает переход z_5, возвращая систему на шаг a_2.

Для снижения размерности информационного множества, необходимого для принятия диагностического решения, формируется паттерн данных a_4 на основе определения информативности диагностических показателей. На этом шаге моделируется условие корректности паттерна данных асинхронными переходами z_6 и z_7. Если паттерн включает в себя наиболее информативные показатели, то срабатывает переход z_6, иначе необходимо применить другой метод формирования паттерна данных a_5 и срабатывает переход z_7.

На следующем шаге производится классификация состояния a_6, то есть сопоставление множества оценок диагностических показателей $\{S\}$ определенному множеству результатов диагностических состояний $\{D\}$ – неисправностей. Здесь проверяется условие корректности классификации с помощью асинхронных переходов z_8 и z_9. Если результаты классификации верны, то срабатывает переход z_8, иначе, срабатывает переход z_9 и применяется другой метод классификации.

Срабатывание перехода z_{10} позволяет интерпретировать результаты классификации a_8 и получить на выходе диагностическое заключение O_1, включающее в себя выводы о стадии и степени работоспособности и оценку риска.

Матрица вероятностей переходов динамической модели имеет вид:

$$P = \begin{pmatrix} p_{01} & p_{12} & p_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & p_{34} & p_{35} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & p_{46} & p_{47} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{68} & p_{69} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{810} \end{pmatrix}. \qquad (5)$$

Строки матрицы характеризуются вершинами графа (a_1, …, a_8), а столбцы матрицы отражают переходы (z_1, …, z_{10}). Очевидно, что при получении входной информации I_1 переход z_1 сработает с вероятностью $p_{i1}=1$. Поскольку переходы z_2 и z_3 асинхронные, то очевидно, что

$$p_{13}=1-p_{12}. \qquad (6)$$

Аналогичное правило действует и для асинхронных переходов z_4, z_5; z_6, z_7; и z_8, z_9:

$$p_{35}=1-p_{34};$$

$$p_{47}=1-p_{46};$$

$$p_{69}=1-p_{68}.$$

Условие достижимости вершин цепи:

$$\sum_{ij} p_{ij} > 0 \qquad (7)$$

выполняется за счет введения обратных связей на каждом шаге выполнения условий переходов. Таким образом, сумма вероятностей переходов по столбцам матрицы всегда отлична от нуля. Последовательное срабатывание переходов отражает принцип функционирования системы и позволяет получать на выходе диагностические оценки состояния ПО.

Полученная динамическая модель является основой обобщенного алгоритма классификации сложных объектов управления.

Логику принятия решений на различных этапах диагностического процесса можно так же представить в виде цепи Маркова.

На рисунке 2 представлена логика принятия решений для определения степени работоспособности ПО (см. рис. 2).

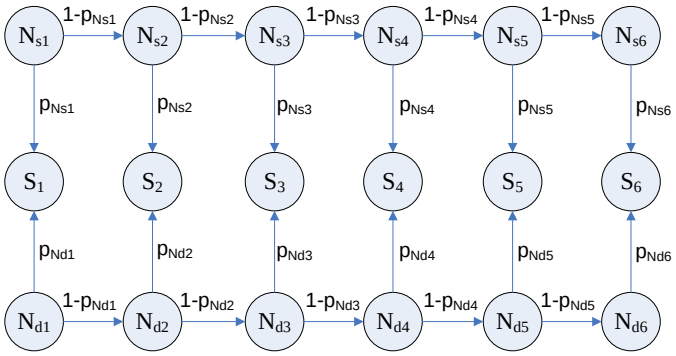


Рис. 2. Ориентированный граф определения степени работоспособности ПО.

Для определения степени работоспособности ПО измеряется состояние работоспособности каждого компонента и последовательно проверяется условие перехода N к следующей степени S:

Ns_1 – уровень отказа компонента минимальный, когда время выполнения f-ой функции i-го компонента $t_f^i \le min(t_f^i)$;

Ns_2 – уровень отказа компонента выше минимального;

Ns_3 – уровень отказа компонента средний;

Ns_4 – уровень отказа компонента выше среднего;

Ns_5 – уровень отказа компонента высокий;

$Ns_{6\,6}$ – уровень максимальный, когда время выполнения f-ой функции i-го компонента $t_f^i \geq max(t_f^i)$;

N_{d1} – неисправность компонента устраняется автоматически в процессе функционирования за незначительный промежуток времени;

N_{d2} – неисправность компонента устраняется автоматически в процессе функционирования за достаточный промежуток времени;

N_{d3} – неисправность компонента устраняется автоматически в процессе функционирования за некритичный промежуток времени;

N_{d4} – неисправность компонента устраняется автоматически в процессе функционирования за значительный промежуток времени;

N_{d5} – неисправность компонента устраняется автоматически с помощью замены его на резервный или устраняется автоматически в процессе функционирования за недостаточный промежуток времени, требующий выполнения дополнительной функции;

N_{d6} – неисправность компонента не устраняется автоматически в процессе функционирования, требуется полная замена за критичный промежуток времени.

Таким образом, вероятности диагностирования степени работоспособности соответственно равны:

$$\begin{aligned} p_{S1} &= p_{Ns1} + p_{Nd1}; \\ p_{S2} &= p_{Ns2} + p_{Nd2}; \\ p_{S3} &= p_{Ns3} + p_{Nd3}; \\ p_{S4} &= p_{Ns4} + p_{Nd4}; \\ p_{S5} &= p_{Ns5} + p_{Nd5}; \\ p_{S6} &= p_{Ns6} + p_{Nd6}. \end{aligned} \qquad (8)$$

где p_{S1} – вероятность определения оптимального уровня работоспособности;

p_{S2} – вероятность определения нормального уровня работоспособности;

p_{S3} – вероятность определения высокого нормального уровня работоспособности;

p_{S4} – вероятность определения степени 1 неработоспособности;

p_{S5} – вероятность определения степени 2 неработоспособности;

p_{S6} – вероятность определения степени 3 неработоспособности;

Логике принятия решения на этапе определения стадии работоспособности соответствует ориентированный граф на рисунке 3.

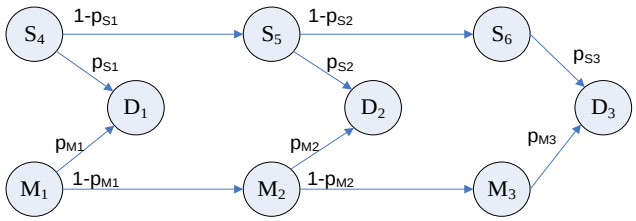


Рис. 3. Ориентированный граф определения диагностических результатов работоспособности ПО.

Стадия работоспособности ПО является интегральным диагностическим показателем, который зависит от степени работоспособности ПО S и степени поражения компонентов-мишеней M. Поскольку степени $S_1 - S_3$ соответствуют условно нормальному уровню работоспособности ИУ, для них степень работоспособности ПО и оценка рисков работоспособности ИУ не диагностируются. Степень поражения компонентов-мишеней стратифицируется на три уровня в соответствии с методикой [1]:

M_1 – функции компонентов ПО не нарушены или нарушены незначительно;

M_2 – функции компонентов ПО умерено нарушены;

M_3 – функции компонентов ПО нарушены значительно.

Таким образом, вероятности диагностирования степени работоспособности ИУ соответственно равны:

$$\begin{aligned} p_{D1} &= p_{S4} + p_{M1}; \\ p_{D2} &= p_{S5} + p_{M2}; \\ p_{D3} &= p_{S6} + p_{M3}. \end{aligned} \qquad (9)$$

где p_{D1} – вероятность I стадии нарушения работоспособности ПО;

p_{D2} – вероятность II стадии нарушения работоспособности ПО;

p_{D3} – вероятность III стадии нарушения работоспособности ПО.

На рисунке 4 приведена логика принятия решения на этапе определения уровня риска работоспособности ПО. В соответствии с методикой [2] риск определяется в зависимости от степени работоспособности ИУ и наличия факторов риска F, поражения компонентов-мишеней M и ассоциированных неисправностей A ПО АСУ.

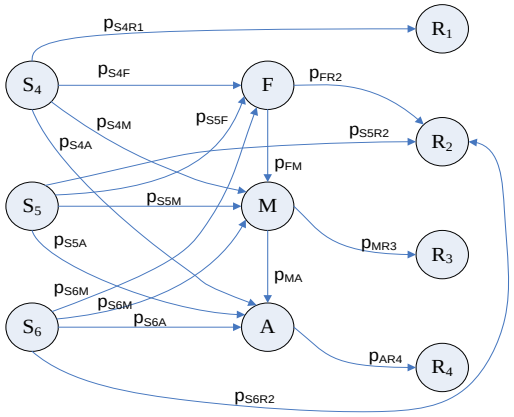


Рис. 4. Ориентированный граф определения риска работоспособности ПО.

Таким образом, вероятности определения уровня риска работоспособности ПО соответственно равны:

$$\begin{aligned} p_{R1} &= p_{S4R1}; \\ p_{R2} &= p_{S5R2} = p_{S6R2} = p_{S4F} + p_{FR2} = p_{S5F} + p_{FR2} = p_{S6F} + p_{FR2}; \\ p_{R3} &= p_{FM} + p_{MR3} = p_{S4M} + p_{MR3} = p_{S5M} + p_{MR3} = p_{S6M} + p_{MR3}; \\ p_{R4} &= p_{MA} + p_{AR4} = p_{S4A} + p_{AR4} = p_{S5A} + p_{AR4} = p_{S6A} + p_{AR4}. \end{aligned} \qquad (10)$$

где p_{R1} – вероятность определения риска 1;

p_{R2} – вероятность определения риска 2;

p_{R3} – вероятность определения риска 3;

p_{R4} – вероятность определения риска 4.

Разработанный комплекс динамических моделей отражает логику функционирования и взаимодействия подсистем диагностирования АСУ КВО для диагностики работоспособности ПО. Полученные вероятностные оценки применяются для определения априорных вероятностей диагностических оценок.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Поляничко М.А. Методика автоматизированного обнаружения конфликтов в комплексе программных средств защиты информации компьютерной системы: дис. ... канд. тех. наук. – СПб: Санкт-Петерб. гос. ун-т путей сообщ., 2013. – 135 с.

2. Управление конфликтами: учебное пособие для вузов / В.П. Балан, А.В. Душкин, В.И. Новосельцев и др. – М.: Горячая линия – Телеком, 2015. – 144 с.

3. Новосельцев В.И., Тарасов Б.В. и др. Логико-лингвистические модели в военных системных исследованиях. – М.: Воениздат, 1988. – 280 с.

АНАЛИЗ ОЦЕНКИ УПРАВЛЯЮЩИХ ВОЗДЕЙСТВИЙ НА ОСНОВЕ АЛГОРИТМА ДИНАМИКИ ХАРАКТЕРИСТИК ОБЪЕКТОВ УПРАВЛЕНИЯ

ANALYSIS OF THE ESTIMATION OF CONTROL ACTIONS BASED ON THE ALGORITHM FOR THE DYNAMICS OF THE CHARACTERISTICS OF CONTROL OBJECTS

Сумин Виктор Иванович
(Воронежский институт ФСИН России);
Смоленцева Татьяна Евгеньевна
(Липецкий государственный технический университет)

Sumin Viktor Ivanovich
(Voronezh institute of the Russian Federal penitentiary service);
Smolentseva Tatyana Evgenevna
(Lipetsk State technical University)

Аннотация: в статье рассмотрен процесс анализа характеристик, оказывающих влияние на функционирование иерархической многоуровневой организационной системы; сформированы алгоритмы оценки управляющих воздействий и прогнозирования характеристик объектов организационной системы.

Ключевые слова: организационная система, управление качеством обучения, максимум функционала.

Annotation: the process of analyzing the characteristics that affect the functioning of the hierarchical multi-level organizational system is considered. An algorithm for estimating control actions and an algorithm for predicting the characteristics of objects of the organizational system are generated.

Key words: organizational system, quality management of training, maximum functional.

Анализ оценки принятых управляющих решений направлен на повышение эффективности функционирования иерархической многоуровневой организационной системы (ИМОС).

Оценка может позволить проводить анализ принятых управленческих решений за определенный промежуток времени и сформировать вывод об эффективности принятых управленческих решений и, в случае необходимости, исследовать причины, по которым они неэффективны.

Анализ данных оценок базируется на сравнении полученных оценок за анализируемый период времени. Если результаты принятых управленческих решений не ухудшились, тогда принятые управленческие решения принимались эффективно, и наоборот.

Для сравнения результатов принятых управленческих решений и последующего анализа данных за прошлый и текущий периоды требуется разбить вначале их на группы, схожие по назначениям характеристик, и оценить их групповые характеристики, что значительно снизит размерность рассматриваемой задачи [3, с. 25].

Объединение групп объектов организационной системы, сформированных на основе выявления схожих характеристик с использованием значений параметров за уже имеющиеся временные интервалы, позволяет провести оценку эффективности принятых управляющих воздействий.

Данную информацию, находящуюся в системе управления качеством обучения (УКО), можно представить в виде множества, включающего: количественное значение характеристик, индексы объектов управления, а также идентификационные данные рассматриваемого объекта.

В результате рассмотрения данного множества получим точность разбиения в процентах и количество классов разбиения.

В процессе формирования групп объектов за текущий, т.е. исследуемый период, по соответствующим значениям их характеристик получаем индексы значений объектов управления и их количественное значение [4, с. 4; 5, с. 119].

Алгоритм оценки управляющих воздействий объектов многоуровневой организационной системы позволяет проводить анализ рассматриваемых характеристик, определять закономерности в изменении значений в определенный временной период и спрогнозировать их возможные значения, считая, что алгоритм принятия управленческих решений останется неизменным.

По результатам прогноза возможна корректировка действий на этапе принятия управленческих решений.

На данном этапе в организационной системе существуют характеристики, которые необходимо анализировать в процессе их изменения.

Значения этих характеристик будут образовывать временной ряд.

Функционирование ИМОС возможно описывать временными рядами, которые представляются в виде дискретной последовательности наблюдений, осуществляемых через определенные промежутки времени.

Описанные временные ряды [3, с. 65] позволяют разрабатывать модели, обладающие максимальной простотой и минимальным числом параметров, а также адекватно описывать ИМОС.

После определения класса моделей идет процесс разработки конкретной модели, который заключается в установлении адекватности выбранного класса авторегрессией проинтегрированного скользящего среднего (АРПСС) с использованием данных исследуемой предметной области [1, с. 124].

Способ диагностических проверок применим для определения адекватности выбранной модели и необходимых изменений, а также возможно произвести несколько итеративных циклов идентификации.

В качестве временного интервала выбирается календарный период, который является значением временного интервала регрессии. Значения характеристик для любого интервала усредняются по каждой характеристике, которые в дальнейшем объединяются в интегрированное значение [2, с. 34].

В результате этого образуется временной ряд по каждому объекту ИМОС. На базе этого ряда разрабатывается его вероятностная модель для формирования оптимального прогноза с последующей корректировкой.

Рассмотрим множество *V*-элементов ИМОС. Для него справедливы условия: для всех $v \in V v_1 \le v_2$; если $v_1 \le v_2$, $v_2 \le v_3$, где $v_1, v_2, v_3 \in V$, тогда $v_1 \le v_3$; и, наконец, если одновременно $v_1 \le v_2$, $v_2 \le v_3$, то $v_1 = v_2$.

Введем на множестве *V* вещественную векторную функцию:

$$\sigma(v)=(\sigma_1(v), \sigma_2(v), \ldots, \sigma_n(v)), \qquad (1)$$

где $\sigma_k(v)$ – степень соответствия объекта *v* классу V_k, $k=1, \ldots, n$.

Максимум функционала определяется выражением:

$$H(Q)=\sum_{k=1}^{n}\sum_{v\in V_k}\sigma_k(v). \qquad (2)$$

Для множества $I^n(V)$ определим произвольное разбиение $\sigma^\gamma \in I^n(V)$ и введем следующие выражения:

$$\sigma^\gamma=\left(V_1^\gamma, V_2^\gamma, \ldots, V_n^\gamma\right); \ \bar{v}_k^\gamma = V \setminus V_1^\gamma \setminus \ldots \setminus V_k^\gamma; \ w^\gamma(v)=\sigma_i(v), \text{где } i \text{ таково, что } v \in V_i^\gamma.$$

Подставляя в (2) $w^\gamma(v) = \sigma_i(v)$, где *i* таково, что $v \in V^\gamma_i$, получим:

$$H\left(\sigma^\gamma\right)=\sum w^\gamma(v) \qquad (3)$$

Определим во множестве $I^n(V)$ отношение порядка:

$\sigma^1 \le \sigma^2$, где $\sigma^1, \sigma^2 \in I^n(V)$, если для $k=1, 2, \ldots, n-1$ $\quad \overline{V_k^1} \in \overline{V_k^2}$.

Очевидно, что для всякого подмножества разбиений $I \in I^n(V)$ определяется точная верхняя (*maxI*) и точная нижняя (*minI*) границы. Пусть $\sigma_1 = minI$, $\sigma_2 = maxI$, тогда

$$\overline{V_k^1} = \bigcap_{\sigma\in I}\overline{V_k}, \ \overline{V_k^2} = \bigcap_{\sigma\in I}\overline{V_k} \qquad (4)$$

$$\bigcap_{\sigma\in I}\overline{V_k} \subseteq \overline{V_k^{\lambda}} \subseteq \bigcup_{\sigma\in I}\overline{V_k},\ \ \lambda = 1,\ 2. \qquad (5)$$

Рассмотренное множество элементов ИМОС позволяет сформировать структуру алгоритма прогнозирования характеристик объектов ИМОС (см. рис. 1).

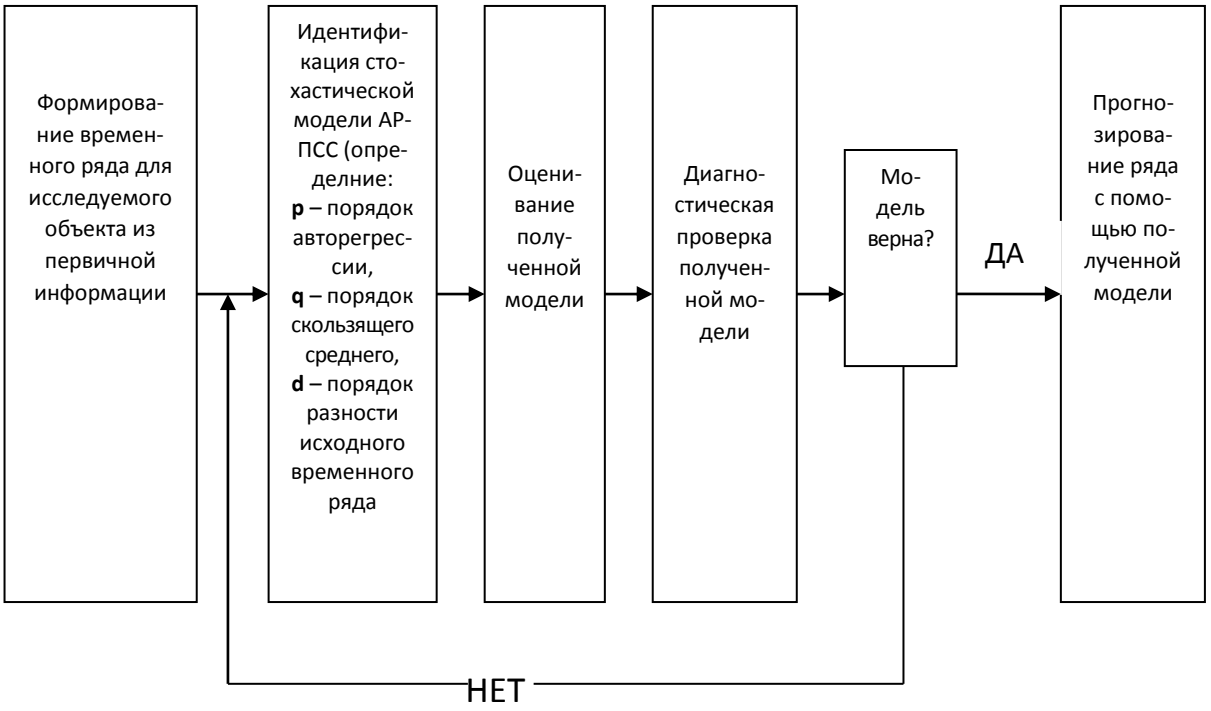


Рис. 1. Структура алгоритма прогнозирования характеристик объектов ИМОС.

С учетом полученных значений формируем ряд

Z_t^i следующим образом: $Z_t^i = \sum_{j=1}^{J}\left(\sum_{S\in\Delta D_{t-1}\div\Delta D_t} P_{i,j}^S \Big/ \sum_{S\in\Delta D_{t-1}\div\Delta D_t} 1\right)K_j$, где:

$t = \overline{1,N}$, порядковые номера временных интервалов от D_N до D_K;

D_N – дата начала исследуемого периода;

D_K – дата окончания исследуемого периода;

Определим: p – порядок авторегрессии, q – порядок скользящего среднего и d – порядок разности исходного временного ряда с последующим использованием в общей линейной модели АРПСС и определением начальных значений параметров.

Приведенный алгоритм является основой для использования формальных и эффективных методов оценивания.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Саати Т.В. Аналитическое планирование: организация систем. – М.: Радио и связь, 1998. – 24 с.

2. Вагин В.Н., Головина Е.Ю. Достоверный и правдоподобный вывод в интеллектуальных системах. – М.: Физматлит, 2004.

3. Замятина О.М. Моделирование систем. – Томск: ТПУ, 2009.

4. Мендель И.Д. Кластерный анализ. – М.: Финансы и статистика, 1988. – 176 с.

К ВОПРОСУ О ПРАВОВЫХ СРЕДСТВАХ ПРОТИВОСТОЯНИЯ УГРОЗАМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СРЕДЫ

TO THE QUESTION OF THE LEGAL MEANS OF OPPOSITION TO CHALLENGE OF THE INFORMATION AND COMMUNICATION ENVIRONMENT

Кривоухов Анатолий Анатольевич
(Курская государственная сельскохозяйственная академия имени И.И. Иванова)

Krivoukhov Anatoly Anatolyevich
(Kursk State Agricultural Academy named after I.I. Ivanova)

Аннотация: в настоящее время продолжает формироваться информационно-коммуникационная среда, которая предопределяет наличие определённых угроз, классифицированы автором на регулируемые посредством социокультурных механизмов (информационное неравенство, киберболезни) или правовых механизмов (использование деструктивной информации, информационная война, информационная преступность, информационный терроризм). Разработка правовых средств противостояния данным угрозам становится сегодня необходимым направлением правотворческой деятельности.

Ключевые слова: информационно-коммуникационная среда, информационные угрозы, правовые средства.

Annotation: at the present time continues to form information and communication environment, which determines the presence of certain threats, classified by the author on adjustable through socio-cultural mechanisms (information inequality, cyberblade) or legal arrangements (the use of destructive information, information warfare, Internet crime, information terrorism). The development of legal means to counter these threats is becoming an essential direction of the law-making activities.

Key words: information and communication environment, information threats, legal means.

В наши дни продолжает формироваться информационно-коммуникационная среда, которая, будучи местом, где синхронизируют информационное взаимодействие множество социальных субъектов, способна наиболее широко обеспечить коммуникацию между индивидами. Информационно-телекоммуникационные технологии становятся рядовым средством коммуникации. А это коренным образом изменяет жизнь общества, не только выдвигая на передний план информационную деятельность, то есть деятельность, связанную с производством, потреблением, трансляцией и хранением информации, но и трансформирует социокультурное пространство жизнедеятельности человека, превращая его в информационно-коммуникационную среду [3]. Информационно-коммуникационная среда как социотехническая система в своём строении является двухкомпонентной структурой, представленной ***системой массовой коммуникации***, построенной на информационно-телекоммуникационных техноло-

гиях, и пространством ***социальных коммуникаций***, опосредованной информационно-телекоммуникационными технологиями [5]. Данная среда, помимо очевидных преимуществ и благ для человечества, предопределяет и наличие определённых угроз, которые, на наш взгляд, могут быть классифицированы на регулируемые посредством социокультурных или правовых механизмов.

К информационным угрозам, которые регулируются социокультурным механизмом, можно отнести *проблему информационного неравенства*. Сущность данной проблемы в том, что далеко не все члены современного общества могут использовать в своей профессиональной и повседневной деятельности те новые возможности, которые информационно-телекоммуникационные технологии могут предоставить человеку. Причем обусловлено это не только экономическими и инструментально-технологическими факторами, связанными с возможностью обеспечения доступа тех или иных пользователей к средствам информатики и информационным ресурсам общества, но главным образом гуманитарными факторами, которые зависят от качеств самого человека. К таким факторам можно отнести информационную культуру личности [6], а также мотивацию индивида, его стремление к познанию, развитию своих интеллектуальных способностей, общей эрудиции. Ведь если у самого человека нет желания быть активным членом современного общества, то никакая техника и технология, никакое нормативное регулирование ему не поможет стать его полноценным гражданином.

Ещё одну угрозу этого класса представляют различные *киберболезни.* К ним относится психологическая зависимость людей от телевидения или Интернет, которые уже в современном обществе стали для многих своеобразным наркотиком. Вызывает вполне обоснованную тревогу и маниакальное увлечение части молодых людей компьютерными играми, особенно того спектра, в которых пропагандируется жестокость и насилие. Эти явления наиболее широко распространены сегодня в информационно развитых странах и являются одним из негативных результатов процесса проникновения информационно-телекоммуникационных технологий в сферу досуга. Можно предположить, что по мере дальнейшего развития этого процесса эти явления также будут прогрессировать, например, все более виртуализировать повседневную жизнь.

К информационным угрозам, которые регулируются посредством права, можно отнести сказывающиеся на информационной безопасности, составляющими которой являются безопасность информационной сферы, личности, информации и информационно-телекоммуникационной инфраструктуры [4].

В этом плане в информационно-коммуникационной среде угрозой для человека становится ***использование деструктивной информации***, которая способна разрушить социокультурные регуляторы его жизнедеятельности [1]. По своей сущности люди очень внушаемы и поэтому легко поддаются целенаправленному информационному воздействию. О его эффективности убедительно и наглядно свидетельствуют, например, результаты выборных и маркетинговых компаний. Это порождает проблемы информационно-психологической безопасности личности.

Совершенно особое место среди угроз информационного общества занимает *информационная война* как латентное воздействие информации на индивидуальное, групповое и массовое сознание при помощи методов пропаганды, дезинформации, манипулирования с целью формирования новых взглядов на социально-политическую организацию общества через изменение ценностных ориентаций и базовых установок личности. По мнению В.Э. Разуваева, информационная война есть целенаправленное воздействие субъектов на социальные процессы и отношения с использованием средств информационных технологий, информационных ресурсов и коммуникаций путём создания факторов торможения, трансформации стабильности, устойчивости государства, общества, человека в целях удержания (достижения) господства, преимущества, монополии в разных сегментах человеческого бытия [8, с. 7]. Информационные войны становятся весьма распространённым и доказавшим эффективность способом противоборства в сфере политики, экономики и идеологии. Можно прогнозировать, что в дальнейшем, по мере развития информационно-телекоммуникационных технологий, данная угроза получит ещё более широкое распространение как в локальном, так и в глобальном масштабе.

Развитие информационно-коммуникационной среды открывает широкие возможности и для развития *информационной преступности*, которая проявляет себя в информационной сфере, т.е. в сфере общественных отношений, связанных с информационными ресурсами, информационной инфраструктурой, производством, распространением (передачей), потреблением информации [2, с. 13]. В интеллектуальной сфере – это преступления, связанные с нарушением прав граждан или организаций на интеллектуальную собственность. В системе массовой коммуникации – это преступления, которые связаны с нарушением информационных прав, гарантированных конституцией. Право на информацию является одним из крупнейших завоеваний демократии, которое способствует становлению и развитию гражданского общества. Эти права включают в себя право на информацию, а также право на защиту персональной информации. Преступления же направлены главным образом на несанкционированный доступ к базам персональных данных, которыми оперируют органы государственной власти, финансовых организаций и промышленных корпораций. Поэтому его нарушение может квалифицироваться как преступление против личности, общества или государства. В этих системах накапливается большое количество весьма конфиденциальной информации не только о деятельности соответствующих организаций, но также и данных персонального характера о гражданах страны, их телефонах, адресах, имуществе, доходах, состоянии здоровья и другой информации о человеке, членах его семьи. Эта информация, конечно же, представляет значительный интерес для преступных группировок, многие из которых уже сегодня прибегают к услугам специалистов в области информационных технологий. Учитывая, что, по данным Европола, масштабы киберпреступности превышают объёмы торговли всеми наркотическими средствами естественного происхождения, а, по прогнозам, к 2020 году она и вовсе превратится в основной криминальный бизнес планеты, России в ближайшие годы стоит ожидать роста числа кибератак, ущерб от которых также будет расти.

Новой информационной угрозой становится информационный терроризм как умышленное применение отдельными лицами, террористическими группами или организациями средств информационного насилия с целью дестабилизации информационной составляющей функционирования объекта атаки [7]. Общая цель информационного терроризма – максимальное снижение уровня информационной защищенности объекта воздействия, в результате которого функционирование той или иной информационной системы может быть практически парализовано. Такой результат достигается в результате специально организованных массированных сетевых атак, которые в последние годы наблюдались неоднократно.

Таким образом, информационно-коммуникационная среда подлежит целенаправленному правовому регулированию, которое, однако, имеет свои особенности, связанные с анонимностью и расспределеностью субъекта правовых отношений. В этой связи можно считать, что при учете особенностей субъекта и объектов, а также своеобразия правоотношений в данной среде возможно правовое регулирование и в данной части общественной жизни. К основным направлениям правового регулирования информационных отношений в Интернет относятся:

– защита от деструктивной информации;

– предотвращение правонарушений и преступлений в Интернет;

– обеспечение информационной безопасности объектов информационных правоотношений в Интернет.

Правовое регулирование отношений в Интернет осуществляется на основе норм информационного законодательства, имеющих административно-правовой характер, и норм гражданского законодательства. Часть правоотношений регулируется нормами международного права, что связано с глобальным характером данной компьютерной сети.

Таким образом, жизнедеятельность человека, общества и государства, вероятнее всего, будет существенно более уязвимой. И к этой перспективе нужно заранее готовиться. Сегодня нужно разрабатывать правовые средства не противодействия, а именно противостояния угрозам информационно-коммуникационной среды. Отличие между двумя видами средств хорошо проиллюстрировано В.Э. Разуваевым. «Противодействие направлено на борьбу с уже свершившимся фактом отдельного проявления информационной войны. Противостояние же включает в себя не только реакцию на уже имеющиеся проявления угроз, но и систему предупреждения, пресечения подобных проявлений (превентивные меры), создание оптимальных механизмов для мониторинга информационного состояния субъектов, профилактических мер» [8]. Поэтому именно разработка правовых средств противостояния угрозам информационно-коммуникационной среды становится сегодня необходимым направлением правотворческой деятельности. Такие правовые средства должны быть способны максимально эффективно защищать интересы человека, общества и государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Варганов В.В., Зотов В.В. Деструктивное информационное воздействие и способы его распознавания // Телекоммуникации. 2013. № 5. С. 42-48.

2. Горшенков А.Г., Горшенков Г.Г., Горшенков Г.Н. Информационная преступность: криминологическая безопасность личности, угрозы и меры ее защиты // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия: Право. 2003. № 1. С. 13-16.

3. Зотов В.В. Становление информационно-коммуникативной среды современного общества: социологический анализ институциональных трансформаций: монография. – Курск: КурскГТУ, 2007. – 232 с.

4. Зотов В.В., Кривоухов А.А. Информационная безопасность как антропосоциотехнический феномен // Коммуникология. 2017. Т. 5. № 4. С. 71-81.

5. Зотов В.В., Лысенко В.А. Структурно-функциональная организация информационно-коммуникационной среды современного общества // Теория и практика общественного развития. 2011. № 2. С. 91-93.

6. Зотов В.В., Шарков Ф.И. Информационная культура как общекультурная компетентность / Государственное управление и развитие России: модели и проекты: сборник статей Международной научно-практической конференции. – М.: ИГСУ РАНХиГС при Президенте РФ, 2017.

7. Логинов Е.Л. Проблемы противодействия информационному терроризму // Национальные интересы: приоритеты и безопасность. 2008. № 4. С. 72-76.

8. Разуваев В.Э. Правовые средства противостояния информационным войнам: дис. ... канд. юрид. наук. – М., 2007. – 174 с.

ВОПРОСЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПРАВОПОРЯДКА С ПОМОЩЬЮ СИСТЕМЫ-112

QUESTIONS OF INCREASE OF EFFICIENCY OF PROTECTION OF LAW AND ORDER WITH THE HELP OF SYSTEM-112

Земляченко Владимир Васильевич
(Белгородский университет кооперации, экономики и права)

Zemlyachenko Vladimir Vasilyevich
(Belgorod University of Cooperation, Economics and Law)

Аннотация: в статье предложены варианты повышения эффективности функционирования дежурных частей органов внутренних дел за счет развертывания системы-112 и дополнительных каналов приема сообщений о чрезвычайных ситуациях.

Ключевые слова: система-12, дежурная часть, территориальные органы МВД России, дополнительные каналы связи.

Annotation: the article suggests options to improve the efficiency of the functioning of active-duty units of internal affairs bodies through the deployment of systems-112 and additional channels for receiving reports of emergencies.

Key words: system-112, the duty of the territorial bodies of MIA of Russia, additional channels of communication.

В реализации основных направлений деятельности полиции, указанных в ст. 2 Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» (далее – Федеральный закон «О полиции»), большую роль играют подразделения, применяющие достижения современной науки и техники [1]. К таким подразделениям прежде всего относятся дежурные части территориальных органов МВД России. Именно дежурные части занимают важное место в структуре аппарата управления органами внутренних дел. От эффективности их работы зависят результаты деятельности всего территориального органа МВД России, повышение имиджа сотрудников органов внутренних дел и укрепление доверия населения к полиции.

В соответствии со ст. 11 Федерального закона «О полиции»личный состав частей и подразделений полиции в своей деятельности обязан использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру. Приказ МВД России от 18 марта 2013 г. № 150 [2] в прямой постановке ставит задачи об организации научного обеспечения и применении положительного опыта в органах внутренних дел Российской Федерации и внутренних войсках МВД России. В настоящее время полиция в порядке, установленном законодательством Российской Федерации, применяет электронные формы приема и регистрации документов, уведомления о ходе предоставления государственных услуг, взаимодействия с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями и организациями. Федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования информационно-телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных.

Известно, что дежурная часть рассматривается как самостоятельное структурное подразделение в системе органов внутренних дел, осуществляющее руководство и контроль за деятельностью разнообразных по характеру и функциям служб и аппаратов различных уровней управления для решения задач в области охраны общественного порядка и борьбы с преступностью [3].

Особенно стоит отметить роль дежурных частей отделов (управлений) внутренних дел городов, районов, иных муниципальных образований, которые ближе всех обращены к человеку на обслуживаемой территории. А учитывая актуальность и содержание задач, возложенных на дежурную часть органа внутренних дел, таких как непрерывный круглосуточный сбор, обработка и передача информации об оперативной обстановке; прием, регистрация поступивших в дежурную часть заявлений, сообщений о преступлениях, административных правонарушениях, чрезвычайных ситуациях и происшествиях, а также своевременное реагирование на них и ряда других, играет определяющую роль в соблюде-

нии принципов обеспечения высокой боевой готовности, оперативности, глубокого знания оперативной обстановки на обслуживаемой территории.

Сотрудник дежурной части – это первый полицейский, к которому обращаются люди, попавшие в беду.

Учитывая, что забота о жизни и здоровье граждан, сохранности имущества, обеспечении личной и общественной безопасности, а также необходимость противодействия угрозам техногенного, природного характера и актам терроризма требуют развития механизма быстрого реагирования на угрозы, во исполнение Постановления Правительства Российской Федерации от 31 декабря 2004 г. № 894 [4] на базе единых дежурно-диспетчерских служб муниципальных образований создана в Белгородском регионе система обеспечения вызова экстренных оперативных служб через единый номер «112».

В указанном постановлении определен перечень экстренных оперативных служб, состоящий из 4 действующих экстренных оперативных служб (служба пожарной охраны, полиции, служба скорой медицинской помощи и аварийная служба газовой сети) и 2 новых служб (служба «Антитеррор» и служба реагирования в чрезвычайных ситуациях). В целях реализации этого постановления проведен определенный комплекс системно-технических и организационных мероприятий по модернизации сетей связи и дежурно-диспетчерских служб, обеспечивающих возможность приема и обработки вызовов (сообщений о происшествиях) от населения в адрес экстренных оперативных служб.

В системе Министерства внутренних дел Российской Федерации круглосуточная регистрация вызовов (сообщений о происшествиях) возложена на дежурные части органов внутренних дел. Все экстренные службы организуют между собой необходимое взаимодействие, которое регламентируется соответствующими ведомственными нормативными документами. Российская Федерация совместно со странами Европейского союза подписала в 1998 году телекоммуникационное соглашение, согласно которому единым номером экстренного вызова стал номер «112».

С 1 по 2 июня 2016 г. на объектах города Белгорода (центр обработки вызовов административного центра; единая дежурно-диспетчерская служба (ЕДДС); центр управления в кризисных ситуациях (ЦУКОС); служба пожарной охраны; полиция; служба скорой медицинской помощи; аварийная служба газовой сети; ДДС «Теплосети»; ДДС «Водоканал») проведена демонстрация функционирования сегмента системы-112. Аналогичные мероприятия по развертыванию единой системы-112 Российской Федерации были проведены в других регионах страны. Результаты внедрения единой системы взаимодействия экстренных оперативных служб при реагировании на происшествия и чрезвычайные ситуации (система-112), стали предметом обсуждения в Общественной палате РФ, где были выявлены следующие основные недостатки в процессе развертывания проекта «система-112»:

- отсутствие на сегодняшний день единой системы оповещения, так как соседние регионы могут иметь другое технологическое программирование, что мешает оперативной реакции на запросы от потерпевших;

- существуют трудности при определении места, откуда поступил звонок от потерпевшего, на момент рассмотрения в Общественной палате ни в одном нормативном документе такая технология не предусмотрена и нет финансовых возможностей для ее реализации;

- опытная эксплуатация сегментов системы-112 выявила проблемы с определением места отсылки SMS, вплоть до региона;

- по словам председателя комиссии Общественной палаты РФ по безопасности и взаимодействию с ОНК (Общественная наблюдательная комиссия), нужно в первую очередь связать заявителя с нарядом, который выехал бы на место преступления. Зачастую сотрудники полиции для идентификации заявителя вынуждены звонить ему с личного телефона.

Заслуживает внимание и сама топологическая схема реализации центра системы-112 (см. рис. 1).

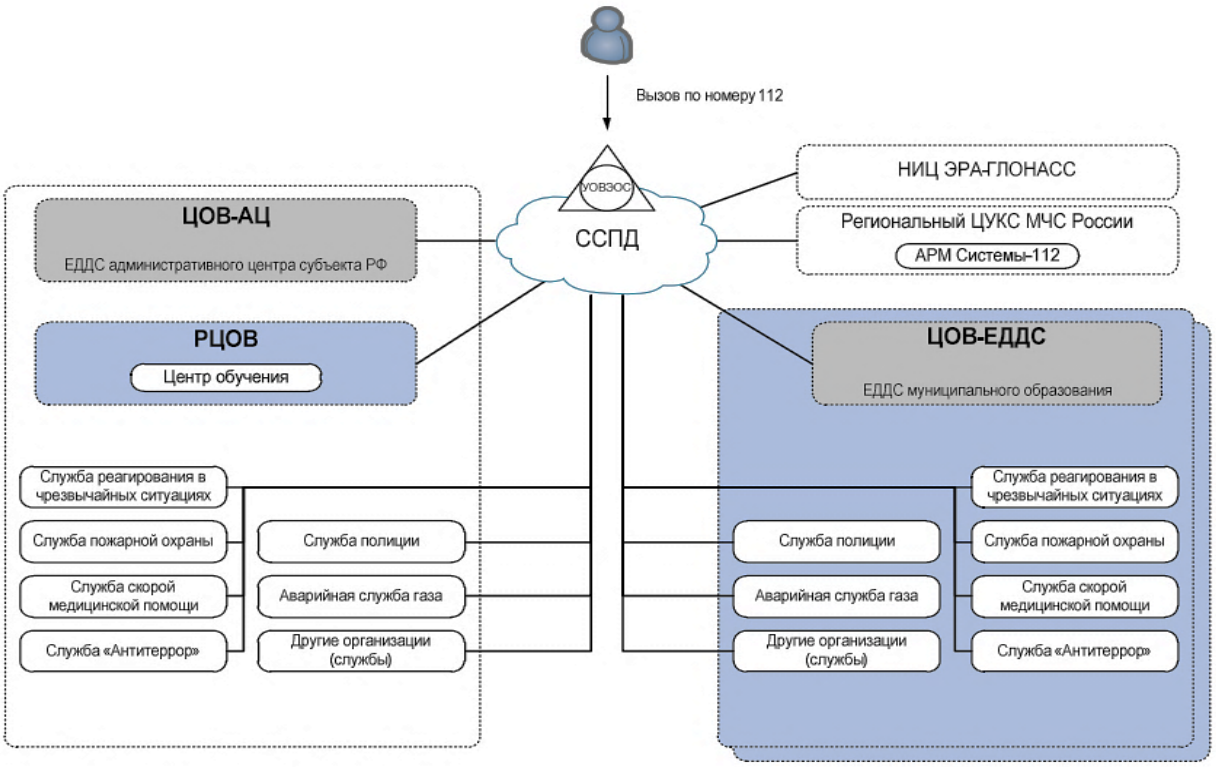


Рис 1. Структурная схема организации подразделений центра системы-112 [5]: а) ЦОВ-АЦ – центр обработки вызовов административного центра субъекта РФ; б) ССПД – сеть связи и передачи данных; в) РЦОВ – резервный центр обработки вызовов; г) ЦОВ-ЕДДС – центр обработки вызовов единой дежурно-диспетчерской службы.

Схема организации взаимодействия подразделений системы-112 реализует концепцию топологии сети в виде звезды, которая была заимствована из области больших ЭВМ, в которой основная вычислительная машина получает и обрабатывает все данные с периферийных устройств как активный узел обработки данных. Такая топология сети получения и обработки поступающей информации обладает рядом достоинств: выход из строя одного источника сооб-

щений или повреждение ее линии связи глобально не отражается на функционировании системы в целом; простота настройки и администрирования; достаточно высокая производительность и т.д.

Однако топологии «звезда» присущи такие возможные недостатки, как выход из строя центрального коммутатора; сбои в работе программного обеспечения; проблемы с обеспечением бесперебойного питания; целенаправленное воздействие на центральный узел со стороны злоумышленника для уничтожения системы и т.д., обернутся неработоспособностью всей сети. Да и последовательность истребования от заявителя оператором системы адресной информации и перенаправления профильному оператору требует определенного времени, что осложняет оперативность принятия решения.

Учитывая опыт внедрения США «системы 991» и в связи с изменением порядка вызова оперативных служб и необходимостью организации информационного взаимодействия этих служб, в рамках системы-112 необходимо:

- помимо подготовки и повышения уровня квалификации персонала дежурно-диспетчерских служб на базе государственных образовательных учреждений дополнительного профессионального образования, учебных центров (пунктов) федеральной противопожарной службы, а также учебно-методических центров по вопросам гражданской обороны и чрезвычайных ситуаций субъектов Российской Федерации, ввести в учебные планы Бел ЮИ МВД России имени И.Д. Путилина по учебной дисциплине «Специальная техника ОВД» дополнительные темы по изучению назначения, структурной организации, целей и задач, стоящих перед системой-112;

- для обеспечения постепенного перехода населения на новую единую систему-112 взаимодействия экстренных оперативных служб при реагировании на происшествия и чрезвычайные ситуации обеспечить непосредственный доступ (по определенному номеру телефона) заявителя в случае характера сообщения по профилю полиции в дежурные части территориальных органов внутренних дел;

- рассматривать возможным для обеспечения оперативности доступа непосредственное дежурство на постах приема сообщений от населения в дежурных частях в качестве прохождения практики в территориальных органах внутренних дел курсантов старших курсов факультетов Бел ЮИ МВД России имени И.Д. Путилина.

Таким образом, учет и устранение выявленных недостатков при опытном внедрении системы-112 обеспечит повышение эффективности функционирования дежурных частей территориальных органов внутренних дел, что способствует росту безопасности и защищенности населения и критически важных объектов от угроз техногенного и антропогенного характера и является одним из гарантов обеспечения национальной безопасности и стабильного социально-экономического развития Российской Федерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» (ред. от 07.12.2017) // СПС «Консультант Плюс».

2. Приказ МВД России от 18 марта 2013 г. № 150 «Об организации научного обеспечения и применении положительного опыта в органах внутренних дел Российской Федерации» (ред. от 30.01.2017) // СПС «Консультант Плюс».

3. Приказ МВД России от 26 февраля 2002 г. № 174 «Наставление по организации деятельности дежурных частей системы органов внутренних дел» // СПС «Консультант Плюс».

4. Постановление Правительства РФ от 31 декабря 2004 г. № 894 «Об утверждении перечня экстренных оперативных служб, вызов которых круглосуточно и бесплатно обязан обеспечить оператор связи пользователю услугами связи, и о назначении единого номера вызова экстренных оперативных служб» // СПС «КонсультантПлюс».

5. Технический проект системы обеспечения вызова экстренных оперативных служб по единому номеру «112» на базе единых дежурно-диспетчерских служб муниципальных образований субъекта Российской Федерации. Приложение 11. [Электронный ресурс]. – Режим доступа:http://dpchs.donland.ru/ Data/ Sites/14/media/.pdf.

ПРОБЛЕМЫ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИИ

PROBLEMS OF COMPUTER CRIME IN RUSSIA

Карпика Анатолий Григорьевич,
Лемайкина Светлана Владимировна,
Петрищева Елена Николаевна
(Ростовский юридический институт МВД России)

Karpika Anatoly Grigoryevich,
Lemaikina Svetlana Vladimirovna,
Petrischeva Elena Nikolaevna
(Rostov Law Institute of the MIA of Russia)

Аннотация: в статье анализируются проблемы борьбы с киберпреступностью в России на фоне тенденции роста неправомерного доступа к компьютерной информации.

Ключевые слова: Интернет, киберпреступность, компьютерные технологии, неправомерный доступ к компьютерной информации.

Annotation: the article analyzes the problems of the fight against cybercrime in Russia on the background of the growth trends of illegal access to computer information.

Key words: Internet, cybercrime, computer technology, illegal access to computer information.

Сегодня Интернет стремительно превратился в общую информационную систему, которая вобрала в себя не только достоинства глобальности, но и глобальные пороки. Возможности Интернета все чаще становятся средством совершения противоправных деяний.

Подогревают интерес к этому виду деятельности, создавая некую атмосферу романтики и славы, успешные вторжения хакеров в те или иные компьютерные объекты. Пользователи компьютерных сетей, в свою очередь, стремясь к упрощению обмена информации и ускорению ее обработки, забывают про безопасность.

Активное применение компьютерных технологий во всех сферах его жизнедеятельности обусловливает значительный рост преступлений с использованием компьютерных технологий.

Так, по данным ФКУ ГИАЦ МВД России, за январь-июль 2017 года в России зарегистрировано с использованием компьютерных и телекоммуникационных технологий 46469 преступлений, из них раскрыто 10950[1].

Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Известно, рассматриваемые правонарушения имеют очень высокую латентность. Более того, факты обнаружения незаконного доступа к информационным ресурсам носят случайный характер. Большая часть преступлений в сфере Интернета не только остается нераскрытой, но даже не регистрируется! Причем число таких преступлений с каждым годом растет. Хакеры постоянно повышают свой уровень и оттачивают свое мастерство. Создаются новые виды зловредных программ, которые с каждым разом становятся все хитрее и изощреннее.

Исходя из данных Microsoft, в I квартале 2017 года примерно на 15% компьютеров в России было зафиксировано вредоносное ПО, в мире этот показатель составил 9%. В прошлом году таких инцидентов было отмечено почти в два раза больше: 27,2% – в России, 18,3% – в мире. На облачные сервисы количество атак по всему миру увеличилось на 300%. За I квартал 2017 года статистика по месяцам в России демонстрирует тенденцию к снижению – 17,2% в январе, 15,1% в феврале и 12% в марте 2017 года. Системой безопасности Windows Defender Security Intelligence (WDSI) данные угрозы были зафиксированы и предотвращены. Данная система ежемесячно сканирует по всему миру более 400 миллиардов электронных писем на наличие фишинговых атак и вредоносного ПО, анализирует 450 миллиардов попыток входа в учетную запись и проверяет более 18 миллиардов веб-страниц. В анализе отмечено, что самой распространенной категорией стали трояны: на конец I квартала 2017 года они были обнаружены у пользователей 10,26% компьютеров. Второе и третье место заняли вирусы (1,59%) и загрузчики троянов и дропперы (0,64%). В этот же период на большинстве зараженных компьютеров среди нежелательного программного обеспечения найдены инсталляторы дополнительного ПО (5,49%), модификаторы браузера (2,14%) и рекламное ПО (0,25%) [1].

[1] Состояние преступности в России за январь-июль 2017 года // Официальный сайт ФКУ ГИАЦ МВД России.

Исходя из вышесказанного, в ближайшем будущем Россия столкнется с резким скачком киберпреступности.

Так, число киберпреступлений в России с 2013 года увеличилось в шесть раз. Такие данные в 2017 году привел генеральный прокурор России Юрий Чайка. Одновременно прокурор России поведал, что ущерб от IT преступлений за первую половину 2017 года превысил 18 млн долларов США и, что характерно, две трети в России преступлений – экстремистской направленности, и каждое девятое преступление террористического характера совершено с использованием компьютерной сети [2].

Развитие компьютерной преступности происходит по следующим путям:

- высочайшие темпы роста компьютерных технологий;
- усложнение способов совершения компьютерных преступлений и появление новых видов противоправной деятельности в сфере компьютерной информации;
- рост криминального профессионализма компьютерных преступников.

Термин «киберпреступность» получил широкое распространение в 70-е годы прошлого века и охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети либо против компьютерной системы или сети [3].

Преступники используют компьютерные технологии при совершении деяний, ответственность за которые уже закреплена в «некомпьютерных» статьях уголовного кодекса.

Если говорить о российском уголовном законодательстве, то наиболее актуальными для нас являются международные правовые акты, принимаемые в Европейском правовом пространстве и Содружестве независимых государств.

В Совете Европы принимаются серьезные меры, направленные на приведение к единообразию законодательств стран-участниц в сфере правового регулирования компьютерных преступлений.

Первым документом Совета Европы в сфере правового регулирования компьютерных преступлений была Рекомендация № R 89 (9) Комитета Министров стран – членов Совета Европы «О преступлениях, связанных с компьютерами» от 13 сентября 1989 г. Документ содержал перечень рекомендованных к обязательному включению в национальное уголовное законодательство деяний. Также там приводился перечень тех деяний, по которым не было достигнуто согласия в признании необходимости их криминализации в законодательстве всех стран. Здесь же был использован такой термин, как «преступление, связанное с использованием компьютерных технологий».

Изучение и последующее включение предложенных в международных актах составов компьютерных преступлений в российское законодательство содействовало бы облегчению преследования лиц, совершающих преступления с использованием компьютерных технологий на межгосударственном уровне.

Еще один документ в данной сфере – это Конвенция Совета Европы о преступности в сфере компьютерной информации, содержащая нормы статей материального уголовного права, регламентирующие преступления, связанные с использованием компьютерных технологий, в соответствии с которыми страны –

участницы обязаны реализовать правовые нормы в собственном законодательстве, т.е. стандартизировать правовое закрепление преступлений в сфере компьютерной информации в национальных законодательствах стран, сближение национальных уголовно-процессуальных норм, упорядочивание международного сотрудничества по предотвращению и расследованию компьютерных преступлений [4].

Хочется отметить, что закрепления в Конвенции необходимости привлечения к уголовной ответственности юридических лиц, статья 12 «Корпоративная ответственность», в нашем уголовном законодательстве нет. Дискуссии о необходимости введения в российское законодательство уголовной ответственности юридических лиц ведется уже несколько лет [5, с. 85-87].

Состав закрепленных в УК РФ норм, устанавливающих ответственность за совершение преступлений с использованием компьютерных технологий, не охватывает всего многообразия противоправных деяний, которые могут быть совершены таким образом и расцениваться как преступные. Необходимо разработать нормы, устанавливающие ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства, для приведения российского уголовного законодательства в соответствие с международными нормами и требованиями действительности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Security Intelligence Report 2017: Microsoft представила отчет по угрозам информационной безопасности [Электронный ресурс]. – Режим доступа: https://news.microsoft.com/ru-ru/.

2. Киберпреступность и Россия [Электронный ресурс]. – Режим доступа: http://summit.tadviser.ru/.

3. Проблемы соответствия российского уголовного законодательства международным нормативным актам в сфере киберпреступности [Электронный ресурс]. – Режим доступа: https://zakon.ru/blog/2012/2/25/.

4. Конвенция о преступности в сфере компьютерной информации (EST № 185) от 23 ноября 2001 г. // СПС «КонсультантПлюс».

5. Попандопуло Д.В., Петрищева Е.Н. Компьютерная преступность в России: состояние и перспективы совершенствования законодательства // Актуальные проблемы с преступлениями и иными правонарушениями. 2017. № 15-2.

МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ В СФЕРЕ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

FRAUD IN THE FIELD OF INFORMATION AND COMPUTER TECHNOLOGIES

Глушков Евгений Леонидович,
Свистильников Александр Борисович
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Glushkov Evgeny Leonidovich,
Alexander Borisovich Svistilnikov
(Belgorod Law Institute of MIA of Russia named after I.D. Putilin)

Аннотация: в статье рассмотрены некоторые проблемы, возникающие в процессе раскрытия и расследования мошенничеств, совершенных с использованием информационных технологий и предложены некоторые пути их решения. Считаем, если не будет предприниматься мер по совершенствованию деятельности сотрудников полиции по недопущению правонарушений с использованием информационных технологий, а также раскрытию данных видов противоправных деяний, то преступность захлестнет весь мир.

Ключевые слова: мошенничество, информационные технологии, Интернет, сотовая связь, онлайн-шоппинг и банкинг.

Annotation: the article discusses some problems encountered in the process of disclosure and investigation of fraud committed using information technologies and suggested some solutions to them. Believe if would be taken measures on improvement of activity of police officers to prevent offences using information technology, and also reveal these types of wrongful acts, crime will engulf the entire world.

Key words: fraud, information technology, the Internet, cell phones, online shopping and banking.

Под определение «мошенничество» попадают многие незаконные действия в самых различных сферах, в том числе и в сфере банковской деятельности, сотовой связи и современных информационных технологий.

«Ассортимент» разнообразных махинаций в наши дни существенно расширился, в основном благодаря приходу в повседневную жизнь современных технологий, таких как Интернет, сотовая связь, онлайн-шоппинг и банкинг. Однако традиционные виды мошенничеств также до сих пор процветают. Среди них можно назвать наперсточников, уличных мошенников, предлагающих купить драгоценные изделия, подставных лиц, устраивающих аварии и предлагающих договориться на месте, псевдомагов и целителей, работников социальных и аварийных служб, беженцев с соседних республик.

Начиная с 2006 года, правоохранительные органы столкнулись с новым видом мошенничеств – телефонным, позже оно вошло в один большой раздел, получивший название «мошенничества, совершаемые с использованием информационных технологий». В настоящее время данный раздел занял лидирующую позицию из всех существующих видов мошенничеств. Его стремительный рост привел к созданию отделов (отделений) на базе управлений уголовного розыска на территории 80-90% всех субъектов Российской Федерации.

Несмотря на различия в технологии, все эти действия объединяет ряд общих признаков:

- обманные действия;
- злоупотребление доверием;
- умышленное искажение фактов или умолчание;
- хищение чужого имущества;
- незаконное приобретение прав на чужое имущество.

В большинстве случаев жертва мошенничества самостоятельно и добровольно передает преступникам свою собственность или права на нее. Обратим внимание на следующие мошенничества.

Виды мошенничества в банке

Мошеннические действия в банках можно условно разделить на несколько групп:

- мошенничество при кредитовании – зачисление сумм, предназначенных для погашения долга на другие счета, оформление кредитов на несуществующих заемщиков, оформление кредитов без ведома клиентов;
- мошенничество при рассчетно-кассовом обслуживании – несанкционированное списание сумм со счета, подмена купюр фальшивыми, вытягивание банкнот из пересчитанной пачки;
- мошенничество с депозитами – изъятие внесенных средств, приуменьшение сумм в документах, списание, перевод средств без ведома клиента.

Виды мошенничества в Интернете

В связи с активным ростом рынка электронных платежей и онлайн-шопинга развиваются и новые современные формы мошенничества с использованием информационных технологий. Самыми распространенными видами мошенничества в Интернете являются следующие:

- фишинг – кража персональных данных (пароля, логина) с целью похищения средств с банковской карты. В основном для фишинга используют почтовую рассылку, содержащую ссылку на фальшивые сайты;
- мошенничество через электронную почту – так называемые «нигерийские письма», они содержат в себе красивую легенду о наследстве от мифического родственника и просьбу перевести деньги на счет для получения оплаты услуг адвоката или выплаты комиссии;
- операции с интернет-кошельками – чаще всего в таких случаях покупатель переводит предоплату продавцу на интернет-кошелек, но в итоге не получает ни товара, ни денег.

Виды мошенничества по телефону

Мошенничество при помощи сотовой связи можно условно разделить на две группы:

– снятие денег непосредственно со счета владельца номера без его ведома. Такими махинациями могут заниматься как сами сотовые операторы, так и не имеющие отношения к их компаниям мошенники;

– абонент сам перечисляет деньги на указанный злоумышленником счет либо отдает их прямо в руки или оставляет в указанном мошенниками месте. В таких аферах сотовая связь выступает лишь в качестве инструмента инсценировки. Например, разыгрывается звонок близкого родственника, попавшего в беду и срочно нуждающегося в деньгах.

Виды мошенничества с деньгами

Мошенничество с деньгами – это одна из самых обширных и всеобъемлющих групп, ведь практически любое мошенничество так или иначе подразумевает незаконное овладение чужими денежными средствами. Однако можно выделить несколько способов мошенничества, связанных косвенно или непосредственно с наличными купюрами. Эти способы могут практиковаться в магазинах, ларьках, обменных пунктах. Самым простым и распространенным является мошенничество путем замены настоящих купюр на фальшивые. Также практикуется «недостача» - из уже пересчитанной пачки купюр вытягивается несколько банкнот. Мошенничество может производиться также с помощью банкомата при попытке снять наличность, на котором устанавливается датчик, считывающий персональные данные.

Все самые распространенные виды мошенничества объединяются одним общим знаменателем – они осуществляются с учетом психологии потенциальных жертв аферистов. Аферы продумываются до мельчайших деталей и способны обмануть бдительность даже самых осторожных и внимательных людей. Именно поэтому необходимо помнить о том, что персональные данные, такие как пароль, логин, номер банковского счета, кодовое слово, CVV2-код на банковской карте, нельзя передавать в третьи руки.

Проблемы, возникающие в процессе раскрытия и расследования мошенничеств, совершенных с использованием информационных технологий:

- отсутствие своевременных ответов на запросы органа (следствия) дознания из кредитных организаций и банков до окончания максимально-возможного срока проведения проверки;

- неполнота сведений, предоставляемых банком-эмитентом на направляемые запросы, ввиду того, что получение всех необходимых сведений может вскрыть вину банка в неправомерном доступе к счетам держателей карт и служить основанием для привлечения банка к гражданско-правовой ответственности;

- отказ представителей банков в принятии претензий от клиентов, в том числе требующих проведения внутреннего расследования, и направление потерпевших в орган внутренних дел без результатов рассмотрения претензий и выписок по счету;

- невозможность определения мест совершения транзакций по обналичиванию денежных средств ввиду нахождения счетов, банков и кредитных орга-

низаций за пределами Российской Федерации и отсутствия международно-правовых актов, обуславливающих возможность получения информации, составляющей банковскую тайну;

- нежелание и фактическое бездействие кредитных и банковских организаций по проведению внутренних расследований по факту несанкционированных транзакций со счетов держателей карт. Указанное обстоятельство лишает орган дознания (следствия) оперативно реагировать на установление места совершения обналичивания похищенных денежных средств и безотлагательно произвести выемку видеоматериалов с устройств самообслуживания (банкоматов);

- нежелание некоторыми должностными лицами органов внутренних дел ряда субъектов РФ принимать процессуальное решение в порядке ст. 146 УПК РФ, в связи с чем материалы проверок необоснованно направляются вопреки порядку, установленному законом.

Исходя из обозначенных проблем, мы можем сформулировать предложения по их решению:

- приобрести аппараты «РЕСТ-М» подразделениями ФСИН России, которые способны пресекать несанкционированные переговоры осужденных лиц, выход в Интернет через абонентские устройства сотовой связи в стандартах GSM/DCS – 900/1800 МГц, CDMA 450 МГц, CDMA 800 МГц, 3G, LTE (UMTS), что положительно скажется на оперативной обстановке в учреждениях ФСИН России;

- выйти с предложением о приобретении во всех регионах ФСИН России оборудования, необходимого для проведения обысковых мероприятий и изъятия мобильных устройств в исправительных учреждениях (например, измеритель спектра вторичных полей «NR-m-Г»: данный прибор показал свою эффективность в исправительных учреждениях Новосибирской, Саратовской областей, в связи с чем было бы целесообразно приобретение указанного прибора во всех регионах);

- приобрести многофункциональный комплекс в подразделениях ФСИН России «ТАиП», созданный для блокирования сигналов сотовой связи на территории исправительных учреждений и поиска мобильных устройств «КИБ 100», которые в паре могут перекрыть большую часть исправительного учреждения;

- настроить тесное взаимодействие с сотрудниками УФСИН России по предоставлению идентификационных номеров, номеров SIM-карт, изъятых у осужденных, для установления причастности к совершению мошеннических действий с использованием информационных технологий;

- взаимодействовать с представителями кредитно-банковских организаций о временном блокировании денежных средств, поступивших на счета злоумышленника, от мошеннических действий, совершенных с использованием информационных технологий, на момент проверки по зарегистрированному преступлению;

- предложить представителям кредитно-банковских организаций внести изменения в программное обеспечение банковских терминалов, заключающиеся в выводе на монитор аппарата текстового сообщения о видах мошенничеств;

- создать специализированную рабочую группу, состоящую из оперативных сотрудников и следователей, в которой будет концентрироваться вся информация, начиная от доследственной проверки, заканчивая расследованием и направлением уголовного дела в суд.

На наш взгляд, предложения, которые попытались рассмотреть в данной статье, помогут сотрудникам оперативных и следственных подразделений наиболее качественно проводить проверки, расследовать уголовные дела по преступлениям, связанным с мошенническими действиями с использованием компьютерных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ в ред. от 29.07.2017 // СПС «КонсультантПлюс».

2. Ефремова М.А. Мошенничества с использованием электронной информации // Информационное право. 2013. № 4.

3. Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно телекоммуникационных технологий: монография. – М.: Юрлитинформ, 2015.

4. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения // Ученые записки КЮИ МВД России. 2016. Вып. 1.

ИСПОЛЬЗОВАНИЕ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

THE USE OF VIDEO SURVEILLANCE SYSTEMS IN THE DETECTION AND INVESTIGATION OF CRIMES

Самсонов Валерий Николаевич,
Карагодина Ангелина Александровна
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Samsonov Valery Nikolayevich,
Karagodina Angelina Alexandrovna
(Belgorod Law Institute of MIA of Russia named after I.D. Putilin)

Аннотация: в статье рассматриваются актуальные проблемы безопасности жителей городов. Возросший уровень преступности и правонарушений, а также вероятность террористических актов являются одной из проблем для руководства города, полиции и общественности. Привлечение системы городского видеонаблюдения в помощь правоохранительным органам значительно повысит эффективность их работы по профилактике правонарушений в городе.

Ключевые слова: полиция, безопасный город, правоохранительная помощь, видеонаблюдение, безопасность.

Annotation: this article presents actual problems of safety of residents. Increased levels of crime and offense and also the chance of terrorist acts is one of the problems for the city government, police and public. Engaging video surveillance systems to help law enforcement agencies will greatly enhance the effectiveness of their work on crime prevention in the city.

Key words: police, secure city, assistance of law enforcement agencies, video surveillance, security.

Одним из серьёзных подспорий в профилактике преступности стало внедрение аппаратно-программного комплекса «Безопасный город», помогающего полиции более оперативно реагировать на всё происходящее на улицах российских городов и других крупных населённых пунктов. Практика показала, что возможно ещё более широкое его применение, нежели задумывалось вначале [1, с. 18].

На сегодняшний день вопрос обеспечения безопасности города выходит далеко за рамки задач наблюдения за различными объектами. Современные цифровые системы способны не только обрабатывать видеопоток и передавать его по компьютерным сетям, но и осуществлять интеллектуальную обработку изображения, распознавать преступников по базам данных, координировать работу охранного оборудования и поворотных устройств, мгновенно реагировать на тревожные события и автоматически выполнять соответствующие действия: тушение пожара, включение вентиляции, блокировка выходов, оповещение городских служб и т.д.

Система «Безопасный город» в настоящем ее виде, можно сказать, выросла на базе видеонаблюдения. Эта подсистема и по сей день остается наиболее «видимой», эффектной и характерной частью проекта. Практически каждая вторая реализация «Безопасного города» начиналась с этой подсистемы. Видеонаблюдение используется чаще всего в местах массового скопления людей: площади, вокзалы, оживленные перекрестки, места отдыха и развлечений горожан. Такая ситуация объяснима сложной криминогенной обстановкой, которая существует в наших городах, а система видеонаблюдения может оказать неоценимую помощь в процессе предупреждения и раскрытия правонарушений.

Однако было бы ошибкой считать, что единственной задачей проекта является борьба с преступностью. Город – очень сложный многоуровневый механизм. Это взаимосвязанная система, для обеспечения безопасности которой необходимо поставить под контроль все ее составляющие. Поэтому со временем система «Безопасный город» дополнилась разнообразными функциональными модулями. Сейчас, кроме уже упомянутого видеонаблюдения, в проект входят следующие подсистемы:

– охранно-пожарная сигнализация – обеспечивает противопожарную безопасность зданий и помещений, как жилых, так и технических;

– инженерная (аварийная) сигнализация – включает в себя датчики на затопление и загазованность помещений. В зависимости от объекта и характера

среды могут дополняться другими видами аварийных датчиков, например, радоновыми;

– мониторинг доступа в технические помещения – система контроля доступа, например, на чердаки и в подвалы, которая предоставляет права доступа только обслуживающему объект техническому персоналу и учитывает время прихода и ухода;

– диспетчеризация лифтового хозяйства – основана на работе специализированных приборов, которые подключаются к лифтовым шкафам и собирают все доступные параметры лифтов;

– включение и выключение инженерного оборудования и освещения – регулирует работу инженерных систем в зданиях и помещениях. Например, включение и выключение помп, дымоудаления, вентиляции;

– общедомовая и индивидуальная интегрированная система учета потребляемых ресурсов. Общедомовая система, помимо сведения баланса, позволяет контролировать качество поставляемого ресурса: горячей и холодной воды, тепла, электроэнергии – путем наблюдения за параметрами подаваемого ресурса. Так, существуют определенные нормы температуры и давления для горячей воды и тепла, напряжения и частоты для электроэнергии, которые должны соблюдаться, и это, соответственно, контролируется системой. Однако индивидуальная система только учитывает поставляемый ресурс. В целом подсчет ресурсов позволяет городским властям контролировать эффективность работы как эксплуатирующей дом организации, так и поставщиков ресурсов. В свою очередь, эксплуатирующей организации эта система дает возможность наблюдать и своевременно восстанавливать жилищный фонд, а значит, предоставлять более качественные услуги;

– диспетчерская и экстренная (голосовая) связь – основана на работе специальных приборов, проводных или беспроводных. Экстренная связь располагается на улицах города, во дворах, около метро, на остановках общественного транспорта и в других местах массового движения горожан. Диспетчерская – устанавливается в соответствии со строительными нормами Российской Федерации. Предоставляют возможность экстренной связи для вызова необходимой помощи, например, сотрудников МЧС или скорой помощи, милиции или аварийной службы. Диспетчерская связь осуществляется через call-центр, в задачи которого входит прием экстренных вызовов, а также их переадресация в соответствующие службы;

– геоинформационная система – это удобный интерфейс взаимодействия, представляющий собой карту местности с учетом всех топографических особенностей района и адресной привязки объектов. Такой подход обусловлен в первую очередь структурой города: любой населенный пункт, будь то деревня или мегаполис, строится и развивается по древовидному принципу. Естественно, что проект «Безопасный город» встраивается уже в существующую инфраструктуру города и отражает все особенности его административного деления [5].

Таким образом, «Безопасный город» также строится по древовидной схеме. Вся информация от телекамер, приборов учета ресурсов, датчиков сигнализации и контроля доступа с одного или нескольких домов сводится в единый опорный узел. Количество домов, которое будет охватывать такой узел, зависит

от характеристик каждого объекта или от технического решения инсталлятора. С точки зрения топологии существуют два варианта: выбор определяется масштабом зоны покрытия. Первый вариант – в каждом доме формируется опорный узел, куда поступают все данные и откуда они передаются дальше - в оперативно-технический центр (ОТЦ). Второй вариант – опорных узлов нет, а все данные и параметры с домов сразу поступают в ОТЦ. Также существует и промежуточный вариант, более гибкий, который, кстати, реализован в Москве. Здесь каждый опорный узел объединяет группу домов. Его место в структуре «Безопасного города» выбирается таким образом, чтобы было удобно получать данные. Естественно, что количество опорных узлов напрямую зависит от масштаба города, в котором реализуется проект. Ничего не мешает инсталлятору реализовать и смешанную топологию «Безопасного города», используя совместно разные варианты построения [5].

В опорном узле размещается сервер, предназначенный для оцифровки видео, преобразования аналогового сигнала и его передачи, кратковременного хранения данных, приема информации учета ресурсов и трансляции всех этих данных в ОТЦ.

Оперативно-технический центр предназначен для сбора всей информации и долгосрочного ее хранения. Иногда ОТЦ целесообразно разделить на два отдельных центра – оперативный и технический. Это может зависеть от пожелания заказчика, решения инсталлятора или особенностей города.

В оперативном центре размещается персонал, который контролирует данные видеонаблюдения, принимает сигналы экстренной связи, инженерной и охранно-пожарной сигнализации, а также ведет контроль параметров учета ресурсов в случае превышения установленных норм расхода. Так, повышенный расход воды может свидетельствовать о прорыве трубы, а падение температуры в помещениях ниже нормы в зимний сезон – о нарушении теплоизоляции.

В техническом центре размещается дежурный административно-технический персонал. Здесь организованы административные рабочие места и специальные рабочие места контроля работоспособности системы. Соответственно, в техническом центре собрано все серверное и телекоммуникационное оборудование системы.

Принципиальными требованиями к глобальной системе безопасности являются надежность, устойчивость и бесперебойность работы системы в круглосуточном режиме. Для соответствия этим требованиям как в аппаратной, так и в программной части всех подсистем комплекса реализованы специальные решения:

- контроль работоспособности системы;
- предотвращение возможных ошибок или сбоев;
- корректное восстановление работоспособности всех подсистем в случае сбоя.

В рамках проекта «Безопасный город» очень четко регламентирован механизм реагирования на опасную ситуацию. Информация с телекамер передается на мониторы, расположенные в ОТЦ. Если видимая картинка выглядит подозрительно, оператор мгновенно подает сигнал дежурному, который высылает по данному адресу группу вневедомственной охраны. По данным работы

системы в Центральном административном округе Москвы, благодаря высокой степени оперативности действий (группа приезжает на место в течение 3-5 минут), удалось предотвратить большое количество правонарушений, а многие преступления раскрыть по «горячим следам». При необходимости в число пользователей могут быть включены службы «Скорой помощи», аварийно-спасательные и другие службы оперативного реагирования [5].

Говоря об особых требованиях, которые предъявляются к системам, призванным обеспечивать безопасность города, в первую очередь необходимо помнить о поиске универсального решения, обладающего рядом признаков. Во-первых, такое решение имеет высокие интеграционные характеристики и обладает хорошей совместимостью специализированного оборудования. Во-вторых, оно дает возможность централизованного и удаленного контроля и управления, что облегчает и унифицирует построение такой системы. В-третьих, способно масштабироваться, что называется, и вглубь, и вширь. В-четвертых, может объединить в одну систему на первый взгляд не имеющие ничего общего между собой объекты, события, задачи, например, контроль лифтового оборудования и видеонаблюдение. Основные требования к глобальной системе безопасности можно сформулировать так: надежность, устойчивость и бесперебойность работы в круглосуточном режиме.

Одной из главных функций системы «Безопасный город» является организация глобального видеонаблюдения: в жилых кварталах, местах скопления людей и проведения массовых мероприятий, на автомобильных магистралях, в государственных учреждениях, на жизненно важных для города объектах.

Городская система видеонаблюдения позволяет решить следующие задачи:

– оперативный контроль ситуации на ключевых объектах города;

– своевременная и достоверная информационная поддержка служб охраны, правопорядка и безопасности, аварийно-спасательных подразделений;

– предоставление визуальной информации, получаемой с мест установки камер наблюдения, расположенных на любом расстоянии от пункта видеомониторинга;

– информирование о возникновении чрезвычайных ситуаций, совершении правонарушений соответствующих служб и организаций;

– цифровое архивирование видео- и аудиоинформации;

– обеспечение возможности восстановления хода событий на основе записанных видеоматериалов;

– передача информации, получаемой от охранных видеокамер как по запросу, так и в автоматическом режиме;

– интеграция с другими автоматизированными системами, при наличии такой возможности у этих систем;

– предоставление информации о ситуации в реальном времени.

Область применения системы «Безопасный город» распространяется на:

– здания и сооружения, используемые органами власти, объекты, принадлежащие силовым ведомствам;

– транспортные сооружения (мосты, путепроводы), нефте- и газопроводы, плотины, электростанции, водохранилища, а также промышленные объек-

ты, представляющие повышенную опасность для окружающей среды – предприятия атомной энергетики, химические производства, склады и прочее;

– транспортные компании, службы аэропортов, портов, вокзалов;

– производственные здания и сооружения – заводы, фабрики, объекты строительства;

– офисные и деловые центры, финансово-кредитные учреждения, магазины, рынки, гостиницы, предприятия сферы услуг;

– многоквартирные дома и индивидуальные жилые постройки, коттеджи, дачи.

Только организация единой для всего города системы видеонаблюдения является эффективным способом обеспечения его безопасности.

Основными результатами создания городской системы видеонаблюдения станут:

– снижение уровня правонарушений, увеличение числа раскрываемых квартирных краж, уличных преступлений, фактов похищения автотранспорта и повышение результативности поиска транспортных средств, находящихся в угоне;

– повышение степени контроля органов власти ситуацией в городе и раскрываемостью преступлений;

– снижение затрат на ремонт и восстановление городского и муниципального имущества в результате краж и вандализма;

– сокращения общего числа правонарушений вследствие осведомленности потенциальных правонарушителей о наличии видеонаблюдения;

– оказание помощи правоохранительным органам в следственно-разыскных мероприятиях, при поиске преступников, правонарушителей.

Органами внутренних дел будут востребованы данные, предоставляемые системой безопасности, такие как:

– обнаружение оставленных и представляющих опасность предметов;

– видеоконтроль обстановки на улицах, площадях, отдельных объектах городской инфраструктуры (образовательные и медицинские учреждения, объекты культуры, др.);

– выявление противоправных действий и событий, представляющих угрозу жизни людей.

Подводя итог по данной главе, отметим, что аппаратно-программный комплекс «Безопасный город» в настоящее время развит достаточно хорошо. Одной из главных функций системы «Безопасный город» является организация глобального видеонаблюдения. В связи с тем, что город – это сложный многоуровневый механизм, взаимосвязанная система, для безопасности такой системы необходимо поставить под контроль все её составляющие. Помимо функций борьбы с преступностью, данная система позволяет решать множество других задач по обеспечению безопасности жителей городов посредством созданных подсистем. Но, проанализировав научные статьи, специальную литературу, мнения различных авторов, можно сделать вывод о том, что со всеми подсистемами и их функциональными возможностями данный проект еще нигде не реализован. Будем надеяться, что все впереди!

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галкина А. Интеллектуальное видеонаблюдение // Полиция России. 2014. № 2.
2. Пашута И. Использование систем видеонаблюдения в раскрытии и расследовании преступлений // Законность и правопорядок. 2011. № 1 (17).
3. «Безопасный город» глобальный проект по охране и жизнеобеспечению жителей мегаполиса [Электронный ресурс]. – Режим доступа: http://www.secuteck.ru/articles2/Sys_svyazi/safe_city.
4. Безопасный город – современная среда обитания [Электронный ресурс]. – Режим доступа: http://www.itv.ru/company/.
5. Безопасный город – структура системы [Электронный ресурс]. – Режим доступа: http://www.mrantenna.ru/.
6. В Белгороде сотрудники полиции раскрыли два грабежа [Электронный ресурс]. – Режим доступа: http://31.mvd.ru/.
7. В Москве заработала система видеонаблюдения «Безопасный город» [Электронный ресурс]. – Режим доступа: http://www. kp.ru/daily/.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВА: ПОНЯТИЕ, УГРОЗЫ И ФАКТОРЫ

INFORMATION SECURITY OF THE STATE: CONCEPT, THREATS AND FACTORS

Безуглый Эдуард Александрович,
Шапошников Виталий Леонидович,
Шумский Виктор Васильевич
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Bezugly Eduard Alexandrovich,
Shaposhnikov Vitaliy Leonidovich,
Shumskiy Victor Vasilievich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin)

Аннотация: в данной статье рассматриваются вопросы определения понятий информационная безопасность, уделяется особое внимание факторам, угрозам и источникам угроз информационной безопасности Российской Федерации.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, защита информации, защищенность информационных ресурсов.

Annotation: this article discusses the definition of information security, with particular emphasis on the factors, threats and sources of threats of information security of the Russian Federation.

Key words: information security, information security threats, information security, security of information resources.

В настоящее время в Российской Федерации наблюдается повышенный интерес к информационной безопасности. Поэтому проблема защиты информации в ЭВМ, обеспечения безопасности автоматизированных систем и информационно-вычислительных сетей находится в центре внимания не только специалистов по разработке и эксплуатации этих систем, но и широкого круга пользователей.

Информационная безопасность является специфичным компонентом национальной безопасности, проблемы которой обозначились только в конце XX века. Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

В современном российском государстве информационная безопасность регламентируется Федеральным законом от 27.07.2006 № 149-ФЗ (в ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.11.2017).

За последние годы в Российской Федерации реализован определенный комплекс практических мер по укреплению информационной безопасности страны. Так, начато формирование нормативной правовой базы обеспечения информационной безопасности.

В настоящее время она включает в себя более 80 законов и свыше 200 других нормативных правовых актов. Также развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти. Созданы государственные системы защиты государственной тайны и информации, системы лицензирования деятельности организаций в области защиты информации и системы сертификации средств защиты информации.

В повседневной жизни часто информационная безопасность понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации.

Существует много разных определений информационной безопасности, в которых указываются отдельные ее свойства, которые представлены в таблице 1 (см. табл. 1).

Таблица 1

Информационная безопасность – это:
комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей
состояние защищенности информационной среды
показатель, отражающий статус защищенности информационной системы
состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации
защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных действий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры

Основными аспектами проблемы обеспечения информационной безопасности являются определение, анализ и классификация возможных угроз.

Угроза безопасности информации – это события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Рассмотрим *виды угроз информационной безопасности,* к которым можно отнести следующее*:*

- нарушение технологии обработки информации;
- утечка информации по техническим каналам;
- использование несертифицированных средств информационной инфраструктуры;
- противоправный сбор и использование информации;
- внедрение в аппаратные средства и программные изделия нерегламентированных компонентов;
- внедрение электронных устройств перехвата информации в помещениях и системах;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств информационной инфраструктуры;
- навязывание ложной информации.

Основными направлениями деятельности государства по защите информации являются:

- *правовое обеспечение*, представляющее собой взаимосвязанный комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов правоотношений, субъектов и объектов защиты, методы, формы и способы защиты и их правовой статус;
- *организационное обеспечение*, которое представляет собой комплекс взаимосвязанных мероприятий, реализующих практические механизмы защиты;
- *техническое обеспечение*, которое представляет собой комплекс взаимосвязанных технических мер, реализующих аппаратно-программные механизмы защиты.

Организация обеспечения безопасности информации должна носить комплексный характер и основываться на глубоком анализе возможных негативных последствий. При этом важно не упустить какие-либо существенные аспекты. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и, как следствие, определение актуальных угроз безопасности информации.

В ходе такого анализа необходимо убедиться, что все возможные источники угроз идентифицированы, идентифицированы и сопоставлены с источниками угроз все возможные факторы (уязвимости), присущие объекту защиты, всем идентифицированным источникам и факторам сопоставлены угрозы безопасности информации (см. табл. 2).

Угрозы сами по себе не проявляются. Все угрозы могут быть реализованы только при наличии каких-нибудь слабых мест – уязвимостей, присущих объекту информатизации.

Таблица 2

Информационные угрозы, могут быть обусловлены:	
1. Естественные факторы	*стихийные бедствия*: пожар, наводнение, ураган, молния и др.
2. Человеческие факторы	*угрозы, носящие случайный, неумышленный характер:* ошибки процесса подготовки, передачи и хранения информации; нецеленаправленная «утечка мозгов», знаний, информации; ошибки в настройках и работе аппаратуры; ошибка процесса подготовки и обработки информации; *угрозы, обусловленные умышленными, преднамеренными действиями:* передача, искажение и уничтожение научных изобретений, открытий, новых технологий по корыстным или другим антиобщественным мотивам; подслушивание и передача служебных и других научно-технических и коммерческих разговоров; целенаправленная «утечка мозгов», знаний, информации

Уязвимость – это некая слабость, которую можно использовать для нарушения информационной автоматизированной системы или содержащейся в ней информации. Особое внимание при рассмотрении информационной безопасности должно уделяться *источникам угроз*, в качестве которых могут выступать как субъекты (личность), так и объективные проявления. Данные источники угроз информационной безопасности представлены в таблице 3 (см. табл. 3).

Таблица 3

Источники угроз информационной безопасности Российской Федерации	
- деятельность иностранных структур против интересов Российской Федерации в информационной сфере;	- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- стремление ряда стран к доминированию в мировой информационной среде;	- усиление технологического отрыва ведущих держав мира;
- обострение международной конкуренции за обладание технологическими и информационными ресурсами, рынками их сбыта;	- недостаточная координация деятельности федеральных органов исполнительной власти в области обеспечения информационной безопасности России;
- деятельность международных преступных сообществ, организаций и групп;	- разработка рядом государств концепций информационных войн;
- неблагоприятная криминогенная обстановка;	- разрушение отечественных отраслей электронной промышленности;
- разрушение системы образования и воспитания;	- отставание России от ведущих стран мира в области кредитно-финансовой сферы, промышленности, здравоохранения, образования и сферы услуг.

По нашему мнению, недооценка угроз информационной опасности может привести к сдерживанию процессов развития системы национальной безопасности и серьёзно осложнить задачи государственного управления страной.

Несмотря на то, что современная Россия оказалась под военным, экономическим, демографическим и информационным давлением со стороны других мировых центров силы, наша страна сохранила особое место в геополитическом пространстве. Однако изменения политической обстановки в современном мире требуют и переосмысления вопросов обеспечения информационной безопасности российского государства. В противном случае Россия может разделить судьбу Советского Союза, не сумевшего защитить и укрепить потенциал государства, утратившего свой политический статус, лидерскую позицию и ведущую роль в мировой и региональной политике.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гафнер В.В. Информационная безопасность: учебное пособие. – Ростов н/Д: Феникс, 2010.

2. Калинина М.Н. Экономическая безопасность региона: сущность, угрозы и меры обеспечения // Сибирский торгово-экономический журнал. 2010. № 10. С. 25-28.

3. Котухов М.М., Кубанков А.Н. Калашникова А.О. Информационная безопасность: учебное пособие. – М.: Академия ИБС: МФТИ, 2009.

4. Кирьянов А.Ю. Сущность информационного аспекта национальной безопасности Российской Федерации // Государственная власть и местное самоуправление. 2005. № 6. С. 34-35.

АНАЛИЗ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

THE ANALYSIS OF MODERN TECHNOLOGIES IN THE SYSTEM OF ENSURING INFORMATION SECURITY ON RAILWAY TRANSPORT

Александров Алексей Николаевич
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Александров Евгений Николаевич
(ООО «Парусник-Белгород»)

Aleksandrov Alexey Nikolaevich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin);
Aleksandrov Evgeniy Nikolaevich
(Open Company «The Sail boat-Belgorod»)

Аннотация: в данной статье рассматриваются существующие и функционирующие системы обеспечения информационной безопасности на объектах железнодорожного транспорта в нашей стране. На основе анализа функционирующих систем приводятся различные способы совершения потенциальных атак на информационные системы, обеспечивающие безопасное функционирование транспортных средств и объектов транспортной инфраструктуры железнодорожного транспортного комплекса.

Ключевые слова: информационная безопасность, железная дорога, информационные системы, транспортная безопасность, транспортные средства, платформа, автоматизация.

Annotation: this article discusses existing and functioning system of information security on objects of railway transport in our country. Based on the analysis of functioning systems are the different ways of committing potential attacks on the information systems ensuring the safe operation of vehicles and transport infrastructure the railway transport sector.

Key words: information security, railway, information systems, transport safety, vehicle, platform, automation.

Данная статья посвящена рассмотрению систем безопасности, которые могут применяться на современных высокоскоростных поездах.

С каждым годом число таких платформ растет и совершенствуется. Хоть такие системы и строятся на основе известных технологий, включая Ethernet, CAN, RS-485 и другие стандарты, часто начинают применяться различные программируемые контроллеры и промышленные компьютеры под управлением ОС Windows и Linux. Также растет популярность систем, использующих радиоканал, например GPS/ГЛОНАСС, GSM-R, Wi-FI и другие [4].

В связи с этим можно отметить, что безопасность огромной системы на основе стандартов, которые хорошо знакомы возможным злоумышленникам, не является достаточно защищенной.

Например, потенциальные уязвимости в GSM-R. Стандарт GSM-R адаптирован для железных дорог таким образом, что зона покрытия простирается вдоль железной дороги. Но стоит обратить внимание на то, что все уязвимости, присутствующие в GSM-R, опасны, а эта технология активно используется для регулирования движения высокоскоростных поездов.

Сигнал GPS можно простым способом заглушить. Если зайти в чащу леса или в какое-либо подвальное помещение, с большой долей вероятности GPS-приемник потеряет спутники, и даже делать ничего не придется. Можно смоделировать ситуацию, когда злоумышленник не только глушит сигнал, но и подменяет данные так, что принимающая сторона получает совершенно другие координаты. А местоположение поезда используется для расчета подвижных блок-участков [2].

В современных поездах используется Wi-Fi. Это, конечно, очень удобно для пассажиров, но не стоит забывать, что стандарт IEEE 802.11 отлично известен злоумышленникам, и его можно легко скомпрометировать. В настоящее время Wi-Fi/Ethernet начинает доминировать при построении Train Communication Network. Таким образом, может сложиться ситуация, когда злоумышленник, подключившись к Wi-Fi в вагоне, получит доступ и к другим узлам на шине MVB/WTB. А разных случаях данные узлы обладают хорошей производительной мощностью.

Еще один из возможных векторов атак – атаки на компьютеры, к которым подключается различное мобильное диагностическое оборудование, «наблюдающее» за работой всех деталей подвижного состава. И потому кажется не очень удачной идеей после каждой поездки отправлять поезд на диагностику по причине некорректной работы мобильного оборудования [6].

Также не стоит забывать о сценарии, когда оборудование заражается вредоносным ПО различными способами, что приводит к утечке информации к злоумышленникам либо шифрованию данных.

До появления автоматических распределенных систем, спутниковых систем логистика осуществлялась вручную: прежде чем отправить поезд, диспетчер звонил на следующую станцию и узнавал – свободен ли перегон, прошел ли предыдущий поезд. Да и на поездах тех времен было немного систем, взаимодействующих между собой, машинистом и диспетчером.

Условно это «разнообразие» можно разделить на несколько категорий:

– диспетчерская автоматика;
– железнодорожная автоматика (бортовая);
– железнодорожная автоматика (путевая).

Также следует отметить, что зачастую бортовая и путевая железнодорожная автоматика является единым программно-аппаратным комплексом, часть которого размещена на поезде, а другая часть – на железнодорожных путях, как клиент-серверная система [8].

В 1999 году принят международный стандарт IEC 61375, который базируется на TCN – Train Communication Network. На момент принятия TCN состоял из двух шин:

– MVB – Multifunction Vehicle Bus – бортовая сеть единицы подвижного состава (это может быть вагон, локомотив);

– WTB – Wire Train Bus – поездная сеть, объединяющая MVB-части в единую систему управления поездом.

В 2014 году был принят новый стандарт, IEC 61375-2-5, который призван заменить WTB на ETB – Ethernet Train Backbone.

В Европе популярен железнодорожный транспорт. Но в каждой стране есть свои стандарты обеспечения безопасности на железной дороге; кроме этого, имеются конструктивные отличия размещения различных датчиков, обеспечивающие аналогичные логические функции. В компании ОАО «РЖД» на новейших участках дороги используется стандарт «ETCS – European Train Control System». Для безболезненного перехода на новый единый стандарт разработано несколько уровней.

ETCS первого уровня. На данном этапе отсутствует применение радиоканала для ведения поезда. Применяются различные системы контроля занятости блок-участка (рельсовая цепь или счетчик осей). Используются реперные точки с фиксированной информацией или с переменной информацией для определения местоположения поезда, дублирование сигналов светофора.

ETCS второго уровня. Использование радиоканала для передачи координат и статуса поезда, разрешение на движение, данные о предстоящем блок-участке. Данные дублируются путевой автоматикой, в частности, на основе устройств контроля загруженности путей.

ETCS третьего уровня. Осуществляется полное ведение поезда по радиоканалу. Переход от фиксированных блок-участков к динамическим. Таким образом, расстояние между поездами можно сократить до необходимого и безопасного, оптимального для торможения поезда [3].

Далее рассмотрим более детально схему, которая может применяться на современных поездах, а также различные системы автоматизации, которые используются для обеспечения безопасности и комфорта пассажиров.

Локомотивная телеметрическая система

Одна из платформ – локомотивная телеметрическая система (см. рис. 1). Как можно увидеть на рисунке, при построении данной системы используются широко распространенные протоколы, в том числе, CAN, Ethernet, RS-232, RS-485. Могут применяться промышленные Ethernet-коммутаторы.



Рисунок 1. Локомотивная телеметрическая система

Одной из платформ, отвечающих за безопасность на перегоне, является система КЛУБ-У, состоящая из различных устройств. Основные функции, выполняемые данной системой: исключение несанкционированного движения локомотива; сравнение фактической скорости с допустимой (при превышении допустимой скорости происходит включение сигнала «Внимание» и снятие напряжения с электромагнита ЭПК); контроль торможения перед запрещающим сигналом светофора; формирование сигналов для системы автоматического управления тормозами САУТ; контроль бдительности машиниста; регистрация параметров движения [5].

«АЛС» – автоматическая локомотивная сигнализация (см. рис. 2).

В состав системы входят напольные передающие устройства, приёмные и дешифрующие приборы на подвижном составе, а также устройства, согласующие работу АЛС с другими компонентами сигнализации и блокировки, индикаторы, датчики и исполнительные устройства на подвижном составе. Входит в состав системы КЛУБ-У.

Принцип действия данной системы следующий: путевая автоматика через рельсовую цепь передает сигнал на определенной частоте о сигнале светофора. Аппаратура, находящаяся на локомотиве, осуществляет прием сигнала из рельсовой цепи, его декодирование с последующей передачей на локомотивный светофор, в систему контроля бдительности машиниста и другой вспомогательный опционал.

Помимо определения свободных блок-участков перед поездом, необходимо проводить самодиагностику и мониторинг поезда. В частности, должна постоянно работать система мониторинга состояния колесных пар. Она отвечает за измерение скорости, вибрации и прочих параметров колесных пар и, в случае отклонения от нормы, формирует сообщения, результатом которых может быть направление на диагностическое обслуживание после прибытия на конечную станцию [7].

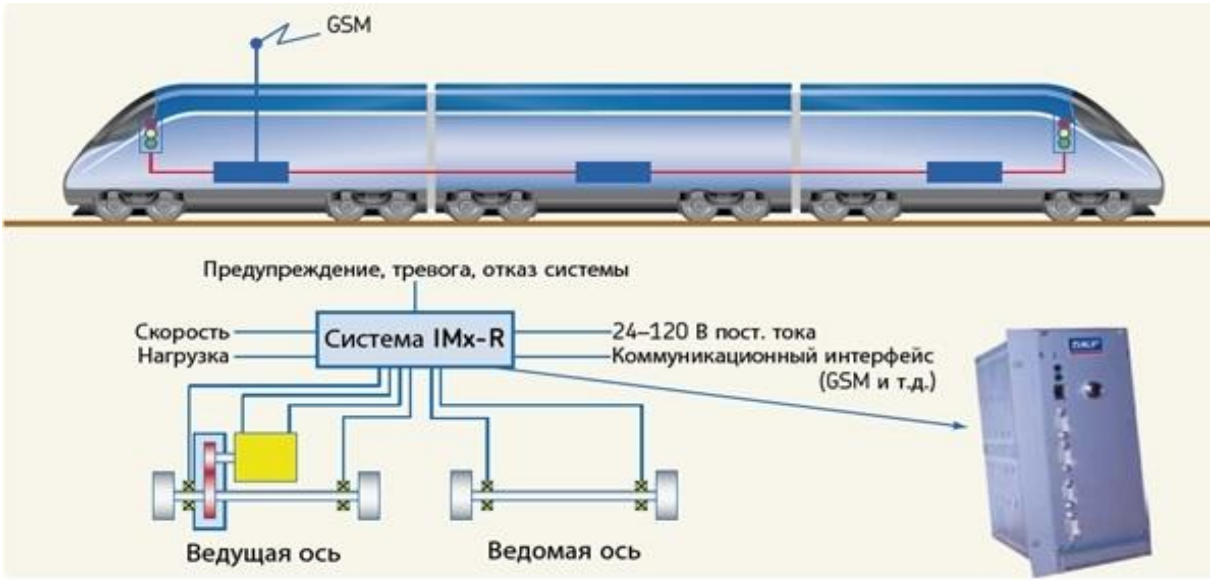


Рисунок 2. Автоматическая локомотивная сигнализация

Электронные билеты и электронная регистрация на поезд – эта процедура в настоящее время используется чаще, чем процедура покупки билетов в кассе вокзалов. Но высокоскоростные поезда в своем арсенале непременно имеют и систему учета и анализа пассажиропотока.

Существует множество систем диагностики, некоторые из которых реализованы в мобильном исполнении (см. рис. 3).



Рисунок 3. Оборудование, используемое для диагностики

Данное оборудование может эксплуатироваться в составе контрольно-проверочной аппаратуры (КПА) комплексных локомотивных устройств безопасности КЛУБ-У. Может имитировать сигналы включения устройств управления локомотивом, сигналы датчиков скорости, телеметрической системы контроля бдительности машиниста, сигналы АЛС.

Выше был представлен небольшой перечень различных систем, которые могут использоваться на поездах. В частности, в России есть пока только один высокоскоростной поезд – «Сапсан», построенный на базе немецкого ICE.

(Intercity-Express). Ниже предоставлена функциональная схема системы управления поездом «Сапсан». И, как уже было сказано, она состоит из модулей MVB, которые объединяются в поездную шину WTB [9].

Система поезда построена на основе SIBAS 32. Сама система SIBAS была разработана для железнодорожного транспорта еще в 1983 году немецкой компанией Siemens. В 1992 году SIBAS16 была модернизирована до SIBAS32, которая в настоящий момент применяется в таких поездах, как «Сапсан» и «Ласточка».

В 2008 году система была модернизирована до SIBAS PN, и ожидается, что первый поезд под управлением данной системы будет пущен в 2016 году. Основное различие между SIBAS 32 и SIBAS PN – в том, что SIBAS32 был основан на Intel 386/486 CPU с применением закрытой ОС SIBAS OS, в то время как SIBAS PN базируется на Power PC и Intel Atom CPU. В качестве среды разработки применяется Simatic Step 7.

Основные свойства SIBAS PN – модульность, соответствие промышленным стандартам, автоматическая адресация, независимость ПО от аппаратной платформы, наличие возможности регистрации и мониторинга через WEB-интерфейс.

Также отмечается независимость от аппаратной платформы, которая достигается за счет применения ОС жесткого реального времени VxWorks и WinAC. Хочется сразу подчеркнуть, что для VxWorks имеется ряд известных уязвимостей, и до 6 версии используется единое адресное пространство. Как показывает практика, на многих современных устройствах используются старые версии данной операционной системы, что может очень негативно сказываться на информационной безопасности.

Проанализировав, из каких информационных систем состоят современные поезда, рассмотрим возможные векторы атак на них.

Как было сказано выше, для ведения поезда и передачи телеметрии используется GSM-R. Через этот канал связи передаются данные о координатах поезда, его скорости, осуществляется прием информации, связанной с подвижными блок-участками. А теперь представьте ситуацию, при которой на поезд поступает информация, что следующие несколько перегонов свободны, а по факту за «ближайшим поворотом» поезд нагоняет впереди идущий состав, т.к. в диспетчерском пункте имеются неверные данные о местонахождении впередиидущего поезда. Такой сценарий атаки нельзя назвать «фантастическим» в силу того, что принципиальных отличий между GSM и GSM-R нет. Основное отличие этих двух стандартов – зона покрытия. Для GSM она представлена как круговая площадь, в центре которой находится базовая станция, для GSM-R – простирается вдоль железной дороги. Помимо этого, согласно требованиям, которые выдвигаются к GSM-R при построении ETCS, должно обеспечиваться двойное перекрытие каждого участка, и, в случае сбоя радиосвязи, поезд должен переключаться в защитный режим вплоть до экстренного торможения [10].

Другим возможным вектором атак может служить различное воздействие на путевую автоматику, взаимодействующую с поездом. Как пример, потенци-

ально возможно подключиться к путевой системе АЛС и получить доступ к внесению изменений в кодовые посылки импульсов.

В результате будет перекодирован сигнал, запрещающий проезд на следующий блок-участок. К этому может привести ложная остановка подвижного состава.

Поскольку в современных поездах применяются такие технологии, как Ethernet и Wi-Fi, которые очень хорошо поддаются компраментации, не стоит исключать и вариант подключения к Ethernet или к Wi-Fi и возможности перепрограммирования различных узлов на основе небезопасного протокола SNMP. Кроме того, у злоумышленника есть прямая возможность подключиться к инфраструктуре поезда, если применяется система анализа пассажиропотока, и тем самым потенциально получить доступ к любому устройству сети.

Для снижения риска от такого рода атак необходимо как минимум проводить сегментацию сети. Некоторые узлы отличаются высокой производительной мощностью. Также осуществляется переход к неким единым и унифицированным системам на основе архитектуры x86/ARM с применением известных операционных систем, например, Linux или Windows, которые, в свою очередь, имеют уязвимости. К сожалению, на промышленное оборудование, находящееся в эксплуатации, не всегда распространяются последние обновления, закрывающие найденные уязвимости.

Может сложиться ситуация, когда происходит атака на компьютер, взаимодействующий с различным диагностическим оборудованием, подключающимся в дальнейшем к системам автоматики, установленным на поезде.

Абсолютно изолированных систем не бывает. В сфере различных объектов АСУ ТП часто бывают инциденты, когда постоянно находятся способы подключения извне. Таким образом, можно предположить, что к компьютерам, к которым подключается различное диагностическое оборудование, тоже можно получить доступ извне. Как результат – возможное заражение компьютера с последующим изменением конфигурации мобильного диагностического оборудования. После этого будет оказано влияние на работу бортовых систем поезда [1].

В каждой системе, будь то программный продукт или какое-либо запрограммированное устройство, есть возможность модификации прошивок по пути следования оборудования от производителя до конечного заказчика.

Часто, помимо удаленных способов конфигурирования и настройки оборудования через специальное ПО, к аппаратуре можно получить непосредственный доступ, подключившись через RS-232. Далее злоумышленник завладеет достаточно широкими возможностями по изменению конфигурации оборудования. Вплоть до обновления прошивки. Зачастую на практике отсутствует контроль подлинности прошивок оборудования. Это может обернуться тем, что атакующий подменит прошивку на самом низком уровне. В итоге по поведению нельзя будет отличить исправное оборудование от зараженного до момента получения «критического» пакета данных.

К сожалению, проблема целостности и подлинности прошивок различного оборудования характерна для многих отраслевых областей.

Итак, начинают доминировать широко известные технологии при построении TCN, включая Ethernet, Profinet. Можно наблюдать переход от закрытых архитектур к x86-подобной архитектуре. Идет переход от проприетарных ОС к широко известным ОС. Наблюдаются увеличение объема передаваемой информации между поездом и другими системами и рост систем автоматики, отвечающей за безопасность и комфорт пассажиров.

Хочется отметить, что многие технологии, которые используются в современном высокоскоростном поезде, по отдельности уже хорошо изучены и скомпрометированы. Поезд представляет собой агрегацию таких технологий в единое целое, поэтому для реализации различного рода атак злоумышленникам придется пройти путь компрометирования сразу нескольких систем, учитывая специфику железной дороги.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Амельчаков И.Ф., Прокопенко А.Н., Жукова П.Н. и др. Особенности использования информационных технологий в органах внутренних дел на транспорте: учебное пособие. – Белгород, 2016.
2. Гнаденберг В.С. Роль информационной безопасности в обеспечении безопасности перевозочного процесса / Транспорт-2012: труды Всероссийской научно-практической конференции: в 3-х ч. – Ростов н/Д, 2012.
3. Горелик В. Как защитить транспортное киберпространство // Мир транспорта. 2014. Т. 12. № 2 (51). С. 258-261.
4. Дружинина О.В., Сычев В.П., Черкашин Ю.М., Качалкин В.В. Теоретические аспекты оценки безопасности систем железнодорожного транспорта // Внедрение современных конструкций и передовых технологий в путевое хозяйство. 2014. Т. 7. № 7 (7). С. 168-181.
5. Замышляев А.М. Прикладные информационные системы управления надежностью, безопасностью, рисками и ресурсами на железнодорожном транспорте / Прикладные информационные системы управления надежностью, безопасностью, рисками и ресурсами на железнодорожном транспорте. – Ульяновск, 2013.
6. Замышляев А.М. Технология анализа и оценки рисков в эксплуатационной работе ОАО «РЖД» на основе показателей эксплуатационной надежности и безопасности // Ядерные измерительно-информационные технологии. 2011. № 2. С. 86-100.
7. Лахно В.А. Обеспечение информационной безопасности корпоративных систем на железнодорожном транспорте // Известия Волгоградского государственного технического университета. 2014. Т. 20. № 6 (133). С. 131-136.
8. Мыльников П.Д., Попов П.А. Информационная безопасность в европейских системах управления движением на железнодорожном транспорте интеллектуальные технологии на транспорте. 2016. № 3 (7). С. 50-55.
9. Нигрей А.А. Информационная безопасность в железнодорожных интеллектуальных транспортных системах / Организация и безопасность дорожного движения: материалы X международной науч.-практ. конференции: в 2 т. – Тюмень, 2017.
10. Розенберг Е.Н. Инновационные системы управления и обеспечения безопасности движения поездов в холдинге ОАО «РЖД» / Новое в науке и образовании: сборник трудов ежегодной международной научно-практической конференции. – М., 2016.

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ СУДЕБНО-АГРОТЕХНИЧЕСКИХ И ЗООТЕХНИЧЕСКИХ ЗНАНИЙ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА

THE USE OF A SPECIAL COURT-AGRONOMICAL AND ZOOTECHNICAL KNOWLEDGE IN THE INVESTIGATION OF CRIMES IN THE FIELD OF AGRICULTURE

Чиненов Евгений Владимирович,
Чиненов Алексей Владимирович,
Чернышёв Сергей Анатольевич
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Chenenov Evgeniy Vladimirovich,
Chenenov Aleksey Vladimirovich,
Chernyshov Sergey Anatolvich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin)

Аннотация: в данной статье рассматриваются аспекты использования специальных судебно-агротехнических и зоотехнических знаний в расследовании преступлений в сфере агропромышленного комплекса.

Ключевые слова: агротехнические знания, весовые нормы посева, мошеннические схемы, оперативно-следственная практика, сельхозпродукция, экспертно-криминалистические подразделения.

Annotation: this article discusses aspects of the use of special forensic agrotechnical and zootechnical knowledge in investigation of crimes in the sphere of agriculture.

Key words: agronomic knowledge, the weight norm of sowing, fraud schemes, investigative practices, agricultural products, forensic units.

Одним из направлений совершенствования правоохранительной работы по пресечению и профилактике преступлений, совершаемых в различных отраслях экономики по производству и переработке сельскохозяйственного сырья и получения от него продукции, доводимой до конечного потребителя, является укрепление следственных, оперативных и экспертно-криминалистических подразделений высокопрофессиональными, подготовленными кадрами. Для этого, как справедливо отмечают А.И. Бастрыкин, А.Ф. Волынский, В.А. Прорвич, необходимы не только современные информационные технологии, но и специальные знания в различных областях, позволяющие создавать модельное представление о содержательных особенностях расследуемого преступления [4, с. 9].

Совершенствование практики выявления, раскрытия и расследования преступлений в области агропромышленного комплекса требует специальных знаний, заключений компетентного лица (специалиста), назначения и производства разноплановых судебно-экспертных исследований сельскохозяйствен-

ных объектов (агротехники, агрохимии, животноводства, растениеводства, переработки сельхозпродукции), площадей, производственных территорий, документов. Действия специалиста сводятся преимущественно к обнаружению, фиксации, изъятию, осмотру вещественных доказательств, консультированию следователей при подготовке и назначении экспертизы и оценке имеющихся в деле материалов. Эксперт, в свою очередь, своим заключением помогает следователю и суду выяснить обстоятельства дела.

Система специальных судебно-агротехнических знаний, используемых при раскрытии и расследовании специфических по способу совершения преступлений в сфере агропромышленного комплекса, имеет сложную структуру.

Эта система включает в себя профессиональные знания (см. табл. 1).

Таблица 1

Виды профессиональных знаний

Агротехнические знания	**Зоотехнические знания**
1	2
о планировании и анализе производственных процессов (полевых работ, их последовательности, начале и окончании, содержании)	о разведении, кормлении, содержании сельскохозяйственных животных
о биологических особенностях возделывания растений	о физиологических особенностях сельскохозяйственных животных
о почвенно-климатических условиях региона	о максимальной и качественной продуктивности
о наиболее эффективном использовании удобрений	о правильном использовании сельскохозяйственных животных
о посадочных материалах, сортовых посевах, и семенном фонде	о техническом обеспечении процессов производства
о хранении фондов семян и готовой продукции	о гигиене и рациональном проектировании знаний
о технологиях борьбы с вредителями и болезнями растений	о технологии производства продукции, получаемой от конкретных видов животных (мясо, рыба, молоко, мед, шерсть, кожа и пр.)
о химических, биологических и других средствах защиты	о разведении и генетике сельскохозяйственных животных

Использование специальных агротехнических и зоотехнических знаний становится все более востребованным при расследовании следующих совершаемых в сфере сельского хозяйства преступлений (см. схему 1).

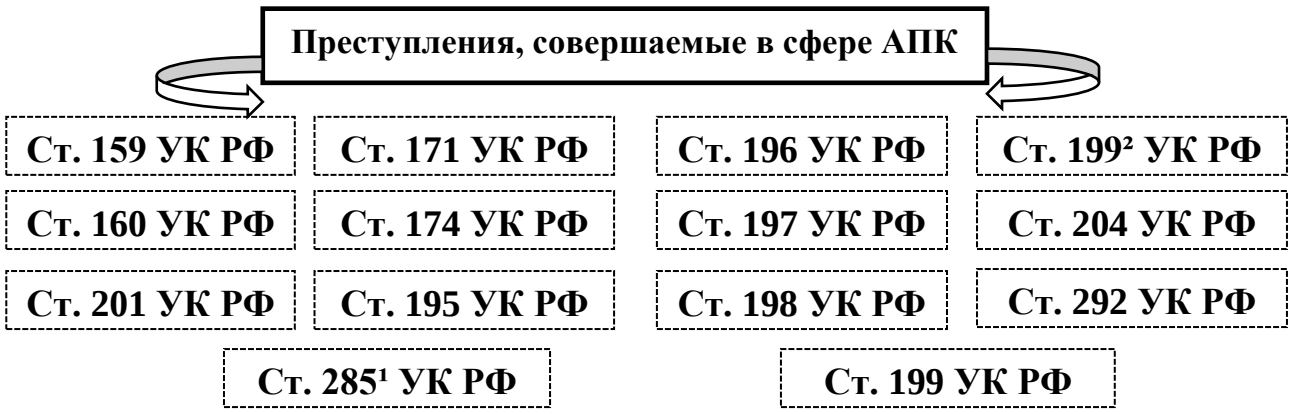


Схема 1. Преступления, совершаемые в сфере сельского хозяйства

Безусловно, каждое преступление в сфере агропромышленного комплекса индивидуально, а потому с учетом изменяющихся в стране экономических условий совершенствуются и видоизменяются способы совершения преступлений, а также тактика их раскрытия и расследования [6, с. 167-173].

Анализ практики органов предварительного следствия системы МВД России в сфере агропромышленного комплекса показывает, что наиболее часто расследуются преступления, предусмотренные ст. 159 УК РФ.

Мошеннические схемы хищений денежных средств, выделяемых на развитие сельскохозяйственных субъектов, призванных стимулировать развитие растениеводства и животноводства, являются типичными для большинства регионов страны и причиняют достаточно крупный ущерб собственникам и государству. Их достаточно подробно описывает в своей работе М.Е. Репин, указывая на значительную часть преступных действий мошеннического характера в сфере агропромышленного комплекса [5, с. 177-180].

Преступные действия мошеннического характера также занимают значительное место в ходе подготовки и осуществления агротехнических и зоотехнических работ, составляющих основу сельскохозяйственного производства. Под сельскохозяйственным производством здесь следует понимать центральное звено агропромышленного комплекса страны, комплекс видов экономической деятельности по выращиванию, производству и переработке сельскохозяйственной продукции, в том числе оказание соответствующих услуг, главным образом в двух базовых сельскохозяйственных направлениях деятельности – растениеводстве и животноводстве [1].

Мошенничество, совершенное в ходе сельскохозяйственных производственных процессов, следует рассматривать как один из видов хищений государственной или иной собственности.

Изучение оперативно-следственной практики позволяет говорить о существовании следующих мошеннических схем.

1. В рамках реализации приоритетного национального проекта «Развитие агропромышленного комплекса»:

- получаются кредиты и субсидии для приобретения сельскохозяйственных животных (в том числе, скота обладающего племенными качествами).

В подтверждение факта осуществления сделок представляются подложные договоры купли-продажи сельскохозяйственных животных, предъявляются требования административным органам сельского хозяйства региона о возмещении процентной ставки по кредиту за счет выделяемых на реализацию национального проекта бюджетных средств;

- осуществляются хищения денежных средств посредством подготовки фиктивных документов о наличии поголовья скота, запасов сельхозпродукции на складах, отвечающих определенным качественным и количественным показателям, обеспечивающим возможность льготного субсидирования финансово-хозяйственной деятельности;

- под видом реконструкции производственно-хозяйственных помещений и площадей агоротехнического и зоотехнического профиля осуществляются хищения денежных средств, получаемых в качестве целевых кредитов, с требованием возмещения выплат.

2. В рамках финансово-хозяйственной деятельности сельскохозяйственного предприятия в сфере растениеводства:

- хищения продукции в ходе посевных компаний лицами, осуществляющими перевозку семян, зерна, к посевным агрегатам посредством припрятывания части груза;

- хищения семян из сеялок в процессе высева;

- хищения семенного материала путем создания неучитываемых резервов посредством регулировки параметров меньшего высева посевных машин;

- припрятывание части семенного материала перед агрохимической обработкой, предшествующей посевным работам;

- создание неучтенных излишков семян за счет искажения количественных показателей высеваемого материала на единицу площади (норма высева на гектар) с учетом таких факторов, как вид культуры, сорт, способ посева, почвенно-климатические условия. Нормы посева устанавливаются опытным путем индивидуально. Примерный расчет может выглядеть так. Необходимое количество семян на 1 га посевной площади определяется путем умножения веса 1000 выборочных зерен на норму высева с последующим делением полученного результата на 1000. *Например, при нормативе посева зерновой культуры (ячмень) 7 млн зерен и абсолютном весе 1000 семян в 30 г норма веса будет равна 210 кг на 1 га. При посевной годности семенного материала 95% необходим 221 кг зерна на 1 га.*

Преступники (агрономы и лаборанты) в документах искусственно завышают весовую норму посева путем увеличения абсолютного веса 1000 семян и занижения процента их посевной годности и, как следствие, всхожести;

- хищения резервов сырья, создаваемого за счет искажения в документах (актах расходования семян) способа высева (узкорядный, перекрестный, сплошной). В первых двух случаях, зависящих от качества и подготовленности почвы, используемых средств агротехники и агрохимии, она увеличивается до 20%;

- завышение площади фактического высева семенного материала;

- вынужденный пересев погибшего первичного посева под воздействием неблагоприятных природно-климатических условий;

- составление фиктивных документов на вымокание, вымерзание, выветривание семян;

- нарушение мер и весов весоизмерительного оборудования;

- искусственное повышение влажности сельскохозяйственной продукции;

- хищения урожая механизаторами и водителями в результате неоприходования его части, маскируемые ремонтом, отдыхом, переездом к новому месту обмолота;

- завышение фактического веса примесей (засоренности) в зерне;

- пересортица высококачественного продукта;

- завышение веса тары;

- списание продукции под видом подложных документов на усушку, гниль, превышение норм естественной убыли.

3. В рамках финансово-хозяйственной деятельности сельскохозяйственного предприятия в сфере животноводства:

- хищения путем создания неучтенных излишков скота (например, в результате приплода);

- хищения с составлением подложных актов падежа, выбраковки скота;

- хищения за счет нарушения технологических операций аналогично сфере растениеводства.

Анализ такого рода материалов показывает, что при доказывании определенные сложности у следователя вызывает недостаточность специальных судебно-агротехнических и зоотехнических знаний в совокупности с экономическими, а также навыков и умений работы со специфическими документами, фиксирующими факты производственных процессов в сфере сельскохозяйственного производства.

По объекту преступления предварительным следствием устанавливается, было ли на самом деле посягательство, и если было, то на какую форму собственности (государственную, частную и пр.) оно было направлено.

Рассматривая объективную сторону квалифицированного мошенничества, следственным путем устанавливается время, место, условия преступного деяния. Наличие состава преступления подлежит определению только при установлении факта самого преступления, связанного с действиями преступника. Таким образом, в ходе расследования собираются доказательства, позволяющие выяснить, было ли в действительности событие, ставшее предметом расследования, а также носило ли оно противоправный характер.

В этой связи экспертным путем устанавливается вид экспертизы (см. табл. 2):

Таблица 2.

Виды сельскохозяйственных экспертиз

Судебно-агротехническая экспертиза	Судебно-зоотехническая экспертиза
1. Каковы наименование и качественные признаки данной сельскохозяйственной культуры (зерна, муки и пр.)? Соответствуют ли они тем, которые указаны в определенных документах?	1. Какое количество кормов для сельскохозяйственных животных было необходимо данному хозяйству в данный период времени?

2. Однородны ли между собой зерно (культура, мука), изъятое в одном месте, и зерно, изъятое в другом месте? Не исключается ли их принадлежность к одной массе? *Установлен следующий порядок отбора образцов для исследования:* *Образец зерна составляется из отдельных небольших выемок зерна, отбираемых щупом или руками. При хранении зерна насыпью выемки берутся щупом в пяти местах и с различной глубины (в верхнем слое, в середине и в нижнем слое) по три выемки в каждом месте (всего 15 выемок). При хранении зерна в таре выемки берутся щупом из трех мест каждого мешка (сверху, в середине, снизу). Для отбора целесообразно привлекать специалистов.* *Вес среднего образца должен быть для зерновых культур не менее 1 кг, для семян трав – 100-250 г, для овощных и фруктовых культур – 50-250 г, в зависимости от величины семян.* *Отобранный образец зерна (семян) следует поместить в чистый сухой мешочек. Внутрь мешочка следует вложить ярлык с указанием в нем даты, места взятия образца, сорта, веса партии и цели изъятия. Затем мешочек с зерном (семенами) необходимо завязать и опечатать, наклеив снаружи второй ярлык с теми же данными. Одновременно для анализа на влажность или зараженность зерна (семян) вредителями отбирается второй образец в стеклянную герметичную банку. Снаружи приклеивается такой же ярлык с теми же данными.* *Об изъятии образцов следователь составляет протокол в двух экземплярах, в котором указывает:* *- наименование организации, крестьянского-фермерского хозяйства, фамилии, имени, отчества лиц, у которых изъяты образцы;* *- название культур изымаемых образцов и их сорта по документам;* *- где и как хранятся подлежащие исследованию семена или зерно (насыпью, в таре и пр.);* *- вид и состояние хранилища, из которого изымаются образцы;* *- какие еще виды культур находятся в хранилище, и изолирована ли от них партия, от которой отобран образец, и как.*	2. Какое количество кормов с учетом их качества, числа животных и их состояния должно было быть израсходовано в данном хозяйстве в определенный период времени?

Желательно указать также вес партии семян или зерна, от которой отобран образец, когда и какой подработке подвергалась эта партия, когда были проверены семена и зерна на физические, биологические и посевные качества (приложить копию последнего анализа). *Эксперту представляются изъятые образцы и копия протокола.*	
3. Является представленное зерно (культура) урожаем нынешнего года или прежних лет? Соответствует ли оно тому, которое указано в определенных документах?	3. Правильны ли были методы определения пастбищной территории и кормовой массы на ней?
4. Является зерно культуры озимым или яровым, селекционным, гибридным растением? Принадлежит ли оно к определенному виду и сорту?	4. Правильно ли было организовано кормление сельскохозяйственных животных в данный период, и, если неправильно, то в чем это выразилось, и какие последствия она вызвала или могла вызвать?
5. Под посевом какой культуры находилось поле (участок)?	5. Правильно ли были составлены рационы кормления скота, и, если нет, то какие последствия это вызвало или могло вызвать?
6. Какова норма высева (посадки) при посеве (посадке) на данной площади определенной сельскохозяйственной культуры и какая норма была фактически применена?	6. Не является ли работоспособность (продуктивность) скота пониженной, и, если да, то не объясняется ли понижение работоспособности результатом неправильно организованного кормления?
7. Какой урожай определенной сельскохозяйственной культуры должен был быть собран с данной площади?	7. Хватило бы при правильной организации кормления сельскохозяйственных животных кормов?
8. Правдивы ли сведения, о том, что на данной площади высеяно такое-то количество сельскохозяйственной культуры?	8. Достаточно ли проведено зоотехнических мероприятий для сохранения поголовья скота от падежа или истощения?
9. Могла ли указанная сельскохозяйственная культура быть собрана с данного поля?	9. Не допускалось ли в данном хозяйстве нарушений зоотехнических правил ухода за животными, их кормления?
10. Правильно ли произведено списание зерна на отходы при сортировке и подработке?	10. Приспособлено ли данное помещение для содержания в нем определенного количества животных?
11. Могло ли протравливание зерна определенными химикатами повлиять на вес зерна?	11. Каков должен быть прирост поголовья скота за определенный период времени?
12. Обоснованно ли списано такое-то количеств зерна на естественную убыль во время хранения?	12. Соответствует ли фактическое наличие поголовья животных по признакам возраста, упитанности и другим учетным данным?
13. Подвергались ли семена, подготовленные для посева, сортированию, протравливанию, намачиванию и яровизации?	13. Какое количество и каких именно продуктов должно было получиться в результате забоя данного скота?
14. Были ли допущены при проведении сева нарушения агротехнических правил, в чем они заключались и какие последствия вызвали? *Для правильного разрешения указанного вопроса в распоряжение эксперта следует представить:*	14. Правильно ли было в хозяйстве организовано воспроизводство поголовья?

- документы о качестве семян, которыми произведен посев; *- документы, подтверждающие, что посев был произведен семенами, апробированными в контрольно-семенной лаборатории, или данные свидетелей, что семена анализу не подвергались;* *- документы по вопросу нормы высева и количества всеянных семян.*	
15. Правильно ли в данном хозяйстве осуществлялись предупредительные и истребительные меры борьбы с сельскохозяйственными вредителями и болезнями, в чем выразились нарушения и последствия? *Для разрешения указанного вопроса в распоряжение эксперта представляются:* *- данные о качестве семян, примененных при посеве;* *- данные о качестве обработки поля (участка);* *- данные об удобрениях, вносившихся в почву;* *- данные о времени начала сева и уборки;* *- данные о мероприятиях, осуществлявшихся в хозяйстве по предупреждению заражения растений и появлению вредителей сельского хозяйства.*	15. Соответствует ли выход продукции от данного продуктивного скота определенным нормам, и если нет, то какие причины могли повлиять на заниженный выход продукции? *Например: соответствует ли количество настриженной шерсти от данного числа овец тому количеству, которое было определено нормативами, если оно ниже, то каковы причины этого?*
16. Были ли допущены в данном хозяйстве при проведении уборки урожая и обмолота нарушения агротехнических правил, в чем они заключались и какие последствия вызвали? *Для разрешения вопроса в распоряжение эксперта следует представить:* *- документы и свидетельские показания, устанавливающие предварительные данные об урожае;* *- документы и свидетельские показания о способах уборки, техническом состоянии уборочных машин;* *- показания, документы о количестве обмолоченного зерна, средствах доставки его с тока на склад. Своевременно ли были начаты работы по уборке урожая и правильно ли была использована при этом сельскохозяйственная техника и рабочая сила?*	
17. Не явилась ли порча сельскохозяйственных культур на корню (или в процессе уборки) следствием нарушения агротехнических правил, и если да, то каких именно?	
18. Какова степень порчи сельскохозяйственных культур? Связана ли порча с условиями хранения?	

Особенностью решения вопросов, связанных с разведением, кормлением, содержанием и правильным использованием сельскохозяйственных животных и птиц, определением их племенных и производственных качеств, является необходимость назначения комплексных ветеринарных, зоотехнических, а в ряде случаев и бухгалтерских экспертиз (когда, например, имеется необходимость исследования процессов, связанных с финансированием искусственного осеменения скота, под видом которого осуществлялись хищения денежных средств, выделяемых на эти цели).

Выполнение перечисленных, а также иных, не менее трудоемких действий эксперта предопределит установление объективной стороны квалифицированного мошенничества при осуществлении производственных процессов в сфере сельскохозяйственного производства [2, с. 566-573; 3, с. 555-566].

Таковы, на наш взгляд основные вопросы, решаемые органом предварительного расследования и экспертом, реализующим специальные судебно-агротехнические и зоотехнические знания.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 29 декабря 2006 г. № 264-ФЗ «О развитии сельского хозяйства» // СПС «КонсультантПлюс».

2. Былинкина А.П. Ветеринарная и зоотехническая экспертизы / Настольная книга следователя. – М., 1949.

3. Блинкова А.В., Былинкина А.П. Агротехническая экспертиза / Настольная книга следователя. – М., 1949.

4. Организация и методика расследования отдельных видов экономических преступлений: учебно-методическое пособие / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. – М.: Спутник+, 2016.

5. Репин М.Е. Характеристика преступлений мошеннического характера, совершаемых в сфере агропромышленного комплекса // Вестник Нижегородской академии МВД России. 2015. № 2 (30). С. 177-180.

6. Янин С.А. К вопросу об организации расследования преступлений в сфере агропромышленного комплекса // Юридическая наука и правоохранительная практика. 2016. № 4 (38).

СЕКЦИЯ № 3.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ, КРИМИНАЛИСТИКЕ, БОРЬБЕ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ ДЛЯ РЕШЕНИЯ ЗАДАЧ СУДЕБНОЙ ФОТОГРАФИИ И ВИДЕОЗАПИСИ

THE USE OF MODERN VIRTUAL REALITY DEVICES FOR SOLVING THE PROBLEMS OF FORENSIC PHOTOGRAPHY AND VIDEO RECORDING

Трущенков Игорь Владимирович,
Кузовлев Владислав Юрьевич
(Московский университет МВД России имени В.Я. Кикотя)

Trushchenkov Igor Vladimirovich,
Kuzovlev Vladislav Yuryevich
(Moscow University of the MIA of Russia named after V.Ya. Kikot)

Аннотация: в статье рассматриваются современные технические средства фиксации сферических фото- и видеопанорам для решения задач судебной фотографии и видеозаписи. Приводятся результаты экспериментальной работы по применению систем виртуальной реальности для визуализации процессов осмотров мест происшествий, даются рекомендации по применению подобных устройств при производстве следственных действий.

Ключевые слова: судебная фотография, судебная видеозапись, виртуальная реальность, осмотр места происшествия, следственные действия, обыск, выемка, проверка показаний на месте.

Annotation: the article discusses modern technical devices of shooting spherical photo- and videopanoramas, for solving problems of forensic photograph and video recording. Also, the results of experimental work on the use of virtual reality systems for the visualization of the processes of inspections of accident sites and recommendations of the use of such devices in the conduct of investigative actions are given.

Key words: forensic photography, forensic video recording, virtual reality, inspection of accident site, investigative actions, police search, police seizure, police verification of the testimony on the spot.

Арсенал технических средств, используемых для решения задач, стоящих перед правоохранительными органами, непрерывно расширяется. Не остаются в стороне судебная фотография и видеозапись, являясь ключевым средством фиксации процесса производства следственных действий и экспертных исследований. За последние несколько лет значительно повысилось качество сферических фото- и видеопанорам, получаемых с помощью новых технических устройств – панорамных камер. Также были разработаны доступные системы виртуальной реальности. Использование этих технологических решений открывает широкие возможности для судебной фотографии и видеозаписи [1].

История современных технических средств виртуальной реальности берет свое начало в 2013 году, когда инженерами американской компании Oculus было анонсировано создание прототипа шлема виртуальной реальности, доступного широкому потребителю, – «Rift». Это устройство, изначально создававшееся для армии США, обеспечивало для пользователя визуальный эффект присутствия в заранее запечатленной или смоделированной виртуальной среде.

Принцип функционирования современного шлема виртуальной реальности основан на демонстрации для каждого глаза зрителя отдельного изображения. Если эти изображения были зафиксированы под разными углами, идентичными восприятию глазами человека, то обеспечивается визуальный эффект объема. С целью увеличения поля зрения используются асферические линзы, благодаря которым расширяется угол обзора. В настоящее время он близок к биологическому зрению человека и составляет 110°. Важнейшей особенностью современных устройств такого типа является использование датчика положения в пространстве (гироскопа), который отличается повышенной точностью. Это позволяет осуществлять наклоны и повороты головы без ощутимой задержки, осматриваясь вокруг себя, что обеспечивает эффект погружения в виртуальное пространство.

С конца 2014 года и до настоящего времени созданы десятки типов коммерческих шлемов виртуальной реальности, работающих по рассмотренному принципу. В некоторых из них используется встроенный дисплей высокого разрешения (к таким устройствам относятся, например, Oculus «Rift», HTC «Vive»), в других для демонстрации изображения используется дисплей смартфона (Samsung «Gear VR», Google «Cardboard», «Homido», «Fibrum» и другие).

Разрешение современных устройств фиксации [1, 2], которые позволяют осуществлять фото- и видеосъемку 360-градусного изображения, также существенно повысилось. Например, доступная широкому потребителю камера Samsung «Gear 360» (2017) позволяет осуществлять фото- и видеофиксацию с разрешением 4к (4096 х 2048 точек на дюйм). При этом для каждого глаза пользователя обеспечивается картинка с разрешением 2048 х 1024, что является достаточным для восприятия четкого изображения высокого качества.

Московский университет МВД России имени В.Я. Кикотя в числе первых проводил эксперименты с использованием технологии фиксации сферических панорам сложных мест происшествий и дальнейших повторных осмотров с использованием устройств виртуальной реальности. Так, на основе сферических панорам реального объекта уже проводится осмотр следовой картины пожара в

сгоревшем доме в рамках пожаротехнической экспертизы. Разработана технология создания виртуальных фототаблиц, позволяющих просматривать заранее запечатленное место происшествия с разных точек обзора, увеличивать и рассматривать следы и объекты, а также получать информацию о размерных характеристиках и дистанциях.

В процессе проведения виртуального осмотра изображение, наблюдаемое пользователем в реальном времени, транслируется на интерактивную доску, что может применяться для демонстрации другим сотрудникам.

По нашему мнению, использование рассматриваемых технологий может осуществляться не только в целях запечатления и дальнейшего осмотра обстановки места происшествия, но и в целях фиксации процесса производства следственных действий. Так, открываются широкие возможности производства обыска, выемки, проверки показаний на месте с использованием средств панорамной видеозаписи. Представление зафиксированных таким образом видеоизображений со звуковым сопровождением в шлеме виртуальной реальности обеспечит аудиовизуальный эффект присутствия на месте производства следственного действия [3] для следствия и суда даже спустя годы, например, в случае новых открывшихся обстоятельств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Акберов С.А., Трущенков И.В. Некоторые вопросы назначения компьютерной экспертизы, и привлечения специалиста для участия в следственных действиях при расследовании преступлений, связанных с использованием компьютерной техники: материалы XI Всероссийской конференции «Правопорядок в России: проблемы совершенствования» 18-21 апреля 2017 г. – М.: МосУ МВД России имени В.Я. Кикотя, 2017.

2. Шорманов В.К. Применение метода ГХ МС и современных IT-систем для анализа многокомпонентной смеси «дизайнерских» каннабиноидов в условиях проведения химической экспертизы. Человек и его здоровье / В.К. Шорманов, Р.А. Юрченко, М.А. Останин, В.Ю. Кузовлев, А.С. Бабухина, А.А. Овчинникова // Курский научно-практический вестник. 2014. Т. 4. С. 97-103.

3. Абдурагимова Т.И., Трущенков И.В. К вопросу о производстве обыска и выемки в целях обнаружения объектов для производства судебной компьютерной экспертизы // Энциклопедия судебной экспертизы. 2017. № 1 (12).

О НЕКОТОРЫХ ПРОБЛЕМАХ ПОЛУЧЕНИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ В СУДОПРОИЗВОДСТВЕ

ON SOME PROBLEMS OF OBTAINING AND USING ELECTRONIC INFORMATION IN LEGAL PROCEEDINGS

Горев Александр Иванович,
Горева Евгения Геннадьевна
(Омская академия МВД России)

Gorev Alexander Ivanovich,
Goreva Evgenia Gennadyevna
(Omsk Academy of the MIA of Russia)

Аннотация: рассматриваются вопросы, возникающие при проведении следственных действий по изъятию средств вычислительной техники, компьютерных носителей информации и информации в компьютерном формате.

Ключевые слова: персональный компьютер (далее – ПК), средства вычислительной техники (далее – СВТ), гаджет, кодирование, носители информации.

Annotation: the questions arising when carrying out investigative actions for withdrawal of computer aids, computer data carriers and information in a computer format are considered.

Key words: the personal computer, computer aids, a gadget, coding, data carriers.

Современное состояние развития информационного общества ставит перед правоохранительными органами задачи, решение которых требует знаний о компьютерных технологиях обработки информации на профессиональном уровне. Современный безбумажный документооборот в организациях, электронная почта, виртуальное общение в социальных сетях и чатах – вот неполный перечень новых технологий, внедрение которых характерно именно для информационной стадии развития общества. Мы намеренно не говорим о преступлениях в сфере компьютерной информации – это отдельная тема, однако современный человек настолько плотно окружен различными устройствами фиксации, хранения, преобразования информации, что уже сейчас правозащитниками ставится вопрос о тотальном контроле общества.

Западноевропейские страны и страны Северной Америки, провозгласившие в XX веке права человека как основную ценность общества, в начале века XXI все больше становятся обществом тотального контроля. Данный процесс проводится под лозунгом борьбы с терроризмом, хотя события последних лет дают основания полагать, что тотальный контроль не является панацеей. По этому пути пошел и отечественный законодатель, приняв Федеральный закон

от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

Однако фиксация и хранение информации с учетом возможностей современных компьютерных систем являются наиболее простыми технологиями: web-камеры, диктофоны и терабайтные винчестеры обеспечивают возможность накопления информации за длительный период. Значительно более сложные проблемы вызывают технологии обработки и защиты информации от несанкционированного доступа. Подробнее остановимся на указанных проблемах, поскольку именно они определяют сложность использования информации в электронном виде в качестве доказательства.

Технологии обработки информации в электронном виде значительно отличаются от технологий предыдущего поколения бумажного документооборота. Первым отличием следует отметить невозможность восприятия непосредственно органами чувств человека информации в компьютерных форматах хранения. Книга и рукопись доступны для чтения, картина воспринимается зрением, скульптура – тактильными ощущениями, виниловая грампластинка может быть прослушана с использованием иглы. Информация, записанная в оцифрованном виде, может быть воспринята органами чувств человека только с использованием специальной аппаратуры. Дополнительную сложность могут создавать технологии защиты и сокрытия информации, легко реализуемые программным способом. Таким образом, возникает проблема изъятия носителей информации, поскольку определить на них наличие информации вообще и информации, значимой для следствия, в частности не всегда представляется возможным. Более того, использование таких методов сокрытия информации как компьютерная стеганография, позволяет с высокой степенью надежности скрывать информацию под другой. Например, на DVD будет записан фильм практически без потери качества и база данных, получить доступ к которой без специальных программ невозможно.

Еще один способ сокрытия информации от несанкционированного доступа представляют стандартные средства операционных систем семейства Windows NT. Файловая система NTFS позволяет пользователю «дополнить» любой файл потоками неограниченного объема. Получить доступ к скрытой информации можно, однако для этого необходимо выявить файл с прикрепленным потоком, что является нетривиальной задачей. Таким образом, внешне пустой носитель будет содержать скрытый большой объем данных.

Другим отличием компьютерного документооборота является множественность форматов хранения данных. Если написанный на бумаге текст человек может прочитать независимо от почерка, то компьютер для распознавания теста должен обладать специальной программой декодирования. В настоящее время для текста используется множество кодировок: КОИ-7, КОИ-8, UNIKOD и др. На их основе построены более 50 форматов хранения текстовой информации, что порождает проблему поиска программы обработки, способную «читать» представленную информацию. Многие текстовые редакторы позволяют

сохранять файл в различных форматах, которые не могут быть прочитаны с использованием других программ. Например, формат *.odt, созданный с помощью текстового редактора OpenOfficeWrite, не может быть прочитан редактором MicrosoftWord.

Если текст намеренно написан транслитом с использованием алфавитов различных языков, задача автоматического распознавания текста возрастает многократно. Например, в слове **ME**R**CE**D**E**S выделенные символы могут быть набраны кириллицей или латиницей. Отсутствие визуального различия в написании символов было использовано при организации госзакупки автомобиля для губернатора Свердловской области в 2011 г. Формальное требование о публикации информации было выполнено, однако только сведущий смог ознакомиться с ней, и торги проводились с участием одного продавца [1]. Наказать исполнителя за подобное нарушение невозможно, поскольку требований по семантической совместимости в электронном документообороте до сих пор нет. Приведенный пример демонстрирует сложность контекстного поиска информации на ПК.

Еще больше разнятся форматы представления мультимедийной информации – в настоящее время их более 100. Графика, аудио- и видеоинформация являются стандартом хранения информации на ПК. Однако существует множество гаджетов с форматами хранения, отличными от форматов ПК: фотоаппараты и видеокамеры, диктофоны, видеорегистраторы, телефоны и смартфоны, навигаторы, трекеры, автомобильные декодеры и пр. Даже считать информацию с некоторых из перечисленных устройств является непростой задачей. А преобразование этой информации для последующего использования на ПК ставит проблему создания или поиска программы-декодера. Возможно, именно это служило причиной столь долгого решения вопроса признания информации видеорегистратора в качестве доказательства. Только в апреле 2016 г. в ст. 26.7. КоАП РФ была внесена норма, согласно которой «документы могут содержать сведения, зафиксированные как в письменной, так и в иной форме. К документам относятся материалы фото- и киносъемки, звуко- и видеозаписи информационных баз и банков данных и иные носители информации».

Необходимость перекодировки или смены формата информации для последующего использования порождает проблему гарантии отсутствия модификации информации при ее преобразовании. Указанная проблема хорошо иллюстрируется неоднозначностью перевода текста на иностранный язык и наоборот. Переводы литературных произведений в разных редакциях существенно отличаются по форме и содержанию. Содержательная идентичность электронных документов в различных форматах является краеугольной проблемой в судопроизводстве. Технологии создания фото- и аудиомонтажа с использованием компьютера существенно повысили качество результата работы и одновременно усложнили процесс распознавания монтажа. Действительно, мультимедийный файл содержит содержательную и служебную части, и любое редактирование оставляет следы в служебной части файла. На выявлении изменений служебной части графических файлов построены большинство программ выявления фотомонтажа [2]. Однако, не вдаваясь в технические подробности, отметим,

что при грамотной обработке электронной информации могут быть успешно модифицированы как содержательная часть файла, так и служебная информация. В этом случае состязательность процесса будет определяться уровнем знаний экспертов со стороны обвинения и защиты и их возможностью донести свои специальные познания до суда и объяснить сложные технические вопросы.

Третье значимое отличие электронного и бумажного документооборота выражается в свойстве копируемости информации. В докомпьютерную эпоху владельцы информационных ресурсов не имели проблемы создания копий документов. Бумажные носители обрабатывались, подшивались в дело, уничтожались или передавались в архив при необходимости. Использование компьютерной аппаратуры для обработки информации породило регламент создания копий информационных ресурсов, поскольку сбой программы или аппаратуры мог привести (и неоднократно приводил) к потере всей накопленной информации. Легкость операции копирования и низкая стоимость носителей информации породили упрощенное отношение к данному вопросу.

В настоящее время вместо операции копирования часто выполняется операция создания образа носителя, поскольку последняя обладает рядом достоинств с точки зрения пользователя, в частности, выполняется значительно быстрее. В практических рекомендациях по проведению следственных действий также часто встречается совет использования операции создания образа. Действительно, любой квалифицированный эксперт будет проводить исследование изъятого носителя только на его копии, поскольку внесение любой информации (даже служебной – о включении ПК или любой программы на нем) на изъятый носитель после проведения следственных действий может явиться причиной отказа признания его в качестве доказательства. Однако операция создания образа не позволяет перенести на носитель эксперта удаленные файлы и остатки файлов, не затертых при перезаписи. Таким образом, существенный объем информации, который мог стать доказательственной базой, теряется на первом этапе изъятия информации.

Еще одну проблему изъятия информации порождает множественность видов носителей. Стандартные флэш-накопители и компакт-диски уже не вызывают вопросов, однако часто сотрудники правоохранительных органов забывают о том, что практически любой личный гаджет пользователя офисного ПК может быть использован как устройство внешней памяти. При этом скопированная информация может не отображаться на дисплее гаджета, что не помешает произвести ее обратное копирование. Обнаружить ее может только эксперт при детальном исследовании. То же относится и к компакт-дискам: записанный мультимедиа-контент может чередоваться с пользовательской информацией или скрывать ее, делая недоступной при стандартных способах просмотра диска. В этом случае лицо, производящее процессуальные действия, встает перед дилеммой – изъять часть носителей и потерять информацию, отсутствующую на ПК, или изъять максимально возможное количество носителей, чем навлечь нарекания со стороны владельцев изымаемой информационной системы по поводу изъятия личных гаджетов и обеспечить работой целое подразделение экспертов. Серьезной проблемой может стать современный спо-

соб облачного хранения информации. Практические работники уже сталкиваются с вопросами изъятия информации, хранящейся за пределами России. Правильным подходом к решению обозначенной проблемы изъятия информации, на наш взгляд, является обязательное предварительное проведение мероприятий по установлению места хранения представляющей интерес информации.

Защита информации от несанкционированного доступа является значимой проблемой рассматриваемой темы. Наличие в открытом доступе программного обеспечения криптографической защиты различных производителей делает указанную задачу трудноразрешимой. Защита объекта обработки информации от несанкционированного доступа может сделать проблему неразрешимой. Примером может быть освещенный СМИ случай обыска офисов фирмы, занимавшейся незаконным обналичиванием денег. За то время (около часа), которое полицейские потратили на применение специального оборудования, чтобы попасть внутрь, вероятные преступники успели уничтожить документы и вывести из строя компьютерную технику. Данный пример наглядно показывает необходимость обязательного предварительного проведения мероприятий по установлению места и способа хранения представляющей интерес информации, разработки легенды беспрепятственного проникновения на территорию объекта.

Изложенное позволяет сделать вывод об обязательности подготовительного этапа при проведении любых процессуальных действий при наличии средств вычислительной техники. Широкое распространение компьютерных устройств, их повсеместное применение, внешняя простота использования и дружественный интерфейс являются причиной частого заблуждения о легкости изъятия вычислительной техники, носителей и информации и возможности проведения действий следователем самостоятельно без привлечения внешнего специалиста. Однако квалифицированный осмотр и обращение с компьютерами и периферийными устройствами может произвести только специалист. При вмешательстве в эту деятельность неквалифицированного сотрудника могут возникнуть проблемы и серьезные последствия на этапе реализации изъятой информации в качестве доказательства. Поэтому данная работа требует, как правило, привлечения специалиста по компьютерным системам. Разнообразие компьютеров и программного обеспечения определяет необходимость специализации IT-специалистов. Хороший специалист может быть компетентен лишь в конкретных компьютерных системах: специалист по операционной системе Windows для ПК, например, не обязательно может уметь обращаться с ПК под управлением MacOC или большими вычислительными комплексами, в которых в качестве операционной системы используется UNIX или LINUX. Именно наименование и версия операционной системы являются тем обязательным элементом, который коренным образом отличает один вычислительный комплекс от другого.

Второй обязательный вопрос для выяснения на подготовительном этапе определяет формат хранимых и обрабатываемых электронных данных. Перечень прикладных программ, применяемых на рабочих местах, позволяет ответить на поставленный вопрос. Кроме того, должен быть получен ответ на вопрос о применимости средств и методов защиты или сокрытия информации. При наличии таких средств должна быть проведена предварительная работа по

нейтрализации данных защитных действий: пароли доступа, электронные ключи, методы сокрытия информации – вот вопросы, отсутствие ответов на которые может свести на нет всю работу по изъятию вычислительной техники и носителей. Например, отсутствие электронного ключа может привести к отображению в программе вымышленных данных, в то время как реальная база данных будет сделана недоступной.

Третий обязательный вопрос для выяснения на подготовительном этапе определяет наличие локальной сети компьютеров и ее структуру. В современном офисе компьютеры и периферийное оборудование может соединяться как по проводным, так и по беспроводным каналам связи. В последнем случае взаимодействие СВТ является неочевидным, что могут существенно усложнить восстановление структуры электронного документооборота и определения авторства изъятых электронных документов. Более того, если взаимодействие рабочих мест между собой организовано по проводным каналам, а связь с сервером осуществляется по беспроводным, неподготовленное следственное действие завершится изъятием рабочих мест, а сервер как основное хранилище информации окажется нетронутым. Блокирование возможности беспроводного подключения к локальной сети необходимо также для успешного проведения следственных действий, поскольку легальный пользователь системы сможет модифицировать или удалить данные на компьютере дистанционно с использованием смартфона или планшета.

Четвертый обязательный для выяснения вопрос определяет подключение к глобальной сети. Важность этого вопроса обусловлена двумя факторами. Во-первых, распространением модного облачного хранения данных, в связи с чем интересная следствию информация может находиться вне юрисдикции Российской Федерации. В этом случае само действие по изъятию СВТ окажется бесполезным. Во-вторых, возможностью модификации или удаления данных на компьютере дистанционно в момент проведения следственных действий. Более того, нельзя исключать возможность установки администратором системы специализированного программного обеспечения, предназначенного для удаленного администрирования рабочих мест, включая передачу аудио- и видеоинформации с места проведения следственных действий по сети Интернет.

Таким образом, при подготовке к проведению должны быть получены ответы как на технические, так и на организационные вопросы, включая вопрос о попытках, которые могут быть предприняты заинтересованными лицами для воспрепятствования достижению поставленной следователем цели, и методах предотвращения этих попыток.

Сбор информации об объекте, где будет проходить следственное действие, может производиться различными способами. Например, получение интересующей информации посредством производства других следственных действий (допроса свидетелей, потерпевших, обвиняемых и др.). Необходимые сведения следователь может почерпнуть и путем обращения к органу дознания с поручением. В таком случае у органа дознания появляется возможность получать информацию как уголовно-процессуальным, так и оперативно-розыскным путем и информировать об этом следователя.

Предложенные варианты получения сведений, необходимых при подготовке к проведению следственного действия, основаны на нормах права и носят официальный характер. Но поскольку в большинстве случаев полученные данные не будут иметь доказательственного значения, а используются как ориентирующая информация для подготовки к проведению следственного действия, они могут быть получены и любым иным способом (например, в ходе беседы с осведомленным в этих вопросах лицом, посредством устного обращения следователя к работникам оперативных аппаратов за необходимыми сведениями и др.).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Балашова Ю. Госзакупки. Мерседес-невидимку оправдали в суде [Электронный ресурс]. – Режим доступа: http://domnikov.novayagazeta.ru/ html.

2. Ляйдель Ш. Digital detectives fight photo manipulations [Электронный ресурс]. – Режим доступа: http://onmedia.dw-akademie.de/.

ИСПОЛЬЗОВАНИЕ АИПС «АИПСИН-АНТИНАРКОТИКИ» В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПРИ ПРОИЗВОДСТВЕ ЭКСПЕРТИЗ «ДИЗАЙНЕРСКИХ» НАРКОТИКОВ

THE USE OF AISS «AIPSIN-ANTINARCOTICS» IN THE FORENSIC ACTIVITIES OF MINISTRY OF INTERNAL AFFAIRS IN THE SPHERE OF EXAMINATION WITH «DESIGNERS» DRUGS

Кузовлев Владислав Юрьевич
(Московский университет МВД России имени В.Я. Кикотя)

Kuzovlev Vladislav Yuryevich
(Moscow University of the MIA of Russia named after V.Ya. Kikot)

Аннотация: в статье рассматриваются аспекты использования автоматизированной информационно-поисковой системы «АИПСИН-АнтиНаркотики» в экспертно-криминалистической деятельности органов внутренних дел при производстве экспертных исследований. Данная система в комплектах с хромато-масс-спектрометрическими комплексами может успешно применяться как рабочее место эксперта-химика.

Ключевые слова: АИПС «АИПСИН-АнтиНаркотики»; «дизайнерские» наркотики; судебная экспертиза; эксперт; правоохранительные органы; органы внутренних дел; хромато-масс-спектрометрический комплекс; новые потенциально опасные психоактивные вещества; наркотические средства; психотропные вещества.

Annotation: the article discusses aspects of the use of the automated information search system «AIPSIN-Antinarcotics» in the forensic activities of the internal Affairs bodies in the sphere of forensic examination. This system is complete with chromate-mass-spectrometric complexes can be successfully used as a workplace of an expert chemist.

Key words: AISS «AIPSIN-Antinarcotics»; «designers» drugs; forensic examination; expert; law enforcement; police; chromate-mass-spectrometric complex; a new potentially dangerous psychoactive substances; narcotic drugs; psychotropic substances.

Правоохранительная практика показывает, что сегодня на смену периоду нелегальных наркотиков пришел период новых, так называемых «дизайнерских» наркотически активных соединений, под которыми мы понимаем *предмет преступного посягательства – синтетическое психоактивное вещество* (*препарат), умышленно синтезированное (произведенное) в противоправных целях в такой специфической молекулярной форме, чтобы обойти направленные на противодействие незаконному обороту наркотиков правовые нормы*. Между тем в настоящее время на территории постсоветского пространства подобные психоактивные предметы злоупотреблений получили широкое распространение и явились настоящим вызовом времени. Их антисоциальные факторы и явная античеловеческая направленность не позволяют применять в борьбе с этим злом устаревшие методы и приемы. Между тем практика свидетельствует о распространенности в наркосообществе более 2000 «дизайнерских» каннабиноидов. Кроме того, существует реальная опасность вливания в оборот целого ряда соединений, не имеющих в списках подконтрольных веществ даже структурных аналогов. Поэтому на современном этапе правоохранительными органами вырабатываются и применяются высокотехнологичные принципы противодействия наркоугрозе. Естественные науки не отстают от ведущейся борьбы и, действуя на опережение, вырабатывают инновационные подходы к оценке физико-химических параметров новых поступающих в нелегальный оборот психоактивных веществ. Работа ученых в этом направлении направлена на применение её результатов в экспертно-криминалистической деятельности правоохранительных органов.

Буква и дух Федерального закона от 08.01.1998 № 3-ФЗ (в ред. от 03.07.2016) «О наркотических средствах и психотропных веществах» диктуют федеральным органам государственной власти и в первую очередь уполномоченным осуществлять контроль за оборотом наркотиков в Российской Федерации – органам внутренних дел вырабатывать действенные государственные меры, направленные на своевременное подведение под контроль именно таких новых наркотически активных веществ, которые только начали поступать в оборот, но стали предметами злоупотребления. Именно для выполнения указанных задач разработано компанией ЗАО «Belhard Group» (г. Минск) и применяется в практике деятельности правоохранительных органов семейство аналитического программного обеспечения по идентификации психоактивных соединений – автоматизированная информационно-поисковая система «АИПСИН-АнтиНаркотики». Этот инновационный по своей сути программный продукт, своего рода IT-система, полностью импортонезависим и предназначен для обеспечения деятельности государственных органов стран бывшего СССР,

осуществляющих контроль за оборотом наркотических средств, психотропных веществ и их аналогов.

Данная IT-система по своей полноте не имеет аналогов в мире и в настоящее время является практически единственным аналитическим интегрированным программным средством, позволяющим экспертам-химикам правоохранительных органов уверенно идентифицировать поступающие в оборот новейшие психоактивные соединения, анализ которых проводится методом хромато-масс-спектрометрии в рамках выполняемых ЭКП правоохранительных органов судебных химических экспертиз и исследований. Как программный продукт указанная система используется в комплекте с современным масс-спектральным оборудованием, которым оснащаются экспертно-криминалистические подразделения [1].

Программная часть «АИПСИН-АнтиНаркотики» состоит более чем из 40 информационных модулей, содержащих информацию по целому спектру областей знаний, которые так или иначе связаны с идентификацией наркотических веществ, их использованием и вызываемыми ими последствиями. Базы данных содержат информацию о психоактивных веществах: о внешнем виде и оболочке препаратов и дозированных форм, о синонимах, общих структурных свойствах и формулах веществ, цветных капельных реакциях и тестах, параметрах тонкослойной, газожидкостной и высокоэффективной жидкостной хроматографии, хроматомасс-спектроскопии (с базой спектров), инфракрасной спектроскопии (с базой спектров), ультрафиолетовой спектроскопии (с базой спектров) и мн. др. Помимо этого, система содержит огромное количество исторических справок, нормативной документации, оригинальных статей и монографий, а также официальную методическую информацию и уникальные вспомогательные дополнительные модули. Система имеет несколько мультилингвальных режимов для возможности просмотра и поиска информации оператором не только на основных европейских языках, но и языках стран бывшего СССР.

Входящая в ее состав масс-спектральная библиотека «AIPSIN MS Database» включает актуальные и научно подтвержденные масс-спектры образцов всех известных в мире «дизайнерских» наркотиков. Каждый из масс-спектров соединений, содержащихся в данной библиотеке, получен или приобретен у правообладателей официально. При использовании данной IT-системы при исполнении судебно-экспертного исследования эксперт-химик имеет возможность ссылаться на саму систему «АИПСИН-АнтиНаркотики» как легитимный научный источник аналитических данных. Следует отметить, что ни в одной из известных в настоящее время масс-спектральных библиотек, за исключением «AIPSIN MS Database», не содержится полного перечня поступающих в оборот на территорию постсоветского пространства «дизайнерских» наркотиков.

Актуальная версия «АИПСИН-АнтиНаркотики» комплектуется масс-спектральным идентификатором, позволяющим эксперту-химику вести поиск по библиотекам спектров в автоматическом режиме, с обработкой хроматограмм. Такой экспертный подход обеспечивает ускоренную и надежную идентификацию содержащихся в образцах соединений, а также исключает возможные случайные ошибки при разметке хроматографических пиков.

Система «АИПСИН-АнтиНаркотики» может быть развёрнута в локальном или сетевом вариантах с тремя типами установок: базовая, специальная и экспертная. Каждая из этих типов установок нацелена на решение определенного круга задач: общеправовой, следственно-оперативной и экспертно-криминалистической. Кроме того, система имеет возможности использования как в стационарном, так и в мобильном вариантах.

В целях усиления оперативности экспертно-криминалистического реагирования при раскрытии и расследовании преступлений, предметами которых являются новые и «дизайнерские» наркотики, компанией «Belhard Group» разработана и внедрена в оперативном режиме интернет-версия для сотрудников ЭКП правоохранительных органов. Данная версия, помимо масс-спектрального идентификатора, содержит аналитический блок просчета подконтрольности соединения по фрагменту структурной формулы, что представляется особенно актуальным для эмпирического анализа веществ, представленных для проведения исследований и подозреваемых на относимость к производным наркотических средств и психотропных веществ. Также данный инновационный по своей сути блок может быть полезен сотрудникам Главного управления по контролю за оборотом наркотиков (ГУНК) МВД России, разрабатывающих предложения Правительству РФ по формированию Перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации. С помощью специального drawing-блока эксперт (сотрудник ГУНК) может изобразить представляющий интерес фрагмент и в раскрывающемся окне выбрать имеющие родство с объектом исследования формулы соединений.

Необходимо отметить, что статистика преступлений в сфере незаконного оборота наркотиков и иных психоактивных веществ свидетельствует о необходимости перехода к новым схемам и концепциям борьбы с наркопреступностью. На наш взгляд, их канвой должна являться идея координации усилий и информационного обмена между государственными органами правоохранительных структур Российской Федерации и стран-членов ОДКБ, стран бывшего СССР, действующих в едином информационном пространстве с использованием единых методологических и методических подходов с опорой на экспертно-криминалистическую деятельность органов внутренних дел. Подобное взаимодействие предполагает установление взаимосвязи между различными уровнями получения, обработки и использования информации и разработку на этой основе новых научных подходов по выявлению подконтрольных объектов с учетом компьютерного мониторинга рисков. Каждый полученный результат является основой для получения следующего, более значимого и ценного результата. Весь сублимат полученного опыта и информации является основой как для обучения новых полицейских кадров, так и переподготовки действующих сотрудников, которые, в свою очередь, получая ценный опыт правоохранительной деятельности, дидактически станут провайдерами новых ценных экспертных данных. Это особенно актуально в условиях раскрытия и расследования деятельности организованных преступных групп и сообществ.

Несмотря на то, что АИПС «АИПСИН-АнтиНаркотики» разработана для правоохранительных органов, системой оснащены далеко не все экспертно-

криминалистические подразделения территориальных ОВД России. Данное обстоятельство не позволяет даже своевременно идентифицировать встречающиеся в обороте предметы злоупотреблений – наркотические средства, психотропные вещества и их прекурсоры. При этом ведение целенаправленной и успешной борьбы с распространением аналогов наркотических средств и психотропных веществ, новых психоактивных потенциально опасных веществ представляется не в полной мере реализуемым [2].

Автором проведен анализ эффективности использования «АИПСИН-АнтиНаркотики» в экспертно-криминалистических подразделениях органов наркоконтроля Российской Федерации, упраздненных в истекшем 2016 году на основании Указа Президента России от 05.04.2016 № 156 «О совершенствовании государственного управления в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров и в сфере миграции». При этом только в одном только подразделении (Базовой экспертно-криминалистической службе управления ФСКН России по городу Москве) из общего количества выполненных в 2013 г., 2014 г., 2015 г., 6 месяцев 2016 г. судебных экспертиз и исследований наркотиков по оперативным материалам с использованием системы «АИПСИН-АнтиНаркотики» было проведено 68%, 76%, 77%, 93% соответственно. Следует отметить, что в подразделении было установлено только 1 подобное рабочее место эксперта-химика, при этом все использовавшиеся масс-спектрометры работали в режиме локальной сети. АИПС была задействована 24 часа в сутки всем экспертно-химическим личным составом подразделения.

Кроме того, в рамках выполнения базовых функций службы для ЭКП территориальных органов ФСКН России, расположенных в пределах Центрального федерального органа, проводились онлайн-консультации экспертов-химиков территориальных управлений по вопросам идентификации «дизайнерских» наркотиков с использованием системы.

Не вызывает сомнения тот факт, что дальнейшее внедрение системы «АИПСИН-АнтиНаркотики» в экспертно-криминалистическую деятельность, осуществляемую правоохранительнами органами, послужит основой успешного противодействия распространению «дизайнерских» наркотиков в Российской Федерации. При этом система «АИПСИН-АнтиНаркотики» в комплектах с хроматомасс-спектрометрическими комплексами и другим экспертным аналитическим оборудованием может и в дальнейшем успешно реализовываться как рабочее место эксперта-химика, занятого по линии экспертной специальности исследования наркотических средств, психотропных веществ, их аналогов и прекурсоров, новых потенциально опасных психоактивных веществ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шорманов В.К., Применение метода ГХ МС и современных IT-систем для анализа многокомпонентной смеси «дизайнерских» каннабиноидов в условиях проведения химической экспертизы. Человек и его здоровье / Шорманов В.К., Юрченко Р.А., Останин М.А., Кузовлев В.Ю., Бабухина А.С., Овчинникова А.А. // Курский научно-практический вестник. 2014. Т. 4. С. 97-103.

2. Мисник В.А. Информационно-поисковая система «Аипсин АнтиНаркотики» и возможности ее использования в правоохранительных / В.А. Мисник, Ю.С. Павловец, Т.А. Шевчук, Р.А. Юрченко // Вопросы оборонной техники. Выпуск 11-12. 2013.

К ПРОБЛЕМЕ СУЩНОСТИ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМОЙ В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ

TO THE PROBLEM OF THE ESSENCE OF ELECTRONIC INFORMATION USED IN CRIMINAL PROCEDURE AS AN EVIDENCE

Лютынский Антон Мечиславович
(Северо-западный институт (филиал) Университета имени О.Е. Кутафина)

Liutynskii Anton Mechislavovich
(North-West institute (branch) of University name after O.E. Kutafin)

Аннотация: в статье сформулирована в дискуссионном ключе авторская позиция о правовых аспектах использования электронной информации в уголовно-процессуальном доказывании. Автор утверждает, что электронная информация может иметь статус вещественного доказательства по уголовному делу. Раскрыты некоторые сущностные особенности электронной информации.
Ключевые слова: вещественное доказательство, электронная информация, доказывание по уголовному делу.

Annotation: the author's position on the legal aspects of the use of electronic information in criminal procedural proof is formulated in the article. The author claims that electronic information can have the status of physical evidence in a criminal case and reveals some of its essential features.
Key words: material evidence, electronic information, proving in a criminal procedure law.

Компьютеризация охватывает все больше сфер человеческой деятельности, добавляет новые особенности в привычные действия и процедуры. Естественно, все большее количество преступлений связано с информацией, воспроизводимой с помощью компьютерной техники. Эти изменения порождают новые задачи перед практиками, законодателями и исследователями: каким образом более точно и полно использовать в расследовании электронную информацию и как точнее применить уголовно-процессуальный закон.

В настоящей небольшой публикации мы кратко рассмотрим некоторые теоретико-правовые аспекты уголовно-процессуального доказывания, связанного с правовой сущностью электронной информации, используемой в доказывании по уголовному делу.

1. В действующем УПК РФ можно найти такие термины, как «электронные носители информации» (ч. 4 ст. 81, ч. 3.1 ст. 183), «электронные сообщения» (ст. 185), содержание которых, впрочем, не раскрывается, видимо, исходя из очевидности термина «электронный». Большой толковый словарь среди значений этого слова указывает и такие как «разработанный на базе электроники»; «осуществляемый через глобальную компьютерную сеть, существующий в глобальной компьютерной сети; сетевой» [2].

Термин «информация» является одним из самых сложных для современных наук, от технических до философских. Для целей доказывания, как представляется, вполне подходит прагматичное, функциональное понимание информации как совокупности любых сведений, которые отражают обстоятельства, имеющие значение для достоверного установления обстоятельств, необходимых для разрешения уголовного дела.

Как видим, электронная информация – это сведения, имеющие форму, приданную средствами компьютерной (вычислительной) техники (электроники) и программного обеспечения.

Как правило, речь идет об информации, хранимой на различных носителях в виде файлов, то есть поименованная совокупность байтов, записанная на жёстком или гибком магнитном диске, в которой хранится отдельный элемент файловой системы, напр. документ Word или рисунок. Вся информация, записанная на магнитный диск, представлена блоками байтов – файлами. Каждый файл имеет обозначение, по которому пользователь и система опознают и используют его [10].

2. Следующим важным вопросом является процессуальный статус электронной информации в уголовном процессе.

На наш взгляд, правильна точка зрения о возможности наделения статусом вещественного доказательства электронной информации, однако было бы неправильным утверждать, что любая компьютерная информация (используемая в расследовании) – это вещественное доказательство [5, с. 51].

По нашему мнению, следует разделять: а) электронный документ, к которым относится электронная форма фиксации результатов следственного действия (например, фонограмма в виде аудиофайла); б) электронное вещественное доказательство – набор электромагнитных сигналов (материальный объект), требующий специфического обеспечения для его восприятия.

В соответствии со ст. 81 УПК РФ «вещественные доказательства – это любые предметы:

1) которые служили орудиями, оборудованием или иными средствами совершения преступления или сохранили на себе следы преступления; 2) на которые были направлены преступные действия и т.д. …; 3) иные предметы и документы, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела».

Электронная информация, хранимая на специальных носителях в виде файлов, на наш взгляд, вполне может быть признана вещественным доказательством, ведь предмет – это «всякое материальное явление…» [7]. Электронная информация как набор электромагнитных сигналов, хранимый, обрабатываемый и используемый с помощью специальный техники и программного обеспечения, является явлением материальным, вполне подходящим по смыслу под определение предмета.

Да, электронная информация видима лишь с помощью специальных средств, но к ней вполне применим сложившийся подход, в соответствии с которым «под вещественным источником доказательственной информации понимается любой материальный носитель, отображающий имеющую для дела информацию в форме физического сигнала» [4, с. 7].

На наш взгляд, материальные следы, оставляемые преступлением, могут иметь не овеществлённый, однако вполне материальный характер. Это не противоречит определениям т.н. «виртуальных следов», под которым В.А. Мещеряков понимает «изменение состояния автоматизированной информационной системы …, связанное с событием преступления и зафиксированное в виде компьютерной информации (то есть информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе на электромагнитном поле» [6, с. 104].

Как отмечает В.Б. Вехов, «эти следы являются материальными невидимыми следами. В основе механизма их образования лежат электромагнитные взаимодействия двух и более материальных объектов» [3, с. 28].

При этом, соглашаясь с утверждением о том, что доказательственное значение электронной информации – не физические свойства материального носителя компьютерной информации, его состав, внешний вид, *как это наличествует у вещественных доказательств* (выделено нами – А.Л.), а содержание данной информации [8, с. 149], стоит оговориться, что внешний вид и форма «привычного» нам вещественного доказательства (например, предмета – ножа – орудия убийства) являются проявлением его внутренних свойств, т.е. содержания. Именно это содержание и имеет доказательственное значение, и противопоставление здесь как раз неуместно. Как отмечалось, основными признаками вещественного доказательства являются отражение преступного события внешней и внутренней структурой этого предмета и передача доказательственной информации в виде следов, доступных непосредственному наблюдению [9, с. 128].

Конечно, создание, восприятие, хранение, использование электронной информации невозможно без электроники и программного обеспечения, но вряд ли можно говорить об отражении, опосредованном интеллектуальным сознанием человека (разработчика программы) [8, с. 150]. Многие другие виды доказательственной информации могут быть исследованы и восприняты с помощью специальных средств, разработанных специалистами. В таком случае интеллектуальное сознание опосредует и исследование папиллярных узоров, следов выстрела, микрочастиц и тому подобных объектов, ничего не говорящих обычному человеку без специальных средств и исследований.

Также вряд ли можно согласиться с утверждением, что «электронным доказательством необязательно должен быть документ (протокол), а … само по себе вещество по своей сути не информативно, доказательством не является, пока не будет субъекта доказывания» [8, с. 151]. Это утверждение в последней своей части (о субъекте доказывания) в равной мере относится к *любой разновидности вещественного доказательства.* В уголовном судопроизводстве доказательство должно приобрести процессуальную форму и быть исследовано и оценено процессуально уполномоченным на это субъектом.

Кроме того, отметим еще раз, что электронное вещественное доказательство и электронная форма фиксации хода и результата следственного действия – принципиально разные понятия. Электронная информация может быть, например, файлом с видеозаписью осмотра места происшествия. В этом случае она является частью протокола следственного действия, приложением к нему и при этом тоже хранится на электронном носителе, не будучи, по сути, самостоятельным доказательством.

В анализируемой публикации утверждается, что «природа вещественного доказательства – быть носителем информации, которая может быть воспринята одинаковым образом любым субъектом доказывания как с помощью специальных технических средств, так и без таковых» [8, с. 151]. Специфика электронного вещественного доказательства такова, что оно само, будучи носителем следа, находится, в свою очередь, на другом, электронном носителе. При этом с содержательной точки зрения механизм образования потенциального электронного вещественного доказательства по существу ничем не отличается от любого другого материального объекта.

Таким образом, можно резюмировать:

1. Электронная информация – разновидность информации, используемой в уголовно-процессуальном доказывании. Она порождается, хранится и используется с помощью специальных технических средств (электроники) и программного обеспечения в виде файлов.

2. Электронная информация в доказывании может иметь две основные правовые формы: а) приложение к протоколу следственного действия, отражающее и иллюстрирующее его ход и результаты; б) электронное вещественное доказательство.

3. Электронное вещественное доказательство – предмет, совокупность материальных явлений, обладающее несколькими специфическими чертами:

- оно требует специального электронного носителя, будучи само носителем данных, имеющих значение для дела;

- оно может быть многократно скопировано. Это обуславливает необходимость дальнейшего научного анализа, уточнения правового регулирования и совершенствования практики использования электронной информации в доказывании по уголовным делам, ее изъятия и исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовно-процессуальный кодекс РФ от 18.12.2001 №174-ФЗ // СПС «КонсультантПлюс».
2. Большой толковый словарь современного русского языка [Электронный ресурс]. URL: https://slovar.cc/rus/tolk/131718.html.
3. Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: автореф. дис… д-ра юрид. наук. – Волгоград, 2008.
4. Вещественные доказательства: Информационные технологии процессуального доказывания / под общ. ред. д.ю.н., проф. В.Я. Колдина. – М., 2002.
5. Кудрявцева А.В., Худякова Ю.В. Вещественные доказательства в уголовном процессе России. – Челябинск, 2006.
6. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж, 2002.
7. Ожегов С.И. Словарь русского языка: около 53 000 слов / под общ. ред. проф. Л.И. Скворцова. - 24-е изд., испр. – М.: Оникс, Мир и Образование, 2007.
8. Пастухов П.С. Электронное вещественное доказательство в уголовном судопроизводстве // Вестник Томского государственного университета. 2015. № 396. С. 149-153.
9. Ульянова Л.Т. Предмет доказывания и доказательства в уголовном процессе России: учебное пособие. – М., 2008.
10. Энциклопедия «Техника». – М.: Росмэн, 2006.

КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМЫЕ ПРИЗНАКИ СПОСОБА СОВЕРШЕНИЯ КРАЖИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

FORENSIC SIGNIFICANT FEATURES OF METHOD OF COMMITTING THEFT WITH USING INFORMATION TECHNOLOGIES

Савченко Оксана Александровна
(Всероссийский государственный университет юстиции)

Savchenko Oksana Alexandrovna
(All-Russian State University of Justice)

Аннотация: по результатам проведенного исследования разработана классификация криминалистически значимых признаков, характеризующих способ совершения кражи с использованием информационных технологий как вида хищений в сфере информационных технологий.

Ключевые слова: информационные технологии, компьютерная информация, хищение, кража, способ совершения преступления.

Annotation: according to results of research, there is a classification of forensic significant features of method of committing theft in sphere of information technologies, which important for investigation of thefts in sphere of information technologies.

Key words: information technologies, computer information, theft, method of committing crime.

Активное внедрение информационных технологий в различные сферы общества повлияло на способы совершения традиционных преступлений [1]. В частности, возникли новые способы совершения хищений в сфере информационных технологий (далее – хищения в сфере ИТ), такие как мошенничество в сфере компьютерной информации, кража с использованием информационных технологий и другие.

В отличие от мошенничества в сфере информационных технологий, в отношении кражи с использованием информационных технологий (далее – кража с использованием ИТ) в УК РФ не предусмотрен специальный состав. Данное обстоятельство не влияет на квалификацию. Однако возникают сложности в расследовании кражи с использованием ИТ в связи с тем, что конкретное описание характеристики способа кражи с использованием ИТ в уголовном законе отсутствует. В данном случае необходима разработка рекомендаций по расследованию кражи с использованием ИТ, детализирующих криминалистически значимые признаки способа совершения указанного хищения, составляющие его криминалистическую характеристику.

Способ кражи с использованием ИТ характеризуется следующими признаками: 1) признаки тайного хищения чужого имущества; 2) использование в качестве оборудования и иных средств совершения хищения информационных технологий и традиционного оборудования и иных средств совершения преступления; 3) совершение преступником действий в сфере компьютерной информации; 4) признаки, предусмотренные ч. 1 ст. 272 УК РФ, ч. 1 ст. 273 УК РФ.

При установлении способа хищения в сфере ИТ следует руководствоваться признаками, указанными в УК РФ, и учитывать, какой именно способ совершения преступления является основным. Родовое понятие кражи предусмотрено ч. 1 ст. 158 УК РФ. Традиционным способом кражи является тайное хищение чужого имущества. Следовательно, способом кражи с использованием ИТ является тайное хищение чужого имущества посредством использования информационных технологий.

В случае когда хищение в сфере ИТ совершено тайным способом с одновременным использованием вредоносной компьютерной программы, основным способом совершения указанного хищения в сфере ИТ следует считать тайное хищение чужого имущества, и, соответственно, преступное деяние квалифицируется по ст.ст. 158, 273 УК РФ. При наличии признаков неправомерного доступа к компьютерной программе преступное деяние также квалифицируется по ст. 272 УК РФ.

В соответствии с результатами исследования способом тайного хищения чужого имущества совершается 32% хищений в сфере информационных технологий (см. табл. 1).

Таблица 1

Процентное соотношение составов хищений в сфере информационных технологий[1]

Составы хищений в сфере ИТ	Процентный показатель
Кража с использованием информационных технологий (ст.ст. 158, 272 и (или) 273 УК РФ)	31,7%
Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ)	35,3%
Присвоение и растрата с использованием информационных технологий (ст. 160 УК РФ)	33%

В качестве оборудования и иных средств совершения кражи с использованием ИТ могут быть использованы: 1) компьютерные программы и иное лицензированное программное обеспечение; 2) вредоносные компьютерные программы и иное вредоносное программное обеспечение. К используемому в целях кражи лицензионному программному обеспечению в основном относятся платежные системы, например, система «Банк-Клиент», «Интернет-банкинг». Кража с использованием ИТ в том числе может быть совершена с использованием технических устройств обработки компьютерной информации (копирования, перехвата, считывания компьютерной информации), так называемого «скиммингового оборудования» и средств доступа к компьютерной информации (логины, пароли) с использованием банковских карт и их реквизитов.

К действиям, совершаемым преступником в сфере компьютерной информации, в основном относятся: ввод компьютерной информации (24%), копирование компьютерной информации (28%), модификация компьютерной информации (24%), перехват компьютерной информации (24%) (см. табл. 2). Указанные действия влекут за собой создание новой компьютерной информации о совершении действий в сфере информационных технологий.

Таблица 2

Способы совершения кражи с использованием информационных технологий

№	Способ совершения кражи с использованием ИТ	Процентный показатель
1.	**С использованием информационных технологий в качестве оборудования и иных средств совершения хищения**	
	с использованием компьютерной программы, службы, сервиса, системы, иного лицензионного программного обеспечения	67%
	с использованием вредоносной компьютерной программы, иного вредоносного программного обеспе-	33%

[1] Процентные показатели в таблицах 1 и 2 рассчитаны на основании результатов исследования 250 уголовных дел о хищения в сфере информационных технологий в 19 субъектах РФ за период времени с 2012 по 2017 год.

	чения	
2.	**Посредством совершения действий в сфере компьютерной информации**	
	ввод компьютерной информации	24%
	копирование компьютерной информации	28%
	модификация компьютерной информации	24%
	перехват компьютерной информации	24%
3.	**Способ кражи с использованием ИТ дополнительно характеризуется признаками, предусмотренными ч. 1 ст. 272, ч. 1 ст. 273 УК РФ**	
	неправомерный доступ к компьютерной информации (ст. 272 УК РФ)	80%
	использование вредоносной компьютерной программы, иного вредоносного программного обеспечения (ст. 273 УК РФ)	20%

Ввод компьютерной информации осуществляется с помощью средств ввода, программного обеспечения, может быть осуществлен преступником непосредственно, дистанционно или автоматизированно, например, в случае использования вредоносного программного обеспечения.

Копирование компьютерной информации осуществляется посредством программного обеспечения, вредоносного программного обеспечения, технических устройств обработки компьютерной информации.

Под модификацией компьютерной информации следует понимать изменение компьютерной информации, которое может быть умышленным действием, совершаемым преступником в целях хищения чужого имущества, и неумышленным изменением компьютерной информации вследствие совершения преступником действий в сфере информационных технологий по независящим от его воли обстоятельствам.

Перехват компьютерной информации часто осуществляется с использованием технических устройств обработки компьютерной информации, например, посредством использования считывающего и копирующего устройства, скиммингового оборудования, и связан с последующим копированием перехваченной компьютерной информации.

Способ кражи с использованием ИТ может дополнительно характеризоваться совершением неправомерного доступа к компьютерной информации. Около 80% краж с использованием ИТ совершается посредством неправомерного доступа к компьютерной информации. Действия по неправомерному доступу к компьютерной информации, предусмотренные ч. 1 ст. 272 УК РФ, в совокупности с тайным хищением чужого имущества образуют способ кражи с использованием ИТ наряду с такими признаками, как использование информационных технологий в качестве оборудования и иных средств совершения хищения и действий в сфере компьютерной информации.

Другим дополнительно характеризующим способ кражи с использованием ИТ признаком может являться использование вредоносной компьютерной программы. И мошенничество в сфере компьютерной информации, и кража с использованием ИТ могут быть совершены с использованием вредоносной компьютер-

ной программы. Тем не менее в настоящее время хищение в сфере ИТ с использованием вредоносной компьютерной программы квалифицируется по ст. 159.6 УК РФ как мошенничество в сфере компьютерной информации в соответствии с Постановлением Пленума Верховного суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» от 27 декабря 2007 г. № 51 [2].

Подводя итог, следует отметить, что способ кражи с использованием информационных технологий характеризуется тремя группами признаков: 1) использованием информационных технологий в качестве оборудования и иных средств совершения хищения в сфере информационных технологий; 2) совершением действий в сфере информационных технологий; 3) дополнительными признаками, предусмотренными ст.ст. 272, 273 УК РФ (совершение неправомерного доступа к компьютерной информации, использование вредоносной компьютерной программы, иного вредоносного программного обеспечения).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

2. Постановление Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. 2008. № 4.

ОСОБЕННОСТИ БЛОЧНОГО ШИФРОВАНИЯ ПОСРЕДСТВОМ СЕТИ ФЕЙСТЕЛЯ

THE FEATURES OF BLOCK CIPHER'S USING FEISTEL NETWORK

Хромых Анна Алексеевна,
Богданов Дмитрий Сергеевич
(Краснодарский университет МВД России)

Khromyh Anna Alekseevna,
Bogdanov Dmitriy Sergeevich
(Krasnodar University of the MIA of Russia)

Аннотация: в статье рассматривается метод криптографической защиты информации, позволяющий повысить устойчивость к информационным атакам. Метод основан на применении блочного алгоритма шифрования с использованием кон-

струкции Фейстеля. В целях демонстрации работы сети Фейстеля была разработана компьютерная программа на языке программирования C# в среде VisualStudio 2017, позволяющая шифровать как текстовую информацию, так и изображения.

Ключевые слова: шифрование, дешифрование, блочное шифрование, сеть Фейстеля, криптография.

Annotation: methods of cryptographic protection of information which allow to enhance resistance to attacks on information are demonstrated in the article. This method is based on using Block cipher's algorithm with Feistel's network. In order to demonstrate Feistel network a computer program on (C#) programming language in VisialStudio 2017 was designed. It allows to code both text information and graphic information.

Key words: encryption, decryption, block encryption, Feistel network, cryptography.

Шифрование – это преобразование информации, делающее ее нечитаемой для посторонних. При этом доверенные лица могут провести дешифрование и прочитать исходную информацию. Существует множество способов шифрования/дешифрования, но секретность данных основана не на тайном алгоритме, а на том, что ключ шифрования (пароль) известен только доверенным лицам.

Шифры условно можно разделить на блочные и поточные. Для тех и других существуют различные алгоритмы шифрования. В данной статье рассмотрим конструкцию Фейстеля, позволяющую усложнить алгоритм блочного шифрования.

Блочные шифры разбивают всю входную информацию на n блоков равной (фиксированной) длинны и шифруют каждый блок в отдельности, по окончании процесса шифрования результирующие блоки складываются, и на выходе получается зашифрованная информация.

ГОСТ Р 50922-2006 выделяет следующие виды защиты информации:

– правовая;

– физическая;

– организационная;

– криптографическая.

Исходя из эмпирического опыта, наиболее эффективным видом защиты информации является криптографическая, в которую входят следующие преобразования информации:

– шифрование;

– стеганография;

– кодирование;

– децентрализованное хранение.

Для передачи зашифрованной информации, как правило, используют открытый канал передачи, а по закрытому передают ключ, необходимый для обратного преобразования.

С помощью шифрования обеспечиваются три состояния безопасности информации [5]:

– конфиденциальность – шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении;

– целостность – шифрование используется для предотвращения изменения информации при передаче или хранении;

– идентифицируемость – шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

На данном этапе развития компьютеризации симметричное шифрование может быть использовано:

– для шифрования данных на удаленных серверах;

– для поддержки алгоритмов, использующих ассиметричные методы шифрования;

– для шифрования сетевых папок;

– для разграничения прав доступа к информации между сотрудниками.

Сеть Фейстеля как элемент, усложняющий алгоритм шифрования, используется во многих современных алгоритмах, в частности, включая ГОСТ 34.12-2015.

Конструкция Фейстеля состоит из ячеек, называемых ячейками Фейстеля. На вход каждой ячейки поступают данные и ключ. На выходе получают измененные данные и измененный ключ. Все ячейки однотипны, и говорят, что сеть представляет собой определенную многократно повторяющуюся (итерированную) структуру. Ключ выбирается в зависимости от алгоритма шифрования/расшифрования и меняется при переходе от одной ячейки к другой. При шифровании и расшифровании выполняются одни и те же операции; отличается только порядок ключей. Ввиду простоты операций сеть Фейстеля легко реализовать как программно, так и аппаратно [5].

Большинство современных блочных шифров (DES, RC2, RC5, RC6, Blowfish, FEAL, CAST-128, TEA, XTEA, XXTEA и др.) используют сеть Фейстеля в качестве основы. Альтернативой сети Фейстеля является подстановочно-перестановочная сеть (AES и др.). Также существуют различные модификации конструкции Фейстеля, которые используют для шифрования 4 ветви, или так называемые «несбалансированные» сети, особенностью которых является различная длина правого и левого подблока. В данном случае сеть состоит из 2 ветвей, длина блока фиксированная.

На рисунке 1 представлено схематическое изображение шифрования и дешифрования с использованием сети Фейстеля (см. рис. 1).

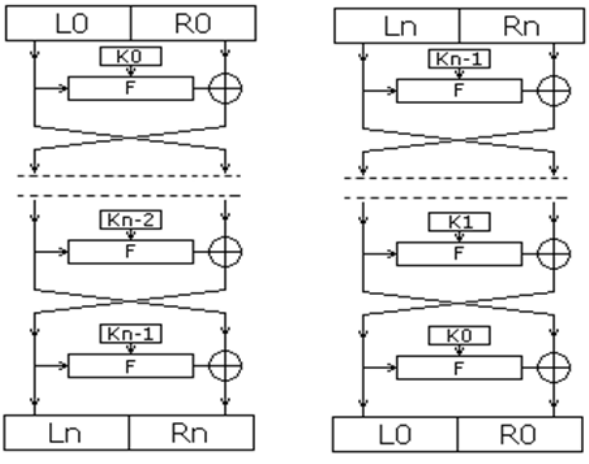


Рис. 1. Процесс шифрования/дешифрования.

Пусть необходимо зашифровать некоторую информацию, представленную в двоичном виде (в виде последовательности нулей и единиц) и находящуюся в памяти компьютера или иного устройства (например, в файле).

Информация разбивается на блоки одинаковой (фиксированной) длины. Полученные блоки называются входными, так как поступают на вход алгоритма. В том случае если длина блока на входе алгоритма меньше, чем размер, который выбранный алгоритм шифрования способен зашифровать единовременно (размер блока), то блок удлиняется каким-либо способом. Как правило, длина блока является степенью двойки, например, составляет 64 бита или 128 бит.

Далее будем рассматривать операции, происходящие только с одним блоком, так как в процессе шифрования с другими блоками выполняются те же самые операции.

Выбранный блок разбивается на две части: L – левая и R – правая.

Левый подблок изменяется функцией f с пользованием раундового ключа k: $x = f(L_0, R_0)$.

Результат складывается по модулю 2 с правым подблоком: $x = x \oplus R_0$.

Результат будет использован в следующем раунде в роли левого подблока: $L_1 = x$.

Левый подблок текущего раунда будет использован в роли правого подблока: $R_1 = L_0$.

По какому-либо математическому правилу вычисляется раундовый ключ k, который будет использоваться в следующем раунде.

В целях демонстрации работы сети Фейстеля была разработана программа (см. рис. 2), позволяющая шифровать текстовую информацию и изображения. ПО было разработано на языке программирования C# в среде VisualStudio 2017 [1, 2].

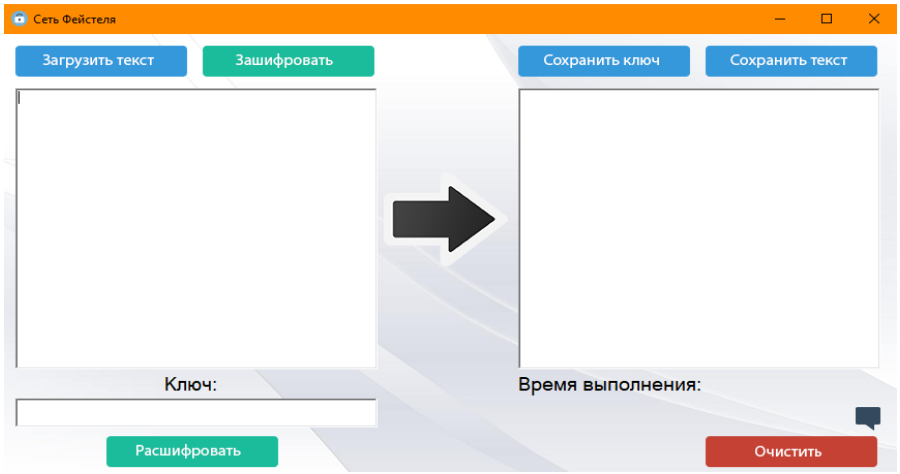


Рис. 2. Главное окно программы.

На рисунке 3 приведен код, осуществляющий шифрование с использованием сети Фейстеля.

```
public static string Feistel_Encrypt (string pt)
        {
            List<string> blocks_inp = new List<string>();
            List<string> blocks_out = new List<string>();
            int step = 0;
            for (int i = 0; i < pt.Length / 8; i++)
            {
                blocks_inp.Add(pt.Substring(step, 8));
                step = step + 8;
            }
            string left, right, new_left, function;
            left = right = new_left = function = "";
            for (int i = 0; i < blocks_inp.Count; i++)
            {
                left = operations.string_to_bit(blocks_inp[i].Substring(0, blocks_inp[i].Count() / 2));
                right = operations.string_to_bit(blocks_inp[i].Substring(blocks_inp[i].Count() / 2,
blocks_inp[i].Count() / 2));
                for (int j = 0; j < 8; j++)
                {
                    function = operations.sum(left, operations.string_to_bit(key.keys[j]));
                    new_left = operations.sum(function, right);
                    right = left;
                    left = new_left;
                }
                blocks_out.Add(string.Concat(left, right));
            }
            string ct = "";
            for (int i = 0; i < blocks_out.Count; i++)
            {
                ct += operations.bit_to_string(blocks_out[i]);
            }
            return ct;
        }
```

Рис. 3. Программный код для шифрования.

На рисунке 4 приведен код, осуществляющий дешифрование с использованием сети Фейстеля.

```
public static string Feistel_Decrypt(string ct)
        {
            List<string> blocks_inp = new List<string>();
            List<string> blocks_out = new List<string>();
            int step = 0;
            for (int i = 0; i < ct.Length / 8; i++)
            {
                blocks_inp.Add(ct.Substring(step, 8));
                step = step + 8;
            }
            string left, right, new_right, function;
            left = right = new_right = function = "";
            for (int i = 0; i < blocks_inp.Count; i++)
            {
                left = operations.string_to_bit(blocks_inp[i].Substring(0, blocks_inp[i].Count() / 2));
                right = operations.string_to_bit(blocks_inp[i].Substring(blocks_inp[i].Count() / 2,
blocks_inp[i].Count() / 2));
                for (int j = 7; j >= 0; j--)
                {
                    function = operations.sum(right, operations.string_to_bit(key.keys[j]));
                    new_right = operations.sum(function, left);
                    left = right;
                    right = new_right;
                }
                blocks_out.Add(string.Concat(left, right));
            }
            string pt = "";
            for (int i = 0; i < blocks_out.Count; i++)
            {
                pt += operations.bit_to_string(blocks_out[i]);
            }
            return pt;
        }
```

Рис. 4. Программный код для дешифрования.

В качестве функции шифрования была использована сумма по модулю 2 [3].

```
public static string Reshuffle(string pt, int shift)
        {
            string substitution = "";
            for (int i = 0; i < pt.Length; i++)
            {
                for (int j = 0; j < vis_8.chars.Length / 2; j++)
                {
                    if (pt[i].ToString() == vis_8.chars[j].ToString())
                    {
                        substitution += vis_8.chars[j + shift];
                        break;
                    }
                }
            }
            return substitution;
        }
```

Рис. 5. Функция подстановки.

В целях улучшения алгоритма шифрования была добавлена функция подстановки (см. рис. 5).

В заключение хочется отметить, что конструкция Фейстеля является довольно криптостойкой при правильной ее реализации, и интеграция ее в алгоритмы шифрования обеспечивает высокую защиту от криптоанализа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Документация сервиса «MSDN – информационный сервис для разработчиков» [Электронный ресурс]. – Режим доступа: https://msdn.microsoft.com.

2. Информационный ресурс «CyberForum – форум программистов и сисадминов» [Электронный ресурс]. – Режим доступа: https://cyberforum.ru.

3. Михайленко Е.В. Дискретная математика: учебное пособие. – Краснодар: Краснодарский университет МВД России, 2016.

4. Петров А.А. Криптографические методы защиты // Компьютерная безопасность. – М.: ДМК, 2000. – 448 с.

МЕТОДЫ ОБНАРУЖЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В ХОДЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

METHODS OF DETECTING DIGITAL INFORMATION IN THE INVESTIGATION OF CRIMES

Жукова Полина Николаевна
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Жукова Наталья Алексеевна
(Белгородский государственный университет (НИУ «БелГУ»));
Насонова Валентина Афанасьевна
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Zhukova Polina Nikolaevna
(Belgorod Law Institute of MIA of Russia named after I.D. Putilin);
Zhukova Natalia Alekseevna
(Belgorod State University (NIU «BelSU»));
Nasonova Valentina Aphanasievna
(Belgorod Law Institute of MIA of Russia named after I.D. Putilin)

Аннотация: в статье рассмотрены вопросы обнаружения цифровой информации в ходе раскрытия и расследования преступлений.
Ключевые слова: информационные технологии, цифровая информация.

Abstract: the paper deals with the detection of digital information in the disclosure and investigation of crimes.
Key words: information technologies, digital information.

На настоящий момент в процессе выявления, раскрытия и расследования преступлений важную роль играет цифровая информация и электронные доказательства. Как показывает следственная практика, электронные доказательства в сегодняшний день используются почти в каждом уголовном деле, что говорит о широком использовании электронных носителей информации как в криминальной деятельности при совершении практически всех составов преступлений, так и в работе правоохранительных органов, использующих новейшие информационные технологии для борьбы с преступностью.

Электронные носители информации как источник доказательств имеют исключительное значение для выявления и раскрытия преступления, а также для изобличения либо реабилитации обвиняемого. Небрежность в обращении с ними нередко оказывается причиной признания их недопустимыми или неотъемлемыми. Порядок обращения с электронными доказательствами изложен в ст.ст. 81, 82, п. 9.1. ст.ст. 182, 213, 220, 299, 309 УПК РФ.

Необходимо отметить, что использование результатов оперативно-разыскных мероприятий (далее – ОРМ) в качестве доказательств предусмотрено федеральным законодательством, а именно ст. 11 Федерального закона от

12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ об ОРД) [2] . Одним из критериев применения результатов ОРМ в качестве доказательств являются их проверка и оценка, проведенные правоприменителями (следователь, дознаватель, оперативный сотрудник, прокурор, суд) с помощью положений криминалистической техники и тактики, в соответствии с алгоритмами расследования, разрабатываемыми конкретной частной методикой.

Кроме того, законодательством разрешается использовать в доказывании обстоятельств совершенного преступления именно результаты ОРД (фактические данные [3], сведения (п. 36.1 ст. 5 УПК РФ) [1]), а не материалы, которые сами по себе только подтверждают факт проведения ОРМ, предусмотренного ФЗ об ОРД.

Следует отметить, что проверка и оценка результатов ОРД как возможных доказательств имеет ряд существенных отличий от такой деятельности в отношении доказательств, полученных в ходе выполнения следственных действий, предусмотренных УПК РФ.

В деятельности правоохранительных органов информационные технологии используются во всех областях деятельности, однако, необходимо отметить проблемные вопросы использования цифровых средств фиксации на стадиях досудебного производства:

- недостаточно разработанные процессуальные, методические и организационно-технические аспекты оформления и дальнейшего применения результатов цифровых средств фиксации;

- отсутствие необходимого количества практических рекомендаций – для сотрудников органов внутренних дел по применению электронных носителей информации.

Особенности механизмов совершения правонарушений с использованием информационных технологий характеризуются специфичностью следовых картин. Таким образом, большое внимание при проведении ОРД уделяется отдельным мероприятиям при осмотре и выемке цифровой информации.

В первую очередь необходимо отметить, что электронные доказательства, обнаруженные в ходе осмотра места происшествия, выемки, обыска, необходимо осмотреть, фиксируя в протоколе его состояние, в силу которых они могут приобрести значение для дела, а также их индивидуальные признаки, выделяющие их из множества иных видов доказательств. Также согласно ст. 182 УПК РФ выемка электронных доказательств происходит в присутствии специалиста (эксперта).

Рассматривая методы изъятия электронных доказательств, необходимо отметить, их различие в зависимости от вида электронного носителя информации.

При осмотрах, обысках, выемках, сопряженных с изъятием как компьютерной техники, так и мобильных телефонов, зачастую возникает ряд общих проблем, связанных со спецификой изымаемых объектов.

Фактически оптимальный вариант изъятия мобильного телефона и носителей информации – это фиксация их и их конфигурации (в случае компьютерной техники) на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнару-

жения, соединить в лабораторных условиях или в месте производства экспертиз с участием специалистов.

В случае изъятия средств мобильной связи согласно ч. 3.1 ст. 183 УПК РФ изъятие мобильного телефона возможно только в присутствии специалиста.

С мобильным устройством связаны следующие виды значимых для следствия следов:

- следы на электронных носителях – сведения о соединениях абонентов, о произведенных финансовых операциях, системе сотовой связи и т.д., хранящиеся у сотовых операторов либо на компьютерах, изъятых у подозреваемого (обвиняемого);

- следы на мобильном устройстве – абонентская книга телефона, сведения о соединениях абонентов сетей сотовой связи (журнал звонков, сообщения SMS, MMS, EMS), о произведенных финансовых операциях, системе сотовой связи, специальные программные средства для прошивки мобильных телефонов, SIM-карт, данные из прикладных приложений Viber, Skype, WhatsApp, Facebook, Vkontakte и др., которые могут содержать данные пользователей мобильных телефонов, IMEI-код, изменение последнего программными средствами, используемые телефонные номера, фотографии и видеозаписи, следы пальцев рук, микрочастиц;

- следы на SIM-карте, абонентская книга, журнал звонков, сообщения SMS, данные о служебных сообщениях.

По прибытии на место осмотра или обыска следует принять меры к обеспечению сохранности информации на находящейся компьютерах, мобильных телефонах и носителях информации. Для этого необходимо:

- не разрешать кому бы то ни было из лиц, присутствующих на месте происшествия или объекте обыска, прикасаться к работающим компьютерам, мобильным телефонам, носителям информации, включать и выключать их;

- самостоятельно не производить никаких манипуляций с компьютерной и сотовой техникой, если результат этих манипуляций заранее не известен;

- при наличии в помещении, где находятся средства компьютерной и сотовой техники, а также носители информации, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов как можно скорее их транспортировать в другое помещение.

Однако в случае его отсутствия обозначим действия рядовых сотрудников правоохранительных органов.

Изъятие информации семантического характера производится путем копирования на иной электронный носитель информации, причем носитель информации должен быть опечатан, после копирования на него информации.

При обнаружении электронного носителя, размещенного в сети Интернет, проводить следующие действия:

- исключить возможность доступа в любой форме к фиксируемому устройству любых лиц, не включенных в состав следственно-оперативной группы;

- убедиться, что электроснабжение объекта осмотра не будет внезапно прервано;

- любые действия производить в присутствии специалиста;

- перед выполнением любых действий на компьютере сохранять скриншоты;

- дополнительно осматривать документацию, находящуюся в непосредственной близости от осматриваемого устройства;

- в протоколе следственного осмотра (обыска) должны быть описаны:

- ключевые характеристики изучаемых электронных устройств;
- различимые частные признаки внешнего вида;
- конфигурация и комплектация каждого устройства;
- формальные индивидуализирующие признаки (номер модели, серия, инвентарные номера).

Все это обусловливает настоятельную потребность углубленного криминалистического изучения компьютерной информации и средств ее обработки как следов преступлений, а также повышения роли научных знаний, базирующихся на отечественном и зарубежном опыте применения компьютерных технологий в борьбе с преступностью. Очевидно, что без фундаментальных исследований объективных закономерностей в этой предметной области деятельность правоохранительных органов в обозначенном направлении будет оставаться малорезультативной.

В то же время нужно отметить, что:

- технико-криминалистическое и информационно-компьютерное обеспечение раскрытия, расследования и предупреждения этих преступлений находится в стадии разработки;

- продолжается процесс формирования криминалистических рекомендаций по тактике подготовки и производства отдельных следственных действий, связанных с обнаружением, фиксацией, изъятием и исследованием компьютерной информации и средств ее обработки;

- далеки от совершенства система взаимодействия следствия со специализированными органами дознания и специалистами различных отраслей знаний, зарубежными правоохранительными органами, а также подготовка кадров по соответствующей специализации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Уголовно-процессуальный кодекс РФ от 18.12.2001 № 174-ФЗ // СПС «КонсультантПлюс».

2. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ // СПС «КонсультантПлюс».

3. Приказ МВД РФ от 27.09.2013 № 776 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // СПС «КонсультантПлюс»

4. Электронные носители информации в криминалистике: монография / под ред. д-ра юрид. наук О.С. Кучина. – М.: Юрлитинформ, 2017.

5. Зуев С.В., Никитин Е.В. Информационные технологии в решении уголовно-процессуальных проблем // Всероссийский криминологический журнал. 2017. Т. 11. № 3. С. 587-595.

ИССЛЕДОВАНИЯ ПЛАТЕЖНЫХ КАРТ ПРИ ПРОВЕДЕНИИ ЭКСПЕРТИЗ

THE RESEARCH OF PAYMENT CARDS DURING EXAMINATIONS

Насонова Валентина Афанасьевна
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Кассим Кабус Дерхим Али
(Курская государственная сельскохозяйственная академии имени И.И. Иванова);
Алдиаб Анас
(Университет Дамаска)

Nasonova Valentina Aphanasievna
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin)
Kassim Kabus Dherhim Ali
(Kursk State Agricultural Academy named after I.I. Ivanov);
Aldiab Anas
(University of Damascus)

Аннотация: в статье рассмотрены вопросы процедуры исследования платежных карт при проведении экспертизы.
Ключевые слова: платежные карты, экспертиза.

Abstract: the paper deals with research of payment cards during the examination procedure.
Key words: payment cards, examination.

С появлением в обращении платежных пластиковых карт правоохранительные органы соприкоснулись с новой и серьезной проблемой – хищениями денежных средств с банковских счетов при помощи платежных карт. Статистика последних лет указывает на ежегодный рост числа выявленных мошенничеств (ст. 159 УК РФ), совершаемых с использованием поддельных кредитных либо расчетных карт.

Предмет рассматриваемого преступления указан в диспозиции ст. 187 УК РФ, однако, перечень строго не определен. К предмету относятся кредитные и расчетные карты, а также платежные документы, не являющиеся ценными бумагами:

– расчетная карта [1] – банковская платежная карта, предназначенная для совершения операций ее держателем в пределах суммы денежных средств клиента, находящихся на его банковском счете, или кредита, предоставляемого кредитной организацией – эмитентом клиенту в соответствии с договором банковского счета при недостаточности или отсутствии на банковском счете денежных средств (овердрафт);

– кредитная карта – банковская платежная карта, предназначена для совершения ее держателем операций, расчеты по которым осуществляются за счет денежных средств, предоставленных кредитной организацией.

Объективной стороной ст. 187 УК РФ являются два самостоятельных действия:

– изготовление в целях сбыта поддельных кредитных либо расчетных карт и платежных документов, не являющихся ценными бумагами;

– сбыт поддельных кредитных либо расчетных карт и платежных документов, не являющихся ценными бумагами.

Поддельная платежная карта должна быть полностью аналогична оригиналу, т.е. должны иметься достаточные основания принять такую карту за настоящую. При этом поддельный образец содержит основные реквизиты оригинала, допускающие ее использование по предназначению. К их числу обычно относятся:

– фирменное (официальное) наименование эмитента карты;
– номер карты;
– имя и фамилия держателя карты;
– срок действия карты;
– образец подписи держателя карты.

С 1 июня 1999 года действует изданное Министром внутренних дел Российской Федерации распоряжение «О формировании и ведении в ЭКЦ МВД России Федерального учета поддельных пластиковых платежных карт и дорожных чеков», созданное в целях установления общности происхождения поддельных пластиковых платежных карт и дорожных чеков по способу и технологии изготовления, а также для выявления лиц, занимающихся их изготовлением.

В связи с тем, что понятия поддельной или подлинной кредитной или расчетной карты являются юридическими, вывод об этом должен делать следователь. Экспертиза же должна дать необходимые и достаточные данные для признания карты подлинной или поддельной.

Рассмотрим особенности назначения экспертиз при расследовании преступлений, связанных с незаконным оборотом платежных карт.

Сразу же необходимо отметить, что значение для расследования преступлений, связанных с незаконным оборотом платежных карт, играет применение в расследовании данных преступлений специальных познаний.

Рассмотрим виды поддельных платежных банковских карт.

1. Полностью изготовленная поддельная карта – карта, имитирующая настоящую карту, включая внешний вид и запись информации на магнитную полосу. В пластик карты может быть вмонтирована микросхема, но использование ее при проведении незаконных операций в настоящее время не осуществляется и информация на нее не записывается. Такие карты предназначены для обмана персонала предприятий торговли, принимающего карты, относительно их подлинности и проведения платежных операций в данных торговых предприятиях.

2. Поддельная карта, изготовленная путем частичной подделки.

- подделка карты, выпущенной законным эмитентом, производителем, платежной системой. Карта, изготовленная путем изменения эмбоссированных реквизитов карты, например, номера карты. Может использоваться для операций, осуществляемых с помощью импринтера. В этом случае информация, записанная на магнитную полосу и микросхему, не имеет для злоумышленника никакого значения;

- карта, изготовленная путем изменения информации, записанной на магнитную полосу карты. Может использоваться для операций, осуществляемых с помощью электронного терминала. Информация, физически нанесенная на карту (номер, срок действия), отличается от информации, записанной на магнитную полосу. В случае нанесения на карту неполного номера (Visa Electron) возможен подбор реквизитов для магнитной полосы, совпадающих с нанесенными на пластике.

Комбинация двух выше названных методов: заготовка карты, предназначенной для совершения мошеннических операций, как правило, для хищения денежных средств в торговых точках при соучастии продавца или в банкоматах, терминалах самообслуживания. В качестве «белого пластика» могут быть использованы любые пластиковые карты со стандартно расположенной магнитной полосой – дисконтные, клубные, идентификационные, подарочные, транспортные, сувенирные, рекламные и т.п.:

- карта, изготовленная путем эмбоссирования реквизитов карты (номер, срок действия, имя держателя). Такие карты предназначены для проведения операций с использованием импринтера. В торговом предприятии операции можно совершить только при пособничестве кассира;

- карта, изготовленная путем нанесения информации с подлинных карт на магнитную полосу.

Возможны несколько вариантов использования:

а) проведение операций на электронных торговых терминалах в предприятиях торговли. При этом необходим сговор с кассиром;

б) совершение операций в торговых (сервисных) терминалах самообслуживания (автоматы по продаже автобусных или железнодорожных билетов, счетчики на автомобильных стоянках, автоматические терминалы на АЗС, телефоны, платные дороги и др.). При данных операциях существует ограничение по максимальной разрешенной сумме;

в) совершение операций в банкоматах. Необходимо знание ПИН-кода.

Исходя из вида поддельных карт, необходимо назначение конкретной судебной экспертизы и формирование конкретных вопросов, которые ставятся на разрешение эксперту.

Рассматривая виды судебных экспертиз, необходимо отметить, что в случае проверки установления подлинности платежных карт могут быть назначены следующие экспертизы:

1. Судебная технико-криминалистическая экспертиза.

2. Судебная компьютерно-техническая экспертиза платежных карт.

3. Судебная почерковедческая экспертиза.

4. Судебная химическая экспертиза.

5. Судебная дактилоскопическая экспертиза.

В данной работе остановимся на особенностях проведения технико-криминалистической экспертизы.

В первую очередь необходимо установить, соответствует ли представленная на исследование платежная карта по способу изготовления и качеству воспроизведения полиграфических реквизитов аналогичной продукции платежных систем.

Размеры карт должны соответствовать требованиям стандарта ISO-7810 «идентификационные карты – физические характеристики» и иметь следующие размеры: ширина (85,595 ± 0,125 мм), высота (53,975 ± 0,055 мм), толщина (0,76 ± 0,08 мм), радиус окружности в углах (3,18 мм).

Обязательные реквизиты: поле для подписи, срок действия карты, полоса для подписи (возможность подчищения), BIN (базовый идентификационный номер – выполнен способом печати, расположен под номером карточки, повторяет первые четыре цифры эмбоссированного номера карточки, причем оба номера всегда начинаются с цифры «4»), логотип (всегда помещается на лицевой стороне карточки справа, выше или ниже голограммы, по периметру логотипа нанесен микротекст), голограмма (при наклоне карточки изображение на голограмме должно двигаться, последние четыре цифры номера карточки должны быть полностью расположены на голограмме), защитный символ (виден только в ультрафиолетовых лучах).

Экспертиза карты заключается в осуществлении следующих основных исследований, по результатам которых можно сделать вывод о поддельной кредитной или расчетной карте, представленной на экспертизу.

1. Определение типа платежной системы, банка эмитента и банковского продукта. Тип платежной системы определяется по логотипу и первым цифрам номера карты. Информация о банке-эмитенте содержится в электронной базе данных, которая регулярно обновляется и рассылается банкам принципиальным членам платежной системы. Информация о карточном продукте (кредитная или расчетная, а также ее тип содержится в таблицах БИН (BIN tables), которые находятся в процессинговых центрах, подключенных к сети и служат для маршрутизации операций по картам сторонних эмитентов в устройствах процессингового центра. Таким образом, в случае несоответствия информации, графически нанесенной на пластиковой карте, со сведениями из баз данных платежных систем – название банка эмитента и (или) карточного продукта, то данная карта является поддельной.

2. Анализ информации, закодированной на магнитной полосе карты. На первой дорожке (трек 1), состоящей из 76 буквенно-цифровых символов, значимой для эксперта является следующая информация: номер карты (длина – 16 цифр), начинается с третьего символа; имя держателя (длина – от 2 до 26 символов), начинается за номером карты после разделительного знака; дата действия карты – 4 символа, начинается за именем держателя после разделительного знака в формате ГГММ; сервис-код – 3 символа, начинается сразу за датой действия карты без разделительного знака.

На второй дорожке (трек 2) значимой для эксперта является следующая информация: номер карты (длина – 16 цифр), начинается со второго символа; дата действия карты – 4 символа, начинается за номером карты после разделительного знака в формате ГГММ; сервис код – 3 символа, начинается сразу за датой действия карты без разделительного знака.

Значения сервис-кода определяют:

- первая цифра международная карта или международная карта с микропроцессором для локального использования или для локального использования с микропроцессором, для карт частных или ограниченных сетей;

- вторая цифра: нормальная авторизация, «позитивная» авторизация – разрешение на проведение транзакции, полученное от эмитента или от альтернативного процессингового центра.

- третья цифра: требование ПИН, нормальная верификация (проверка), только товары и услуги в POS (не наличные), действительна только для сети Plus, запрашивает ПИН, если есть пин-пад.

Другие значения, например, коды PVV, CVV, CVC, не являются значимыми для экспертизы, так как проверить их может только эмитент.

Полученная с магнитной полосы информация позволяет получить недостающие реквизиты карты в случае отсутствия их графического нанесения и провести сравнение с графически нанесенной информацией.

В случае несовпадения реквизитов карты, нанесенных графически и закодированных в электронном виде, имеем перекодированную поддельную карту. Возможность проведения электронных операций с использованием терминалов устанавливается с использованием трека 2 по номеру карты, дате действия, сервис коду. Номер карты, записанный на втором треке, позволит также определить название банка эмитента, тип карточного продукта и отнести карту к кредитной, расчетной или предоплаченной, аналогично вышеописанной методике, указанной ранее. Данный анализ позволяет идентифицировать «белый пластик» как поддельные кредитные, расчетные карты и выявлять перекодированные карты.

В случае использования перекодированной карты для проведения операции по магнитной полосе с использованием электронного терминала в платежной системе отразится номер карты, записанный на магнитную полосу, и банк эмитент именно этот номер занесет в отчет о мошенничестве как операцию по поддельной карте.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием: ЦБ России от 24.12.2004 № 266-П. П. 1.5 // СПС «КонсультантПлюс».

2. Обзор мобильных мессенджеров [Электронный ресурс]. – Режим доступа: http://www.voipoffice.ru/tags/mobil%27nye_messendzhery.

3. Мессенджеры в России: цифры и тренды, весна 2017 [Электронный ресурс]. – Режим доступа: http://blog.br-analytics.ru/messendzhery-vesna-2017.

4. Электронные носители информации в криминалистике: монография / под ред. д-ра юрид. наук О.С. Кучина. – М.: Юрлитинформ, 2017.

СЕКЦИЯ № 4.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

О ВОЗМОЖНОСТЯХ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОГО УЧЕБНОГО ПОСОБИЯ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ» В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

ON THE POSSIBILITIES OF USING THE ELECTRONIC TEXTBOOK «FUNDAMENTALS OF INFORMATION SECURITY IN INTERNAL AFFAIRS AGENCIES» IN THE EDUCATIONAL PROCESS

Мухачев Сергей Валентинович,
Чудин Денис Алексеевич
(Уральский юридический институт МВД России)

Mukhachev Sergei Valentinovich,
Chudin Denis Alekseevich
(Ural Law Institute of the MIA of Russia)

Аннотация: статья посвящена возможностям повышения эффективности образовательного процесса на основе использования электронного учебного пособия «Основы информационной безопасности в органах внутренних дел», изложена структура учебного пособия, предложены способы его интеграции в образовательный процесс.
Ключевые слова: информационная безопасность, информационные технологии, образование, учебное пособие, компетенции, лекция, фотогалерея.

Annotation: the article is devoted to the possibilities of increasing the effectiveness of the educational process on the basis of the use of the electronic textbook «Fundamentals of Information Security in Internal Affairs Bodies», the structure of the training manual is described, and ways of integrating it into the educational process are proposed.
Key words: information security, information technology, education, training manual, competences, lecture, photo gallery.

Применение современных информационных технологий и систем, информационно-телекоммуникационной инфраструктуры позволяет повысить эффективность оперативно-служебной и служебно-боевой деятельности подразделений МВД России. Это обстоятельство нашло отражение в ст. 11 Федерального закона «О полиции» от 07.02.2011 № 3-ФЗ: «полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру».

Однако применение для работы с информацией названных технологий сопряжено с множеством угроз различного характера, которые могут так или иначе реализоваться и повлечь негативные последствия, связанные с воздействием на информационные ресурсы. Поэтому обеспечение информационной безопасности в практике органов внутренних дел имеет большое значение.

Учебная дисциплина «Основы информационной безопасности в органах внутренних дел» достаточно давно вошла в учебные планы образовательных организаций МВД России. Ее актуальность обусловлена широким использованием информационных технологий во всех областях деятельности органов внутренних дел – от делопроизводства до оперативно-разыскной деятельности.

Объем времени, отводимого на освоение учебной дисциплины «Основы информационной безопасности в органах внутренних дел», составляет 72 часа. В соответствии с примерной программой содержание дисциплины разбито на пять тем. Для ее освоения предусмотрены лекции, семинары, практические занятия и аудиторная контрольная работа. Перед преподавателем стоит непростая задача: имея скромный бюджет времени, сформировать соответствующие компетенции по учебной дисциплине, достаточно сложной для освоения, но очень важной в практическом плане. Сложность также обусловлена тем, что учебная дисциплина многогранна – она включает программно-технические, правовые, организационные аспекты.

Для повышения эффективности образовательного процесса на кафедре информационного обеспечения органов внутренних дел Уральского юридического института МВД России подготовлено электронное учебное пособие по учебной дисциплине «Основы информационной безопасности в органах внутренних дел» [1]. В качестве содержательной основы использовано ранее подготовленное печатное учебное пособие [2].

Для реализации содержания электронного учебного пособия использована специализированная инструментальная среда. На ее основе разработан электронный интерфейс с применением методов визуализации в текстовом и графическом виде. Проработана и реализована система размещения информации; подготовлены дополнительные учебно-методические материалы по учебной дисциплине.

Учебное пособие имеет электронный формат, поэтому появилась возможность организовать его таким образом, чтобы обучающийся легко ориентировался в учебных материалах; имел возможность быстро перейти к нужной теме; мог оперативно обратиться к иллюстративным материалам, заданиям, вопросам для самоконтроля.

Электронное учебное пособие включает электронное оглавление и несколько разделов.

Оглавление представляет собой гиперссылки для оперативного поиска материала и быстрого перехода к нему.

В пособие включены следующие разделы.

1. Словарь терминов. В алфавитном порядке представлены термины, относящиеся к информационной безопасности, с определениями и разъяснениями. Приведены наиболее часто встречающиеся аббревиатуры. Этот раздел поз-

воляет обучающимся вникнуть в проблематику, получить разъяснения по наиболее важным понятиям и терминам, найти расшифровку распространенных в области информационной безопасности сокращений.

2. Лекции. В разделе представлены лекции, подготовленные преподавателями кафедры, по всем изучаемым темам.

3. НПА, литература. Содержит наиболее важные нормативно-правовые акты и перечень рекомендуемых для изучения источников.

4. Вопросы, изучаемые на семинарских и практических занятиях. Раздел позволит обучающимся готовиться к занятиям, планировать последовательность работы по учебной дисциплине.

5. Вопросы для самоконтроля по всем изучаемым темам. Обучающийся, используя этот раздел, может самостоятельно определить, насколько полно он знает материал, выявить пробелы, обратить внимание на наиболее сложные вопросы.

6. Фотогалерея. Содержит тщательно подобранные разнообразные графические и фотоматериалы, иллюстрирующие содержание лекций. Раздел призван иллюстрировать текст лекций, мотивировать обучающихся к более внимательному рассмотрению некоторых вопросов.

Для иллюстрации материала в учебное пособие включено большое количество различных рисунков и схем. Они позволяют обучающемуся воспринимать теоретические сведения в привычной для нынешнего поколения форме - в визуальном систематизированном виде.

Таким образом, в электронном учебном пособии аккумулированы все необходимые для работы учебно-методические материалы по учебной дисциплине «Основы информационной безопасности в органах внутренних дел».

Структура и содержание электронного учебного пособия таковы, что возможно его использовать для организации работы в различных формах и на разных видах занятий.

Пособие повысит эффективность образовательного процесса на всех видах занятий: лекциях, практических и семинарских занятиях, для которых имеются задания и необходимый теоретический материал. Оно будет полезно обучающимся для самостоятельной работы: теоретический материал полностью охватывает содержание учебной дисциплины, имеются вопросы для самоконтроля; ключевые термины и понятия можно найти в словаре.

Следует отметить, что работа с таким учебным пособием сегодня привычна для обучающихся, активно пользующихся электронными коммуникационными средствами, компьютерными информационными технологиями, Интернетом, что также стимулирует применять его в образовательном процессе. Можно сказать, что сформирована информационная среда для обучающегося, включающая привычный интерфейс для работы.

Технически для использования в образовательном процессе возможны два варианта: на переносном устройстве (оптический диск или флеш-накопитель) и на сервере компьютерной сети, т.к. учебное пособие реализовано в виде исполняемого файла. Первый вариант удобен для самостоятельной работы обучающегося, второй – для аудиторных занятий в компьютерном классе.

Таким образом, электронное учебное пособие является удобным средством формирования соответствующих компетенций по учебной дисциплине «Основы информационной безопасности в органах внутренних дел». Опыт использования электронного учебного пособия в образовательном процессе показал его эффективность и методическую состоятельность, возможность использования в организации различных видов учебных занятий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Костюченко К.Л., Мухачев С.В., Чудин Д.А. Основы информационной безопасности в органах внутренних дел: учебное пособие [электронное издание]. – Екатеринбург: Уральский юридический институт МВД России, 2016.

2. Костюченко К.Л., Мухачев С.В. Основы информационной безопасности в органах внутренних дел: учебное пособие. – Екатеринбург: Уральский юридический институт МВД России, 2015. – 156 с.

ПРОБЛЕМЫ ПОДГОТОВКИ СОТРУДНИКОВ ОВД К ПРИМЕНЕНИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И ПУТИ ИХ РЕШЕНИЯ

PROBLEMS OF PREPARING THE STAFF OF THE INSTITUTES OF INTERNAL AFFAIRS FOR USING INFORMATIONAL TECHNOLOGIES IN PROFESSIONAL ACTIVITIES AND THE WAYS OF SOLVING THESE PROBLEMS

Ходякова Наталия Владимировна
(Волгоградская академия МВД России)

Khodyakova Nataliya Vladimirovna
(Volgograd Academy of the MIA of Russia)

Аннотация: в статье рассматриваются проблемы выбора актуальных целей, содержания и методов обучения информатическим дисциплинам в вузе МВД России, а также требования к компетентности преподавателей. В контексте анализа многолетнего опыта автора предлагаются варианты решения данных проблем.

Ключевые слова: информационные технологии, информационные компетенции, электронное обучение.

Annotation: problems of choosing urgent aims, content and methods of teaching informatics disciplines at higher educational institutes of the MIA of the Russia, as well as requirements to teachers' competence, are considered in the article. Variants of solving these problems are suggested in terms of the author's long experience.

Key words: informational technologies, informational competencies, e-learning.

Информатизация образовательных организаций МВД России началась более 25 лет назад. За это время в ведомственных вузах накоплен большой опыт обучения информационным технологиям, который позволяет сформулировать ряд актуальных проблем и предложить варианты их возможного решения.

Первая из проблем связана с *корректной постановкой целей* обучения по информатическим дисциплинам. В начале информатизации органов внутренних дел (начало 1990-х годов), сопровождавшейся появлением на рабочих местах сотрудников ОВД первых персональных компьютеров, цель обучения в вузах МВД России формулировалась как «компьютерная грамотность» и подразумевала знание обучающимися устройства персонального компьютера, владение умениями управления им с помощью команд дисковой операционной системы (MS DOS) или программ-оболочек (Norton Commander, PCTools и др.), составления алгоритмов простейших программ и их перевода на язык программирования (BASIC и др.). К середине 1990-х годов в связи с появлением на рынке информационных продуктов множества прикладных программ компьютерная грамотность трансформировалась в цель «подготовка пользователя персонального компьютера». Эта цель предполагала дополнительное освоение обучающимися умений работы с: текстовыми редакторами (ЛЕКСИКОН), электронными таблицами (SuperCalc), базами данных (DBASE) и другими программами (клавиатурные тренажеры, графические редакторы, звуковые редакторы и т.д.). В конце 1990-х годов в вузах МВД России, как и по всей стране, в качестве целевого ориентира в преподавании информатических дисциплин стала рассматриваться цель «информационная культура специалиста», предусматривавшая, помимо знаний информатики и информационных технологий и умений пользователя персонального компьютера также знание обучающимися социально-гуманитарных проблем информатизации и умение их предупреждать и преодолевать. Обе цели находили свое отражение в нормативных документах и реализовывались в обучении тем или иным информатическим дисциплинам в зависимости от предпочтений педагогических работников. С присоединением России к Болонскому процессу (2003 год) и появлением государственных образовательных стандартов нового поколения в качестве целей обучения в вузах стало заявляться формирование у обучающихся информационных компетенций, предполагающих не только компьютерную грамотность и сформированность умений пользователя, но и формирование готовности к решению профессиональных задач с использованием информационных технологий. В отличие от информационной культуры, формируемой в ходе непрерывного образования в течение всей жизни человека, компетентность специалиста в области информационных технологий – цель, которая может быть достигнута за период обуче-

ния в вузе, поэтому именно эта цель обучения информационным технологиям представляется наиболее подходящей для высшего образования.

Вторая проблема состоит в адекватном дидактической цели *отборе содержания обучения* будущих специалистов: определении состава и объема преподаваемых дисциплин в учебных планах, выделении дидактических единиц рабочих программ дисциплин, выборе источников учебной информации. Ретроспективный анализ учебного содержания показывает, что в начальный период информатизации в учебных планах вузов МВД России были представлены как минимум две информатические дисциплины: первая преподавалась на первом курсе и была ориентирована на изучение компьютера и теоретические основы информатики («Правовая информатика и вычислительная техника»), а вторая преподавалась на старших курсах и предполагала освоение информационно-профессиональных приложений («Информационные технологии в деятельности ОВД», «Информационное обеспечение деятельности ОВД» и др.). В настоящее время примерные учебные планы для информатических дисциплин («Информатика и информационные технологии в профессиональной деятельности», «Основы информационной безопасности в ОВД») отводят 1-й и 2-й курсы обучения, в то время как на старших курсах такие дисциплины не преподаются. Думается, что такое решение должно быть подвергнуто ревизии. Во-первых, на первом курсе обучающийся не имеет необходимых представлений о профессии, а значит, и обсуждать с ним вопросы оптимизации этой профессиональной деятельности с помощью информационных технологий рано. Во-вторых, информатизация развивается столь стремительно, что содержание обучения, освоенное на первых курсах, через 3-4 года безнадежно устаревает, поэтому есть объективная необходимость в разделении учебной дисциплины «Информатика и информационные технологии в профессиональной деятельности» на две: первую из них – «Информатику» – следует преподавать на первом курсе, а вторую «Информационные технологии в профессиональной деятельности» – на выпускном или в крайнем случае на предвыпускном курсе.

Кроме того, выделение дидактических единиц профессионально ориентированного учебного курса целесообразно проводить в соответствии с типологией профессиональных задач, решаемых специалистом. В этом случае содержание учебной дисциплины будет максимально отвечать цели формирования информационно-профессиональных компетенций.

Что касается выбора источников учебной информации, то наряду с фундаментальными учебниками, имеющими гриф Минобрнауки или МВД России, помогающими сформировать у обучающихся системные знания по информатике, в учебном процессе должны использоваться дополнительные источники – современные электронные образовательные ресурсы, создаваемые в вузах МВД России и представленные в единой ведомственной компьютерной сети, которые раскрывают профессиональные аспекты использования информационных технологий в деятельности специалиста соответствующего профиля, закрепленного за данным вузом.

Третья проблема обусловлена *выбором продуктивных методик и средств обучения.* Многолетний опыт поиска наиболее результативных методик обучения по информатическим дисциплинам привел нас к выводу о необходимости сочетания методов и средств традиционного и электронного обучения: 1) предъявление новой учебной информации в мультимедийной форме (мультимедийные презентации, обучающие видеокурсы, интерактивные обучающие программы); 2) выполнение практикума по применению и конкретизации знаний, освоению умений и навыков (работа с компьютерными тренажерами; лабораторные работы); 3) контроль приобретенных знаний и умений (компьютерные опросы, экспресс-опросы); 4) решение профессионально ориентированных ситуационных задач; 5) дистанционная поддержка на занятиях учебной деятельности каждого обучающегося (использование сетевой компьютерной программы iTalc); 6) участие в конкурсе учебно-исследовательских проектов по инновационной кафедральной тематике; 7) предметные викторины и олимпиады, в том числе в режиме видеосвязи с другими вузами; 8) использование имитационного профессионального программного обеспечения (ИБД-Р); 9) организация коллективно-распределенной учебной деятельности (задания с использованием сетевых возможностей); 10) рейтинговая оценка успешности учебной деятельности и др.

Четвертая проблема связана с особыми требованиями к *компетентности педагогических работников*, преподающих информатические дисциплины. Эта проблема состоит в том, что преподаватель, обучающий дисциплине «Информатика и информационные технологии в профессиональной деятельности», должен обладать двумя группами компетенций. Первую группу составляют информационные компетенции, вторую – компетенции в той профессиональной области, по которой осуществляется подготовка будущих специалистов. Без знания основ профессии, которой овладевают курсанты, невозможно обучать курсантов применению информационных технологий в этой профессии. То есть речь идет о получении образования двух профилей: естественнонаучного (или технического) и юридического. В случае отсутствия второго образования его следует получить в форме заочного обучения или обучения по дополнительным профессиональным программам.

Резюмируя, отметим, что проблемы постановки целей, отбора содержания, определения методик обучения и соответствующей подготовки преподавателей не могут сегодня решаться без учета более чем 25-летнего опыта информатизации ведомственного высшего образования.

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВЫСШЕМ ОБРАЗОВАНИИ

THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY IN HIGHER EDUCATION

Перепелкин Игорь Николаевич,
Дунаев Роман Алексеевич
(Белгородский государственный институт искусств и культуры)

Perepelkin Igor Nikolaevich,
Dunaev Roman Alekseevich
(Belgorod State Institute of Arts and Culture)

Аннотация: в статье рассматривается актуальный вопрос внедрения информационно-коммуникационных технологий в образовательную деятельность высших учебных заведений. Показано, что применение информационных технологий имеет как положительные, так и отрицательные стороны в решении задачи получения высококвалифицированных специалистов.
Ключевые слова: дистанционное образование, информационно-коммуникационные технологии, образовательная деятельность, виртуальный объект.

Annotation: the article deals with the topical issue related to the implementation of information and communication technology in educational activities of higher education institutions. It is shown that the use of information and communication technology has both positive and negative sides concerning the problem of highly skilled professionals training.
Key words: long distance education, information and communication technology, educational activities, virtual object.

В последние годы очень активно идет модернизация российского образования, которая предполагает широкое использование информационно-коммуникационных технологий в учебном процессе. С развитием сети Интернет проявилась возможность развивать дистанционное образование, что обеспечит доступность образовательных ресурсов для всех слоев населения [1, с. 61].

Внедрение информационно-коммуникационных технологий в высшее образование имеет ряд преимуществ по сравнению с традиционным обучением. Применение информационных технологий способствует повышению уровня доступности образования, дает возможность студентам пользоваться размещенными на серверах электронными учебниками и учебно-методическими комплексами дисциплин. Также студенты имеют возможность построения индивидуальной траектории обучения, что позволяет определять время и последовательность изучения дисциплин. Кроме того, появляется возможность несколько раз выполнить лабораторные и практические работы, что в реальных условия бывает очень проблематично. Использование информационно-комму-

никационных технологий дает возможность студентам и преподавателям общаться посредством электронной почты, форумов, чатов.

Несмотря на достоинства внедрения информационно-коммуникационных технологий в образование, имеется ряд негативных факторов, которые нельзя не учитывать. Применение информационных технологий ориентирует студентов в основном на репродуктивный характер деятельности, который не требует даже понимания смысла. Использование информационно-коммуникационных технологий приводит к замещению сложного и сверхсложного мышления простым. При наличии простого способа решения задач сознание человека не стремится использовать более сложные методы, и студент, который имеет возможность механически выполнить требования преподавателей, идет по самому простому пути, не вникая в суть процесса или явления.

Еще один вариант негативного воздействия информационных технологий – ситуация с сообщениями, рефератами и докладами [2, с. 117]. Студенты имеют возможность не тратить время на поиск и обработку информации, а воспользоваться готовым рефератом из сети Интернет, совершенно не вникая в его суть. Самостоятельная работа по написанию требует рационального мышления, а простое скачивание – выполнение неосмысливаемого стандартного алгоритма. В результате этого многие преподаватели отказываются от практики проверки знаний в виде рефератов и докладов.

Еще одним минусом внедрения информационных технологий в образование является переход к электронным лабораторным работам, которые обладают рядом неоспоримых достоинств. К ним можно отнести дешевизну, простоту проведения, унификацию оборудования. Электронные лабораторные работы – это компьютерная имитация некоторого процесса: студенты должны воспользоваться объектом, провести ряд манипуляций и получить требуемый результат. В данной ситуации все эти действия студенты совершают не с самим объектом, а с его виртуальным образом. Такая замена объекта на виртуальный имеет ряд существенных недостатков.

Во-первых, практические действия в электронных лабораторных работах заменяются только чтением и наблюдением. Известно, что человек запоминает 90% информации, когда он что-то делал сам. Следовательно, внедрение электронных лабораторных работ резко снижает эффективность восприятия студентами учебной информации.

Во-вторых, заложенные в программу свойства виртуального объекта имеют существенные отличия от свойств реального объекта. При создании электронной лабораторной работы учитываются лишь те свойства объекта, которые важны в данной ситуации.

В-третьих, виртуальный объект по своей природе существенным образом отличается от материального. Например, в виртуальных объектах не выполняются законы сохранения, виртуальный объект не обладает инерцией и т.д. Все подобные свойства реального материального объекта могут учитываться при создании виртуальной модели, но набор этих свойств будет ограничен, и результаты будут отличаться от данных реального эксперимента.

Наконец, электронные лабораторные работы не могут учитывать возможные ошибки обучающихся. В ходе выполнения работы возможны различные ошибки, которые невозможно в полном объеме учесть при программировании работы. Исправление ошибок требует от студентов более глубоких знаний процесса, так как в реальности любая ошибка может сделать невозможным выполнение работы или эксперимента. Выполнение электронной лабораторной работы может быть механическим, бездумным, без физических и материальных последствий, а в реальности необходимо понимать свои действия и прогнозировать возможные последствия.

Рассмотрим, активно развивающийся в последние годы вид образования – дистанционное образование. Данный вид обучения предполагает общение студента с преподавателем при помощи компьютерной сети. На первый взгляд, – отличная идея. Но, к сожалению, есть и негативные стороны данного вида деятельности. Известно, что человек запоминает 10% того, что читал, 20% того, что слышал, 30% процентов того, что видел, 50% того, что слышал и читал. Поэтому классическая лекция является незаменимой в образовательном процессе. На лекции студенты слушают излагаемый преподавателем материал, видят чертежи, таблицы, формулы, рисунки и т.п., отбирают и записывают важную информацию, что подразумевает понимание и отбор. В итоге студенты читают, слушают, смотрят, совершают некоторые действия, а также проводят аналитическую работу, что обеспечивает максимальное восприятие. Лекция пока остается самой эффективной формой учебных занятий.

В сложившейся ситуации самым эффективным средством противодействия тенденции упрощения учебной деятельности студентов для сохранения результатов деятельности может служить усиление контроля деятельности и состояния сознания студентов со стороны преподавателя, снижение формальности контроля. Если раньше для проверки, например, курсовой работы достаточно было проверить правильность результатов работы, то сейчас необходимо провести мини-экзамен, чтобы выяснить, сам ли студент выполнил работу и что он реально знает и умеет. В настоящее время мы видим внедрение упрощенных процедур контроля: тесты, интернет-зачеты и интернет-экзамены. Внедрение таких форм контроля методологически ошибочно и противоречит логике и смыслу образовательного процесса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Минеева О.П. Использование информационно-коммуникационных технологий в высшем профессиональном образовании // Современные наукоемкие технологии. 2010. № 2. С. 61-62.

2. Большаков Н.Н., Калачевский Б.А., Носов А.В., Рахуба Л.Ф. О применимости компьютерных (информационных) технологий в образовании // Наука о человеке: гуманитарные исследования. 2009. № 4. С. 115-122.

ПРОБЛЕМЫ И ПРОТИВОРЕЧИЯ ЛИЧНОСТНО-РАЗВИВАЮЩЕГО ЭЛЕКТРОННОГО ОБУЧЕНИЯ

PROBLEMS AND CONTRADICTIONS OF THE PERSON-DEVELOPING E-LEARNING

Петрякова Светлана Викторовна
(Волгоградская академия МВД России)

Petryakova Svetlana Viktorovna
(Volgograd Academy of the MIA of Russia)

Аннотация: в статье автором рассмотрены актуальные проблемы и противоречия электронного обучения в образовании в целом и личностно-развивающем обучении в частности и предприняты попытки предложить решение некоторых из них. В частности, в статье сформулированы критерии качества электронного обучения.

Ключевые слова: электронное обучение, личностно-развивающее электронное обучение, среда электронного обучения.

Annotation: in the article the author examined the actual problems and contradictions of e-learning in education as a whole and personal developmental learning in particular, and attempts were made to offer a solution to some of them. In particular, the article sets forth the criteria for the quality of e-learning.

Key words: e-learning, personal-developing e-learning, e-learning environment.

Электронное обучение является результатом интенсивного развития информационных технологий как в обществе в целом, так и в образовании в частности. Современный уровень информатизации образования позволяет обеспечить субъектам процесса обучения доступ к массивам информации, что положительно влияет на повышение качества самостоятельной работы, открывает перспективы для творческой деятельности и возможности проявить и выявить способности, обрести и закрепить различные навыки.

Педагогические исследователи последних лет (И.В. Роберт, А.В. Хуторской, Е.С. Полат и др.) отмечают, что педагогически грамотное использование информационно-телекоммуникационных технологий позволяет актуализировать специфические средства развития личности обучающихся, связанные с принятием личности обучающегося как ведущей цели и ценности образования, его восприятием как субъекта своего образования и социального самоопределения [7].

Мы разделяем это мнение и считаем электронное обучение, обладающее личностно-развивающим потенциалом, дидактической системой, включающей личностно-развивающие цели, содержание и педагогические технологии обучения, реализующиеся с использованием аппаратно-программных средств обработки, приема, передачи, представления, хранения различных типов учебной

информации и телекоммуникационных технологий обеспечения учебного взаимодействия.

При этом в процессе распространения электронного обучения в образовании в целом и личностно-развивающем обучении в частности встречаются определенные трудности.

В педагогической литературе встает вопрос о необходимости резкого увеличения объёма доступных информационных и образовательных электронных ресурсов. Основным инструментом учебной деятельности в среде электронного обучения являются электронные образовательные ресурсы (ЭОР), к которым можно отнести: электронные учебники, презентации, симуляторы, видеотренинги, тесты и др. Одной из функций педагога в среде электронного обучения является разработка ЭОР, обеспечивающих психолого-педагогическую поддержку обучения, которая осуществляется путем учета системой ЭОР познавательной активности студента и проектируется педагогом с целью повышения творческой активности, самостоятельности, обеспечивая положительную мотивацию учения [3, с. 169]. ЭОР в личностно-развивающей парадигме должны формировать накопление личностного опыта обучающихся путем переживания проблемной ситуации, а именно: ситуации адаптации и первичной когнитивной ориентировки в экранной среде; ситуации предметно-деятельностного ориентирования; ситуации ценностно-смыслового ориентирования; ситуации творческой самореализации и самоутверждения [8].

Несмотря на различные классификации моделей электронного обучения («Moodle», «STELLUS», «Прометей», «АСТ» и др.), к сожалению, в системе отечественного образования нет единых требований к содержанию контента: к структуре учебно-методического наполнения электронного обучения; порядку его применения; порядку проведения экспертизы качества в среде электронного обучения. Разработчики систем электронного обучения ставят задачу создать такую универсальную конфигурацию системы электронного обучения на основе многофункционального ядра, обеспечивающего совместимость различных систем и отдельных элементов. Данная модель позволит в сжатые сроки и экономически выгодно развивать новые образовательные технологии и методики в электронном обучении.

Остро стоит проблема оценки качества как программ электронного обучения, так и оценки результатов обучения. В определении понятия качества электронного обучения можно соотнести критерии оценивания качества образования в традиционной форме, а именно: качество содержания образования; качество результатов образования (качество образованности личности); качество образовательных технологий (качество методов обучения и воспитания) [1].

Гриценко А.Г. предлагает оценивать подходы и результаты обучения посредством матрицы, показывающей структуру элементов и признаков в табличном формате, и результат экспертизы оценивать в баллах по каждой отдельной программе электронного обучения [2]. Мы разделяем мнение автора о необходимости оценивания отдельных элементов системы электронного обучения, но с точки зрения оценки личностно-развивающего электронного обучения данные

критерии недостаточны. Как оценить уровень развития личности с помощью количественного показателя?

Решением данной проблемы может стать введение одним из критериев оценивая качества электронного образования определение субъектного статуса личности обучающегося в процессе взаимодействия с электронной образовательной средой: адаптирующийся к среде индивид; субъект познания и самостоятельной деятельности в среде; субъект рефлексии и общения; субъект творчества и саморегуляции [8].

Также система оценки качества в электронном обучении невозможна без привлечения в качестве эксперта личности обучающегося. Рефлексия собственного опыта по окончании изучения курса может проводиться в форме анкетирования и содержать следующие позиции: целесообразность изучения дисциплины в электронной форме; качество коммуникации между субъектами процесса обучения; технологии сопровождения курса; разнообразие форм учебных заданий; интерактивность курса; информационную поддержку и сопровождение обучающегося и др. [1].

Другой не менее важной проблемой является подготовка и переподготовка лиц педагогического и административно-технического сопровождения. Возникает противоречие между требованиями федеральных государственных образовательных стандартов в части обеспечения и реализации электронной информационно-образовательной среды и отсутствием категории подготавливаемых образовательными организациями специалистов в области электронного обучения. Причем мало научиться использовать телекоммуникационные технологии для передачи учебно-методического материала, необходимо осуществить перевод процесса обучения всех дисциплин на преподавание с помощью информационных и сетевых технологий. Отсюда возникает вопрос о должном мотивировании преподавателя на освоение новых методов с осознанием того, что это достаточно тяжелый процесс. Однако если не будет создано должное стимулирование, то процесс реального развития электронного обучения будет проходить весьма медленно. Статус педагогического работника в электронном обучении не отражен в нормативном регулировании субъектов образования, а именно: отсутствует разграничение между лицами, которые действительно осуществляют обучение в электронной среде, с теми, кто осуществляет функции сопровождения и администрирования.

При этом проектирование электронной среды, обладающей личностно-развивающим потенциалом, – процесс трудоемкий и требующий от педагогического работника разработки отдельных компонентов, ориентированных на различные этапы развития личности [8]. Так, для адаптирующегося индивида важно психофизическое благополучие – доступный и эмоционально-привлекательный интерфейс. Для субъекта познания и самостоятельной деятельности основным является систематизированный научно-предметный контекст – возможность выбора различных ЭОР. Для субъекта рефлексии и общения на первый план выходит социально-диалогический контекст – различные формы коммуникации. Субъект творчества и саморегуляции участвует в генерировании авторского и культурно-инновационного контекста среды, поэтому компо-

нент модели среды электронного обучения должен позволять представлять свои достижения и возможность изменять саму среду.

Подводя итог, сделаем вывод, что если появятся единые подходы и методики решения нормативно-регулятивных, структурных, методологических, комплектующих, коммуникативных проблем электронного обучения, то не будет сомнений в эффективности и целесообразности повсеместного использования электронного обучения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бубнов Г.Г., Плужник Е.В., Солдаткин В.И. Критерии оценки качества в системе электронного обучения // Cloud of science. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/kriterii-otsenki-kachestva-v-sisteme-elektronnogo-obucheniya.

2. Гриценко А.Г. Оценка качества программ электронного обучения: дис. … канд. эконом. наук. – М., 2006.

3. Гура В.В. Теоретические основы педагогического проектирования личностно-ориентированных электронных образовательных ресурсов и сред. – Ростов н/Д: ЮФУ, 2007. – 320 с.

4. Красильников И.В. Классификация электронных средств обучения // Информационные технологии. 2012. № 9. С. 75-78.

5. Красильников И.В. Способы классификации электронных обучающих систем: сб. науч. трудов кафедры информатики. Вып. 5. – М., 2009.

6. Постановления Главного государственного санитарного врача РФ от 24 декабря 2015 г. № 81 «О внесении изменений № 3 в СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения, содержания в общеобразовательных организациях» // СПС «КонсультантПлюс».

7. Сериков В.В. Общая педагогика: избранные лекции. – Волгоград: Перемена, 2004. – 278 с.

8. Ходякова Н.В. Личностно-развивающая образовательная среда: концепция и технологии проектирования: монография. – Волгоград, 2003. – 123 с.

О НЕОБХОДИМОСТИ ВНЕДРЕНИЯ ВИРТУАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ В ДЕЯТЕЛЬНОСТЬ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

ABOUT NECESSITY OF IMPLEMENTATION OF VIRTUAL EDUCATIONAL ENVIRONMENT IN ATTIVITY OF THE EDUCATIONAL ORGANIZATION

Черкесова Кристина Ивановна
(Белгородский государственный институт искусств и культуры)

Cherkesova Kristina Ivanovna
(Belgorod state institute of arts and culture)

Аннотация: в статье рассматривается вопрос необходимости создания виртуальной образовательной среды в образовательной организации с использованием инновационных средств проектирования и разработки. Проводится анализ основных проблем организации и оптимизации учебного процесса.

Ключевые слова: информационные технологии, облачные сервисы, образовательная среда, автоматизация, моделирование, оптимизация.

Annotation: the article considers the need to create a virtual educational environment in a educational organization using innovative design and development tools. The main problems of organization and optimization of the educational process are analyzed.

Key words: information technologies, cloud services, educational environment, automation, modeling, optimization.

Повышение престижности высшего учебного заведения и увеличение потока студентов не оставляют без внимания вопрос организации и оптимизации учебного процесса, процессов социально-культурных коммуникаций, а также взаимодействия студентов и преподавателей посредством современных информационных технологий и систем. Как правило, вопросы оптимизации учебного процесса во многих вузах слабо проработаны, в некоторых подразделениях присутствует частичная автоматизация, однако этого недостаточно для того, чтобы создать достойную информационную среду высшего учебного заведения.

Таким образом, необходимость анализа и моделирования информационных процессов института становится очевидной. Предметом исследования являются информационные процессы, протекающие внутри образовательного учреждения. Именно их детальное изучение позволит создать инновационную образовательную среду и автоматизировать учебный процесс вуза для повышения информационной культуры обучающихся и сотрудников в соответствии с требованиями современного общества.

Для достижения поставленной цели необходимо решить следующие задачи:

− изучить организационную структуру института и, в частности, проанализировать информационные процессы, протекающие в нем;

− на основе анализа выявить недостатки в существующей технологии организации учебного процесса;

− определить ключевых участников образовательного процесса;

− спроектировать информационно-логическую модель портала образовательного учреждения;

− подобрать необходимое информационное и техническое обеспечение, на его базе разработать и подготовить к работе портал образовательного учреждения, отвечающий новейшим требованиям федеральных государственных образовательных стандартов (ФГОС).

В случае когда в основу образовательного процесса положена научно разработанная и апробированная модель с преемственностью учебных планов и программ ее реализация в полной мере возможна лишь с использованием новейших информационных технологий. Как показывает практика, данная модель является достаточно эффективной в достижении основной цели вуза – подготовки квалифицированных кадров.

Во многих учебных заведениях высшего и среднего образования выполнение важнейших операций, таких как составление расписания, планирование учебного процесса и прочее, возможно лишь с использованием рукописного ввода данных сотрудниками учебно-методического управления и деканатов. Это значительно усложняет планирование и организацию учебного процесса, так как велика вероятность допущения большого количества ошибок и неточностей. Особенно остро эта проблема встает в начале учебного года, когда поток документации резко возрастает.

Помимо всего прочего, не налажен процесс электронного документооборота, что заметно увеличивает время на доставку и обработку данных, также велика вероятность запаздывания предоставления локальных распоряжений от руководства, что непременно ведет к неисполнению распоряжений.

В такой ситуации дистанционное обучение и удаленный доступ к образовательным ресурсам вовсе не представляются возможными, так как отсутствует виртуальная корпоративная среда. На рисунке представлены основные информационные потоки, протекающие в образовательном процессе (см. рис. 1). Для проектирования информационных потоков был выбран инструмент моделирования, анализа, документирования и оптимизации бизнес-процессов AllFusionProcessModeler 7.

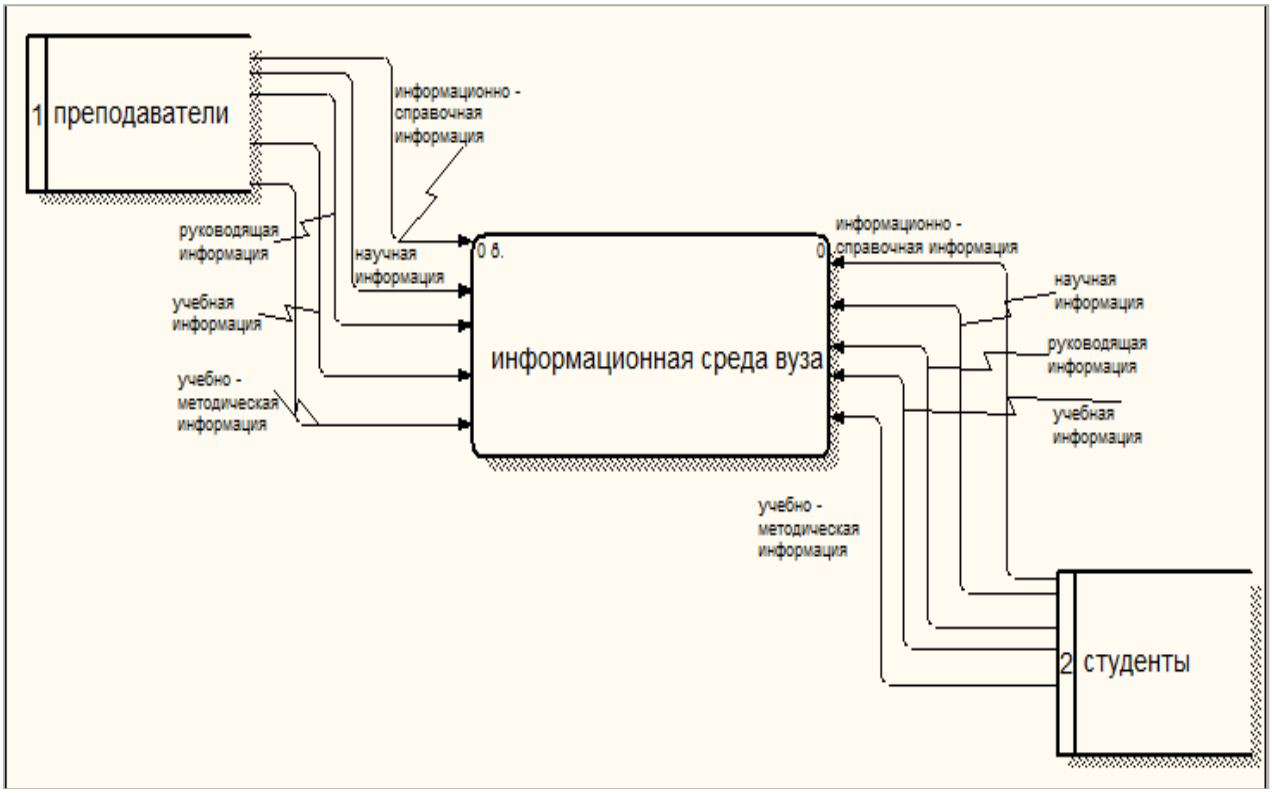


Рис. 1. Модель информационной среды вуза.

Из модели информационной среды вуза видно, что преподаватели и студенты в своей деятельности оперируют большим объемом разнородной информации. Это в первую очередь учебная, учебно-методическая информация, а также научная, руководящая и информационно-справочная информация. Как правило, доступ к такой информации оказывается затруднительным в силу отсутствия портала образовательной организации, где данные будут упорядочены и представлены в наглядной форме, где студенты и преподаватели смогут напрямую взаимодействовать друг с другом, обмениваясь информацией и накопленным опытом [3].

Таким образом, становится очевидной потребность в создании инновационной образовательной среды и автоматизации учебного процесса вуза для повышения информационной культуры обучающихся и сотрудников в соответствии с требованиями современного общества. Разрабатываемая система должна решать задачу автоматизации учебного процесса вуза и выполнять функции:

– аттестационного контроля знаний;

– обеспечения самостоятельной (внеаудиторной) работы студентов;

– разработки учебно-методических материалов по дисциплинам в электронном виде;

– создания учебно-методических комплексов дисциплин, включающих лекционный, учебный и методический материал, контрольные и практические задания;

– построения интерактивных моделей изучаемых процессов и явлений;

– составления отчетов о выполнении самостоятельной работы студентов и др.;

– создания презентаций;
– разработки и публикации нормативных документов;
– ведения персональных страничек преподавателей и студентов и другие.

Использование высококачественных программных продуктов является главным структурообразующим элементом функционирования организации. Внедрение в организацию корпоративной информационной системы позволяет организовать и четко отладить взаимодействие между разными отделами. Основным преимуществом является единое информационное пространство. Процесс обмена информацией, передачи отчетов, оформления различных документов становится более быстрым и удобным. Доступ к файлам, базам данных, подключение к печатающим устройствам осуществляется дистанционно [2].

Разработка и внедрение портала образовательной организации позволит устранить ряд недостатков, которые были выявлены при анализе учебного процесса вуза. С точки зрения получения косвенного эффекта улучшится работа подразделений, непосредственно задействованных в планировании учебного процесса: сократится время выполняемых операций, увеличится объем обрабатываемой информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Маторин С.И. Информационные технологии: учебно-практическое пособие – Белгород: БелГУ, 2007.

2. Семыкина Л.Н., Проектирование экономических информационных систем: учебник для студентов экономических вузов, обуч. по спец. «Прикладная информатика в экономике». – Белгород: Бел ГУ, 2011. – 511 с.

3. Смирнова Г.Н. Проектирование экономических информационных систем: учебник / Г.Н. Смирнова, Ю.Ф. Тельнов, А.А. Сорокин. – М.: Финансы и статистика, 2013 – 512 с.

4. Соколов Е.А., Середа С.Н. Информационный сервис электронного документооборота вуза // Современные проблемы науки и образования. 2015. № 5.

КЛАССИФИКАЦИЯ ОБЛАЧНЫХ СЕРВИСОВ

CLASSIFICATION OF CLOUDY SERVICES

Михайликов Виталий Леонидович,
Гуржий Алексей Александрович,
Дрога Андрей Анатольевич
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Mihaylikov Vitaly Leonidovich,
Gurzhy Alexey Aleksandrovich,
Droga Andrey Anatolyevich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin)

Аннотация: данная статья посвящена рассмотрению облачных сервисов. Подробно описана их классификация, указаны преимущества и недостатки облачных технологий. Рассмотрены основные модели облачных технологий, такие как SaaS, PaaS и IaaS. Приводятся примеры существующих интернет-приложений, указывается, к какой модели приложение относится. В статье рассматриваются модели развёртывания облачных сервисов. Подробно описывается каждая из моделей.

Ключевые слова: облачные технологии, облачные сервисы, информационные технологии, образовательные системы, компьютерное моделирование, SaaS, PaaS, IaaS.

Annotation: this article is devoted to the consideration of cloud services. Their classification is described in detail, the advantages and disadvantages of cloud technologies are indicated. The basic models of cloud technologies, such as SaaS, PaaS and IaaS are considered. Examples of existing Internet applications are given, it is indicated to which model the application belongs. The article discusses the deployment of cloud services. Each model is described in detail.

Key words: cloud technologies, cloud services, information technologies, educational systems, computer modeling, SaaS, PaaS, IaaS.

Вошедший в историю XXI век по праву называется информационным. Информационные технологии получили колоссальное, бурное развитие, что позволило этой индустрии интегрироваться во все сферы общественной жизни. Информационные и коммуникационные технологии, созданные, безусловно, не для нужд системы образования, ведут к подлинной революции и в этой сфере, внося качественные изменения в работу всех ее звеньев. С развитием сети Интернет интенсивно начали развиваться и облачные технологии.

Основная задача облачных технологий сводится к предоставлению рядовым пользователям удаленного динамического доступа к приложениям, вычислительным ресурсам, а также ресурсам (в том числе операционные системы и инфраструктуру) через глобальную сеть Интернет. Активное развитие услуг по

размещению программного обеспечения клиента на территории провайдера с возможностью подключения его к каналам связи объясняется появившейся потребностью в приложениях и цифровых услугах, которые отличались бы экономичностью и эффективностью.

В настоящее время самыми популярными облачными услугами, предоставляемыми провайдерами, являются виртуальный выделенный сервер, виртуальный хостинг, SaaS (Software as a Service, то есть программа как услуга). Самой распространённой облачной услугой является форма SaaS. Примером подобного программного обеспечения являются такие сервисы, как Microsoft Hosted Exchange и Share Point.

Сервисы облачных технологий состоят из множества серверов, расположенных в центрах обработки и хранения информации, обеспечивающих работу огромного числа приложений, которые используют миллионы пользователей. Обязательным условием оптимального и эффективного управления такой огромной системой является полная автоматизация. Стоит отметить, что для обеспечения различным пользователям – операторам, провайдерам, посредникам, IT-администраторам, пользователям приложений – защищенного доступа к вычислительным ресурсам облачная инфраструктура должна предусматривать возможность самоуправления и передачи полномочий.

Идея облачных технологий существенно изменила общепринятый подход к распространению, управлению и установке программного обеспечения. В сравнении с традиционным подходом облачные вычисления предоставляют возможность управлять объёмными системами, но появляется полная зависимость от провайдера облачных услуг. Однако данная зависимость является таковой лишь в теории, ведь если компания-провайдер допустит хоть один прецедент кражи информации, это станет колоссальным ударом по всей индустрии предоставления удаленных мощностей.

Для обеспечения слаженной работы персонального компьютера, который предоставляют услугу облачных вычислений, используется специальное программное обеспечение, обобщённо называющееся «middlewarecontrol». Это программное обеспечение предоставляет возможность мониторинга оборудования, балансировки нагрузки, предоставление ресурсов для решения поставленных задач.

Основной проблемой при работе облачных вычислений является неравномерность использования ресурсов со стороны клиентов. Решением описанной проблемы является создание ещё одного слоя, расположенного между реальным железом и middleware, называемого виртуализация серверов. Серверы, предоставляющие ресурсы приложениям, виртуализируются, и балансировка нагрузки производится как средствами специализированного программного обеспечения, так и средствами распределения виртуальных серверов по реальным.

В целом сервисами облачных технологий являются онлайн-приложения, доступ к которым предоставляется с помощью интернет-браузера. Не имеет значения, являются ли эти сервисы развлекательными или специализированными приложениями. Основная идея одна: пользователю не обязательно обладать дорогостоящим, производительным «железом» для использования специ-

фического программного продукта. Пользователю необходимо всего лишь обратиться через глобальную сеть к определённому провайдеру и использовать желаемую услугу, при необходимости оплатив её.

Национальный институт стандартов и технологий США (National Instituteof Standardsand Technology – NIST) в документе «NIST Definitionof Cloud Computing v15» [1, с. 244] определил облачные технологии как модель предоставления повсеместного и удобного удалённого доступа к общему источнику конфигурируемых вычислительных ресурсов, которые могут быть мгновенно предоставлены пользователю и освобождены с минимальными усилиями по управлению системой. При использовании облачных технологий информация размещается на серверах, расположенных в облаке. Более того, данные постоянно кэшируются на персональных компьютерах пользователей. При разработке облачной системы используют одну из трех основных моделей: SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), IaaS (Infrastructure-as-a-Service).

Разберём подробнее каждую из моделей [3].

1. SaaS (Software-as-a-Service). Программное обеспечение как услуга – модель, в которой пользователю даётся возможность работы с прикладным программным обеспечением провайдера, функционирующий в облачной инфраструктуре и доступным из всевозможных клиентских приложений, таких как браузер. Примером является электронная почта, доступ к которой совершается при помощи браузера. Стоит отметить, что провайдер осуществляет управление и контроль как физической, так и виртуальной инфраструктурой облака.

Функционируют приложения на сервере провайдера, а пользователи получают доступ к ним через web-браузер. Стоит отметить, что потребители не покупают SaaS-приложения, а арендуют его, то есть платят за использования приложения определённый период времени. За счёт этого и достигается экономический эффект, являющийся одним из важнейших преимуществ. Работоспособность приложений, их обновление, техническая поддержка пользователей, защита информации – это главная задача SaaS-провайдера. То есть потребитель SaaS-приложения не беспокоится о технической стороне вопроса и имеет возможность сосредоточиться на своих задачах.

Стоит отметить основные преимущества SaaS-технологий над обычным программным обеспечением:

– низкая стоимость приложений;
– более быстрое внедрение и разработка;
– низкий порог входа (возможность быстро и бесплатно протестировать приложение);
– поддержка работоспособности приложения лежит на плечах провайдера;
– мобильность пользователей приложений;
– возможность работать с удалёнными разработчиками приложений;
– низкие требования к мощности компьютера;
– кроссплатформенность.

Недостатками SaaS считаются:

– опасность передачи коммерческих данных стороннему провайдеру;

– зависимость от работоспособности Интернета.

Существуют и альтернативные технологии. Эти технологии являются промежуточным вариантом перехода от обычного программного обеспечения к SaaS-приложениям. Но разрабатываются подобные приложения всё реже. К альтернативным технологиям относят:

- S+S – технология, разрабатываемая компанией Microsoft. Отличается эта технология от SaaS тем, что на персональном компьютере потребителя используется не интернет-браузер, а специально разработанный программный клиент;

- аренда программного обеспечения. Такая технология отличается от SaaS только лишь структурой серверной части приложения. Вследствие этого хостеры таких программ часто именуют свои услуги SaaS-сервисами. Так в чём же отличия? Разница заключается лишь в том, что традиционные SaaS-приложения имеют multitenant-архитектуру, то есть одно приложение может обслуживать множество пользователей, в то время как аренда приложений подразумевает установку отдельной копии для каждого пользователя. Пользователям такой технологии предоставляется возможность более гибко настраивать приложение, но в то же время, процесс администрирования и обновления становится более затруднительным, следовательно, стоит такое приложение дороже.

2. PaaS (Platform-as-a-Service). Платформа как услуга – модель, в которой пользователю выдаётся возможность пользоваться облачной инфраструктурой с целью размещения базового программного обеспечения для последующего размещения на нём новых или существующих приложений (собственных, разработанных на заказ или приобретённых тиражируемых приложений). Подобные платформы состоят из инструментальных средств, предназначенных для создания, тестирования, а также запуска прикладных программ, таких как прикладное программное обеспечение, системы управления базами данных, среды исполнения языков программирования. Облачный провайдер осуществляет управление и контроль виртуальной и физической инфраструктурой облака, включая сети, сервера, операционные системы. Исключением являются установленные и разработанные приложения, а также параметры конфигурации платформы [2].

3. IaaS (Iaa Sor Infrastructure-as-a-Service). Пользователь системы может устанавливать, настраивать и запускать произвольное программное обеспечение, которое может быть операционной системой, платформенной или прикладной программой. Пользователь имеет возможность работать с операционными системами, виртуальными системами хранения данных. Контроль и управление основной физической и виртуальной инфраструктурой облака осуществляется облачным провайдером.

Классификация моделей развёртывания [5]:

1) частное облако – инфраструктура, предназначенная для работы только одной организации, включающей множество пользователей. Примером может быть подразделение одной организации. Частное облако обычно располагается в собственности, управлении и обслуживании как самой организации, так и

сторонней компании. Физически облако может располагаться как внутри организации, так и вне юрисдикции владельца;

2) публичное облако – инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца - поставщика услуг;

3) гибридное облако – это комбинация из двух или более различных облачных инфраструктур (частных, публичных), остающихся уникальными объектами, но связанных между собой стандартизованными или частными технологиями передачи данных и приложений (например, кратковременное использование ресурсов публичных облаков для балансировки нагрузки между облаками);

4) общественное облако – вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи. Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или более из организаций сообщества или третьей стороны (или какой-либо их комбинации), и она может физически существовать как внутри, так и вне юрисдикции владельца. На практике границы между всеми этими типами вычислений достаточно размыты.

При использовании облачных вычислений потребители информационных технологий могут существенно снизить капитальные расходы – на построение центров обработки данных, закупку серверного и сетевого оборудования, аппаратных и программных решений по обеспечению непрерывности и работоспособности – так как эти расходы поглощаются провайдером облачных услуг [4].

Благодаря облачным технологиям затраты пользователей стали более оптимальны. Финансовые средства направляются только на необходимые услуги облачных провайдеров. Безоговорочным преимуществом использования облачных технологий является легкий, круглосуточный и повсеместный доступ к информации, хранящейся на облаке, который могут получить каждый сотрудник и студент отдельного института (учащийся школы), имеющий идентификационный номер и пароль. С помощью облачных технологий расширяется спектр интерактивных образовательных программ, происходит ведение электронной базы данных всего университета, создаются личные кабинеты для студентов и работников института, организуются тематические форумы и другие полезные информационные ресурсы. Примером работы облачных технологий являются: электронные библиотеки с неограниченным запасом и регулярным пополнением литературы; информационно-обучающие порталы, реализующие дистанционное обучение и совместную работу над разнообразными образовательными проектами.

Достаточное количество очевидных преимуществ применения облачных технологий в образовании превосходит по величине устранимые недостатки, главными из которых являются: обеспечение конфиденциальности, надежности и безопасности данных.

Единственным уязвимым местом инновации является трудоёмкость предоставления широкополосного доступа в глобальную сеть Интернет в труднодоступные регионы страны. Однако специалисты информационной индустрии пророчат стремительное и беспрерывное развитие данного направления, систематически модернизируя качество и скорость интернет-соединений. И, возможно, в ближайшем будущем этот существенный минус, являющийся барьером развития одной из самых прогрессивных отраслей, будет превращен в огромный плюс, несущий предпосылки масштабных открытий в мире облачных технологий.

Все это привело к тому, что облачные сервисы стали привлекательны для предпринимательских структур разных уровней. Возможность гибкого управления сервисами в сочетании с экономической целесообразностью сделала облака чрезвычайно популярными среди пользователей, с одной стороны, и подтолкнуло развитие облачных технологий в направление расширения функциональности – с другой. Изначальное лидерство на рынке облачных сервисов для пользователей держали американские разработчики. Но в последнее время в российском сегменте Интернета их вытесняют такие сервисы, как Yandex и Mail.

Перспективное участие облачных технологий в образовательной системе высших учебных заведений МВД, несомненно, будет способствовать должному воспитанию высококвалифицированных и отвечающих современным требованиям специалистов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гребнев Е.С. Облачные сервисы. Взгляд из России. – М., 2011. – 282 с.

2. Доклад на тему о возможности применения облачных технологий в образовании [Электронный ресурс]. – Режим доступа: http://fs.nashaucheba.ru/docs/270/index-1752687.html.

3. Будущее облачных технологий: европейский взгляд [Электронный ресурс]. – Режим доступа: http://www.bureausolomatina.ru.

4. Заоблачные вычисления: Cloud Computing на пальцах [Электронный ресурс]. – Режим доступа: http://www.xakep.ru.

5. Облачные технологии и распределенные вычисления [Электронный ресурс]. – Режим доступа: http://it.sander.su.

ИНТЕРАКТИВНЫЕ СРЕДСТВА РЕШЕНИЯ ОБРАЗОВАТЕЛЬНЫХ И УПРАВЛЕНЧЕСКИХ ЗАДАЧ

INTERACTIVE MEDIA SOLUTIONS EDUCATIONAL AND MANAGEMENT TASKS

Макото Курита
(Фабрика AVC Networks Company, Panasonic Corporation в России (Япония));
Козиоров Евгений Львович
(ООО «Инфологика ЛТД»);
Акапьев Виктор Львович
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Makoto Kurita
(Factory AVC Networks Company, Panasonic Corporation in Russia);
Koziorov Evgeniy Lvovich
(JSC «Infologika LTD»);
Akapyev Victor Lvovich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin)

Аннотация: изменение социальных задач системы образования и общества в целом, переход его из производственной в информационную фазу развития выводят на передний план задачи реформирования не только содержательной части профессионального образования, но и его информационного и технического сопровождения.

Ключевые слова: интерактивная доска, информационно-технологическая компетентность педагога, мультимедийность, мультитач, профессиональное обучение, технические средства интерактивных технологий, тренинги, видеоконференции.

Annotation: changing the social tasks of the education system and society in General, its transition from the industrial to the informational phase of development brings to the forefront the task of reforming not only the substantial part of professional education, but also its information and technical support.

Key words: interactive whiteboard, information technology competence of the teacher, multimedia, multi-touch, professional training, technical means of interactive technologies, training, video conferencing.

Компьютерные информационные технологии, созданные отнюдь не для решения учебных задач, произвели в образовании настоящую революцию. Применение компьютеризированных средств обучения ограничивается лишь фантазией педагога и уровнем его информационно-технологической компетентности.

В то же время из обширного перечня возможностей компьютера как инструмента образования можно выделить два его основных преимущества перед другими средствами обучения: моделирование процессов и визуализация учеб-

ного материала. В связи с этим актуализируется использование в образовательном процессе интерактивных и мультимедийных технологий. Необходимость их применения обусловлена и рядом других объективных и субъективных психолого-педагогических факторов.

С помощью интерактивных технологий обеспечивается наглядность и вовлеченность субъектов образовательного процесса, экономится драгоценное время, повышается точность и обоснованность принимаемых решений, увеличивается эффективность формирования зрительных образов у обучаемых, что способствует в конечном итоге повышению качества образования.

В настоящее время можно выделить несколько направлений применения интерактивных и мультимедийных технологий в образовании:

- профессиональное обучение, в том числе и дистанционное;
- корпоративное обучение и повышение квалификации;
- тренинги;
- видеоконференции;
- вебинары и др.

Рассматривая мультимедийность как подачу учебного материала по нескольким каналам восприятия, а интерактивность – как активное вовлечение всех субъектов образования в образовательный процесс, необходимо остановиться на некоторых аспектах обеспечения реализации обучения с использованием указанных средств.

Единая информационная среда образовательной организации, помимо организационного, методического и кадрового компонентов, в обязательном порядке должна включать техническое и информационное обеспечение, а также сопровождение производителя.

Зачастую отрицательные результаты информатизации образовательной среды и негативного отношения педагогических работников к компьютерным технологиям обучения определяются ошибочным выбором интерактивного оборудования. Стремление сэкономить и боязнь нарушить нормативные акты, регламентирующие закупки оборудования для государственных нужд, заставляют чиновников федерального и регионального уровней и руководителей образовательных организаций покупать доски малоизвестных производителей – не всегда качественные, с ограниченными функциональными возможностями, слабым программным обеспечением и без информационного наполнения [2].

Интерактивные доски уже не редкость на российском рынке и их многообразие вынуждает провести сравнительный анализ продукции их основных производителей по наиболее востребованным функциональным возможностям [3].

В целом можно заключить, что наибольший набор стабильно работающих и востребованных в практической работе возможностей предлагают интерактивные доски Elite Panaboard UB-T880. В рамках более ограниченной функциональности качественное и надежное решение предлагает Smart. Доски Interwrite предлагают интересное решение не столько для многопользовательского режима, сколько для объединения нескольких устройств. Несмотря на смелую идею компании Hitachi, в свое время первой выпустившей сенсорную многопользовательскую доску, их продукт нуждается в доработке.

Elite Panaboard UB-T880 – уникальная по возможностям интерактивная доска, которая обеспечивает одновременную работу трех пользователей, причем по всей поверхности доски, без деления на отдельные рабочие зоны – функция «мультитач», оснащена встроенными в корпус звуковыми стереоколонками, а также содержит в комплекте специальный многофункциональный электронный маркер, позволяющий с помощью поворотного переключателя на торце выбирать режим мыши, цветного маркера (4 цвета), полупрозрачного маркера-выделителя, ластика. Кроме того, в маркер встроен пульт дистанционного управления, позволяющий удаленно листать страницы интерактивного урока. Благодаря этим особенностям работать с мультитач-доской UB-T880 намного удобнее.

Несмотря на то, что образовательные структуры достаточно консервативны в выборе оборудования, доски с функцией «мультитач» – одновременного распознавания нескольких касаний – оказались востребованы именно в образовательной сфере. В частности, можно использовать жесты, т.е. перемещать, поворачивать объекты, менять масштаб изображения при помощи одновременного касания пальцами. Но самое главное – появляется возможность организовать совместную работу нескольких человек на общем рабочем пространстве, выполнять одно задание, например, создавать общий рисунок или выполнять совместный проект.

Интерактивные комплексы на базе интерактивных досок – на сегодня наиболее развитое, наиболее проработанное решение для сферы образования. При этом очень быстро развиваются интерактивные панели и интерактивные проекторы, которые впитали все достижения и наработки, достигнутые с помощью досок.

Необходимо отметить, что интерактивные системы последнего поколения - интерактивная доска с ультракороткофокусным проектором или интерактивная ЖК или плазменная панель – резко повысили комфортность работы педагога: не мешает тень от работающих у доски, не слепит глаза.

Можно долго спорить о технических преимуществах тех или иных моделей, но для педагогического работника практическое значение, определяющее эффективность использования инновационных технологий, имеют две вещи – поддержка, осуществляемая производителем, и информационные ресурсы в виде учебных материалов.

Если они есть, педагог считает свою доску самой лучшей, если нет – доску используют лишь как экран для мультимедийных презентаций. Но многие ли производители вкладывают силы и средства в поддержку и обучение российских педагогических кадров? Увы, нередко, получив доску, преподаватель вынужден осваивать ее методом проб и ошибок и тратить много времени на поиски интерактивных учебных ресурсов и программных средств их создания [1, с. 80-82].

Производитель интерактивных досок и компания-поставщик могут оказать существенную помощь администрации образовательной организации во внедрении нового оборудования, поэтому условия для эффективного использования интерактивных досок создаются не после того, как они были приобретены, а уже на этапе выбора [2, с. 72-76].

Компания Panasonic, разрабатывая доски для образования, ориентировалась в первую очередь на российский рынок и потребности российских педагогов. Panaboard – это единственные интерактивные доски, программное обеспечение для которых разрабатывается в России.

Из всех производителей интерактивных досок только Panasonic имеет в России официальное представительство, обеспечивающее поддержку пользователей, и сеть сервисных центров по всей России.

Что касается образовательных ресурсов, то в настоящее время можно выделить их три основных источника: традиционные учебники с электронными приложениями, интернет-ресурсы и образовательные ресурсы разработчиков интерактивных средств обучения. Существует вариант разработки образовательных ресурсов и самими педагогами, но здесь возникают проблемы опять же с уровнем их информационно-технологической компетентности и сложностью обучения соответствующим технологиям в рамках системы повышения квалификации, что требует отдельного рассмотрения. Возможности педагогов как носителей образовательного контента буквально натыкаются на информационно-технологические ограничения уровня их квалификации.

Зачастую полноценное использование электронных приложений в учебном процессе невозможно. Такие ресурсы разрабатываются без учета квалификации педагогических работников, уровня подготовки обучаемых, учебно-тематических планов, рабочих программ и еще целого ряда объективных факторов. А реализация такого рода ресурсов в варианте загрузочного модуля подавляющему большинству педагогов не позволяет использовать даже их отдельные фрагменты.

Качество и доступность образовательных интернет-ресурсов – еще один камень преткновения. Поэтому на первое место выходят образовательные ресурсы разработчиков интерактивных средств обучения. И здесь наиболее оригинальное решение предлагает Panasonic, предлагая отработанную систему конкурсов авторских разработок среди российских педагогов и учащихся и программу поддержки учителей.

Необходимо отметить и концепцию готовых образовательных ресурсов, воплощенную в коллекции интерактивных ресурсов PebSTUDIO. PebSTUDIO – это коллекция наглядных пособий, упражнений и заданий, разработанных специально для использования с интерактивными досками Panaboard. Ресурсы созданы в формате базового программного обеспечения Elite Panaboard book, которое поставляется со всеми интерактивными досками Panasonic. На каждом из дисков коллекции содержится более 300 интерактивных заданий по одному из предметов школьной программы.

В PebSTUDIO реализован новый подход к созданию цифровых образовательных ресурсов. Открытая архитектура PebSTUDIO позволяет преподавателю не только использовать готовые ресурсы «как есть», но и самостоятельно дополнять и изменять их в соответствии с собственными методическими предпочтениями. При этом от педагога не требуется специальных знаний по программированию, достаточно знакомства с базовыми инструментами программного обеспечения интерактивной доски.

Ресурсы PebSTUDIO не навязывают определенную структуру урока и не подразумевают передачу функций учителя компьютеру – в них нет автоматических проверок, текстовых и звуковых комментариев, дублирующих или заменяющих объяснения преподавателя. Кроме того, интерактивные задания PebSTUDIO построены таким образом, чтобы обучающий мог выбирать способ использования того или иного ресурса. Благодаря своей многофункциональности интерактивные ресурсы могут использоваться как на стадии отработки учебного материала – в форме «упражнения», так и на стадии контроля знаний – в форме «опроса» [1].

В последнее десятилетие интенсивное развитие новых технологий обучения, использующих интернет-ресурсы и средства мультимедиа, вызвало ряд принципиальных изменений на рынке корпоративного и профессионального образования. Акцент на работе в команде и потребность в постоянном обучении и повышении квалификации в современной бизнес-среде привели к размыванию традиционной модели обучения, которая основана на предварительном отборе информации для слушателей, центральной роли преподавателя, процессе более или менее пассивной передачи знаний и навыков.

Слушатели в новой среде обучения используют «сырые», максимально характеризующие реальную ситуацию данные, активно участвуют в процессе получения необходимых им установок и навыков, делают это посредством интерактивных методов обучения.

Реализация принципов повышения эффективности обучения также возможна на базе использования тренингов, направленных на развитие знаний и умений. Сегодня одна из главных задач преподавателя-тренера состоит в максимально активном вовлечении обучающихся в процесс в основном самостоятельного, мотивированного получения реальных навыков, необходимых для их личного и профессионального развития.

Переход к подобной модели требует от преподавателя активного и выверенного подхода к взаимодействию с аудиторией и умения использовать новые технологии и инструменты обучения при разработке тренингов и семинаров.

Ясно, что никакие технические средства не способны заменить воздействие личности преподавателя. Но сегодня для того чтобы быть на уровне современных требований и ожиданий участников тренинга, особенно нового поколения, преподавателю необходимо уметь владеть новыми технологиями и эффективно задействовать в своих тренингах те возможности, которые они открывают.

К сожалению, полноценные интерактивные средства и их сопровождение для системы образования еще дороги и несколько «сыроваты» с точки зрения их использования, а для деловой сферы, где требования не такие глубокие, в методическом плане им нет альтернативы. Без преувеличения можно сказать, что интерактивная панель или доска – инструмент руководителя.

Можно отметить основные преимущества таких средств:

- оперативность внесения любых изменений;

- сохранение результатов совещания и моментальная выдача всем участникам в виде распечатки или по электронной почте;

- наглядность;
- возможность задействовать электронные карты, схемы, плакаты и т.п.;
- вовлеченность и активное участие участников в обсуждении.

Даже просто функция сохранения результата бурных обсуждений в виде скриншотов имеет огромную ценность для руководителя – у ВСЕХ участников совещания остается КОНКРЕТНЫЙ и ОДИНАКОВЫЙ документ – итог совещания, а не каша в голове – один понял так, другой – этак.

С интерактивной доской намного проще решаются и оперативные задачи управления, связанные с распределением сил и средств: выводим карту района на экран, указываем маршруты патрулей, отображаем криминогенную обстановку и т.п.

Сейчас в программном обеспечении всех нормальных досок есть функция видеозаписи, так что есть возможность еще и протоколировать ход совещания.

Интерактивные доски и панели активно используются при проведении видеоконференций и вебинаров, когда взаимодействуют удаленные друг от друга группы сотрудников и субъектов образовательного процесса. Современные программные средства таких конференций позволяют передавать и картинку участников, и рабочий стол с рукописными пометками и записями участников поверх какого-нибудь приложения.

На основании приведенных вариантов использования интерактивных средств как для решения задач обучения, так и для задач управления возможно сделать вывод об их эффективности и необходимости формирования единой информационной политики в этом направлении, отсутствие которой тормозит формирование единого информационного пространства как конкретной образовательной организации, так и всего министерства в целом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приезжая М.Н. Цифровые образовательные ресурсы для интерактивных досок // Управление начальной школой. 2011. № 3.

2. Приезжая М.Н. Почему интерактивные доски используются неэффективно? // Справочник руководителя образовательного учреждения. 2010. № 8.

3. Приезжая М.Н. Многопользовательские интерактивные доски – сравнение // http://www.panaboard.ru.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ФСИН РОССИИ

FEATURES OF FORMATION OF UNIFORM INFORMATION SPACE OF EDUCATIONAL INSTITUTIONS OF THE FPS OF RUSSIA

Немыкин Николай Иванович
(Белгородская вечерняя школа ИК-5 ФСИН России);
Немыкина Наталья Владимировна
(Белгородский институт развития образования);
Акапьев Виктор Львович
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Nemykin Nikolay Ivanovich
(Belgorod evening school of CL-5 FPS of Russia);
Nemykina Natalia Vladimirovna
(Belgorod Institute of education development);
Akapyev Victor Lvovich
(Belgorod Law Institute of the MIA of Russia named after I.D. Putilin)

Аннотация: определение структуры единого информационного пространства образовательного учреждения, принципов и источников формирования его составных подсистем в конечном итоге определяет успешность реализации задач, сформулированных в федеральном государственном образовательном стандарте.

Ключевые слова: единое информационное пространство, интерактивность, информационное обеспечение, мультимедийность, участники образовательного процесса, цифровые образовательные ресурсы, этапы формирования единого информационного пространства.

Annotation: determining the structure of a common information space of educational institutions, principles and sources of formation of its constituent subsystems ultimately determine the success of implementation of the tasks formulated in the Federal state educational standard.

Key words: common information space, interactivity, information, multimedia, the participants of educational process, digital educational resources, the steps of forming a single information space.

Отталкиваясь от контекста Федерального государственного образовательного стандарта нового поколения, можно с уверенностью констатировать, что поставленные в нем задачи решаются непосредственно в условиях сформированного единого информационного пространства образовательного учреждения.

Помимо специфики функционирования образовательного учреждения на базе исправительных колоний ФСИН России, такого как «Белгородская вечер-

няя школа», следует отметить, что существует множество подходов как к пониманию структуры и функций единого информационного пространства (ЕИП) школы, так и к используемой терминологии [4]. Например, наряду с термином ЕИП используется схожий по своей сути термин – единая информационная образовательная среда (ЕИОС) [5]. В условиях отсутствия единообразного подхода к понятию единого информационного пространства нам представляется возможным рассматривать указанный феномен как некоторую систему, включающую в свою структуру множество динамически развивающихся подсистем.

Такое поведение системы можно рассматривать как ее естественную эволюцию, обусловленную изменениями образовательных стандартов, технического прогресса и социальных процессов. Например, содержательная часть регулярно должна обновляться в связи с появлением новых требований к педагогам, сформулированных в их профессиональных стандартах [2], и к их компетенциям [3].

ЕИП школы – это система, в которой функционально задействованы и на информационном уровне связаны все участники учебного процесса. Цели формирования ЕИП школы:

– оптимизировать и модернизировать процесс обучения;

– осуществлять диагностику и управление учебным процессом;

– использовать возможности информационных технологий в образовательном процессе;

– повысить интерес обучающихся к различным дисциплинам;

– помочь учащимся влиться в мировое информационное пространство;

– повысить качество знаний обучающихся.

Основные задачи формирования ЕИП школы:

– формирование единой базы данных;

– предоставление пользователям возможности общения между собой и доступа к общим ресурсам;

– обеспечение использования компьютерных технологий в учебном процессе;

– освоение педагогами и обучающимися новых информационных технологий.

Этапы формирования единого информационного пространства:

1 этап: создание общей информационной базы данных – компьютерной модели информационного поля школы;

2 этап: создание локальной сети, позволяющей объединить и систематизировать внутри информационные ресурсы;

3 этап: создание и открытие доступа всем заинтересованным лицам к сайту школы.

Ожидаемые результаты:

– формирование насыщенного и полноценного ЕИП школы;

– повышение качества обучения;

– обеспечение доступа к глобальным информационным ресурсам;

– внедрение в учебный процесс современных электронных средств поддержки и сопровождения образовательного процесса;

– создание, обновление и поддержка сайта школы;

– создание электронной библиотеки.

Рассмотрение структурного состава информационного пространства образовательного учреждения неоднократно выступало предметом научных исследований. В ряде работ дается четкое представление о необходимости включения в рассматриваемую структуру материально-технического, программного, правового и организационного обеспечений.

При этом на второй план отходят проблемы кадрового и учебно-методического сопровождения процесса формирования единого информационного пространства школы, хотя введение профессиональных стандартов, в которых сформулированы новые требования к уровню профессиональной подготовки педагогических работников, их компетентности, дает новое наполнение структуре единого информационного пространства школы.

Одним из ключевых элементов единого информационного пространства является *информационное обеспечение*. Именно указанная подсистема является фундаментом универсального инструментария для решения образовательных задач [1]. В данном контексте можно сказать, что ядром информационного обеспечения образовательной деятельности являются цифровые (электронные) образовательные ресурсы (ЦОР/ЭОР).

В современной школе решение образовательных задач и построение его ЕИП невозможно без информатизации. Ясно, что именно информатизация является основой для создания ЕИП, которое включает совокупность технических, программных, телекоммуникационных и методических средств, позволяющих применять информационно-коммуникационные технологии (ИКТ) в образовательном процессе, а также осуществлять сбор, хранение и обработку данных о различных аспектах учебно-воспитательного процесса. Последующее полноценное развитие ЕИП школы напрямую зависит от темпов и качества ее информатизации.

При существующем многообразии подходов к проблемам создания, классификации и использования современных ЦОР в рамках отдельной статьи возможно остановиться лишь на некоторых моментах. Педагогические работники школы должны четко понимать, что разработка ЦОР базируется на реализации двух ключевых аспектов: мультимедийность и интерактивность.

В рамках решения образовательных задач под *мультимедийностью* понимается подача учебного материала по нескольким каналам восприятия обучаемого. И чем больше будет таких каналов, тем больше вероятность запоминания учащимися новых сведений. При этом требуется учитывать специфику психики, андрагогики и ряд других моментов.

Современная педагогическая наука отмечает, что традиционные принципы и методы обучения молодежи крайне неэффективны. Почему это происходит? Одним из объяснений указанной ситуации может быть рассмотрение информационной составляющей процесса обучения. В какой форме и из каких источников получает информацию современный молодой человек? В основном

это анимация, компьютерная графика, 3D-графика, видео, персональные компьютеры, планшеты, сотовые телефоны и другие электронные гаджеты.

В каком же виде поступает к нему учебный материал в рамках обучения в школе? Твердые носители информации (учебно-методическая литература), вербальное изложение достаточно сложных понятий и определений, плакаты, стенды и т.д. Он бы и рад учиться, но возникает двойная проблема восприятия: незнакомая информация представлена в форме, вызывающей отторжение. Поэтому занятие, проводимое в вербальной форме, не даст сколь-нибудь положительных результатов.

Даже подготовленная аудитория при такой форме проведения занятия в состоянии зафиксировать не более трети учебного материала. Сразу же по окончании занятия полученные знания можно делить на два, а если в течение недели эти знания не нашли прикладного значения, их объем сокращается до трех процентов от первоначального объема. Другими словами, все делали вид, что учат и учатся, но результат такого обучения практически нулевой.

В свою очередь, под *интерактивностью* следует понимать активное вовлечение обучаемых в образовательный процесс. Учащийся не должен быть сторонним наблюдателем, он должен стать активным участником процесса обучения. Именно это может стать одним из залогов успешности образовательного процесса.

На современном этапе создания единого информационного пространства разработка ЦОР возможна лишь с использованием специальных программных оболочек, которые во многом предопределяют качество конечного информационного продукта.

При этом необходимо четко понимать, что ни педагог, ни IT-специалист по отдельности не в состоянии создать полноценный ЦОР. Педагог должен знать особенности и возможности соответствующей программной оболочки, а программист – ориентироваться в методических принципах построения ЦОР.

При этом все участники процесса разработки информационного обеспечения образовательного процесса (а педагогические работники – в особенности) должны понимать, что дидактические и педагогические основы построения цифровых образовательных ресурсов не имеют ничего общего с принципами построения их классических аналогов.

Попытка создания ЦОР на основе текстовой информации и статической графики обречена на провал. По причинам, рассмотренным выше, их эффективность будет крайне низкой. Необходимо как можно более активно использовать динамическую визуализацию образовательной информации, основанную на реализации, в частности, принципа кадрирования. С такой задачей очень сложно справиться без специальной подготовки и знания структуры и состава ЦОР.

При всем многообразии образовательных ресурсов на начальном этапе формирования информационного пространства образовательного учреждения необходимо сосредоточить усилия на разработке отдельных, небольших по объему элементов, которые в дальнейшем по блочно-модульному принципу можно будет объединять в более глобальные структуры.

Помимо единой программной платформы для разработки ЦОР должна быть сформулирована и реализовываться единая информационная политика в рамках образовательного учреждения ФСИН России.

То есть, если мы хотим получить требуемое качество образования, нам необходимо, в частности, переходить на современные информационные технологии образования, базирующиеся на принципах интерактивности и мультимедийности. Но здесь наиболее актуальным становится вопрос: а в должной ли мере владеет данными технологиями педагогический состав школ ФСИН России? Следовательно, актуализируется аспект *кадрового обеспечения* формирования единого информационного пространства. Ключевой фигурой здесь выступает педагогический работник. Не касаясь проблемы качества его профессиональной подготовки, необходимо рассмотреть значение наличия у него сформированной информационно-технологической компетентности.

Информационно-технологическая компетентность преподавателя – профессионально-личностное, интегральное качество, проявляющееся в поисково-аналитической, информационно-коммуникационной и информационно-инструментальной компетенциях с целью информационного обеспечения образовательной практики преподаваемых дисциплин и использования особенностей процесса обучения.

Информационно-технологическая компетентность – осмысленное владение информацией (ее поиск, сбор, анализ, обобщение, хранение и использование), умениями и способами, основываясь на ней, принимать решения, делать отбор, согласовываясь с нравственными нормами, необходимыми для практического использования ее конкретного содержания в педагогической практической деятельности для реализации целей и задач обучения, воспитания и развития учащихся.

Следует отметить, что в педагогической науке используются также сходные понятия информационно-коммуникационной компетентности и информационно-коммуникативной компетенции. Терминологические тонкости и различия между этими понятиями выходят за рамки данной работы.

В качестве компонентов информационно-технологической компетентности преподавателей как личностной характеристики можно выделить:

- поисково-аналитическую;
- информационно-коммуникационную;
- информационно-инструментальную.

Информационно-технологическая компетентность преподавателя школы как психолого-педагогическое *явление* представляет собой:

- *ценность* (государственную, общественную, социальную, личностную), определяющую возможности расширения и формирования образовательного пространства и образовательной среды посредством их формирования;

- *процесс*, по окончании которого преподаватель в ходе повышения квалификации достигает более высокого уровня информационно-технологической компетентности.

- *систему*, т.е. модель психолого-педагогического явления, объединяющую все виды деятельности по формированию информационно-техноло-

гической компетентности преподавателя (овладение знаниями, умениями, навыками, способами деятельности) в структурную целостность – психолого-педагогический механизм, который продуцирует, формирует информационно-технологическую компетентность, управляет процессом этого формирования на основе замыслов, ценностей, целей, задач; систему, выполняющую тройную функциональную нагрузку: как способ познания теории и практики информационно-технологической компетентности преподавателя, как теоретико-методологический принцип ее осмысления и осуществления в действительности и как методологическое условие педагогической деятельности по ее *реализации;*

- *результат* воздействия объективных сил личности преподавателя, направленных на самообразование, самообучение, саморазвитие, самореализацию, самоактуализацию, самооценку уровней своей информационно-технологической компетентности в системе повышения квалификации.

Структурообразующим основанием информационно-технологической компетентности преподавателя является информационный опыт. Под информационным опытом понимаются конкретные образы, знания, представления, получение которых обусловливает свободный доступ к значимой информации, обеспечивающей руководство обучением в мысленном конструировании его, в опоре на эту информацию как при выполнении действий целеполагания, планирования, так и при выполнении ответных действий, осуществляя контроль и оценку результатов каждого действия в деятельности. Содержание информационного опыта включает полную, исчерпывающую информацию о психологическом образе предмета деятельности (его содержании, структуре, функциях), программе действий (внутренний план деятельности), корректируемой на основе непрерывно поступающей информации из всех источников, в том числе с помощью информационных компьютерных и интернет-технологий.

Педагогические условия, способствующие повышению уровня формирования информационно-технологической компетентности преподавателя школы:

а) мотивация преподавателей на овладение информационно-технологической компетентностью;

б) опора на имеющийся информационный опыт преподавателей;

в) ориентация учителей в образовательном процессе на непрерывный профессиональный рост и саморазвитие информационно-технологической компетентности;

г) алгоритмизация информационной деятельности преподавателей;

д) наличие формализованного стандарта информационного опыта;

е) развитие формализованного опыта на основе решения типовых информационных задач.

В ходе внедрения в педагогическую практику новых, регулярно обновляемых стандартов общего образования основной целью обучения становится не формирование совокупности знаний, умений и навыков, а основанной на них личной, социальной и профессиональной компетентности, которая заключается в умении самостоятельно добывать, анализировать и эффективно использовать информацию, рационально и эффективно жить и работать в быстро изменяющемся мире.

На наш взгляд, одна из причин снижения качества образовательного процесса кроется в терминологической неопределенности ключевых понятий теории компетентностного подхода в образовании. Вольно или невольно многие субъекты учебного процесса до сих пор под компетентностью понимают сумму знаний, умений и навыков. При этом игнорируется вторая составная часть указанного определения: «а также способов их применения (деятельности)».

Но даже полная трактовка данного определения компетентности далека от идеала. Не вторгаясь в научную дискуссию основных понятий компетентностного подхода, представляется возможным рассматривать компетентность как интегральную личностную характеристику, определяющую способность специалиста решать профессиональные проблемы и типичные профессиональные задачи, возникающие в реальных ситуациях профессиональной деятельности с использованием знаний, жизненного опыта, ценностей. Т.е. компетентность является средством нового подхода к оценке качества профессиональной подготовки специалиста, который получил название «компетентностный».

Компетентностный подход предполагает изменение приоритетов: отклонение от преобладающей ранее образовательной технологии, в основе которой лежит получение обучающимися знаний и формирование навыков, и переход к условиям, позволяющим обучающимся в конечном итоге приобрести требуемую совокупность компетенций, позволяющих будущему специалисту конкурировать и стабильно функционировать в условиях современного общества.

В основе компетентностного подхода лежат не просто знания, умения, навыки, а в первую очередь способность решать задачи, возникающие в ходе профессиональной деятельности и в различных жизненных ситуациях:

- познание и интерпретация явлений окружающего мира;
- освоение, владение, грамотное и эффективное использование современными техническими средами и технологиями, в том числе и информационно-телекоммуникационными;
- взаимоотношения между индивидами во всех сферах деятельности и др.

Сущность образовательного процесса при компетентностном подходе заключается в создании таких ситуаций и развитии соответствующих действий, которые сначала приближают, а затем приводят к формированию определенных компетенций.

Таким образом, новая модель образования, утвержденная федеральными государственными образовательными стандартами нового поколения, должна интегрировать интеллектуальные, физические, политические, социальные и эстетические аспекты знаний, поскольку компетентность должна выступать в ее самых различных проявлениях. К областям, развивающим компетентность в широком смысле, относят учебу, работу, сферу заботы о здоровье, культуру, политику, окружающую среду, экологию, мир. В качестве инструментов формирования такой компетентности выступают: общее образование, профессиональная подготовка, обучение без отрыва от производства, воспитание в семье, общинное развитие, средства массовой информации, культурно-просветительные учреждения и все виды деятельности человека, способствующие выполнению активной роли в обществе.

В современной педагогической теории понятие компетентности выступает в качестве основного, поскольку компетентность объединяет в себе, с одной стороны, интеллектуальную и навыковую составляющую образования, а с другой – в ней заложена идеология интерпретации содержания образования, формируемого «от результата». Кроме того, ключевая компетентность обладает интегративной природой, так как она содержит в себя ряд однородных или близкородственных умений и знаний, относящихся к различным областям деятельности человека.

Следует отметить, что существуют различные подходы к определению компетентности специалиста. Так, например, Н.Ф. Талызина считает, что она определяется только тремя составным частями: качеством, знаниями, умениями. В этом определении, на наш взгляд, явно упускается составляющая, обусловленная деятельностью. С учетом нового широкого понимания компетентности необходимо разрабатывать новое содержание образования. Новые учебные программы должны строиться исходя из новой концепции взаимоотношений между школой и остальными общественными структурами в рамках стратегии развития компетентности человека.

В последние десятилетие, несмотря на то, что изучением профессиональной компетентности активно занимались как отечественные, так и зарубежные специалисты, в современной научной литературе, как отмечалось выше, нет однозначного определения рассматриваемого понятия. В разных работах под профессиональной компетентностью понимаются:

– психическое состояние, позволяющее действовать самостоятельно и ответственно;

– уровень собственно профессионального образования;

– способность должностного лица успешно решать относящиеся к его компетентности задачи;

– сумма знаний, умений, навыков, усвоенных субъектом в ходе обучения, в узком смысле и уровень успешности взаимодействия с окружающей средой – в широком;

– сложное образование, включающее комплекс знаний, умений, свойств и качеств личности, которые обеспечивают вариативность, оптимальность и эффективность построения учебно-воспитательного процесса;

– способность работника качественно и безошибочно выполнять свои функции как в обычных, так и в экстремальных условиях, успешно осваивать новое и быстро адаптироваться к изменяющимся условиям;

– совокупность таких признаков, как наличие знаний для успешной деятельности, понимание значения этих знаний для практики; набор операционных умений; владение алгоритмами решения трудовых задач; способность творческого подхода к профессиональной деятельности;

– сочетание психических и личностных (человеческих) качеств и такое психическое и личностное (душевное) состояние, которое позволяет действовать самостоятельно и ответственно; способность и умение выполнять определенные трудовые функции;

– специфическая способность, необходимая для эффективного выполнения конкретного действия в конкретной предметной области и включающая узкоспециальные знания, предметные навыки, способы мышления, а также понимание ответственности за свои действия;

– не просто обладание знаниями, а постоянное стремление к их обновлению и использованию в конкретных условиях, т.е. владение оперативными и мобильными знаниями; это гибкость и критичность мышления, подразумевающая способность выбирать наиболее оптимальные и эффективные решения и отвергать ложные.

Из анализа приведенных определений следует, что многие из них чрезмерно просты, и здесь возникает необходимость детализации структуры и компонентов компетентности, но без привязки к конкретному виду профессиональной деятельности. Ясно, что такая универсальная профессиональная компетентность может дополняться в зависимости от вида профессиональной деятельности, в контексте которой она рассматривается. При этом содержательная часть компонентов компетентности гораздо в большей степени, чем ее общая структура будет определяться конкретным видом профессиональной деятельности.

Вследствие разнообразия описанных подходов к понятию компетентности предлагаются и различные ее структуры с дифференцирующимся элементным составом.

На наш взгляд, компетентность должна иметь следующую структуру:

1) готовность к появлению компетентности;

2) владение знанием и содержанием компетентности;

3) опыт проявления компетентности в разнообразных стандартных и нестандартных ситуациях;

4) отношение к содержанию компетентности и объекту ее приложения;

5) эмоционально-волевая регуляция процесса и результата проявления компетентности.

Помимо элементного состава, следует выделить еще и сущностные черты компетентности:

- характеризует способность и готовность личности выступать в качестве целостного совместного субъекта саморазвития системы «человек-мир»;

- отражает субъективную позицию обучающегося в обучении, обеспечивает реализацию личностных смыслов;

- имеет метапредметный характер;

- реализует дидактический принцип связи обучения с жизнью через обогащение витагенного опыта выявления и решения проблем;

- проявляется и контролируется в процессе практического осуществления деятельности.

Отсюда вытекает, что понятие компетентности включает не только когнитивную и операционально-технологическую составляющие, но и мотивационную, этическую, социальную и поведенческую. Оно включает результаты обучения (знания и умения), систему ценностных ориентаций, привычки и др.

И здесь актуализируется проблема соотношения понятий «компетентность» и «компетенция». Исходя из вышеизложенного, получается, что приведенное нами в начале понятие компетентности таковым и не совсем является. Более верно сказать, что это *компетенция*. То есть компетенция представляет собой норму, требование к образовательной подготовке обучаемого, в то время как компетентность – уже состоявшееся личное качество в совокупности с минимальным опытом деятельности в заданной сфере. Другими словами, компетенция – это идеал, к которому нужно стремиться, а компетентность – вторичное по отношению к компетенции понятие, характеризующее степень владения качеством.

В то же время данный подход не отменяет ту точку зрения, в соответствии с которой профессиональную компетентность можно рассматривать как определенный набор компетенций специалиста.

Рассмотренный состав структурных элементов единого информационного пространства школы системы ФСИН России не является исчерпывающим и требует более детального и углубленного анализа.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Блинов В.И. Профессиональные стандарты педагогической деятельности // Педагогика. 2010. № 5. С. 14-42.

2. Корнилова Е.А., Савотченко С.Е. О формировании информационно-коммуникационной компетентности педагогов // Научные ведомости «БелГУ». Сер. История. Политология. Информатика. 2014. Вып. 32/1. № 21(192). С. 175-181.

3. Наливалкин А.Ю. Анализ понятия информационно-образовательной среды // Вестник РМАТ. 2012. № 1 (4). С. 101-103.

4. Понятие информационно-образовательной среды ОУ / Открытый класс [Электронный ресурс]. – Режим доступа: http://www.openclass.ru/node/21749.

5. Смирнова И.Г. Инновационные аспекты формирования информационно-коммуникативной компетенции в образовательном пространстве современного школы // Вестник Воронежского института МВД России. 2015. № 2. С. 212-214.

ПРОЦЕСС ПРИВЕДЕНИЯ ИНФОРМАЦИОННОЙ МОДЕЛИ ОРГАНИЗАЦИОННОЙ СИСТЕМЫ К ИЕРАРХИЧЕСКОЙ СТРУКТУРЕ

THE PROCESS OF BRINGING THE INFORMATION MODEL OF THE ORGANIZATIONAL SYSTEM TO HIERARCHICAL STRUCTURE

Иванов Игорь Петрович
(Краснодарский университет МВД России)

Ivanov Igor Petrovich
(Krasnodar University of the MIA of Russia)

Аннотация: объектом исследования является организация образовательного процесса в условиях современного информационного общества. Предметом исследования является роль информационных технологий в повышении качества обучения. На основе системного анализа результатов работ других авторов и собственных исследований сделаны выводы о необходимости применения сбалансированного метода оценивания результатов учебной деятельности, который ведет обучающихся к востребованному развитию компьютерной грамотности и самостоятельности гармонического развития личности.

Ключевые слова: методы и критерии оценивания, сбалансированный образовательный процесс, качество обучения, информационные технологии, активные участники образовательной деятельности.

Annotation: the subject of investigation is organization of education process in conditions of modern information society. The subject of education is the role of information technologies in enhancing the education level. Conclusions were made based on systematical analyze of other authors'works and personal investigation conclusions were made that there is a necessity in using balanced method of evaluating the results of educational activities, which leads students to enhance their computer knowledge and self-development.

Key words: methods and evaluation criteria in a balanced educational process, the quality of teaching, information technology, active participants of educational activities.

В настоящее время перед образовательными организациями общество ставит принципиально новые задачи. Одной из главной задач считается повышение качества обучения на основе разработки актуальных обучающих систем и проведения социальной адаптации обучающихся. Эффективным инструментом решения обозначенной проблемы считается включение в образовательную деятельность информационных технологий (ИТ). Каждая образовательная организация считает наиболее важным направлением своей деятельности формирование сбалансированного образовательного процесса, который должен охватывать формирование новых знаний и стимулирование деятельности обучаю-

щегося. В рассматриваемом контексте изучение дисциплины «Информатика и информационные технологии в профессиональной деятельности» становится одной из важнейших составляющих развития у обучающихся необходимых профессиональных компетенций.

Современная школа готовит не пассивных участников образовательной деятельности, которых преподаватели должны научить и привить им знания, а активных участников образовательной деятельности, имеющих свой опыт обучения.

Из психологии известно, что развитие разных полушарий мозга человека оказывает непосредственное влияние на мыслительные функции человека или склад ума. От обучающихся в образовательных организациях МВД на занятиях по точным дисциплинам можно часто услышать фразу: «Я этого не понимаю, так как у меня гуманитарный склад ума». Необходимо определиться, когда человек делает выводы, что у него гуманитарный склад ума, на что он надеется? Показывает свое превосходство перед другими или наоборот, расписывается в полном бессилии при преодолении возникающих трудностей? Гуманитарный склад ума основывается на развитой интуиции и творческом начале (на так называемом креативе). А где взять ответы на новые неизвестные вопросы, основываясь только на природной интуиции и творчестве, когда не хватает общеобразовательных базовых школьных знаний?

В настоящее время актуальными становятся исследования по проектированию комплексов занятий в условиях обучения в изменившейся окружающей среде. Курсанты ведомственных образовательных организаций, попадая после школы в изолированную среду, нередко выбиваются из привычной для них колеи обучения и познавательной деятельности. Преподаватель, приходя на занятие в группу, где до 40% составляют граждане иностранных государств, которые не сдают единые государственные экзамены по профильным предметам и российские школьники, имеющие при сдаче ЕГЭ по математике в среднем около 30 баллов, начинает задумываться о возможностях логического рассуждения и решения ситуационных задач. Рене Декарт, размышляя о поиске истины вещей, писал: «… я до сих пор разрабатывал эту всеобщую математику так, чтобы потом я мог считать себя способным изучать несколько более возвышенные науки с усердием, отнюдь не преждевременным» [1]. Поэтому обучающимся необходимо повышать уровень образованности за счет терпеливости и усердия.

Во время проведения практических занятий преподаватель пытается показать на примерах влияние своего опыта и знаний на правильное выполнение действий и решение задач. Если преподавателю приходится очень подробно объяснять простые задания, то «продвинутые» пользователи теряют интерес к обучению, а начать со сложных – не будет полного адекватного восприятия понимания у остальной части обучающихся. Дополнительным фактором изменения роли обучения для курсантов, граждан зарубежных государств считается преодоление языкового барьера. Курсанты, обучающиеся в разных школах, имеют разный уровень подготовки, чаще всего резко выраженные возможности интеллектуального развития, а в группах с иностранными обучающимися – и тем более, когда их математические навыки основаны на простейших операциях счета.

Рассматривая внедрение информационных технологий в образовательный процесс с позиции системного подхода, можно выделить три основных аспекта ИТ:

1. Объект изучения.
2. Средство обучения.
3. Инструментарий автоматизации образовательной деятельности.

Первый аспект находит свое отражение в названии изучаемой дисциплины. Второй аспект реализуется преподавательским составом образовательных организаций при разработке заданий различного уровня сложности для изучения учебного материала. Третий аспект находит реализацию при постоянном обеспечении доступа обучающихся к единым информационным ресурсам не только образовательной организации, но и к электронным ресурсам сети Интернет. Для автоматизации образовательной деятельности недостаточно только желания преподавательского состава по выработке специализированных инновационных образовательных методик, необходим комплексный подход всего постоянного состава к изменению ситуации и внедрению современных информационных технологий в образовательную деятельность.

Чтобы выровнять интеллектуальное развитие обучающихся, разработанные задания должны иметь повышение уровня сложности, для слабых – больше, для сильных – меньше. При подготовке нескольких вариантов заданий различного уровня сложности перед преподавателем встает дилемма, а как оценивать знания и навыки обучающихся. За выполнение сложных заданий грамотным обучающимся ставить одинаковые оценки, как и за выполнение простых менее подготовленными? Где справедливость? Если оценивать критерий знаний в общем одинаково для всех обучающихся, то результаты оценивания будут практически однородными, как говорят в статистике, не будет вариации знаний. Поэтому изучение одного и того же материала позволяет одним обучающимся затрачивать на восприятие и получение навыков больше времени, чем другим. Для постоянного мониторинга деятельности обучающихся на практических занятиях преподавателем можно использовать программные продукты, которые позволяют в режиме реального времени подключаться к компьютерам пользователей и постоянно отслеживать результаты их действий по выполнению поставленных заданий, но для этого необходимо в компьютерных классах устанавливать и однотипное программное обеспечение. Исключение формализма при выставлении оценок может достигаться при оценивании множественности критериев, которые будут влиять на конечный оценочный результат:

1. Оценочный балл за выполненную правильно работу.
2. Оценочный балл качественной составляющей: сделано по шаблону, без/с пониманием материала.
3. Оценочный балл за поощрение выполнения задания (слабому добавить, чтобы появился стимул к дальнейшему изучению, сильному снизить за пассивность изучения).

4. Оценочный балл за стимулирование изучения предмета (я сделал сегодня хуже, чем мог, или что надо выполнить на занятии, чтобы получить удовлетворительную оценку).

5. Оценочный балл за проявление творческих способностей (подготовка выступлений по изучаемой теме).

Для достижения желаемых показателей, можно вводить и другие критерии оценивания деятельности обучающихся [2]. Практика показывает, что сбалансированный метод оценивания результатов учебной деятельности ведет обучающихся к востребованному развитию компьютерной грамотности и самостоятельности гармонического развития личности.

Как писал Декарт, «если кто-либо всерьёз хочет исследовать истину вещей, он не должен выбирать какую-то отдельную науку: ведь все они связаны между собой и друг от друга зависимы; но пусть он думает только о приумножении естественного света разума, не для того, чтобы разрешить то или иное школьное затруднение, но для того, чтобы в любых случаях жизни разум (intellectus) предписывал воле, что следует избрать, и вскоре он удивится, что сделал успехи гораздо большие, чем те, кто занимался частными науками, и не только достиг всего того, к чему другие стремятся, но и превзошёл то, на что они могут надеяться» [1]. Основываясь на его мысли, опубликованной в работе «Правила для руководства ума», хочется пожелать обучающимся не останавливаться перед трудностями обучения и всегда стремиться превзойти свои достигнутые успехи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Декарт Рене. Сочинения в двух томах. Т. 1. – М: Мысль, 1989. – 654 с.

2. Иванов И.П., Литвинов В.А., Максимов А.П. Рейтинговая оценка успеваемости и общественной активности курсантов и студентов // Вестник учебного отдела Барнаульского юридического института МВД России. 2005. № 4. С. 21-25.

О РАЗРАБОТКЕ ПРОГРАММНЫХ ПРИЛОЖЕНИЙ ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ ЗАДАНИЙ ПО РАЗДЕЛУ «МЕТОДЫ ОПТИМИЗАЦИИ» ДИСЦИПЛИНЫ «ПРИКЛАДНАЯ МАТЕМАТИКА»

ON THE DEVELOPMENT OF SOFTWARE APPLICATIONS FOR THE IMPLEMENTATION OF PRACTICAL ASSIGNMENTS IN THE SECTION «METHODS OF OPTIMIZATION» DISCIPLINE «APPLIED MATHEMATICS»

Михайленко Евгений Владимирович
(Краснодарский университет МВД России)

Mikhaylenko Evgeny Vladimirovich
(Krasnodar University of MIA of Russia)

Аннотация: в статье представляется созданный автором комплекс программ для выполнения практических заданий по разделу «Методы оптимизации» дисциплины «Прикладная математика». Автор раскрывает предпосылки, описывает основные методы и технологии, применяемые при разработке комплекса программ. Описываемые приложения иллюстрируются рисунками.

Ключевые слова: автоматизация, алгоритм, линейное программирование, матричные игры, прикладная математика, программный модуль.

Annotation: the author presents a set of programs for performing practical assignments in the section «Methods of optimization» in the discipline of «Applied mathematics». The author reveals the prerequisites, describes the main methods and technologies used in the development of a set of programs. The described applications are illustrated in Figures.

Key words: automation, algorithm, linear programming, matrix games, applied mathematics, software module.

Перед образовательными организациями МВД России стоит задача качественной подготовки специалистов для органов внутренних дел. В связи реализуемыми в Краснодарском университете МВД России специальностями 10.05.05 Безопасность информационных технологий в правоохранительной сфере, 38.05.01 Экономическая безопасность, 40.05.03 Судебная экспертиза на кафедре информатики и математики изучаются такие математические дисциплины, как «Математика», «Прикладная математика», «Математические основы обработки информации», «Эконометрика», «Статистика», «Численные методы», «Математика и информатика».

Специфика изучения математических дисциплин состоит не только в получении курсантами и слушателями определенных знаний. Важны устойчивые

навыки применения обучаемыми изученного теоретического материала для решения практических задач.

Важное место в процессе изучения математических дисциплин обучающимися занимает подготовка заданий на практические занятия и самостоятельную работу. Традиционно для этих целей преподавателями подбираются задачи из общеизвестных либо самостоятельно написанных учебников, пособий, сборников задач и других учебно-методических изданий. Однако эффективность использования такого рода материалов крайне мала. Необходимо отметить существенную ограниченность количества типовых задач в изданиях. Преподаватель вынужден выдавать, например, на самостоятельную подготовку общий список задач для всех курсантов или в лучшем случае задания по нескольким вариантам.

В связи с этим обучающиеся теряют мотивацию самостоятельно выполнять такие общие для всех задания. Часто происходит простое копирование выполненных работ у добросовестных однокурсников или даже переписывание решений прошлых лет. Наконец, проверка таких работ создает серьезные трудности и у преподавателя. Для анализа рукописных работ учащихся требуется огромное количество сил и времени. Кроме того, оценить качество работ, выполненных курсантами во внеаудиторное время, в лучшем случае совместными усилиями всей учебной группы, просто невозможно.

В связи с этим на кафедре информатики и математики появилась и развивается идея автоматизации подбора заданий и проверки выполненных курсантами работ по математическим и естественно-научным дисциплинам. В связи с широким использованием компьютерной техники в учебных аудиториях университета, развитием компьютерной сети на всей территории учебного заведения, подключения к ней через Wi-Fi-соединения личных ноутбуков и планшетов курсантов и слушателей появилась возможность реализовать эту идею программными методами.

При детальном исследовании технических, финансовых, правовых возможностей кафедры и обучаемых выбор программного обеспечения для реализации идеи пал на общедоступный пакет программ Microsoft Office. Удобство использования пакета MS Office заключается также и в том, что перечень заданий, выведенный в виде документа Word или Excel, не требует разработки специальных печатных форм. В соответствии с выбором среды все программные продукты, реализующие идею, написаны в виде макросов на языке Visual Basic for Application, являющегося основным инструментарием данного пакета.

Суть проекта заключается в генерации числовых и символьных значений для подобранных преподавателем типовых задач. Документ с незаполненным шаблоном заданий и ответов помещается в виртуальный учебно-методический кабинет кафедры информатики и математики, размещенный на сервере компьютерного центра университета. Кроме того, задания распространяются преподавателями с использованием облачных технологий, и доступ к домашним заданиям открыт через Интернет для всех обучаемых круглосуточно.

В этом случае преподаватель создает виртуальную интерактивную группу, к ней подключаются все курсанты, которые впоследствии могут использо-

вать выложенные преподавателем актуальные учебные ресурсы: мультимедийные слайды, тексты лекций, индивидуальные задания на самостоятельную подготовку, примеры решения задач, справочные материалы. С помощью облачных технологий можно также задавать преподавателю и другим участникам группы вопросы, высылать на проверку выполненные работы, организовывать видео- и аудиозапись конференции.

Для осуществления генерации заданий курсанту необходимо заполнить поле «Фамилия и инициалы». Введенные им данные, а также дата и время запуска генерации, автоматически выводимые на лист, используются для расчета номера варианта. В дальнейшем при автоматизированной проверке работы, производится верификация соответствия номера варианта указанным в работе времени и фамилии курсанта. Данная процедура позволяет избежать подлогов выполненных работ, и при нестыковке всех трех компонентов: варианта, времени и записи, идентифицирующей обучаемого, проверка работы не проводится. Генерация параметров каждого задания в предлагаемых работах осуществляется по разработанным алгоритмам, обязательно включающим номер варианта.

В процессе работы над созданием программных продуктов по различным разделам математики пришлось столкнуться с рядом проблем, большинство из которых удалось благополучно решить. Рассмотрим пример разработки программного обеспечения практических занятий и самостоятельной работы для курсантов, обучающихся по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, и изучающих раздел «Методы оптимизации» по дисциплине «Прикладная математика».

Комплекс программ обеспечивает практические работы и самостоятельную подготовку по темам «Методы решения задач математического программирования», «Двойственные задачи», «Линейная транспортная задача» и «Теория игр» и состоит из 10 программных модулей:

1. Графический метод решения задач линейного программирования.
2. Метод Жордана-Гаусса.
3. Преобразования однократного замещения.
4. Симплексные преобразования.
5. Симплексный метод решения задач линейного программирования.
6. Двойственные задачи.
7. Опорный план транспортной задачи.
8. Метод потенциалов.
9. Принцип максимина.
10. Решение матричных игр.

Модуль «Графический метод решения задач линейного программирования» (см. рис. 1) предназначен для решения задач линейного программирования двух переменных.

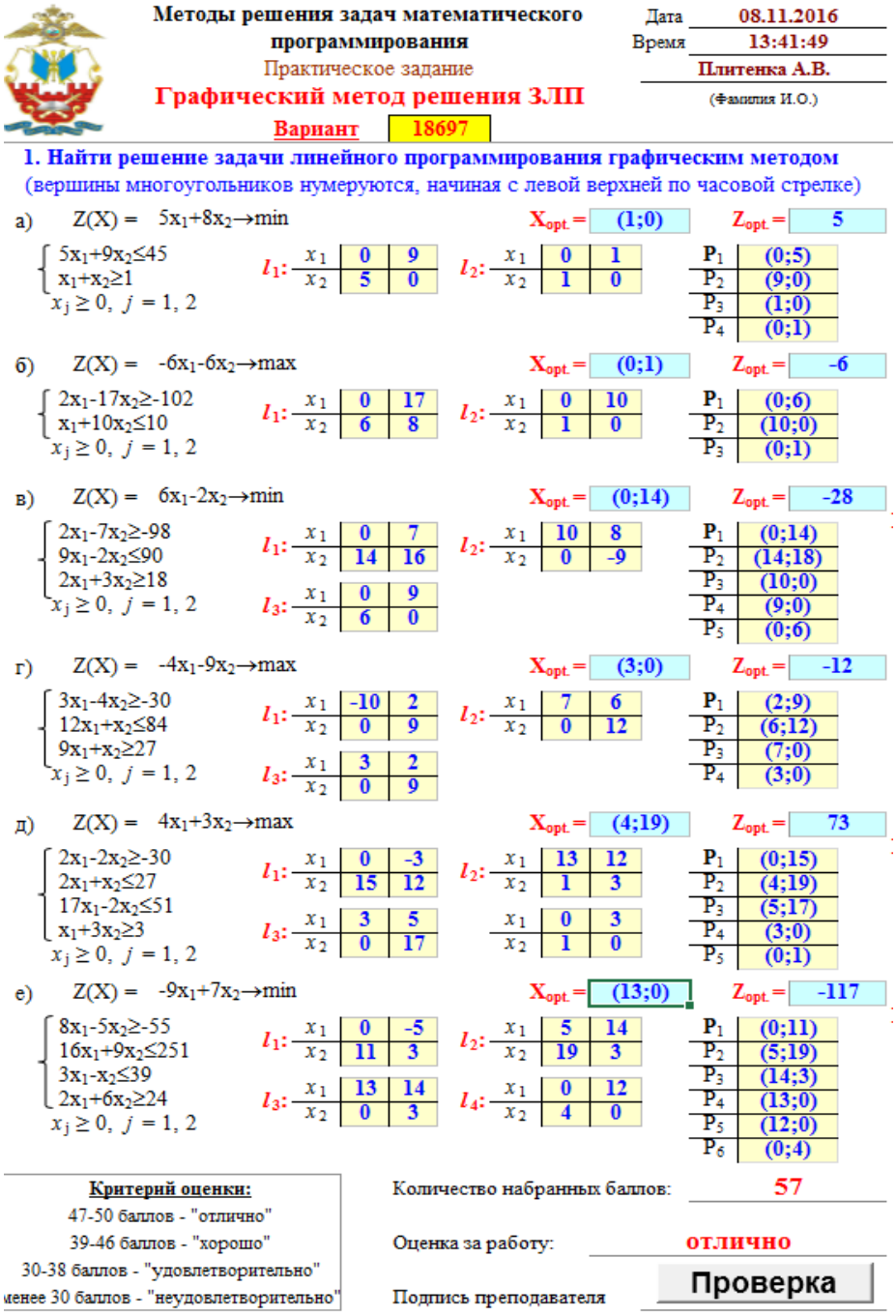


Рис. 1. Модуль «Графический метод решения ЗЛП».

Метод основывается на возможности графического изображения области допустимых решений задачи и нахождения среди вершин полученного многоугольника оптимального решения. Область допустимых решений задачи строится как пересечение полуплоскостей решений каждого из заданных ограничений. При решении генерируемых задач обучаемому необходимо вывести координаты любых точек, по которым строятся прямые, ограничивающие решения неравенств, вершины многоугольника, являющегося областью допустимых решений задачи линейного программирования, а также оптимальные решения.

Модуль «Метод Жордана-Гаусса» (см. рис. 2) посвящен решению систем линейных уравнений с использованием алгоритма Жордана-Гаусса.

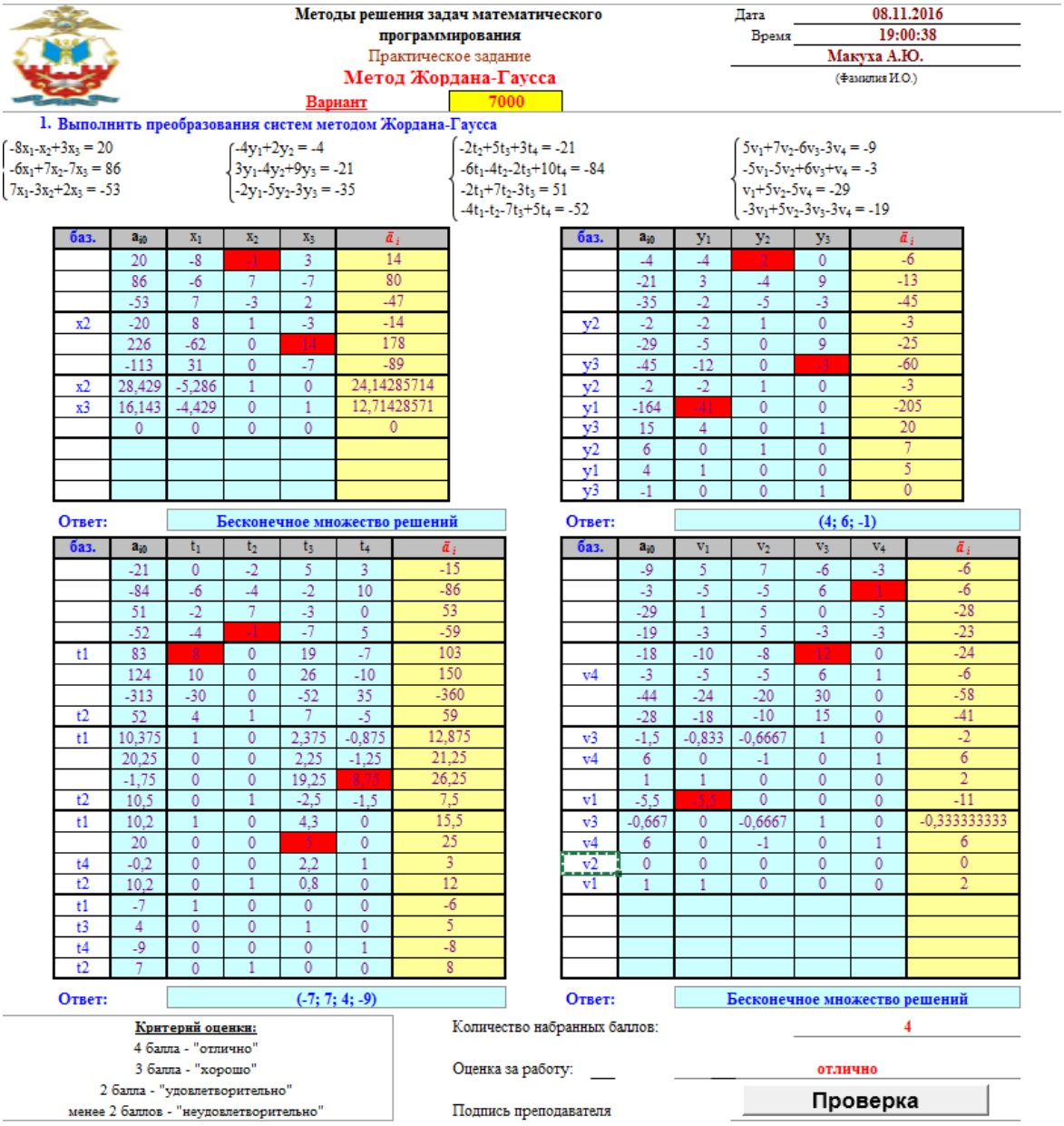


Рис. 2. Модуль «Метод Жордана-Гаусса».

Выполняя преобразования Жордана-Гаусса, курсант определяет, является генерируемая система совместной или несовместной, а в случае совместности – определенной или неопределенной. На каждом шаге преобразований коэффициенты системы заносятся в таблицы, отмечаются базисные переменные и проводится вычисление контрольных сумм по каждой рассчитываемой строке.

В работе с модулем «Преобразования однократного замещения» (см. рис. 3) курсанты также используют алгоритм метода Жордана-Гаусса. Решая систему из m линейных уравнений с n неизвестными, они приводят систему к единичному базису. Введя свободные переменные в базис, базисные переменные превращаются в свободные и получаются новые базисные решения. Такие преобразования называются однократными замещениями. Задача обучаемых – с помощью преобразований однократного замещения найти все базисные решения генерируемых систем. Результаты всех преобразований заносятся в таблицы, а затем выписываются и базисные решения.

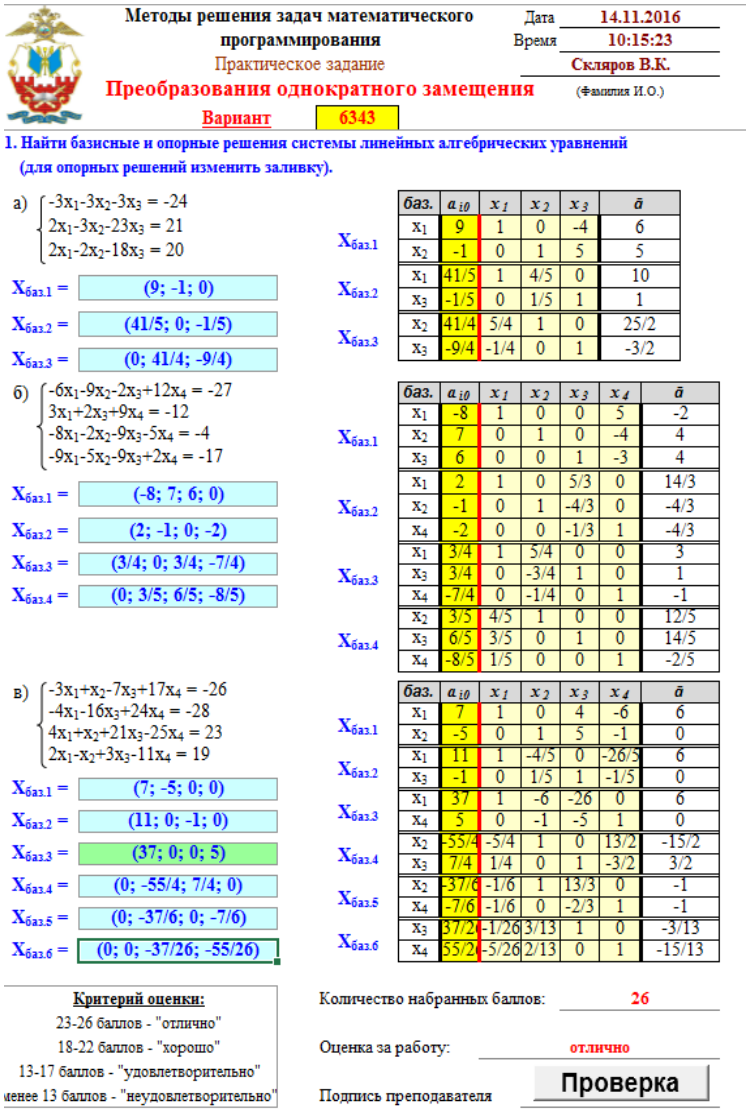


Рис. 3. Модуль «Преобразования однократного замещения».

В модуле «Симплексные преобразования» (см. рис. 4) обучаемые также выполняют преобразования однократного замещения. Однако на выполняемый процесс накладывается ряд ограничений:

1) разрешающий элемент выбирают только в том столбце, где есть положительные элементы;

2) если положительный элемент один, то он берется в качестве разрешающего элемента;

3) если положительных элементов несколько, то в качестве разрешающего элемента берется тот, для которого отношение свободного члена к нему будет наименьшим [1].

В результате выполнения данного алгоритма определяются все опорные решения.

В первом задании работы требуется произвести симплексные преобразования уже готовых опорных решений, а во втором необходимо найти любое опорное решение и с помощью симплексных преобразований определить все остальные.

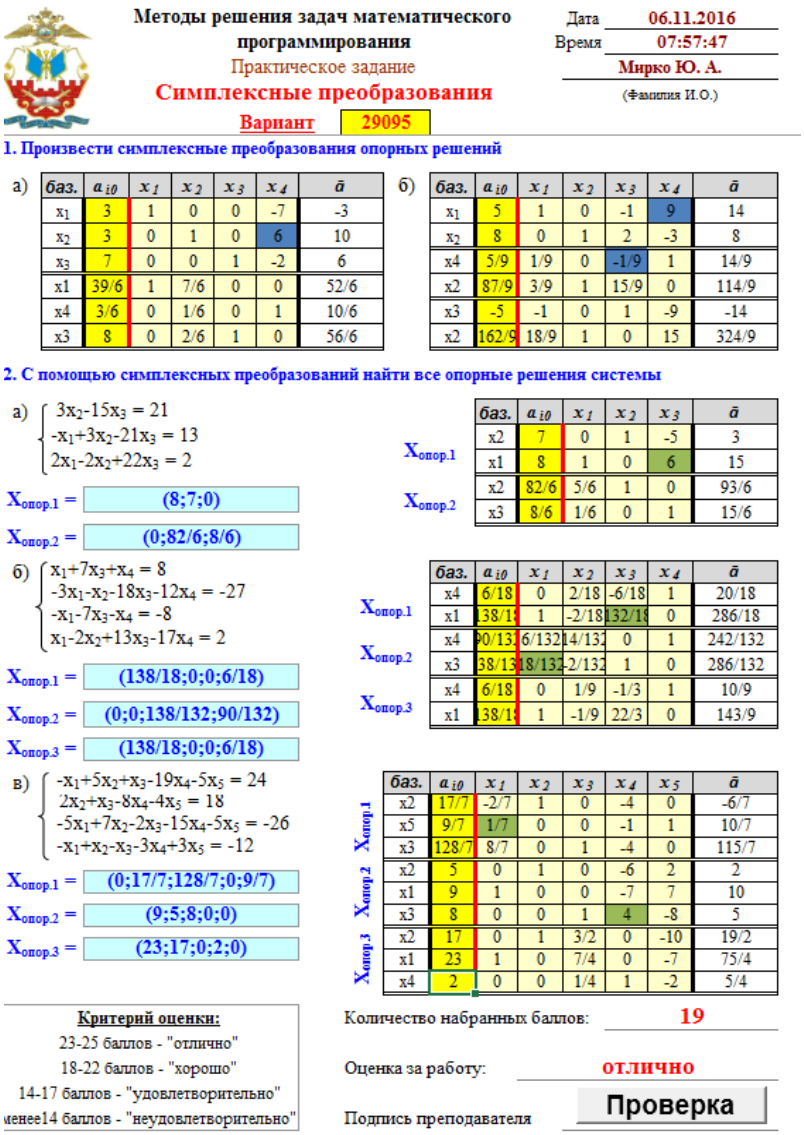


Рис. 4. Модуль «Симплексные преобразования».

Пожалуй, самым трудоемким для выполнения является модуль «Симплексный метод решения задач линейного программирования» (см. рис. 5).

Прежде чем решать задачу симплексным методом, обучаемые преобразуют генерируемую систему таким образом, чтобы правые части системы ограничений были неотрицательными. Затем полученная система записывается в каноническом виде.

Далее система уравнений при помощи симплексных преобразований приводится к начальному опорному решению и происходит проверка полученного решения на оптимальность. В случае неоптимальности опорного решения симплексным методом выбирается разрешающий элемент и производится переход к другому базисному решению.

Для решения каждой задачи потребуется несколько шагов. Результаты нахождения исходного опорного и оптимального решений необходимо занести в таблицы.

В программе реализованы задачи линейного программирования на максимум и минимум, приводящие к системам в каноническом виде из четырех и пяти переменных соответственно.

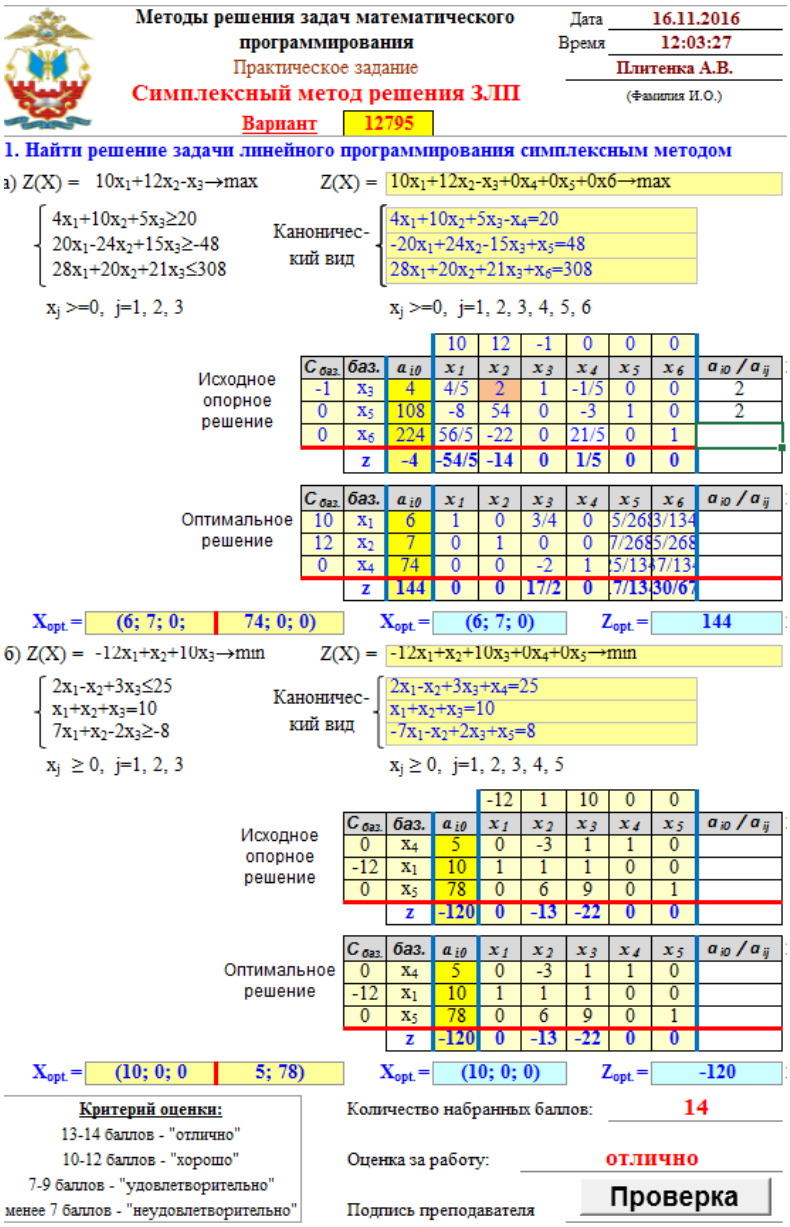


Рис. 5. Модуль «Симплексный метод решения ЗЛП».

Модуль «Двойственные задачи» (см. рис. 6) предназначен для решения задач линейного программирования с использованием теорем двойственности. Обучаемым предлагается для сгенерированной задачи линейного программирования с количеством переменных более двух составить двойственную задачу с двумя аргументами и решить ее графически.

В программе обучаемые должны ввести параметры новой целевой функции и соответствующую ей систему ограничений, выписать координаты угловых точек области допустимых значений, а также оптимальные решения пары двойственных задач.

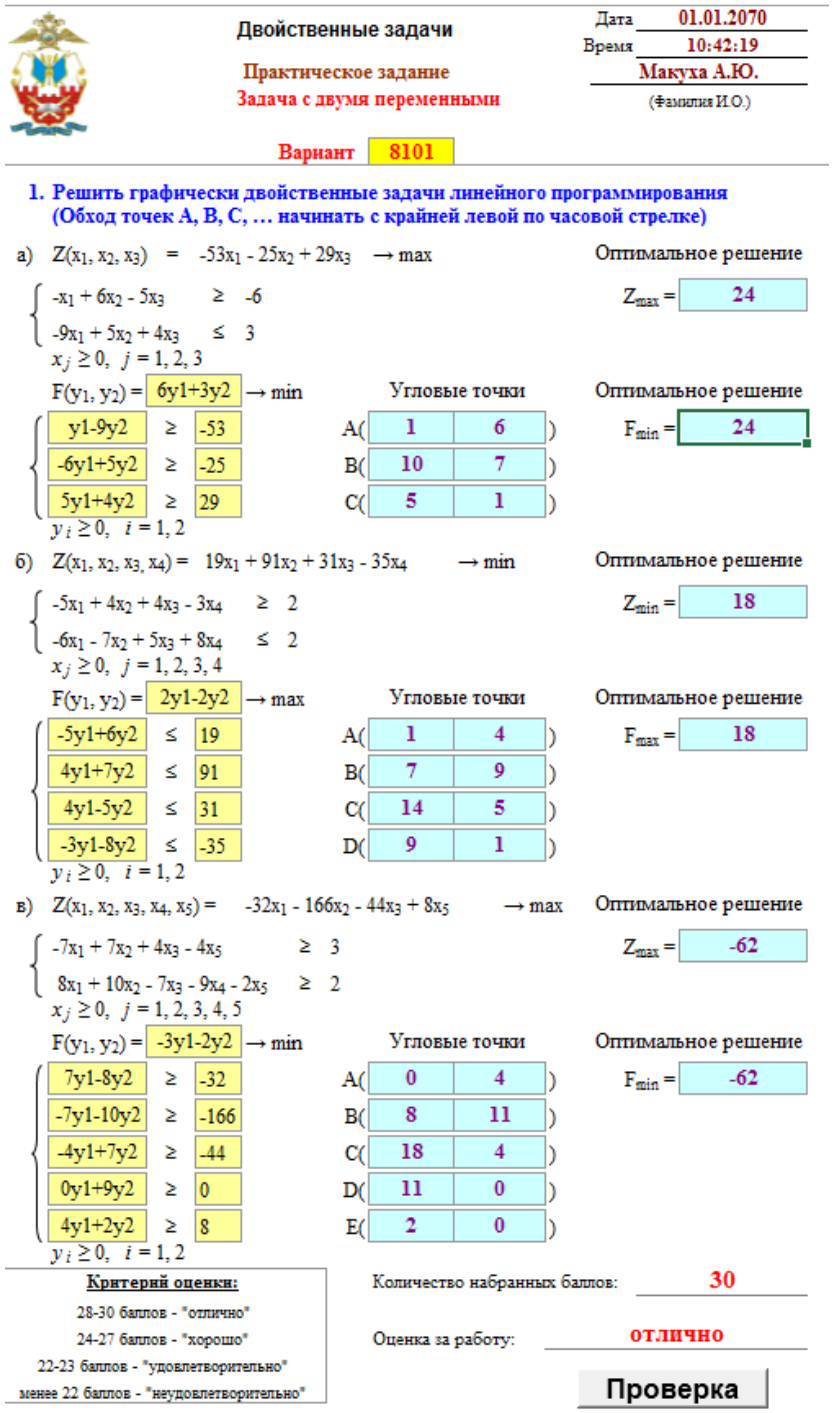


Рис. 6. Модуль «Двойственные задачи».

Модуль «Опорный план транспортной задачи» (см. рис. 7) используется курсантами при изучении темы «Линейная транспортная задача». В программе генерируются начальные условия и таблицы издержек для двух задач: открытого и закрытого типа. Обучаемым, используя метод северо-западного угла и метод минимального элемента, требуется построить начальные планы перевозок и определить затраты на эти перевозки. Алгоритм генерации данных построен таким образом, что заполнение опорных планов решения производится однозначно.



Рис. 7. Модуль «Опорный план транспортной задачи».

Для выполнения заданий нахождения оптимального решения транспортной задачи используется модуль «Метод потенциалов» (рис. 8).

В первом задании представлен план перевозок, не являющийся оптимальным. Обучаемым необходимо проверить представленный план на оптимальность и улучшить его, выполнив только один шаг перераспределения поставок. Для этого необходимо отметить все базисные ячейки и ввести недостающие, рассчитать потенциалы, вычислить коэффициенты критерия оптимальности, пометить критическую ячейку, построить цикл, пометить вершины цикла, определить величину перераспределения груза, выполнить перераспределение поставок, заполнить транспортный план и рассчитать новую стоимость перевозок.

При проверке задания возникла проблема идентификации линий, построенных курсантами при организации циклов. Проблему удалось решить, анализируя в программе все графические объекты, исследуя экранные координаты и цвета линий.

Во втором задании предполагается решение всей транспортной задачи, однако заполняются только опорный и оптимальный планы, а также соответствующие им стоимости перевозок.

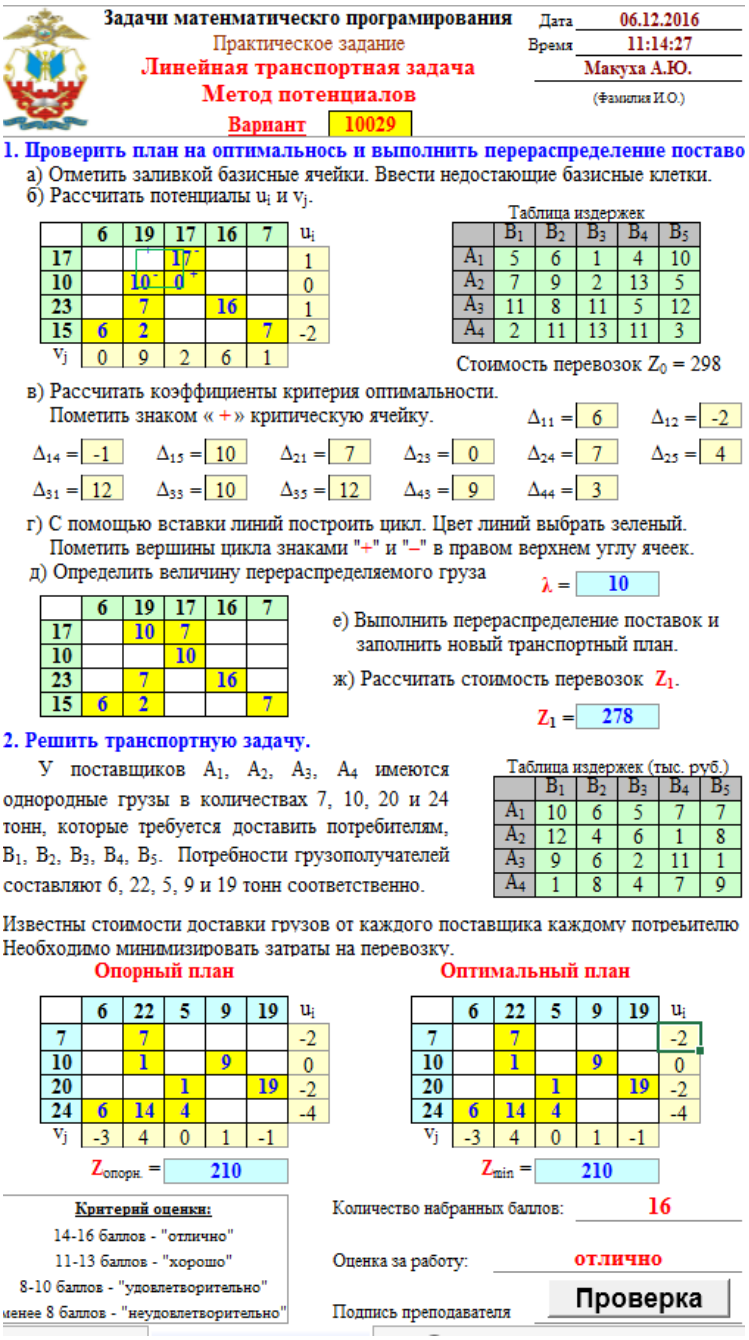


Рис. 8. Модуль «Метод потенциалов».

При выполнении модуля «Принцип максимина» (см. рис. 9) обучаемым представлены два задания по теории матричных игр в чистых стратегиях. В первом для сгенерированных платежных матриц необходимо определить нижнюю и верхнюю цены игры. А во втором представлены матричные игры с седловой точкой. Здесь, используя принцип максимина, нужно найти цену игры и выделить все седловые точки.

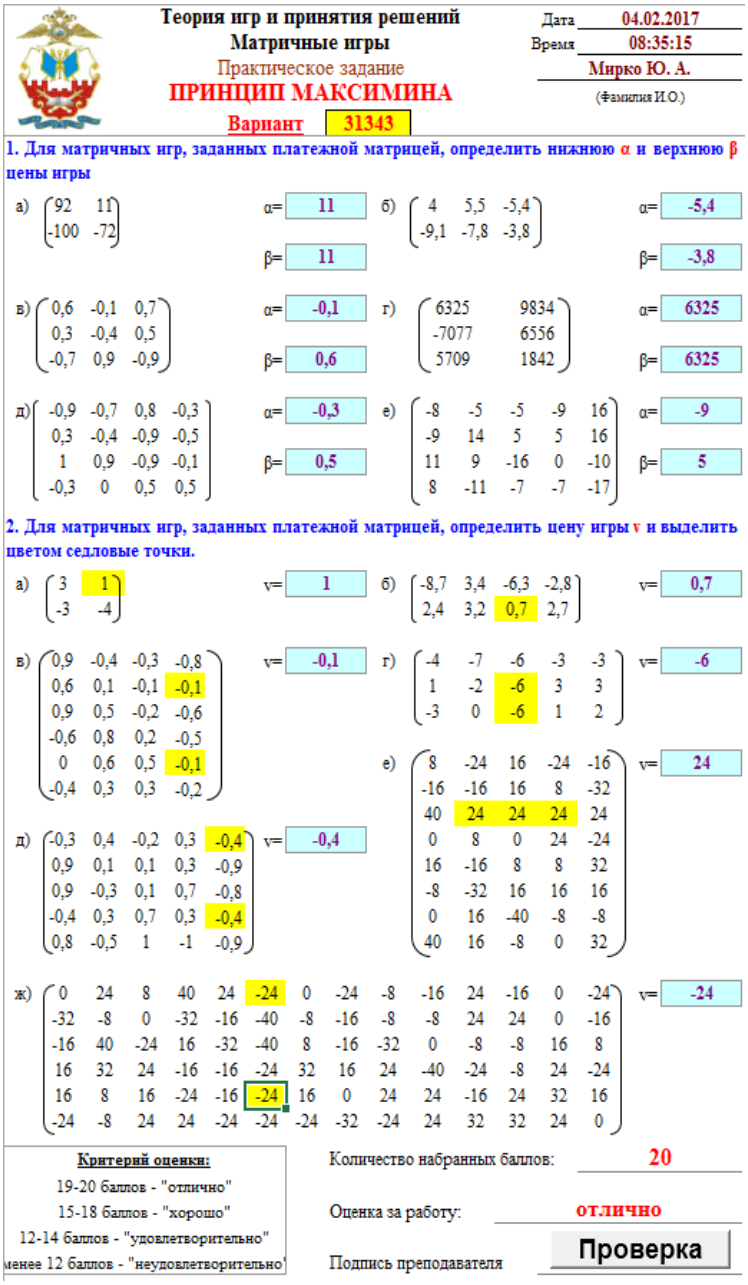


Рис. 9. Модуль «Принцип максимина».

В модуле «Решение матричных игр» представлены игры в смешанных стратегиях. Используя основные теоремы и свойства матричных игр, курсанты должны выполнить три задания.

В первом задании представлены платежные матрицы 2x2. Здесь необходимо при отсутствии седловой точки найти смешанные стратегии игроков, а также определить цену игры. Во втором предлагается упростить платежные матрицы, исключив дублирующие и доминируемые строки и столбцы. Наконец, третье задание предполагает решение матричных игр больших размерностей в смешанных стратегиях.

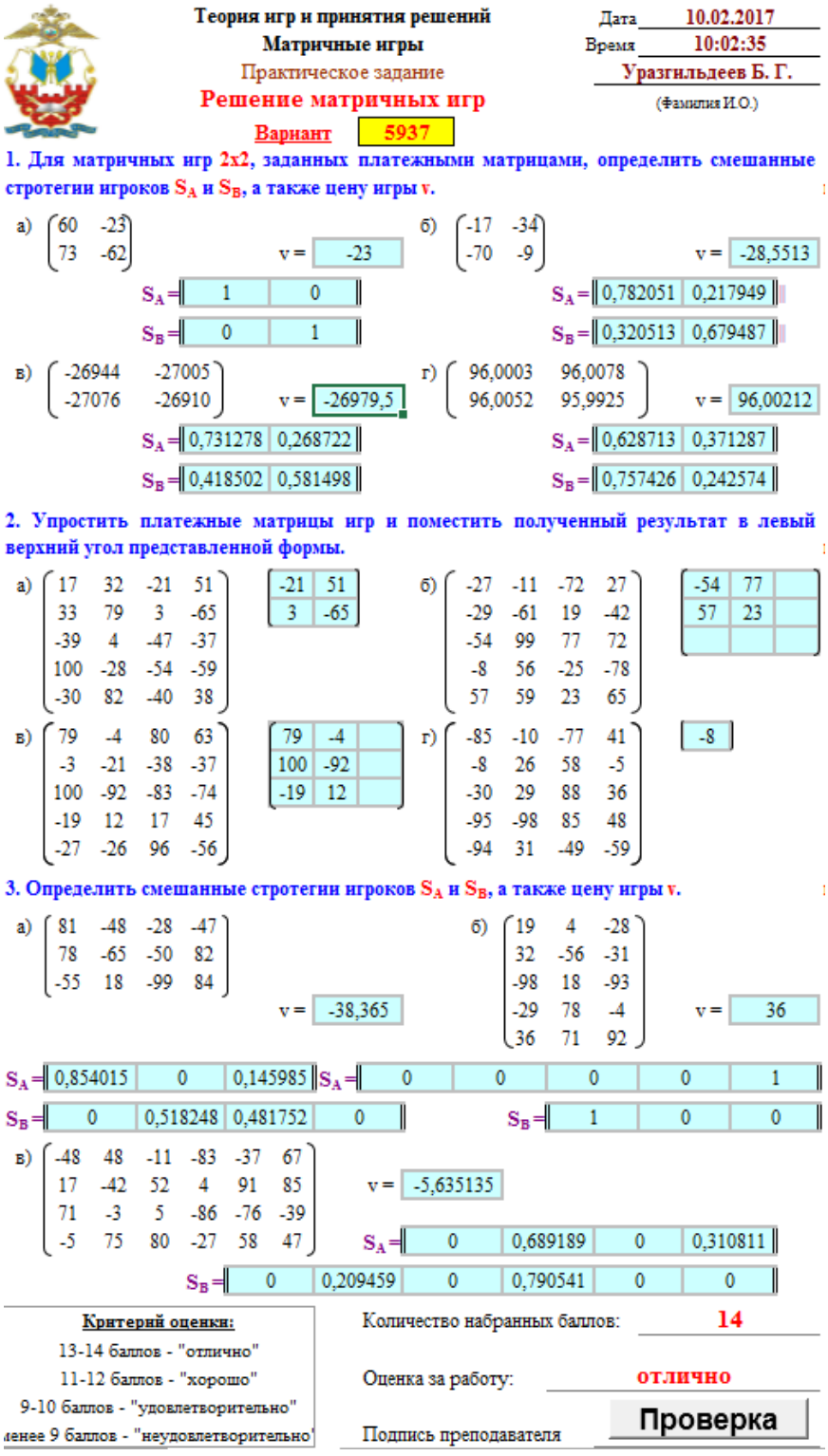


Рис. 10. Модуль «Решение матричных игр».

Представленный комплекс программ внедрен в образовательную деятельность кафедры информатики и математики. Опыт использования его в учебном процессе дал положительные результаты. В настоящее время ведутся работы над созданием ряда подобных программ для обеспечения дисциплин «Математика», «Прикладная математика» и «Численные методы».

МОДЕЛИРОВАНИЕ ПРОЦЕССА ФОРМИРОВАНИЯ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ КОМПЕТЕНЦИИ БУДУЩИХ БИБЛИОТЕКАРЕЙ СРЕДСТВАМИ ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА

MODELING OF PROCESS OF FORMATION OF INFORMATION-TECHNOLOGICAL COMPETENCE OF FUTURE LIBRARIANS THE TOOLS OF ELEARNING RESOURCE

Капуста Марина Валерьевна,
Сергеева Алина Юрьевна
(Белгородский государственный институт искусств и культуры)

Kapusta Marina Valerjevna,
Sergeeva Alina Urjevna
(Belgorod State Institute of arts and culture)

Аннотация: в статье рассматривается методология функционального моделирования на примере создания электронного образовательного ресурса для студентов-библиотекарей.

Ключевые слова: функциональное моделирование, нотация IDEF0, электронный образовательный ресурс, информационно-технологическая компетенция, библиотекари.

Annotation: the article discusses the methodology of functional modeling on the example of creation of electronic educational resource for students-librarians.

Key words: functional modeling, IDEF0 notation, electronic educational resources, information technology competence, librarians.

Для теоретического обоснования эффективных путей формирования информационно-технологической компетенции будущих библиотекарей средствами электронного образовательного ресурса осуществлялось моделирование этого процесса, которое включает в себя решение ряда последовательных исследовательских задач, направленных на выделение системы внешних и внутренних факторов, его детерминирующих. За основу моделирования мы выбрали теорию подобия, а модель выступает в качестве приближенного, сущностного аналога прототипа. На начальном этапе процесса моделирования изучались требования образовательного стандарта на специалиста-библиотекаря; разрабатывалась иерархия целей и задач моделируемого процесса; определялись исходные методологические позиции, проектировалось содержание образования с использованием электронного образовательного ресурса.

По мнению Ф.С. Воройского, невысокая эффективность создаваемых и действующих автоматизированных систем недостаточно применяется в след-

ствии недостаточного качества предоставляемой информационной продукции (в первую очередь электронных каталогов), услуг пользователям АБИС, а также в потерях трудовых и материальных ресурсов. Последнее – результат непродуманности технологии работы библиотеки, различных «нестыковок», возникающих за счет «устных» изменений, вносимых в процессы отдельными руководителями, а также из-за отсутствия автоматизированных средств контроля технологической дисциплины и качества работы исполнителей… будучи не документированы и системно не поддержаны, технологические процессы в библиотеке или информационном органе поставлены в жесткую зависимость от уровня компетентности и добросовестности работающих в этих организациях специалистов» [2].

Применение метода моделирования в библиотечных процессах заключается в том, чтобы правильно поставить и решить проблему поиска эффективной технологии, повышения качества и оперативности выполнения.

Результатом деятельности является модель проектирования ЭОР «Информационное обеспечение профессиональной деятельности». Чтобы вывести будущих библиотечных специалистов на высокий уровень, необходимо применять данную систему знаний в практике создания ЭОР для дальнейшего использования в процессе формирования информационно-технологической компетенции.

Функциональное моделирование есть технология анализа системы в общем как набора связанных между собой действий или функций. Действия системы анализируются независимо от объектов, которые обеспечивают их исполнение. Моделировать объект или процесс можно исходя из различных целей и временных рамок. В нашей работе мы моделировали процесс создания ЭОР «Информационное обеспечение профессиональной деятельности».

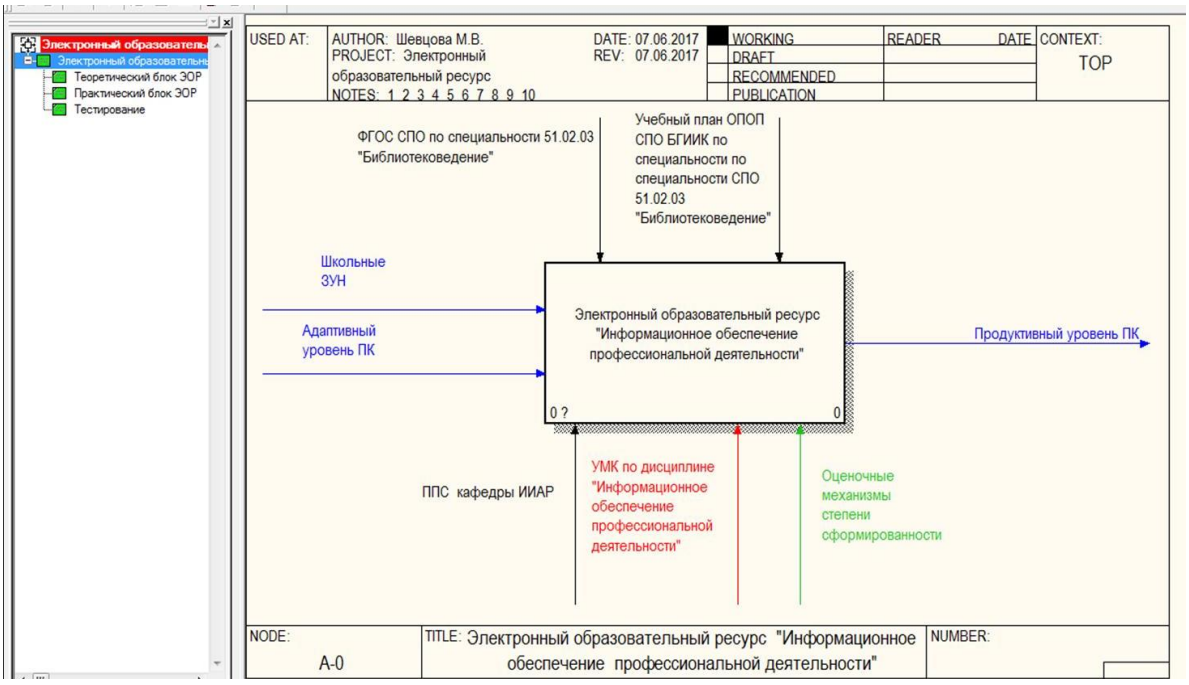


Рис. 1. Функциональная модель проекта.

Для описания процессов функционального моделирования в рамках образовательной среды наиболее оптимальной представляется методология функционального моделирования IDEF0, реализующая процессный подход, являющийся основой менеджмента качества. Стандарты есть набор моделей идеальных процессов TO-BE – «как должно быть», с которыми разработчик должен сравнивать свои процессы, чтобы понять, способны ли они качественно осуществлять образовательную деятельность, а если нет, то с чем это связанно и какие процессы у них запущены неправильно, где возможны ошибки и сбои.

Процесс построения функциональной модели включает в себя такие этапы, как:

– построение контекстной диаграммы;
– функциональная декомпозиция 1 уровня;
– сеанс экспертизы, следующий за каждым сеансом декомпозиции.

Процесс моделирования какой-либо системы в IDEF0 начинается с определения контекста, т.е. наиболее формального уровня описания системы в целом. В контекст включены определение субъекта, моделирование, цели, описания модели.

Необходимо отметить, что методологии функционального моделирования позволяют охватить весь жизненный цикл разрабатываемого электронного образовательного ресурса. Использование методологии схематично изображено на рисунке 1 (см. рис. 1).

Первоначально разрабатывается функциональная модель, с помощью функциональной модели производится анализ и определяются требования к структуре функций и составу системы, т.е. определяется цель системы, ее функции. На этой же модели указываются исходная информация, промежуточные и итоговые результаты работы системы.

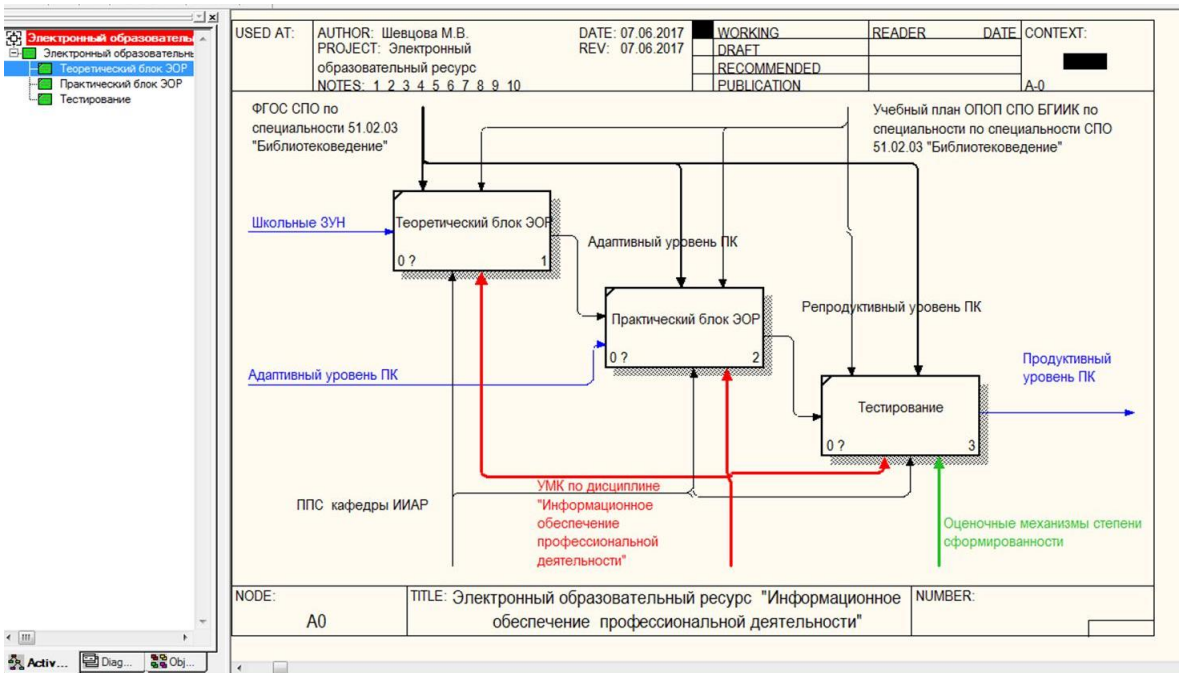


Рис. 2. Декомпозиция функциональной модели.

Затем мы провели декомпозицию модели 1 уровня. Декомпозиционный уровень модели 1 уровня применяется для того, чтобы дать более детальную описательную характеристику блоков. Каждый из них также может быть декомпозированным. После каждой декомпозиции создается новая диаграмма.

Методология функционального моделирования – мощный инструмент моделирования, который применяется для анализа, документирования и унифицирования сложных процессов. Модель, созданная с помощью методологии структурного анализа и проектирования, позволяет безошибочно документировать различные аспекты деятельности – работу, действия, которые необходимо предпринять, методы для их реализации, ресурсы для их обеспечения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Роберт И.В. Современные информационные технологии в образовании. – М.: Школа-Пресс. 1994. – 141 с.

2. Воройский Ф.С. Разработка средств организационно-технологического обеспечения АБИС // Научные и технические библиотеки. 2001. № 9. С. 71-86.

МИРОВОЗЗРЕНЧЕСКОЕ ВЛИЯНИЕ СОЦИАЛЬНОЙ ИНФОРМАЦИИ НА ФОРМИРОВАНИЕ ЛИЧНОСТИ КУРСАНТОВ

THE IDEOLOGICAL INFLUENCE OF SOCIAL INFORMATION ON THE FORMATION OF PERSONALITY OF CADETS

Остапенко Владимир Савельевич
(Центральный филиал Российского государственного университета правосудия);
Дудкин Юрий Андреевич
(Воронежский институт МВД России);
Хоменко Андрей Анатольевич
(Воронежский институт ФСИН России)

Ostapenko Vladimir Savel'evich
(Central Department of Russian state University of justice);
Dudkin Yuri Andreevich
(Voronezh Institute of the MIA of Russia);
Khomenko Andrey Anatolyevich
(Voronezh Institute of the FPS of Russia)

Аннотация: в статье рассматривается актуальная проблема мировоззренческого влияния социальной информации, объемы которой постоянно возрастают, на формирование личности курсантов ведомственных вузов.

Ключевые слова: мировоззрение, социальная информация, личность, процесс формирования, курсанты.

Annotation: the article considers the actual problem of the ideological influence of social information, the volume of which is constantly increasing, and the formation of personality of cadets of departmental institutions of law enforcement agencies.

Key words: world: worldview, social information, personality, process of formation, the cadets.

Социальная информация касается прежде всего отношений людей, их взаимодействия, формирования взглядов, ценностей и в этом аспекте всегда выполняет мировоззренческую функцию. Важная роль социальной информации в обществе связана в первую очередь с формированием личности. Без нее становление и развитие индивидуума в условиях демократического общества невозможно, и влияние информационных потоков на личность постоянно возрастает [4].

Социальная информация – это информационные потоки в обществе, которые формируют мировоззрение человека, выражающее взгляды и убеждения на законность, права и свободы человека, демократию, основополагающие ценности – государственность, гражданственность, патриотизм. Управление социальной информацией можно рассматривать как определенную деятельность, совершаемую субъектами управления вуза (начальники, воспитатели, преподаватели) по отношению к объекту управления (курсанты, учебные группы, курсы, факультеты), с тем, чтобы обеспечить его движение к заданной цели – формирование мировоззренчески зрелой личности. Необходимым признаком управления социальной информацией является регулирование ее потоков в вузе с целью отбора позитивной и блокирования негативной для формирования личности курсанта. В то же время социальная информация как система имеет свойства и самоорганизации, основанной на принципах синергетики, что свидетельствует о сложности и неоднозначности рассматриваемого явления [5]. Применительно к образовательным организациям силовых ведомств социальная информация активно воздействует на курсантов и нуждается в определенной подаче в вузе с целью формирования мировоззрения личности обучающихся.

Важным принципом управления информационными потоками в вузе является обратная связь, т.е. получение субъектом управления информации о сформированности мировоззренческих взглядов и убеждений курсантов, морально-психологическом состоянии, отклонениях в их формировании. Субъекты управления (начальники, командиры, преподаватели) перерабатывают обратную информацию в решения, команды, передают их объекту управления (курсантам), корректируя сам процесс. Объект управления реагирует не на любую информацию, а избирательно лишь на ту, которая соответствует природе объекта и необходима для управления в определенное время и в определенных условиях [1].

Процесс управления начинается с получения и обработки исходной социальной информации. Она используется для разработки стратегии управления (перспективных целей и задач), выбора управленческих решений, организации их выполнения, регулирования и контроля, оценки результатов. Высшей целью управления всякой системой является оптимизация функционирования системы, достижение возможно большего полезного эффекта при наименьших усилиях и затратах. Сбор и переработка ценной и надежной социальной информации, ее эффективное использование, блокирование ненужной и вредной информации обеспечивают эффективное, оптимальное управление процессом формирования личности курсанта в вузе [6].

Важно знать и умело использовать основные принципы управления социальной информацией в вузе: демократизм, позволяющий сочетать единоначалие с широкой демократией, использованием инициативы курсантов; научность, объективность и конкретность, требующие учета в управлении объективных закономерностей и их специфического проявления в конкретных условиях вуза; основное звено, предполагающее выбрать из множества задач основную, решение которой позволяет решить комплекс вопросов мировоззренческого обучения и воспитания и др. [2].

Отсутствие или недостаток объективной социальной информации может приводить к субъективизму, необоснованным решениям и действиям, противоречащим формированию мировоззренческих взглядов, убеждений курсантов. Также данный процесс зависит от подготовленности субъекта и объекта управления к использованию социальной информации в специфических условиях ведомственных вузов силовых ведомств. Научность, достоверность и убедительность, полнота и точность, ценность и новизна, оперативность и актуальность - таковы основные требования к социальной информации, используемой в процессе формирования мировоззрения курсантов [3].

Управленческая функция социальной информации неразрывно связана с коммуникативной, т.е. с обеспечением связей и общения командиров, начальников, преподавателей с курсантами в процессе их взаимной деятельности, что способствует усвоению мировоззренчески значимой информации. Суть коммуникативной переработки социальной информации заключается в разъяснении курсантам целей, задач предстоящей профессиональной деятельности, во взаимообмене информацией, ее обсуждении, уточнении и конкретизации, усвоении ее курсантами (с учетом их потребностей и интересов) как руководства к действию.

С управленческой и коммуникативной функциями связана учебно-воспитательная функция социальной информации, непосредственно обеспечивающая формирование мировоззрения курсантов. Она возникает в процессе целенаправленного овладения знаниями, навыками, умениями в процессе мировоззренчески ориентированного обучения и воспитания. Эта функция социальной информации взаимосвязана и с научной работой курсантов. Научная деятельность предполагает использование накопленной научной информации как компонента социальной информации и получение новой научной информации, удовлетворяющей различные потребности курсантов. Новая научная информация включается в систему научных и иных социальных коммуникаций.

Социальная информация – явление неоднозначное, оказывающее как положительное, так и отрицательное воздействие на личность. Развитие информационной среды создает предпосылки для повышения культурного и образовательного уровня курсантов, однако одновременно с этим возможно увеличение числа обучающихся, имеющих компьютерную зависимость, отрицательно влияющую на качество образования и культуры. Поэтому, как отмечает В.И. Ярочкин, «создание системы информационной безопасности – явление не одноразовое – это систематическая, целенаправленная работа, включающая в себя как правовые, так и организационные вопросы и их своевременное обеспечение» [8, с. 12-13].

Особо следует сказать о негативном воздействии социальной информации на личность курсанта. Обеспечение информационной безопасности личности означает ее право на получение объективной информации и предполагает, что полученная человеком из различных источников информация не препятствует свободному формированию и развитию мировоззрения курсанта.

В качестве негативного воздействия на личность курсанта могут выступать:

- целенаправленное информационное давление с целью изменения мировоззрения, политических взглядов и морально-психологического состояния курсантов;

- скрытое распространение недостоверной, искаженной, неполной информации;

- умышленное использование дезинформации в различных сферах с целью сформировать необходимые для источника такой информации мировоззренческие характеристики личности (ненависть, страх, агрессивность и т.п.).

Информационные воздействия опасны или полезны не столько сами по себе, сколько тем, что управляют мощными вещественно-энергетическими процессами человека и общества. Суть социальной информации как раз и заключается в ее способности контролировать вещественно-энергетические процессы, параметры которых на много порядков выше самой информации. Учеными установлено, что пользователи в псевдореальном мире гораздо в большей степени, чем в мире обычном, реальном, подвержены внушению и гипнозу. Запрограммировать игровую программу на ту или иную установку не представляет труда. Виртуальную систему можно заразить вирусом, который будет кодировать определенные слова, что позволит в дальнейшем осуществлять зомбирование человека. Сегодня учеными ставится вопрос о необходимости развития информационной экологии, формирующей здоровый информационный образ жизни людей в социальной и природной среде. Соблюдение правил информационной гигиены приводит к сознательно избранному информационному образу жизни, способствующему повышению его качества. Необходимость подобных исследований продиктована тем, что у разных людей и у различных социальных групп проявляется самая разнообразная мировоззренческая устойчивость к процессам информатизации, что может выражаться в следующем:

- страх человека перед стремительно совершенствующейся информационной техникой, ростом и усложнением информационных потоков (компьютерофобия);

- компьютерная зависимость как болезнь человека, отдающего приоритет общению с ЭВМ, а не с людьми. Существует такой термин, как киберболезнь, которой подвержены люди, часто находящиеся в виртуальной реальности;

- психическая незащищенность и утомляемость людей при работе на компьютере и т.д.

Все это предполагает создавать соответствующие рекомендации для разработчиков ЭВМ, специалистов по эргономике, а также пользователей компьютерной техники, в которых будут отражены мировоззренческие и социально-психологические аспекты информатизации, что необходимо учитывать и в образовательном процессе вузов. В социальном отношении очень важна практическая реализация уже имеющихся нормативных положений, направленных на защиту обучающихся, постоянно использующих в своей работе компьютерную технику (например, санитарные требования к расстоянию между компьютером и обучающимся, о количестве квадратных метров, необходимых для организации каждого рабочего места, на котором применяется компьютерная техника и т.п.) [7].

В условиях развертывания информатизации каждое из диалектически взаимосвязанных начал человека (физическое, психическое и социальное) требует специального учета, так как только в этом случает новые возможности информационного общества могут быть в полной мере использованы для всестороннего мировоззренческого развития личности. Пренебрежение спецификой этих начал личности, стихийная информатизация чреваты трудно прогнозируемыми отрицательными последствиями для человека и общества. «Информационная среда, – подчеркивает Ю.Н. Тарасов, – являясь систематизирующим фактором деятельности всех сфер жизни общества активно влияет на данные сферы и в то же время является самостоятельной сферой, требующей защиты с целью дальнейшего развития» [9, с. 35]. На это и направлены усилия государственных структур, в том числе и силовых, призванные обеспечить информационную безопасность общества и личности [10].

Таким образом, в условиях стремительного совершенствования информационных технологий и неконтролируемого развития предоставляемых ими возможностей одним из самых актуальных продолжает оставаться вопрос о формировании целевых жизненных установок курсантов в вузах под воздействием социальной информации. И в этом аспекте социальная информация выполняет важнейшую функцию – мировоззренческую, формирует социально необходимые для личности курсанта мировоззренческие взгляды, ценности, убеждения, идеалы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ракитов А.И. Философия компьютерной революции. – М., 1991. – 234 с.

2. Урсул А.Д. Информатизация общества и переход к устойчивому развитию цивилизации // Вестник РОИВТ. 1993. № 1-3. С. 35-45.

3. Кастелье М. Информационная эпоха: экономика, общество, культура. – М., 2001. – 321 с.

4. Романова Ю.Д. Информатика и информационные технологии: учебное пособие. – М.: Экспо, 2006. – 221 с.
5. Чернавский В.С. Синергетика и информация. – М., 2002. – 334 с.
6. Мелюхин И.С. Информационное общество: истоки, тенденции, проблемы развития. – М., 1999. – 217 с.
7. Соколов А.В. Эволюция социальных коммуникаций. – СПб, 1995. – 154 с.
8. Ярочкин В.И. Информационная безопасность: учебник. – М., 2000. – 233 с.
9. Тарасов Ю.Н. Философские проблемы информатики: учебное пособие. – Воронеж, 2007. – 315 с.
10. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. 29 июля.

СВЕДЕНИЯ ОБ АВТОРАХ

1. Акапьев В.Л., доцент кафедры ИКТД ОВД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат педагогических наук.
2. Алдиаб А., преподаватель факультета агрономии сельского хозяйства Университета Дамаска.
3. Александров А.Н., начальник кафедры обеспечения безопасности на объектах транспорта Белгородского юридического института МВД России имени И.Д. Путилина, кандидат юридических наук, доцент.
4. Александров Е.Н., специалист по технологиям автоматизации ООО «Парусник-Белгород».
5. Безуглый Э.А., доцент кафедры управления и административной деятельности Белгородского юридического института МВД России имени И.Д. Путилина, кандидат экономических наук.
6. Богданов Д.С., курсант Краснодарского университета МВД России.
7. Глушков Е.Л., старший преподаватель кафедры ОРД Белгородского юридического института МВД России имени И.Д. Путилина.
8. Горев А.И., доцент кафедры управления и информационных технологий в деятельности ОВД Омской академии МВД России, кандидат юридических наук, доцент.
9. Горева Е.Г., старший преподаватель кафедры управления и информационных технологий в деятельности ОВД Омской академии МВД России, кандидат физико-математических наук.
10. Гуржий А.А., преподаватель кафедры ИКТД ОВД Белгородского юридического института МВД России имени И.Д. Путилина.
11. Дрога А.А., заместитель начальника кафедры ИКТД ОВД Белгородского юридического института МВД России имени И.Д. Путилина.
12. Дудкин Ю.А., преподаватель кафедры тактико-специальной подготовки Воронежского института МВД России.
13. Дунаев Р.А., доцент кафедры информатики и информационно-аналитических ресурсов Белгородского государственного института искусств и культуры, кандидат философских наук.
14. Душкин А.В., начальник кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России, доктор технических наук, доцент.
15. Жукова Н.А., заведующая кафедрой судебной экспертизы и криминалистики Юридического института Белгородского государственного национального исследовательского университета, кандидат юридических наук, доцент.
16. Жукова П.Н., профессор кафедры ИКТД ОВД Белгородского юридического института МВД России имени И.Д. Путилина, доктор физико-математических наук, доцент.
17. Земляченко В.В., доцент кафедры организации и технологии защиты информации Белгородского университета кооперации, экономики и права, кандидат технических наук, доцент.

18. Иванов И.П., доцент кафедры информатики и математики Краснодарского университета МВД России, кандидат педагогических наук, доцент.

19. Иванов С.В., адъюнкт кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России.

20. Исаев О.В., преподаватель кафедры технических комплексов охраны и связи Воронежского института ФСИН России, кандидат технических наук.

21. Капуста М.В., преподаватель кафедры информатики и информационно-аналитических ресурсов Белгородского государственного института искусств и культуры.

22. Карагодина А.А., курсант Белгородского юридического института МВД России имени И.Д. Путилина.

23. Карпика А.Г., доцент кафедры информационного обеспечения ОВД Ростовского юридического института МВД России, кандидат технических наук, доцент.

24. Кассим К.Д., доцент Курской государственной сельскохозяйственной академии имени И.И. Иванова, кандидат технических наук, доцент (Йемен).

25. Кирюшин И.И., преподаватель кафедры информатики и специальной техники Барнаульского юридического института МВД России.

26. Коваленко Д.Н., курсант Барнаульского юридического института МВД России.

27. Козиоров Е.Л., генеральный директор ООО «Инфологика ЛТД», кандидат технических наук.

28. Колтунов Н.Л., заместитель начальника отдела информационно-технического обеспечения учебного процесса Белгородского юридического института МВД России имени И.Д. Путилина.

29. Колтунова Т.В., специалист по учебно-методической работе I категории отдела методической работы управления образовательной политики НИУ «БелГУ».

30. Корень А.И., курсант института психологии служебной деятельности Московского университета МВД России имени В.Я. Кикотя.

31. Кочедыков С.С., профессор кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России, кандидат технических наук, доцент.

32. Кочеткова Н.Д., доцент кафедры административного права и административной деятельности ОВД Орловского юридического института имени В.В. Лукьянова, кандидат юридических наук.

33. Кривоухов А.А., доцент кафедры гуманитарных дисциплин Курской государственной сельскохозяйственной академии имени И.И. Иванова, кандидат юридических наук, доцент.

34. Кузовлев В.Ю., старший преподаватель кафедры технико-криминалистического обеспечения экспертных исследований учебно-научного комплекса судебной экспертизы Московского университета МВД России имени В.Я. Кикотя.

35. Лемайкина С.В., преподаватель кафедры информационного обеспечения ОВД Ростовского юридического института МВД России.

36. Линьков В.В., старший преподаватель кафедры информационных технологий в деятельности ОВД Орловского юридического института имени В.В. Лукьянова, кандидат технических наук.

37. Лютынский А.М., доцент Северо-западного института (филиала) Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, доцент.

38. Макото К., представитель фабрики AVC Networks Company, Panasonic Corporation в России (Япония).

39. Матросова Л.Д., начальник кафедры информационных технологий в деятельности ОВД Орловского юридического института имени В.В. Лукьянова, кандидат юридических наук.

40. Михайленко Е.В., заместитель начальника кафедры информатики и математики Краснодарского университета МВД России, кандидат физико-математических наук, доцент.

41. Михайликов В.Л., начальник кафедры ТСП Белгородского юридического института МВД России имени И.Д. Путилина, кандидат юридических наук, доцент.

42. Молбасин С.И., научный сотрудник научно-исследовательского института Карагандинской академии МВД Республики Казахстан имени Баримбека Бейсенова, магистр юридических наук.

43. Мухачев С.В., начальник кафедры информационного обеспечения органов внутренних дел Уральского юридического института МВД России, кандидат физико-математических наук, доцент.

44. Наджаджра М.Х., заведующий кафедрой управления информационных систем, Университет Аль-Истикляль, г. Иерихон, Палестина, доктор наук.

45. Насонова В.А., профессор кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат физико-математических наук, доцент.

46. Немыкин Н.И., директор БВШ ИК-5 ФСИН России.

47. Немыкина Н.В., доцент Белгородского института развития образования, кандидат педагогических наук.

48. Остапенко В.С., профессор кафедры гуманитарных и социально-экономических дисциплин Центрального филиала Российского государственного университета правосудия, доктор педагогических наук, профессор.

49. Перепелкин И.Н., доцент кафедры информатики и информационно-аналитических ресурсов Белгородского государственного института искусств и культуры, кандидат физико-математических наук.

50. Петрищева Е.Н., преподаватель кафедры информационного обеспечения ОВД Ростовского юридического института МВД России.

51. Петрякова С.В., преподаватель кафедры информатики и математики Волгоградской академии МВД России.

52. Печенкова Е.А., преподаватель кафедры психологии учебно-научного комплекса психологии служебной деятельности Московского университета МВД России имени В.Я. Кикотя.

53. Прокопенко А.Н. начальник кафедры ИКТД ОВД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат технических наук, доцент.

54. Пузикова И.Ю., курсант Орловского юридического института имени В.В. Лукьянова.

55. Росоха А.Ю., студентка Белгородского государственного национального исследовательского университета.

56. Савотченко С.Е., профессор кафедры ИКТД ОВД Белгородского юридического института МВД России имени И.Д. Путилина, доктор физико-математических наук, профессор.

57. Савченко О.А., аспирант кафедры уголовно-процессуального права и криминалистики Всероссийского государственного университета юстиции.

58. Самсонов В.Н., профессор кафедры административно-правовых дисциплин Белгородского юридического института МВД России имени И.Д. Путилина, доктор юридических наук, профессор.

59. Свистильников А.Б., профессор кафедры ОРД Белгородского юридического института МВД России имени И.Д. Путилина, кандидат юридических наук, доцент.

60. Семенов Е.Ю., старший преподаватель кафедры информационных технологий в деятельности ОВД Орловского юридического института имени В.В. Лукьянова, кандидат юридических наук.

61. Сергеева А.Ю., преподаватель кафедры издательского дела и библиотековедения Белгородского государственного института искусств и культуры.

62. Смоленцева Т.Е., преподаватель кафедры информатики Липецкого государственного технического университета, кандидат технических наук, доцент.

63. Сумин В.И., профессор кафедры информационной безопасности телекоммуникационных систем Воронежского института ФСИН России, доктор технических наук, профессор.

64. Тимакина Ю.А., доцент кафедры информационного обеспечения ОВД Ростовского юридического института МВД России, кандидат экономических наук.

65. Тримасов Е.А., начальник отдела информационно-технического обеспечения учебного процесса Белгородского юридического института МВД России имени И.Д. Путилина.

66. Трущенков И.В., преподаватель кафедры технико-криминалистического обеспечения экспертных исследований учебно-научного комплекса судебной экспертизы Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук.

67. Ходякова Н.В., начальник кафедры информатики и математики Волгоградской академии МВД России, доктор педагогических наук, доцент.

68. Хоменко А.А., преподаватель кафедры физической и огневой подготовки Воронежского института ФСИН России.

69. Хромых А.А., старший преподаватель кафедры информатики и математики Краснодарского университета МВД России, кандидат физико-математических наук.

70. Черкесова К.И., ассистент кафедры информатики и информационно-аналитических ресурсов Белгородского государственного института искусств и культуры.

71. Чернышёв С.А., заместитель начальника кафедры криминалистики Белгородского юридического института МВД России имени И.Д. Путилина, кандидат социологических наук, доцент.

72. Чиненов А.В., преподаватель кафедры ОРД Белгородского юридического института МВД России имени И.Д. Путилина.

73. Чиненов Е.В., начальник кафедры криминалистики Белгородского юридического института МВД России имени И.Д. Путилина, кандидат экономических наук, доцент.

74. Чудин Д.А., курсант Уральского юридического института МВД России.

75. Шапошников В.Л., заместитель начальника кафедры управления и административной деятельности Белгородского юридического института МВД России имени И.Д. Путилина, кандидат юридических наук, доцент.

76. Шумский В.В., старший преподаватель кафедры управления и административной деятельности Белгородского юридического института МВД России имени И.Д. Путилина.

СОДЕРЖАНИЕ

СЕКЦИЯ № 1.
ТЕОРЕТИЧЕСКИЕ, ОРГАНИЗАЦИОННЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И ПРАВОВЫЕ ПРОБЛЕМЫ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Жукова П.Н., Прокопенко А.Н., Гуржий А.А.	Использование информационных технологий в системе ведомственного образования на современном этапе (на примере Бел ЮИ МВД России имени И.Д. Путилина)…….	**3**
Молбасин С.И.	Правовые интернет-ресурсы Республики Казахстан и их роль в построении правового государства ……..	**12**
Акапьев В.Л., Дрога А.А., Савотченко С.Е.	Развитие информационных ресурсов МВД России …….....	**19**
Печенкова Е.А., Корень А.И.	Обеспечение информирования в образовательных организациях системы МВД России …….	**24**
Савотченко С.Е., Наджаджра М.Х.Н.	Возможности применения информационных систем анализа и моделирования в правоохранительной деятельности…….	**27**
Кирюшин И.И., Коваленко Д.Н.	Использование беспилотных летательных аппаратов в деятельности государственной инспекции безопасности дорожного движения …	**31**
Тимакина Ю.А.	Применение Web-расширения для доступа к функциональным интерфейсам информационных систем ……..	**35**
Тримасов Е.А., Колтунов Н.Л., Колтунова Т.В.	Опыт внедрения и эксплуатации систем электронного документооборота в ведомственных образовательных организациях (на примере Бел ЮИ МВД России имени И.Д. Путилина) ….	**40**
Семенов Е.Ю., Пузикова И.Ю.	Возможности использования социальных сетей сотрудниками правоохранительных органов …..	**46**

Кочеткова Н.Д. Информатизация миграционной системы России – важнейшая составляющая миграционного учета ... **50**

Линьков В.В. Вопросы развития электронного правительства в Российской Федерации …… **55**

Матросова Л.Д. К вопросу совершенствования управления информационно-технического обеспечения деятельности Госавтоинспекции с целью повышения эффективности безопасности дорожного движения ……. **57**

Росоха А.Ю. Особенности проведения видеотехнической экспертизы ……... **62**

СЕКЦИЯ № 2.
ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сумин В.И., Исаев О.В., Душкин А.В., Кочедыков С.С., Иванов С.В. Описание дуального подхода управления охранными организациями …… **66**

Кочедыков С.С., Душкин А.В., Сумин В.И., Иванов С.В. Разработка динамических моделей процессов принятия диагностических решений о работо-способности программных компонентов автоматизированных управляющих систем критического назначения …….. **74**

Сумин В.И., Смоленцева Т.Е. Анализ оценки управляющих воздействий на основе алгоритма динамики характеристик объектов управления …….. **80**

Кривоухов А.А. К вопросу о правовых средствах противостояния угрозам информационно-коммуникационной среды …… **84**

Земляченко В.В. Вопросы повышения эффективности обеспечения защиты правопорядка с помощью системы-112 … **88**

Карпика А.Г.,
Лемайкина С.В.,
Петрищева Е.Н.
Проблемы компьютерной преступности в России …… **93**

Глушков Е.Л.,
Свистильников А.Б.
Мошеннические действия в сфере информационно-компьютерных технологий …… **97**

Самсонов В.Н.,
Карагодина А.А.
Использование систем видеонаблюдения в раскрытии и расследовании преступлений ….. **101**

Безуглый Э.А.,
Шапошников В.Л.,
Шумский В.В.
Информационная безопасность государства: понятие, угрозы и факторы …… **107**

Александров А.Н.,
Александров Е.Н.
Анализ современных технологий в системе обеспечения информационной безопасности на железнодорожном транспорте ……. **112**

Чиненов Е.В.,
Чиненов А.В.,
Чернышёв С.А.
Использование специальных судебно-агротехнических и зоотехнических знаний в расследовании преступлений в сфере агропромышленного комплекса …… **120**

СЕКЦИЯ № 3.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ, КРИМИНАЛИСТИКЕ, БОРЬБЕ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ

Трущенков И.В.,
Кузовлев В.Ю.
Использование современных технических средств виртуальной реальности для решения задач судебной фотографии и видеозаписи……. **129**

Горев А.И.,
Горева Е.Г.
О некоторых проблемах получения и использования электронной информации в судопроизводстве ……. **132**

Кузовлев В.Ю.
Использование АИПС «АИПСИН-антинаркотики» в экспертно-криминалистической деятельности органов внутренних дел при производстве экспертиз «дизайнерских» наркотиков …….. **138**

Лютынский А.М. К проблеме сущности электронной информации, используемой в уголовно-процессуальном доказывании …… **143**

Савченко О.А. Криминалистически значимые признаки способа совершения кражи с использованием информационных технологий ……... **147**

Хромых А.А., Богданов Д.С. Особенности блочного шифрования посредством сети Фейстеля …….. **151**

Жукова П.Н., Жукова Н.А., Насонова В.А. Методы обнаружения цифровой информации в ходе расследования преступлений ……. **157**

Насонова В.А., Кассим К.Д.А., Алдиаб А. Исследования платежных карт при проведении экспертиз …….. **161**

СЕКЦИЯ № 4.
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ

Мухачев С.В., Чудин Д.А. О возможностях использования электронного учебного пособия «Основы информационной безопасности в органах внутренних дел» в образовательном процессе ……. **166**

Ходякова Н.В. Проблемы подготовки сотрудников ОВД к применению информационных технологий в профессиональной деятельности и пути их решения …… **169**

Перепелкин И.Н., Дунаев Р.А. Использование информационно-коммуникационных технологий в высшем образовании …….. **173**

Петрякова С.В. Проблемы и противоречия личностно-развивающего электронного обучения ……. **176**

Черкесова К.И. О необходимости внедрения виртуальной образовательной среды в деятельность образовательной организации ……... **180**

Михайликов В.Л., Гуржий А.А., Дрога А.А. Классификация облачных сервисов ……. **184**

Макото Курита, Козиоров Е.Л., Акапьев В.Л. Интерактивные средства решения образовательных и управленческих задач ……. **190**

Немыкин Н.И., Немыкина Н.В., Акапьев В.Л. Особенности формирования единого информационного пространства образовательного учреждения ФСИН России …… **196**

Иванов И.П. Процесс приведения информационной модели организационной системы к иерархической структуре ……..…… **206**

Михайленко Е.В. О разработке программных приложений для выполнения практических заданий по разделу «Методы оптимизации» дисциплины «Прикладная математика» ……. **210**

Капуста М.В., Сергеева А.Ю. Моделирование процесса формирования информационно-технологической компетенции будущих библиотекарей средствами электронного образовательного ресурса …….. **223**

Остапенко В.С., Дудкин Ю.А., Хоменко А.А. Мировоззренческое влияние социальной информации на формирование личности курсантов.. **226**

Сведения об авторах ……... **232**

НАУЧНОЕ ИЗДАНИЕ

Проблемы информационного обеспечения деятельности правоохранительных органов

Сборник статей 4-й Международной научно-практической конференции
13 октября 2017 года

Редактор ***Ю.Н. Удалова***
Комп. верстка ***И.Ю. Чернышева***

Подписано в печать 2018 г., 15,13 уч.-изд. л. бумага офсетная,
печать трафаретная.
Тираж 30 экз. Заказ № 23

Отпечатано в отделении полиграфической и оперативной печати
Белгородского юридического института МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-224-1

9 785917 762241