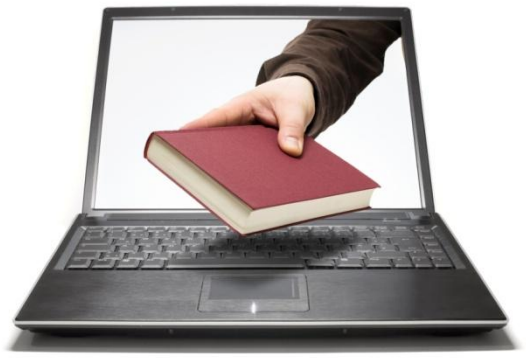
БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ ИМЕНИ И.Д. ПУТИЛИНА

ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Сборник статей
7-й Всероссийской научно-практической конференции

22 мая 2020 года



Белгород
Белгородский юридический институт МВД России
имени И.Д. Путилина
2020

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 7-й Всероссийской научно-практической конференции (22 мая 2020 г.). – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2020. – 225 с.

ISBN 978-5-91776-346-0

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 978-5-91776-346-0

УДК 004.4

ОБ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ БЕЛГОРОДСКОГО ЮРИДИЧЕСКОГО ИНСТИТУТА МВД РОССИИ ИМЕНИ И.Д. ПУТИЛИНА

Прокопенко А.Н.,
кандидат технических наук, доцент;
Тримасов Е.А.;
Гуржий А.А.;
Федосеев А.Э.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье проводится анализ информационного обеспечения образовательного процесса Белгородского юридического института Министерства внутренних дел Российской Федерации имени И.Д. Путилина.

Ключевые слова: информационные ресурсы, системы, образовательный процесс, информационные технологии.

ON THE EFFECTIVENESS OF USING INFORMATION RESOURCES IN THE EDUCATIONAL PROCESS OF THE PUTILIN BELGOROD LAW INSTITUTE OF MINISTRY OF THE INTERIOR OF RUSSIA

Prokopenko A.N.,
Candidate of Technical Sciences, Associate Professor;
Trimasov E.A.;
Gurzhiy A.A.;
Fedoseev A.E.
(Putilin Belgorod Law Institute of the MIA of Russia)

Abstract: the information support of the educational process of the Putilin Belgorod Law Institute of MIA of Russia has been analyzed.

Keywords: information resources, systems, educational process, information technologies.

В Белгородском юридическом институте МВД России имени И.Д. Путилина используется 59 автоматизированных информационных систем. Все эти системы можно разделить на десять групп:

1. Правовые информационные ресурсы.
2. Ресурсы научно-исследовательской и редакционно-издательской деятельности института.

3. Информационно-библиотечные ресурсы.
4. Образовательные информационные ресурсы.
5. Системы видео-конференц-связи.
6. Справочные информационные системы, автоматизация ведения делопроизводства и организации работы по контролю за исполнением поручений в институте.
7. Кадровые информационные ресурсы.
8. Материально-технические информационные ресурсы.
9. Финансово-хозяйственные информационные ресурсы.
10. Информационные ресурсы обеспечения безопасности.

Рассмотрим эффективность использования некоторых наиболее используемых профессорско-преподавательским составом информационных систем.

1. *Справочно-правовая система «КонсультантПлюс»* активно используется не только в образовательном процессе при подготовке курсантов и слушателей, но и в профессиональной деятельности сотрудников постоянного состава. Ввиду того, что в классах отсутствует доступ к сети Интернет, интернет-версия данного программного продукта не доступна для изучения. Кроме того, в институте запрещено использование мобильных телефонов, следовательно, и использование мобильной версии приложения «КонсультантПлюс» тоже не доступно для обучающихся института. СПС «КонсультантПлюс» в институте используется в двух вариантах: внутреннем и учебном, которые отличаются по имеющимся в них базам. Использование обоих вариантов позволяет ознакомиться с международными правовыми актами, комментариями законодательства, проектами нормативных актов, нормативными актами Белгородского региона. Это позволяет более эффективно решать учебные и научные задачи, чем при подключении к интернет-версии.

Наличествующая в институте система *СТРАС «Юрист»* позволяет получить доступ ко всем нормативным правовым актам МВД России, кроме ДСП и секретных. Это, в свою очередь, позволяет расширить возможность решения учебных и научных задач обучающимися и научно-педагогическим составом института.

Автоматизированная информационная система института «Локальные нормативные акты» предназначена для размещения приказов, в том числе о привлечении к выполнению служебных обязанностей в выходной день и приказов о назначении суточного наряда. Используется в справочных целях для повседневной работы и достаточно эффективна. Некоторые проблемы вызывает недостаточно функциональный механизм поиска.

2. Созданные *системы научно-исследовательской и редакционно-издательской деятельности института* не решают никаких необходимых задач кафедр и используются только один раз в год при составлении планов, представляются излишними.

Система контроля научно-исследовательской и редакционно-издательской деятельности профессорско-преподавательского состава института (АИС «Мониторинг») практически не используется в повседневной деятельности из-за большого количества излишней информации и не востребо-

ванности самими научно-исследовательским и редакционно-издательским отделами. Для составления научного рейтинга по-прежнему используются бумажные документы, а рейтинг слабо применяется для оценки деятельности педагогов. Требуется полноценное использование в постоянном режиме, что даст объективную картину участия профессорско-преподавательского состава в научной и публикационной деятельности.

Программно-аппаратный комплекс для проверки текстовых документов на наличие заимствований *«Антиплагиат ВУЗ»* представляет из себя интернет-сервис, ориентированный на поиск заимствований в текстах любого характера. Доступ осуществляется только через Интернет, используется как в научных, так и в учебных целях. Недостатком данной системы является отсутствие стабильности в дневное время, а также отсутствие приложения, устанавливаемого на компьютер.

3. Библиотечные ресурсы состоят из привлеченных библиотечных ресурсов и библиотечных информационных ресурсов института.

Библиотечные информационные ресурсы института включают электронный библиотечный каталог и электронные библиотечные ресурсы изданий института. Указанные ресурсы работают эффективно, как и алгоритмы поиска. Недостатком библиотечных информационных ресурсов института является их малый объем. Представляется целесообразным размещение в указанных базах не только изданий института, но и в рамках информационного обмена изданий других образовательных и научных организаций МВД России. Это значительно повысит их эффективность и значимость.

Электронно-библиотечная система ZNANIUM.COM является специализированной электронной библиотекой, которая декларирует возможность обеспечить курсантов, слушателей и преподавателей электронными учебниками, пособиями, электронными версиями научных изданий и энциклопедий. В данной системе представлены издания учебников, учебных пособий, монографий, сборников научных трудов, энциклопедий, справочников, законодательно-нормативных документов. Однако использование данной системы подразумевает доступ к сети Интернет и наличие логинов и паролей для доступа, что ограничивает её использование в компьютерных классах института. Соответственно, знакомиться с изданиями можно только в самой системе, не выходя из помещения библиотеки, на компьютерах которой установлен доступ к системе. Основная проблема данной системы состоит в том, что в ней, как правило, для скачивания доступно не более 10% текста указанных выше изданий. Это обуславливает ее малое использование и, соответственно, низкую эффективность. Преподаватели и обучающиеся предпочитают скачать одну книгу по теме, но полную, вместо 50 книг, но по 10% от каждой.

Научная электронная библиотека eLIBRARY.RU обеспечивает легитимный доступ заинтересованных пользователей к объектам интеллектуальной собственности, выраженным в цифровой форме. Данная система позволяет получить доступ к различным материалам научных журналов. Система доступна только из сети Интернет. Недостатком eLIBRARY.RU является фактическое

отсутствие текстов работ, за исключением научных статей. В системе крайне редко размещаются учебники, монографии и учебные пособия.

4. Образовательные информационные ресурсы включают в себя несколько составляющих, предназначенных как для обучающихся, так и для профессорско-преподавательского состава.

Электронная информационно-образовательная среда института в локальной вычислительной сети и сети Интернет на базе программного обеспечения «Moodle» (ЭИОС Бел ЮИ МВД России имени И.Д. Путилина) обеспечивает размещение электронных учебных материалов для обучающихся. Программный комплекс даёт возможность преподавателям размещать для обучающихся материалы как в текстовом формате, так и в графическом, видео- и аудиофайлы, тестовые задания и презентации. В системе имеется наличие обратной связи с преподавателем через встроенный чат. Доступ к ресурсу обеспечен как и из сети Интернет, так и из локальной сети института. Недостатком системы является отсутствие возможности работы в системе при нарушении работы сети. С точки зрения преподавателя недостатками являются:

– отображение всех учебных дисциплин, в том числе тех, которые этому преподавателю не доступны;

– отображение всех обучающихся по специализации с 1-го по 5-й курс, что в процессе анализа успеваемости обучающихся требует большого количества лишней работы. Представляется целесообразным размещать учебные материалы не по специальностям и специализациям, как это удобно проверяющим, а по факультетам и курсам, как это будет удобно всем участникам образовательного процесса;

– отображение избыточной информации при настройке тестов и вопросов к ним, сложное создание тестовых материалов, проблемы в использовании вопросов, созданных для одного теста в другом (при обычном доступе педагога невозможно, позволено только администратору);

– очень сложная система копирования материалов из одного курса в другой, в результате которой копирование фактически не применяется педагогическим составом.

Указанные недостатки ЭИОС, активно проявившиеся в условиях дистанционной работы, увеличивают время, необходимое для создания учебных курсов преподавателем, а также для проверки успеваемости не менее чем в два раза. Требует обязательной доработки.

Программное обеспечение для создания и подготовки тестов MyTestX позволяет эффективно проводить тестирование в компьютерных классах института. Достоинством системы является простота в использовании, интуитивно понятный интерфейс программы, возможность тестирования обучаемых как с использованием локальной сети института, так и на отдельном персональном компьютере без доступа к сети, возможность активации тестирования по таймеру. Недостатком программы является необходимость обращения в ОИТО УП для размещения сетевых тестовых материалов с последующим оформлением документов для их размещения.

Электронная база института «Выпускные квалификационные работы» обеспечивает полнотекстовый просмотр квалификационных работ выпускников, что обеспечивает наглядный пример в подготовке работ для будущих выпускников института. К преимуществам системы можно отнести доступ через локальную сеть института.

Информационно-аналитическая система института «Электронный журнал». Применяется для внесения оценок в электронном виде. Достоинством системы является дублирование оценок журнала, что даёт возможность ознакомиться с оценками в электронном виде. Электронный журнал предоставляет подробную статистическую информацию об образовательном процессе. Рассчитывается средний балл за любой период как по отдельному курсанту, так и по взводу и факультету. Рассчитывается нагрузка по преподавателям. К недостаткам можно отнести отсутствие «горячих клавиш». Интуитивное нажатие клавиши «Enter» на некоторых страницах не даёт никакого результата. При разделении взвода на несколько групп выставить оценки за занятие может только одна группа, которая введёт оценки первой. Также недостатками являются недоработанная система вывода выполненной учебной нагрузки и отсутствие полноценных инструментов анализа успеваемости педагогами (для факультетов доступен полный функционал). Например, нельзя посмотреть успеваемость взвода по учебной дисциплине при проведении занятий разными преподавателями.

5. *Система видео-конференц-связи TrueConf* обеспечивает проведение видеосвязи, видеоконференций, дистанционных лекционных занятий, прием дистанционных зачетов через сеть Интернет. Преимуществом системы является простота в настройке и использовании, возможность отправления текстовых сообщений. Недостатком программного продукта является отсутствие возможности сохранять в системе идентификаторы конференций, отправлять файлы в конференцию или отдельному контакту, отсутствие возможности сохранения переписки чата при выходе из конференции.

Прикладной сервис видео-конференц-связи ИСОД МВД России (СВКС-м). Применяется в сети ИСОД МВД России. Обеспечивает удаленную видеосвязь, проведение дистанционных совещаний и конференций.

6. *Система внутренней телевизионной сети института* информирует сотрудников постоянного и переменного состава о памятных датах и предстоящих мероприятиях, прогнозе погоды, а также используется для трансляции информационных и образовательных видеоматериалов.

Информационный портал института «Информационный вуз» объединяет целый ряд информационных систем и информационных ресурсов и позволяет осуществить простой доступ к ним. Содержит в том числе справочную информацию, удобно организован и работает эффективно. Преимущества: сортировка всех сервисов института по группам. К недостаткам можно отнести отсутствие быстрого поиска нужного сервиса и отсутствие «горячих клавиш».

Информационная система «Телефонный справочник института» обеспечивает оперативный поиск и навигацию по рабочим контактным данным сотрудников и подразделений. Преимуществом данной системы является возмож-

ность поиска сотрудника по начальной части фамилии, имени, а также группировка сотрудников по подразделениям. К недостаткам можно отнести отсутствие фотографий некоторых сотрудников и отсутствие информации о номере его кабинета.

Автоматизированная система «Календарь памятных дат» предназначена для вывода на экран пользователя информации о памятных датах. К преимуществам программы можно отнести возможность поиска по реквизитам, отображение фотографии сотрудника, отображение напоминания на главной странице приложения «Информационный вуз». К недостаткам системы можно отнести отсутствие сортировки записей по подразделениям института.

Информационный портал института «Электронная кафедра» обеспечивает выставление протоколов, планов и прочих служебных материалов кафедры в электронном виде. Достоинством системы является возможность размещения в системе документов в электронной форме, что даёт доступ к ним из любого компьютера, подключенного к локальной сети института. Недостатком системы является отсутствие возможности доступа к информационной системе через сеть Интернет.

Внутренняя электронная почта института на базе Microsoft Outlook. Позволяет обмениваться информацией всем сотрудникам и работникам института. К недостаткам можно отнести неустойчивую работу.

Система электронного документооборота института на базе системы «Дело». Позволяет контролировать выполнение поручений как исполнителям, так и руководителям. Существенно облегчила автоматизацию ведения делопроизводства и контроль за исполнением поручений.

Система электронной почты МВД России используется для обмена информацией с внешними пользователями. Внутри института не используется.

Система электронного документооборота МВД России используется для электронного движения и исполнения документов с внешними пользователями. Внутри института используется только в справочных целях.

Недостатком использования систем электронной почты и систем электронного документооборота в институте является необходимость создания и подписания бумажных документов, что превращает электронный документооборот в фикцию.

Система контроля личного состава «Электронная строевка» предназначена для контроля присутствия сотрудников и работников в институте. Недостатков не выявлено, работает эффективно.

Подводя итог, можно отметить, что обучение с использованием дистанционных образовательных технологий с каждым годом становится всё более популярным. Информатизация образовательного процесса повышает качество образования и создаёт благоприятные условия для обучения. Эффективным инструментом для преподавателя служат автоматизированные информационные сервисы, но стоит иметь в виду, что программные системы должны не только решать поставленные задачи, но и быть простыми в использовании и интуитивно понятными. Только тогда эффективность использования информационных систем будет высокой.

УДК 004.4

ОБЛАЧНЫЕ ХРАНИЛИЩА И БЕЗОПАСНОСТЬ

Иванов В.Ю.,
кандидат технических наук, доцент;
Абдрахманова Л.Р.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассматриваются вопросы безопасности использования «облачных» хранилищ с точки зрения способа размещения информации.

Ключевые слова: облачные хранилища информации, информационная безопасность.

CLOUD STORAGE AND SECURITY

Ivanov V.Yu.,
Candidate of Technical Sciences, Associate Professor;
Abdrakhmanova L.R.
(Kikot Moscow University of the MIA of Russia)

Abstract: the article discusses the security issues of using «cloud» storage in terms of the way information is placed.

Keywords: cloud storage of information, information security.

В настоящий момент персональный компьютер имеется практически в каждой семье. Все это появилось не так давно, но стало неотъемлемой частью нашей жизни. На персональном компьютере пользователи хранят файлы, которые необходимы для учёбы, работы и личного пользования. Никто не готов потерять все свои документы из-за поломки техники.

Также существует еще одна проблема, с которой сталкиваются многие пользователи, – это необходимость в удобной передаче файлов между компьютерами. Привычные для нас способы, такие как флэш-накопители, жесткие диски, имеют свои недостатки. Например, нехватка свободного места на носителе. Чтобы решить данный вопрос и сделать доступность файлов немного проще, создали облачные хранилища.

В Интернете есть сервисы, которые предоставляют возможность хранить файлы на них. По факту мы загружаем их на какой-то удаленный компьютер в Интернете, на котором они хранятся, доступ к которым мы можем получить по адресу сервиса, который предоставил такую возможность. Эта технология позволяет не думать пользователю о способе размещения своей информации. Он имеет выделенный ему объем свободного места и может использовать его по своему усмотрению. В российском Интернете наиболее известны такие облачные хранилища, как «Яндекс.Диск», «Облако@mail.ru», «Google Drive»,

«Dropbox», «iCloud», «OneDrive». Практически все облачные хранилища имеют как бесплатные, так и платные аккаунты. В разных сервисах доступен разный объем памяти в бесплатном варианте. При необходимости можно докупить место на сервере, где объём и цена будет зависеть от конкретного облачного хранилища.

Преимущества облачных хранилищ.

Во-первых, облачные хранилища очень удобны для передачи файлов больших размеров, так как по электронной почте размеры файлов ограничены несколькими сотнями мегабайт. Например, если вы хотите поделиться своими фотографиями с отпуска со своими знакомыми, то подборку из пары сотен фотографий лучше загрузить в облачное хранилище, а вашим знакомым переслать ссылку в электронном письме.

Во-вторых, можно получить доступ к информации через Интернет с любого компьютера и из любой точки мира. Если вы работаете над документами совместно с вашими коллегами, то размещение документов в одном облачном хранилище даст доступ к одному и тому же документу и пропадает необходимость постоянной пересылки документа от одного человека к другому, от чего не будет появляться множество копий документа. Также можно установить определённые программы, которые устанавливаются на любое устройство, благодаря которым будет постоянный доступ к файлам, загруженным в облако.

Третье преимущество облачных сервисов – это то, что они используют технологии резервирования данных, то есть для всех данных, которые загружаются в облако, используется резервное хранение. Это уменьшает вероятность потери данных даже если произойдет аппаратный сбой, как у конечного пользователя, так и провайдера облачного хранилища. Речь идёт о накопителе на магнитном диске компьютера пользователя, если данные хранились на нём, так и о потере данных непосредственно на облачном сервисе, так как данные тоже хранятся на различных накопителях компьютеров, которые относятся к структуре сервисов облачных хранилищ.

Недостатки облачных хранилищ.

Остаётся открытым вопрос безопасности. Не стоит забывать, что ко всем загруженным файлам имеет доступ сам сервер и его сотрудники. Очень многое зависит от того, каким образом происходит хранение файлов на самом сервере, но тем не менее физически к информации имеет доступ сам сервер. Если произойдет какая-либо хакерская атака и случится взлом серверов облачного хранилища, то все загруженные файлы могут попасть в открытый доступ.

Главными угрозами безопасности в «облаке» являются:

1. Кража данных.

Кража конфиденциальной информации всегда пугает организации, так как, по их мнению, «облако» открывает новые пути атак для злоумышленников. При недостаточном продумывании архитектуры облачного сервиса изъян в приложении одного из клиентов может открыть злоумышленникам доступ к данным всех пользователям сервиса.

У каждого «облака» есть несколько уровней защиты, каждый из которых защищает информацию на своем уровне.

Первый уровень защиты – это физическая защита сервера. Речь идет о воровстве или порче носителей информации. Для обеспечения безопасности своих серверов организации хранят информацию в дата-центрах с видеонаблюдением, охраной и ограничением доступа не только от посторонних, но и от большинства сотрудников компании, так что вероятность того, что злоумышленник пройдёт и заберет информацию, близка нулю.

Многие SaaS-компании[1] не держат всю информацию на одном сервере, а распределяют ее, иногда даже территориально. Таким образом, взлом не принесет много ущерба, который может чем-то грозить пользователю. Как показывает практика, чаще всего при взломе сервера воруют базу email-адресов. Это значит, что пользователь получит спам-сообщения на свой почтовый ящик.

Второй уровень защиты – защита в процессе передачи данных.

SaaS-компании шифруют весь трафик с помощью https-протокола с использованием SSL-сертификата. Так данные будут в безопасности от попыток анализаторов траффика перехватить их. Http (Hypertext Transfer Protocol) – базовый протокол передачи данных между клиентом и сервером. По этому протоколу данные между браузером и клиентом отсылаются в виде обычного текста, позволяя владельцу сети видеть содержимое. Это проблема безопасности, поэтому был разработан протокол HTTP Secure (HTTPS), позволяющий пользователю и серверу сначала установить зашифрованное соединение, а после отправлять HTTP-сообщения, не волнуясь, что их прочитают третьи лица. SSL-сертификат – это цифровая подпись сайта, которая необходима для безопасного соединения. При его помощи вся информация между пользователем и сайтом шифруется таким образом, что она становится нечитаемой для других лиц (мошенников, системных администраторов и провайдеров). Также он является подтверждением подлинности сайта.

2. Потеря данных.

Потеря данных в облачном хранилище может произойти не только по вине злоумышленников, но и по другой причине. Данные случайно может удалить сам провайдер или они пострадают при стихийном бедствии или пожаре. Однако такое может произойти крайне редко. Компании постоянно и не менее двух раз в сутки автоматически копируют всю информацию. Таким образом, в случае потери данных пользователь всегда может обратиться в техническую поддержку и информацию можно будет восстановить.

3. Кража аккаунтов.

В облачной среде взломщик может использовать украденную регистрационную информацию, чтобы перехватывать, подделывать или выдавать искажённые данные реальных пользователей. Впоследствии это можно использовать для перенаправления их на вредоносные сайты. Данные действия можно обнаружить в процессе исследования компьютерного инцидента, однако сам пользователь может нанести себе и своим знакомым существенный вред [1].

[1] SaaS (software as a service) – одна из форм облачных вычислений, модель обслуживания, при которой пользователям предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое провайдером.

Внедрение надёжной, двухфакторной аутентификации позволит снизить этот риск. Также уменьшает риск запрет использования одних и тех же паролей для всех сервисов.

4. Незащищенные интерфейсы и API.

Слабые интерфейсы ПО или Application Programming Interface (API), используемые заказчиками для управления и взаимодействия с облачными услугами, подвергают пользователей целому ряду угроз, особенно если они размещены в социальных сетях [2]. Эти интерфейсы должны быть правильно спроектированы и обязательно включать аутентификацию, управление доступом и шифрование, чтобы обеспечить необходимую защиту и готовность облачных услуг.

Организации и сторонние подрядчики часто используют облачные интерфейсы для предоставления дополнительных услуг, что делает их более сложными и увеличивает риск, поскольку может потребоваться, чтобы заказчик сообщил свои регистрационные данные такому подрядчику для упрощения предоставления услуг.

5. DDoS-атаки.

На облако могут быть предприняты атаки типа «отказ в обслуживании», которые вызывают перегрузку инфраструктуры, заставляя задействовать огромный объём системных ресурсов и не давая заказчикам пользоваться этой услугой.

6. Злонамеренный инсайдер.

В среде IaaS, PaaS или SaaS, где не обеспечен должный уровень безопасности, инсайдер, имеющий корыстные намерения (например, системный администратор), может получить доступ к конфиденциальной информации, которая ему не предназначена.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Попов Д.О., Иванов В.Ю. Правовые основы проведения компьютерной технической экспертизы / Технологии информационной безопасности в деятельности органов внутренних дел: сборник X-XI научно-практической конференции. – Москва, 2014. С. 116-122.

2. Родкина Е.А., Иванов В.Ю. Некоторые аспекты мониторинга социальных сетей / Технологии информационной безопасности в деятельности органов внутренних дел: сборник научных трудов XIII научно-практической конференции. – Москва 2016. С. 86-89.

УДК 519.688

ОСОБЕННОСТИ РАЗРАБОТКИ КОМПЬЮТЕРНЫХ ПРИЛОЖЕНИЙ ДЛЯ ГЕНЕРИРОВАНИЯ И ВЕРИФИКАЦИИ ПРАКТИЧЕСКИХ ЗАДАНИЙ, ВКЛЮЧАЮЩИХ ОБРАБОТКУ МАТРИЦ

Михайленко Е.В.,
кандидат физико-математических наук, доцент
(Краснодарский университет МВД России)

Аннотация: в статье рассматриваются общие принципы, методы и технологии разработки компьютерных приложений для генерирования и верификации практических заданий по изучаемым курсантами математическим и естественно-научным дисциплинам, раскрываются особенности реализации программ на VBA, включающих обработку матриц. Описываемые приложения иллюстрируются рисунками.

Ключевые слова: VBA, автоматизация, матрица, матричные игры, обратная матрица, определитель, смешанные стратегии, учебный процесс.

FEATURES OF THE DEVELOPMENT OF COMPUTER APPLICATIONS FOR THE GENERATION AND VERIFICATION OF PRACTICAL TASKS, INCLUDING MATRIX PROCESSING

Mikhaylenko E.V.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Krasnodar University of the MIA of Russia)

Abstract: the article discusses the general principles, methods and technologies for the development of computer applications for the generation and verification of practical tasks in the mathematical and natural sciences studied by cadets, reveals the features of the implementation of VBA programs, including matrix processing. The described applications are illustrated by drawings.

Keywords: VBA, automation, matrix, matrix games, inverse matrix, determinant, mixed strategies, learning process.

В настоящее время широко внедряются методы и технологии оптимизации образовательного процесса с использованием различного рода программных продуктов [2, 5]. Прежде всего это использование текстовых редакторов и электронных таблиц для подготовки методического материала, компьютерных приложений для создания и показа презентаций, применение специализированных пакетов программ математических и инженерных вычислений, а также систем автомати-

зированного проектирования [6]. Большое место в программном обеспечении занимают контролирующие системы для оценивания знаний обучаемых.

Использование вышеперечисленных программных продуктов эффективно влияет на скорость и качество подготовки учебного материала, активизирует процессы восприятия и усвоения представляемой информации обучаемыми, формирует устойчивые навыки расчета требуемых значений в инженерных и экономических исследованиях, позволяет производить качественную оценку знаний курсантов с использованием основных стандартных форм тестовых заданий [1].

Данная статья посвящена особенностям применения некоторых методических приемов и технологий при разработке компьютерных программ для подготовки практических заданий и анализа их выполнения курсантами по дисциплинам блока математических дисциплин: математика, прикладная математика и математические методы обработки информации, изучаемых на первом, втором и третьем годах обучения курсантами Краснодарского университета МВД России по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

Во многих разделах общематематических и естественно-научных дисциплин используются матрицы и определители. Особенность обработки матричных выражений заключается в том, что объектами вычислений являются не отдельные числа, а двумерные числовые массивы, и порой разработчику учебных приложений необходимо приложить немало труда для составления специфических алгоритмов их обработки [7].

Рассмотрим пример генерации задания 2.в «Выполнить действия над матрицами» из практической работы «Обратная матрица. Ранг матрицы» раздела «Матрицы и определители» (рис. 1). При выполнении задания обучаемый сначала должен найти обратную матрицу для второго множителя, а затем умножить первую матрицу на полученный результат. Но генерировать задание в таком порядке не следует, так как в процессе нахождения обратной матрицы могут получаться элементы с дробными значениями, что затруднит выполнение работы курсантами.

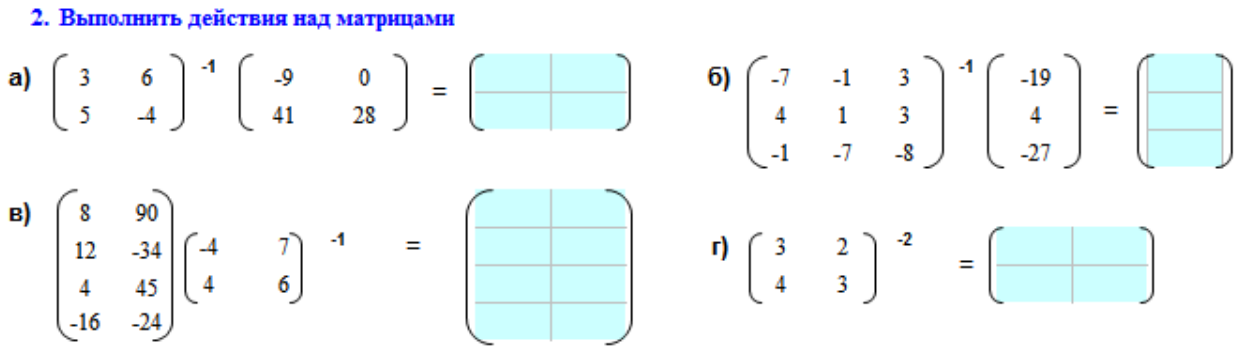


Рисунок 1. Задание «Выполнить действия над матрицами»

Формируемое задание 2.в можно представить в матричной форме следующим образом: $A \cdot B^{-1} = C$. В приводимом примере матрицы *A* и *B* выведены на лист, а значения коэффициентов матрицы *C* нужно внести. Если в матричном выражении перенести второй множитель в правую часть, то получим $A = \frac{C}{B^{-1}}$ или $A = C \cdot B$. Учитывая данный факт рассчитывать коэффициенты матриц будем в следующем порядке: начнем с матрицы *C*, затем, генерируя произвольные целочисленные коэффициенты, сформируем матрицу *B*, а уж потом рассчитаем матрицу *A*.

В представленном фрагменте кода программы (рис. 2) мы видим, что во вложенных циклах с параметрами *i* и *j* генерируются коэффициенты двумерного массива *c*, являющегося решением задачи. При формировании матрицы *b*, для которой обучаемый будет строить обратную, в цикле Do .. Loop Until происходит проверка матрицы на вырожденность. Массив *a* получим, перемножая уже сформированные элементы массивов *c* и *b*. При разработке алгоритма расчета коэффициентов матрицы *A* необходимо использовать определение матричного произведения и учитывать некоммутативность данной операции.

```
'Задание 2.в. Выполнить действия над матрицами.
' Матрица 4x2 умножается на обратную матрицу 2x2

For i = 1 To 4
  For j = 1 To 2
    c(i, j) = Rnd(v) * 18 - 9
Next j, i

Do
  For i = 1 To 2
    For j = 1 To 2
      b(i, j) = Rnd(v) * 16 - 8
      Cells(i + 24, j + 3) = b(i, j)
  Next j, i
Loop Until (b(1, 1) * b(2, 2) - b(1, 2) * b(2, 1)) <> 0


For i = 1 To 4
  For j = 1 To 2
    a(i, j) = 0
    For k = 1 To 3
      a(i, j) = a(i, j) + c(i, k) * b(k, j)
    Next k
    Cells(i + 23, j + 1) = a(i, j)
Next j, i
```

Рисунок 2. Генерация задания «Выполнить действия над матрицами»

При проверке выполненного задания следует иметь в виду, что в ней необходимо осуществить расчет всех параметров задания точно так же, как и при генерации задачи обучаемым (рис. 3) [4]. В первом блоке представленного программного кода осуществляется вычисление значение элементов массива *c* и

сравнение этих значений с записанным на листе ответом. Расчет значений массива *b* выполняется только для того, чтобы количество обращений к функции *Rnd* с параметром *v* совпадало с генерацией этого задания курсантом. На самом деле значения массива *b* можно было и не рассчитывать, а заменить рассматриваемую структуру восьмикратным вызовом инструкции *Rnd*(*v*).

```
'Задание 2.в. Выполнить действия над матрицами.
' Матрица 4x2 умножается на обратную матрицу 2x2
                                                    'Проверка
For i = 1 To 4
  For j = 1 To 2
    c(i, j) = Rnd(v) * 18 - 9
    If Cells(i + 23, j + 7) = c(i, j) And Cells(i + 23, j + 7) <> "" Then
        mark = mark + 1
      Else
        Cells(i + 23, j + 7) = krest(i + 23, j + 7)
      End If
Next j, i

For i = 1 To 2
  For j = 1 To 2
    b(i, j) = Rnd(v) * 18 - 9
Next j, i
```

Рисунок 3. Код проверки задания «Выполнить действия над матрицами»

Иногда при генерации заданий, связанных с обработкой матриц, приходится неоднократно генерировать параметры условия задачи, оценивая пригодность сформированного задания для его выполнения [5]. Рассмотрим задание 3 «Определить смешанные стратегии игроков S_A и S_B, а также цену игры v» из практической работы «Решение матричных игр» раздела «Теория игр и принятия решений» (рис. 4).

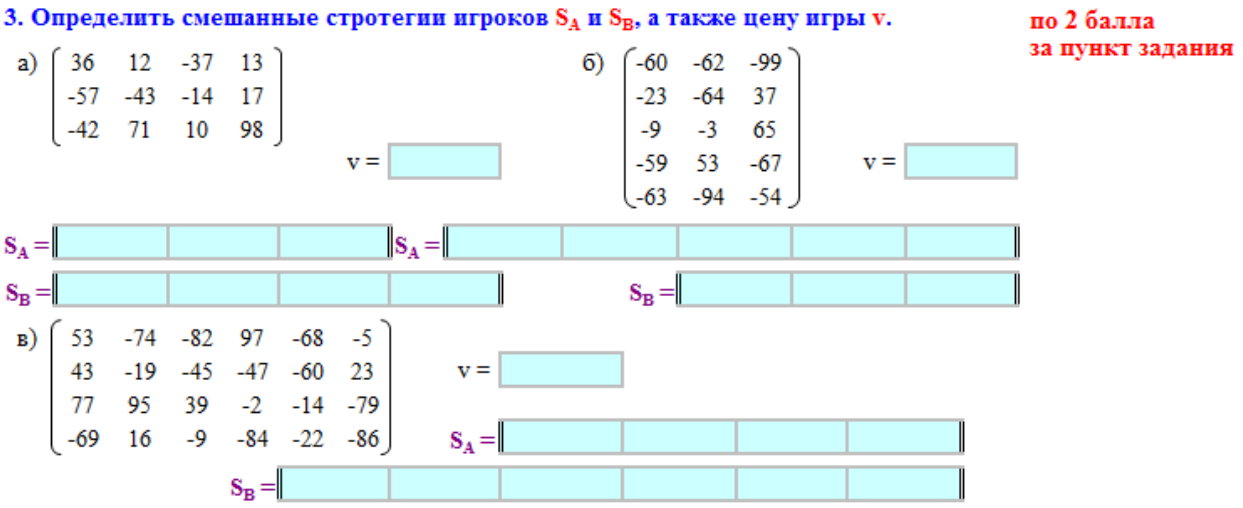


Рисунок 4. Задание «Определить смешанные стратегии игроков S_A и S_B, а также цену игры v»

Задание состоит из трех задач нарастающей сложности. Решая эти задачи, обучаемые должны упростить платежную матрицу до двух строк и двух столбцов, найти нижнюю α и верхнюю β цены игры, применить вероятностные подходы для расчета смешанных стратегий игроков A и B, а затем, учитывая найденные вероятности применения каждой стратегии, рассчитать цену матричной игры.

Опишем методы подбора параметров задачи 3.в. Программный код генерации параметров задания можно условно разбить на две части. В первой из них происходит предварительный расчет платежной матрицы (рис. 5).

```
Do
  Do          'Находим коэффициенты платежной матрицы mA(i,
    For i = 1 To 4
      For j = 1 To 6
        Do
          mA(i, j) = Round(Rnd(V) * 200 - 100)
          k = 0
          For i0 = 1 To 4
            For j0 = 1 To 6
              If mA(i, j) = mA(i0, j0) Then k = k + 1
          Next j0, i0
        Loop Until k = 1
    Next j, i
                      'Находим нижнюю границу Alfa
    For i = 1 To 4
      mAlfa(i) = mA(i, 1)
      For j = 1 To 6
        If mA(i, j) < mAlfa(i) Then mAlfa(i) = mA(i, j)
      Next j
    Next i
    alfa = mAlfa(1)
    For i = 1 To 4
      If mAlfa(i) > alfa Then alfa = mAlfa(i)
    Next i
                      'Находим верхнюю границу Betta
    For j = 1 To 6
      mBetta(j) = mA(1, j)
      For i = 1 To 4
        If mA(i, j) > mBetta(j) Then mBetta(j) = mA(i, j)
      Next i
    Next j
    betta = mBetta(1)
    For j = 1 To 6
      If mBetta(j) = betta Then betta = mBetta(j)
    Next j
  Loop Until alfa < betta
```

Рисунок 5. Расчет коэффициентов платежной матрицы

Как видим из листинга программы, при определении коэффициентов матрицы в каждой итерации производится верификация на уникальность генерируемого элемента. Для сформированной матрицы находятся нижняя *alfa* и верхняя *betta* цены игры, и в случае появления седловых точек, когда игра решается в чистых стратегиях, происходит возврат к генерации коэффициентов. В случае неравенства *alfa* и *betta* матрица заносится в массив *mA0*.

Вторая часть генерации задания упрощает сформированную платежную матрицу, уменьшая их размерность путем исключения дублирующих и заведомо невыгодных стратегий. На рисунке 6 представлен фрагмент программного кода, в котором происходит поиск и удаление дублирующих и доминируемых стратегий игрока *A*.

```
m = 4: n = 6
For p = 1 To 10
                    'Проход слева направо
  qi = 0
                    'Находим доминируемую строку
  For i1 = 1 To m - 1
    For i2 = i1 + 1 To m
      k1 = 0: k2 = 0
      For j = 1 To n
        If mA(i1, j) <= mA(i2, j) Then k1 = k1 + 1
        If mA(i2, j) <= mA(i1, j) Then k2 = k2 + 1
      Next j
      If k1 = n Then qi = i1
      If k2 = n Then qi = i2
  Next i2, i1
                    'Удаляем доминируемую строку
  If qi > 0 Then
    For i = qi To m - 1
      For j = 1 To n
        mA(i, j) = mA(i + 1, j)
    Next j, i
    m = m - 1
  End If
```

Рисунок 6. Поиск и удаление дублирующих и доминируемых строк

Аналогичным образом (рис. 7) в программе попарно анализируются столбцы платежной матрицы, а также удаляются дублирующие и доминируемые стратегии игрока *B*.

```
                    'Проход сверху вниз
    qj = 0
                    'Находим доминируемый столбец
    For j1 = 1 To n - 1
      For j2 = j1 + 1 To n
        k1 = 0: k2 = 0
        For i = 1 To m
          If mA(i, j1) >= mA(i, j2) Then k1 = k1 + 1
          If mA(i, j2) >= mA(i, j1) Then k2 = k2 + 1
        Next i
        If k1 = m Then qj = j1
        If k2 = m Then qj = j2
    Next j2, j1
                    'Удаляем доминируемый столбец
    If qj > 0 Then
      For j = qj To n - 1
        For i = 1 To m
          mA(i, j) = mA(i, j + 1)
      Next i, j
      n = n - 1
    End If
  Next p
Loop Until m = 2 And n = 2
                    'Выводим платежную матрицу
For i = 1 To 4
  For j = 1 To 6
    Cells(i + 48, j + 1) = mA0(i, j)
Next j, i
```

Рисунок 7. Поиск и удаление дублирующих и доминируемых строк

Если после десяти проходов упрощения платежной матрицы у каждого из игроков останутся по две стратегии, то рассчитанная в первой части программы матрица размерностью 4x6 выводится на лист заданий. В противном случае происходит повторное генерирование платежной матрицы. Опыт использования программного продукта показал, что при генерации курсантами заданий совершаются десятки итераций, однако скорость нахождения платежной матрицы, сводящейся после преобразований к двум строкам и двум столбцам, достаточно велика.

Процесс проверки задания рассматривать не будем. Достаточно сказать, что алгоритм нахождения платежной матрицы здесь такой же, как и описанный ранее, а для нахождения оптимального решения в смешанных стратегиях используется вероятностный подход.

Представленные компьютерные программы внедрены в образовательную деятельность кафедры информатики и математики. Опыт использования практикума в учебном процессе дал положительные результаты. В настоящее время ведутся работы над созданием ряда подобных программ для обеспечения других дисциплин кафедры информатики и математики.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Лаптев В.Н., Михайленко Е.В. О технологиях разработки программных приложений для генерирования и проверки практических заданий по математическим дисциплинам [Электронный ресурс] // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2020. № 1(155). IDA [article ID]: 1552001013. – Режим доступа: http://ej.kubagro.ru/2020/01/pdf/13.

2. Лаптев В.Н., Михайленко Е.В. Некоторые аспекты применения среды Visual Basic for Application для создания учебных приложений по математическим дисциплинам [Электронный ресурс] // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 9(103). С. 222–233. – IDA [article ID]: 1031409014. – Режим доступа: http://ej.kubagro.ru/2014/09/pdf/14.

3. Михайленко Е.В. Автоматизация подготовки заданий и проверки выполненных работ по математическим и естественнонаучным дисциплинам / Проблемы информационного обеспечения деятельности правоохранительных органов: материалы международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России, 2015. С. 107–114.

4. Михайленко Е.В. О разработке обучающих программ в среде Visual Basic for Application / Математические методы и информационно-технические средства: материалы XII Всерос. науч.-практ. Конф. 17 июня 2016 г. / редкол.: И.Н. Старостенко, Е.В. Михайленко, А.А. Хромых, М.В. Шарпан. – Краснодар: Краснодарский университет МВД России. 2016. С. 179–184.

5. Михайленко Е.В. Особенности разработки в VBA программных приложений для генерирования практических заданий и анализа их выполнения / Математические методы и информационно-технические средства: материалы XI Всерос. науч.-практ. конф., 19 июня 2015 г. / редкол.: И.Н. Старостенко (отв. ред.), Е.В. Михайленко, Ю.Н. Сопильняк, А.В. Еськов, М.В. Шарпан. – Краснодар: Краснодар. ун-т МВД России, 2015. С. 159–162.

6. Михайленко Е.В. Особенности разработки компьютерных программ для подготовки практических заданий и анализа их выполнения по разделам булевой алгебры / Проблемы информационного обеспечения деятельности правоохранительных органов: материалы 2-й международной научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2016. С. 268–274.

7. Михайленко Е.В. Технологии разработки программных приложений для генерации и проверки выполнения практических заданий по математическим дисциплинам / Математические методы и информационно-технические средства: материалы XIII Всерос. науч.-практ. конф. (16 июня 2017 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко; М.В. Шарпан, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2017. С. 192–199.

УДК 004.738.5

ОСОБЕННОСТИ ЦЕЛЕВОГО ПОИСКА В ИНТЕРНЕТЕ

Страхов А.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье проведен обзор методов и средств целевого поиска открытой информации в сети Интернет на примере персональных данных человека, а также дана их правовая оценка.

Ключевые слова: информационное общество, Интернет, информационный поиск, поисковый запрос, SEO-оптимизация, веб-аналитика, социальные сети.

FEATURES OF THE TARGET SEARCH ON THE INTERNET

Strahov A.A.
(Kikot Moscow University of the MIA of Russia)

Abstract: the article reviews methods and means of targeted search for open information on the Internet on the example of personal data of a person, as well as their legal assessment.

Keywords: information society, Internet, information search, search query, SEO optimization, web Analytics, social networks.

С развитием Интернета все труднее обеспечить конфиденциальность информации и анонимность ее владельца. У каждого информационного ресурса есть конкретный сетевой адрес, у каждого сообщения – свой автор. Попав в Интернет, каждый пользователь сознательно или непредумышленно оставляет следы, по которым его можно идентифицировать, собрать о нем персональные данные и даже воспользоваться его электронной личностью. Случайно или целенаправленно при техническом сбое или под влиянием человеческого фактора любые сведения могут попасть в открытый доступ.

В 40-х годах прошлого века сформировалось самостоятельное направление информационной разведки по открытым источникам OSINT (Open-Source Intelligence), методы и средства которой постоянно совершенствуются при государственной поддержке.

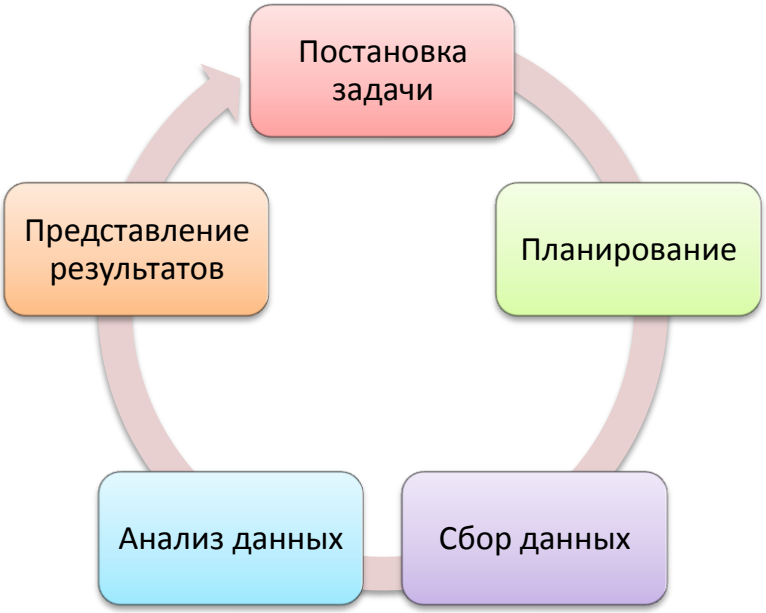
Данная статья не ориентирована на подготовку профессиональных разведчиков. Автор предлагает заинтересованным читателям познакомиться с общими принципами и конкретными приемами целевого поиска информации в Интернете, не нарушающими законодательство Российской Федерации.

Для получения ответов на интересующие вопросы большинство пользователей сети Интернет не используют ничего, кроме контекстного поиска в Ян-

декс, Google, Mail.ru и т.п. Но довольно часто ответы на подобные запросы содержат огромные массивы документов, среди которых 99% информационного мусора, включая дубликаты, репосты или ретвиты оригинальных источников, спам, рекламу, фэйки (fake), ссылки на похожие объекты-омонимы.

Непоследнюю роль в дезориентации пользователя играет поисковая оптимизация SEO (search engine optimization) – современная информационная технология продвижения информационного ресурса в топ списка отклика на запрос поисковых систем. Специальные алгоритмы поисковых машин формируют список документов по принципу «дайте я угадаю, что Вам нужно на самом деле», и обычный пользователь, только начав текстом или голосом формировать свой запрос, получает варианты-подсказки поисковых фраз. Релевантность подборки или степень формального соответствия запросу пользователя подменяется в современных поисковых системах пертинентностью – информационной потребностью пользователя, определенной исходя из ранее сделанных запросов.

Целевой поиск в Интернете – это циклический информационный процесс, повторяющийся многократно до получения требуемого результата или максимально возможного набора сведений об интересующем объекте или событии (target). Основные этапы информационного поиска представлены на рисунке.



На этапе постановки задачи важно:

– правильно определить конечный результат – необходимый и достаточный объем интересующих сведений о цели;

– установить наиболее значимые исходные данные в контексте поставленной задачи;

– определить сегменты информационного пространства и условия ведения поиска.

Формулирование и проверку рабочих гипотез о характеристиках и вероятных связях цели с чем-то или с кем-то целесообразно осуществлять последовательно от наиболее очевидных до маловероятных.

Если целью является физическое лицо, то его характерными признаками могут быть телефон, домашний адрес, место работы, адрес электронной почты, никнэймы и аватары в социальных сетях, мессенджерах или на публичных форумах. Связи зависят от места проживания, родства, профессиональной деятельности, сферы интересов, контактов в социальных сетях и т.п.

В соответствии с выдвинутыми гипотезами подбираются информационные ресурсы – потенциальные источники информации о цели.

Если на старте про цель известно немного (имя, фамилия, примерный возраст, город проживания), то начинать нужно с автоматизированных информационно-поисковых систем Интернета, которые интегрируют сведения о содержимом миллионов сайтов белого (открытого) Интернета. Основным недостатком поисковиков является масса избыточных страниц, которые нужно просматривать, отбирать и анализировать самостоятельно.

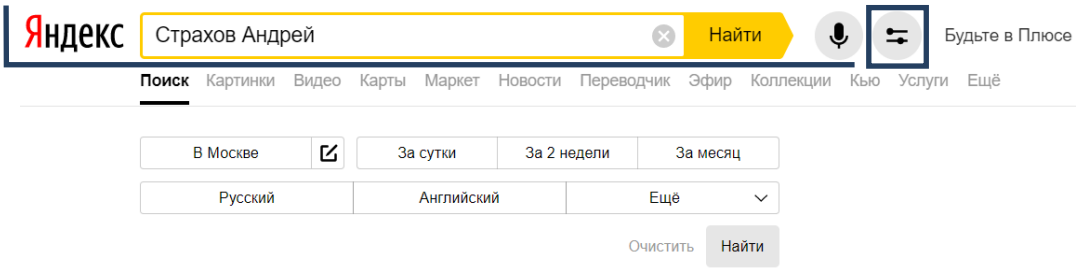
Чтобы конкретизировать запрос и отсечь лишний информационный шум в поисковых системах, следует использовать специальные фильтры и языки запросов. Ниже в таблице представлены некоторые команды Яндекс и Google, которые могут значительно повысить эффективность поиска конкретного человека во Всемирной паутине.

Операция	Яндекс	Google
Поиск документов, содержащих конкретный текст	"Страхов Андрей"	"Страхов Андрей"
Объединение запросов по ИЛИ	Олег | Игорь	Олег OR Игорь
Обязательное присутствие слова (фразы) во всех формах	+(Пешков Максим)	+(Пешков Максим)
Исключение результатов с отмеченными словами	-Александр	-Александр
Поиск документов по контексту с любым словом вместо *	"Котов * Олегович"	"Котов * Олегович"
Поиск по всем страницам сайта и поддоменам	Кутузов site:vk.ru	Кутузов site:gov
Поиск слова в заданной форме	!Смирнов	
Поиск в социальных сетях		@vkontakte
Поиск по хештегам		#александров
Фильтрация документов по типу файла (pdf, rtf, doc, xls, ppt, …)	Лапин mime:doc	Лапин filetype:doc

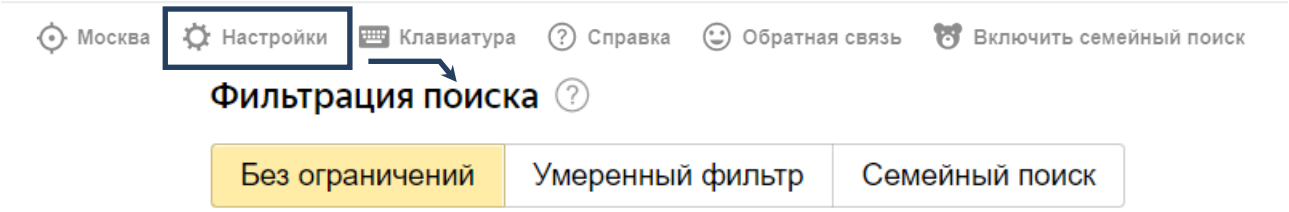
Операторы в запросе можно комбинировать в соответствии с правилами логики высказываний.

Команды языка запросов не обязательно знать наизусть для ввода в строку поиска. Большинство команд дублируются с помощью специальных фильтров расширенного поиска.

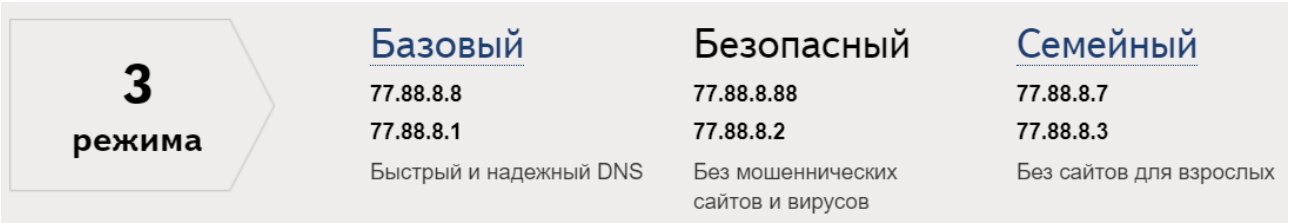
Интерфейс настройки фильтров расширенного поиска в Яндексе вызываются щелчком мыши по круглой кнопке справа от поисковой строки.



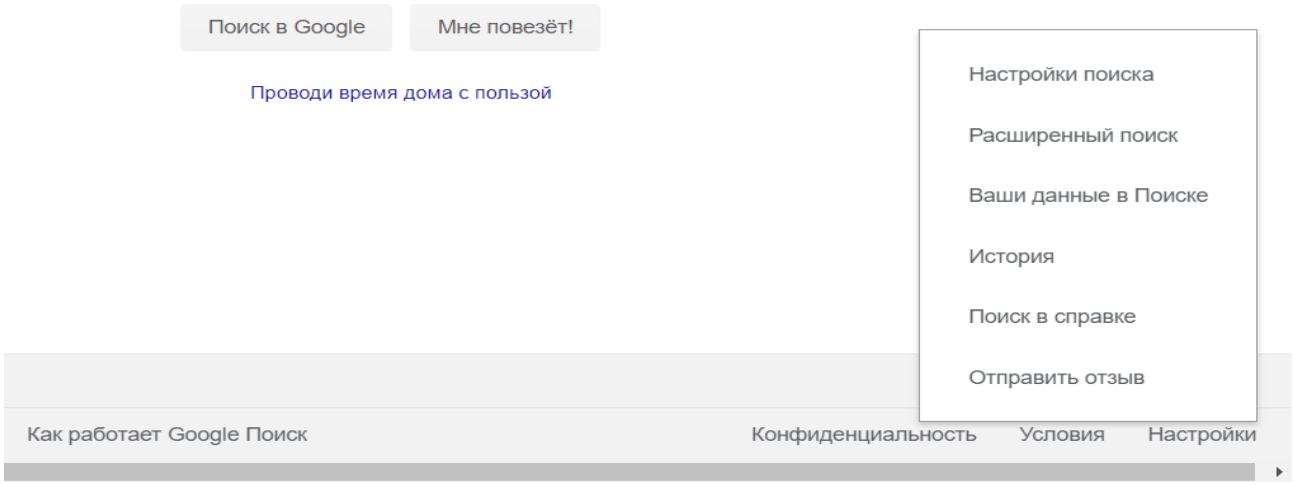
Чтобы снять запрет на ненормативную лексику и контент «для взрослых», следует выбрать режим *Без ограничений* на странице *Настройка поиска* (вызывается по гиперссылке *Настройки* в подвале (footer) страницы поисковой выдачи).



У Яндекса более 80 DNS-серверов в разных городах, что позволяет достаточно быстро обрабатывать запросы пользователей. Но в Интернете легко наткнутся на сайты, способные заразить компьютер, украсть персональные данные, пароли, заблокировать доступ к информационным ресурсам. Предотвратить загрузку вредоносного кода можно с помощью антивируса, который установлен на безопасных серверах Яндекс.DNS (https://dns.yandex.ru/).



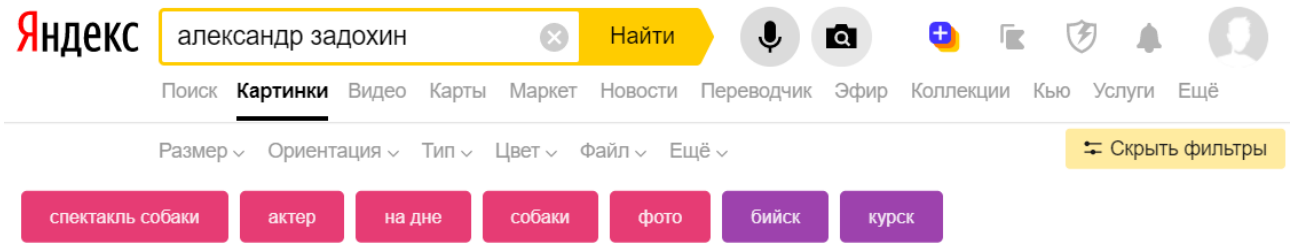
Окно настройки фильтров расширенного поиска Гугла вызывается из меню *Настройки* в подвале главной страницы или по прямой ссылке https://www.google.ru/advanced_search.



В Гугле, как и в Яндексе, фильтры расширенного поиска могут устанавливаться на страну, сайт или домен, расположение слов, формат файлов, безопасность и т.п.

Для обоих поисковиков следует отметить наличие возможности поиска изображения по заданным параметрам или информации об изображении.

Сервис Яндекс.Картинки для поиска изображений в Интернете вызывается по гиперссылке *Картинки* из меню поисковой строки и позволяет искать изображение требуемого формата с заданными параметрами. Фильтры поиска изображений расположены под поисковой строкой и активируются по кнопке *Показать фильтры/Скрыть фильтры* в правой части строки. Все результаты поиска отображаются на одной странице и доступны для просмотра в нескольких режимах.



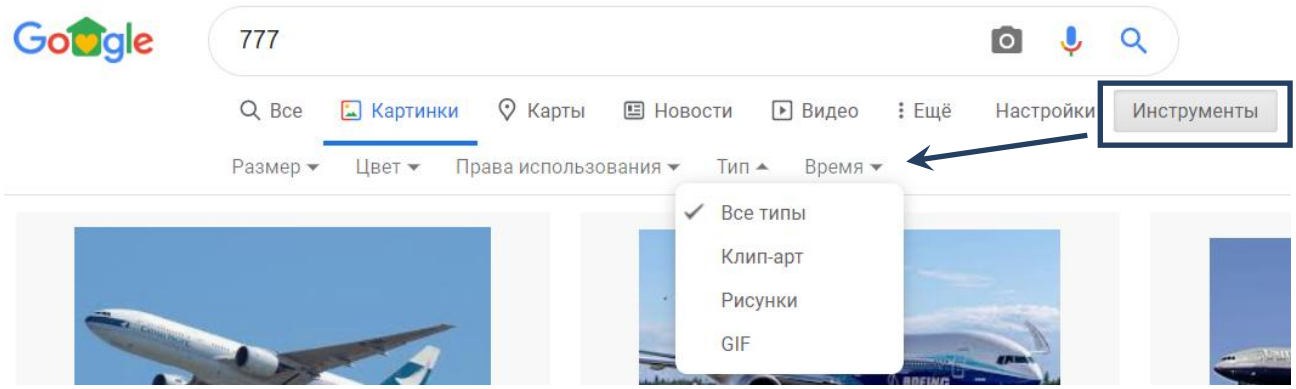
Поиск информации по самой картинке в Яндексе осуществляется двумя способами:

– кликнуть мышью по иконке с фотоаппаратом справа от поисковой строки и в появившееся поле перетащить картинку или ввести ее адрес;

– нажать правой кнопкой мыши на любую картинку в окне Яндекса и выбрать из контекстного меню *Найти это изображение в Яндексе*.

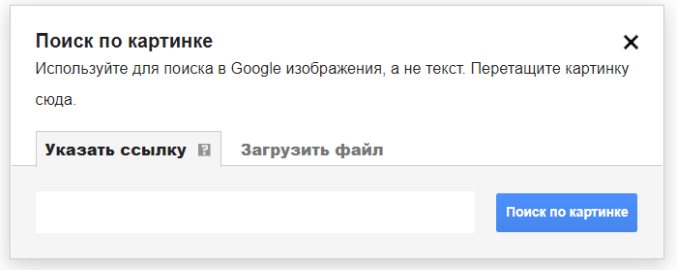
С помощью этого поиска можно узнать, кто изображен на фото, по части фотографии найти целую или похожие фото с конкретным человеком, перейти на оригинальный источник и т.п.

Сервис Google.*Картинки* также позволяет искать и анализировать фотографии с любого сайта и с персональных страниц в социальной сети.



Окно настройки фильтров расширенного поиска изображений вызывается из меню Настройки поисковой строки в режиме *Картинки* или по прямой ссылке https://www.google.com/advanced_image_search.

По аналогии с Яндексом в Гугле можно искать дополнительную информацию по имеющемуся изображению либо через иконку с фотоаппаратом справа от поисковой строки, либо через контектсное меню картинки.

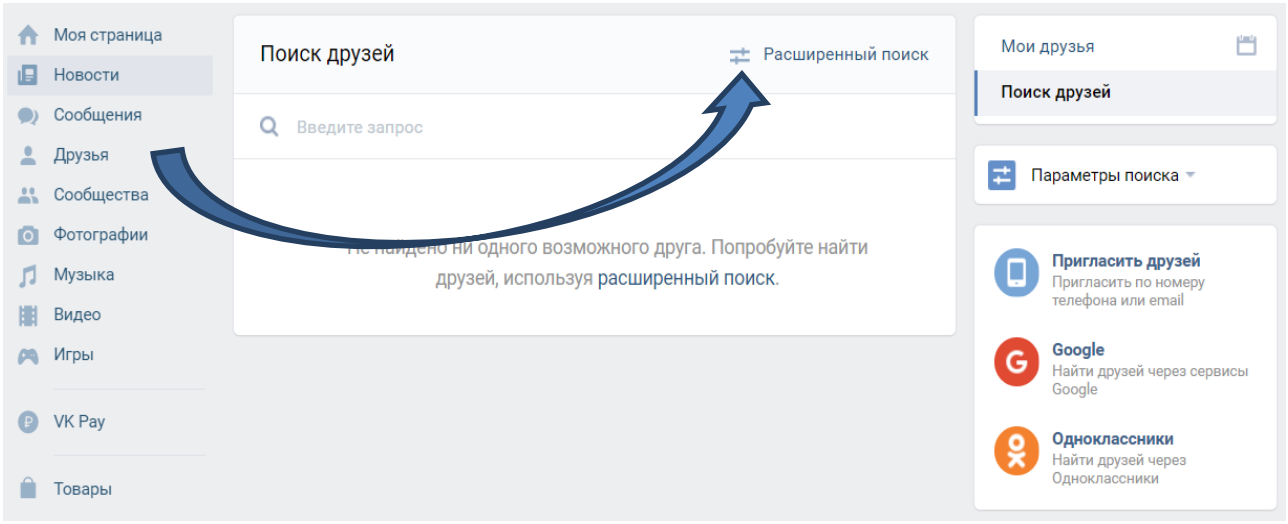


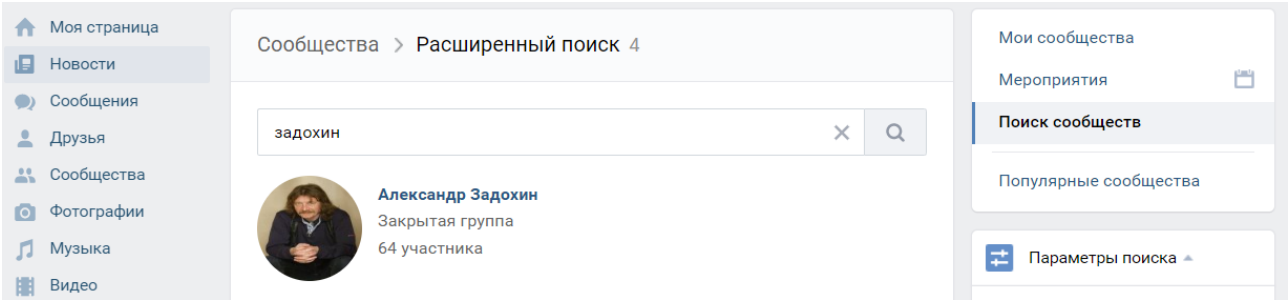
Подстановка Яндекса или Гугла как инструмента поиска изображения в его контекстном меню зависит от того, какая поисковая система настроена в браузере основной.

Современные смартфоны при фотосъемке сохраняют вместе с изображением метаданные EXIF (Exchangeable Image File Format), такие как дата, тип фотокамеры, параметры съемки, географические координаты (геотеги). Исследовать метаданные можно, например, с помощью сервиса pic2map (https://www.pic2map.com), специальных видеоредакторов или приложений для просмотра изображений (viewer).

Огромный информационный массив о людях (персональные данные, контакты, фото с геолокацией, друзья, членство в группах по интересам, персонализированная лента новостей, онлайн-переписка) содержится непосредственно в социальных сетях «ВКонтакте», «Одноклассники», «Facebook», «Twitter», «Instagram» и т.п.

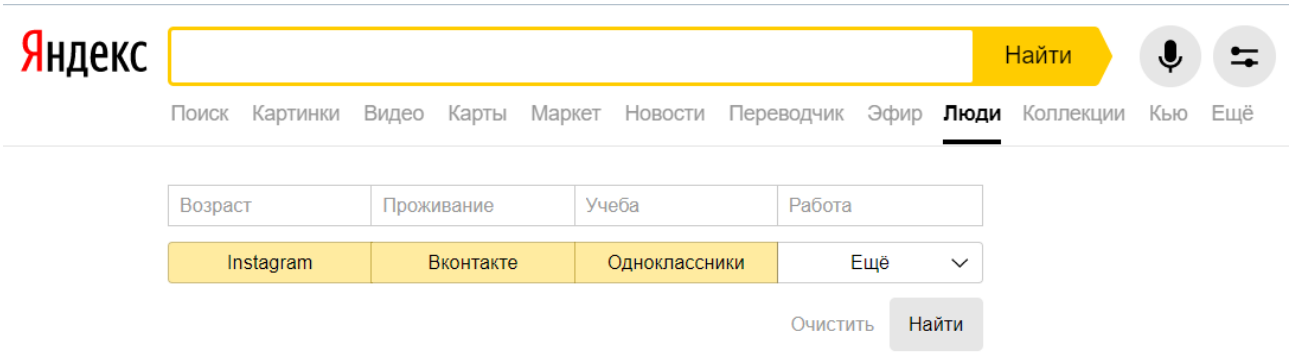
Поиск людей в социальных сетях достаточно эффективно можно вести с помощью встроенных инструментов этих сетей.





На скриншотах сети «ВКонтакте» видно, что в дополнение к запросу в поисковой строке категории *Друзья, Люди, Сообщества* содержат дополнительные фильтры поиска.

Дополнительным целеуказателем может стать телефонный номер или электронный почтовый ящик. Но запрос по этим данным следует делать не в самой сети, а в поисковике с помощью фильтров расширения сервисов *Поиск людей* (Яндекс) или *Поиск по блогам*.



В Гугле фильтром для социальной сети является оператор @.

Много открытой информации размещается на сайтах, где оказываются государственные и муниципальные услуги в электронном виде. Персональные данные добросовестных граждан чаще всего закрыты. В таблице ниже приведены некоторые адреса, где можно поискать официальные сведения о человеке в разрешенных законом случаях.

URL ресурса	Характер информации
https://www.mos-gorsud.ru	Деятельность судов общей юрисдикции г. Москвы
http://fssprus.ru/iss	Сервисы ФССП: Банк данных исполнительных производств; Реестр розыска по исполнительным производствам; Лица, находящиеся в розыске по подозрению в совершении преступлений
https://минобразования-реестр.рф	Проверка наличия сведений о документе в федеральном реестре документов государственного образца об образовании, об учёных степенях и учёных званиях Рособрнадзора
https://www.rusprofile.ru/	Проверка информации о российских юридических лицах и предпринимателях по базам данных: ФНС (ЕГРЮЛ и ЕГРИП и специальные реестры ФНС); Арбитражные суды (участие организаций в судебных процессах); Казначейство (участие в государственных закупках по 44, 94, 223-ФЗ); Росстат (бухгалтерская отчетность организаций и коды государственной статистики); ФССП (исполнительные производства в отношении организаций)
http://podvignaroda.ru https://obd-memorial.ru https://pamyat-naroda.ru	Обобщенные банки данных о людях и документах Великой Отечественной войны, созданные по инициативе МО РФ

Белый интернет с открытым доступом для поисковых роботов, ежедневно обновляющих свои базы о миллионах страниц, является лишь маленькой верхушкой айсберга Всемирной паутины.

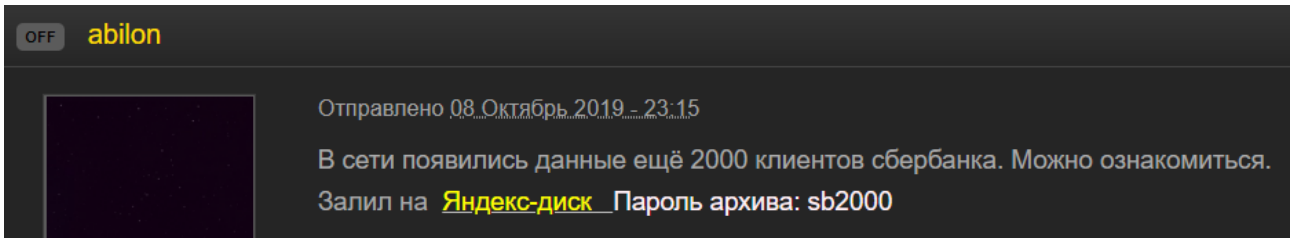
Множество веб-страниц, которые поисковые системы проиндексировать не могут, например, по причине отсутствия внешних гиперссылок или ограничения доступа и обязательной авторизации, формируют сегмент *глубинного интернета* (deep web). Поиск в глубинном интернете требует специальных знаний таких, например, как порядок доступа к сетевому ресурсу, структура универсального локатора ресурса URL (Uniform Resource Locator), HTML-код веб страницы (HyperText Markup Language), каскадные таблицы стилей CSS (Cascading Style Sheets), в данной статье не рассматривается.

Не нужно путать глубинный интернет и темный интернет (darknet), который манит новичков своей загадочностью и анонимностью.

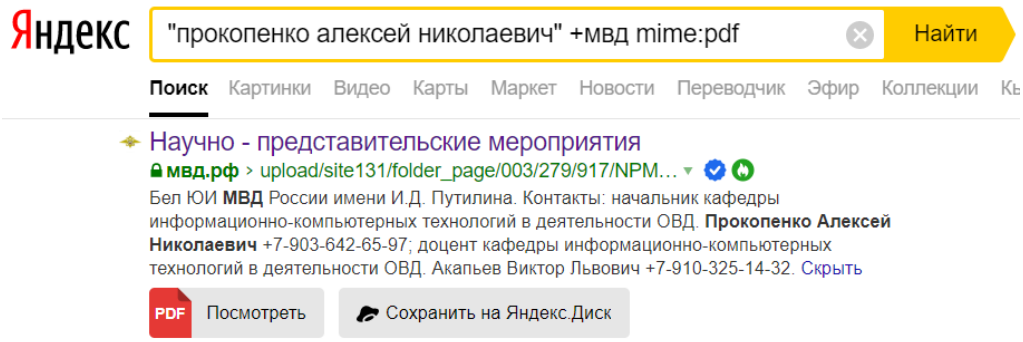
Темный интернет – скрытый сегмент Глобальной сети, в которой контакт устанавливается только между доверенными абонентами (pear-to-pear) с использованием шифрованных каналов, нестандартных протоколов и портов. Темный интернет – это зона криминала, хакеров и спецслужб. Неподготовленному пользователю туда лучше не соваться. Несмотря на отсутствие прямого запрета на использование в нашей стране различных анонимайзеров, VPN (Virtual Private Network), пиринговых сетей (BitTorrent, Direct Connect, TOR), пребывание в подпольной информационной сети может повлечь юридические санкции.

Законодательство Российской Федерации запрещает предоставлять доступ к персональным данным для ознакомления и использования без согласия их владельца, за исключением случаев, прямо прописанных в федеральных законах. Таким образом в открытом доступе можно найти либо сознательно выложенную информацию от владельца (как в социальных сетях), либо это утечка данных из официальных закрытых баз. Те, кто внимательно следят за новостями о хакерских атаках, могут использовать выложенные в открытый доступ базы данных о клиентах банков, торговых и социальных сетей, государственных и коммерческих организаций.

Так, в конце октября 2018 года на специализированном форуме phreaker.pro появился список из 421 тыс. сотрудников Сбербанка с ФИО и логинами для входа в служебный компьютер. По этой базе, учитывая, что довольно часто логины являются именами электронных почтовых ящиков, несложно было определить три e-mail-адреса, принадлежащие президенту банка Герману Грефу. Осенью 2019 года СМИ со ссылкой на издание «Коммерсантъ» распространили информацию о появлении на черном рынке базы данных о 60 миллионах действующих и закрытых картах клиентов Сбербанка. Автор не ставил себе задачу – найти эти списки, но простенький тематический запрос вывел на форум с сообщением:



Чтобы найти персональные данные непосредственно в файлах на страницах Интернета, в поисковом запросе следует использовать фильтрацию документов по типу файла: mime:doc; filetype:xls.



В сети есть много специализированных информационных ресурсов с услугами поиска персональных данных из различных источников. Причем услуга может предоставляться в режиме онлайн самообслуживания (on-line self-service) или как профессиональный сбор сведений по запросу пользователя (on-demand service), что характерно для детективных агентств. На подобных сайтах довольно часто для организации поиска людей требуется регистрация с предоставлением собственных персональных данных, но тогда следует понимать, что не исключены ситуации, когда ищущий сам становится целью.

При обращении к подобным ресурсам и сервисам следует руководствоваться п. 4. ст. 28 Конституции Российской Федерации: «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Следовательно, если конфиденциальная информация находится в свободном доступе по сети Интернет, то это проблема ее владельца, но ее использование в интересах посторонних лиц может быть ограничено федеральными законами (детская порнография, экстремизм, терроризм, наркотики, шантаж и т.п.). Блокировку провайдера можно обойти, используя VPN, например, встроенный в браузер Opera, или сеть Tor.

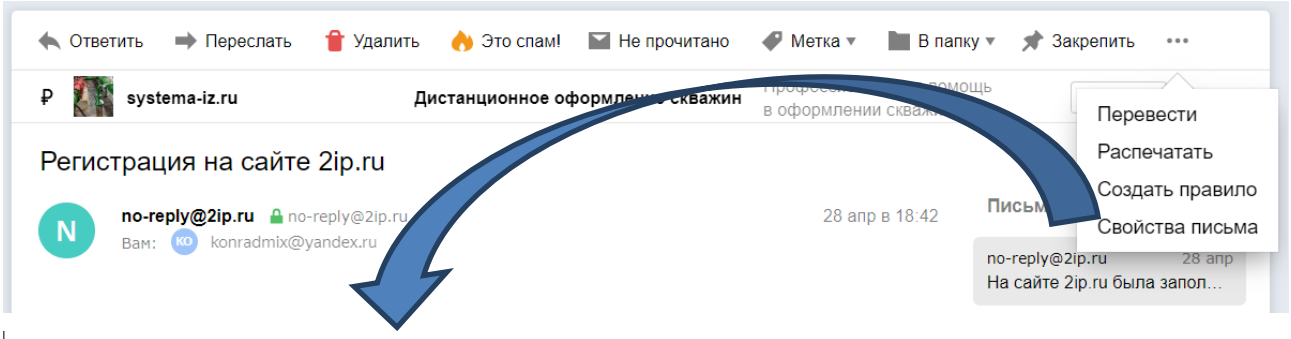
В следующей таблице приведены адреса некоторых сетевых проектов, где размещены персональные данные и иная информации о жизнедеятельности граждан.

URL ресурса	Характер информации
https://poisk.vid.ru	Международный проект поиска людей по всему миру телекомпании ВИД
https://www.moypolk.ru	Официальный сайт общественного движения «Бессмертный полк»
http://numplate.ru	База для связи с водителем через государственный номер его автомобиля
http://neo.spravkaru.net	Телефонный справочник по СНГ
https://telpoisk.com	Телефонный справочник по СНГ
http://allnum.ru	База телефонных номеров и номеров авто с комментариями очевидцев
http://nomer-org.world	Телефонный справочник по СНГ
https://zhuteli.rosfirm.info	Справочник жителей по городам России
http://bankludei.ru/moscow/num	Телефонный справочник Москва
https://fotostrana.ru	Сайт для знакомств с фотографиями
https://tineye.com	Поиск похожих изображений

URL ресурса	Характер информации
https://web.archive.org	Архив Интернета с 1996 года (свыше 330 миллиардов веб-страниц)
http://220vk.com	Онлайн-программа для наблюдения за пользователями «ВКонтакте»
http://vk.city4me.com	Онлайн-программа для наблюдения за активностью пользователя «ВКонтакте»
http://www.vkonta.ru	Народ «ВКонтакте»
http://kontragenta.net	Проверка контрагента по разным базам
http://stop-list.info	Онлайн проверки человека, компании, транспорта, недвижимости и т.п.

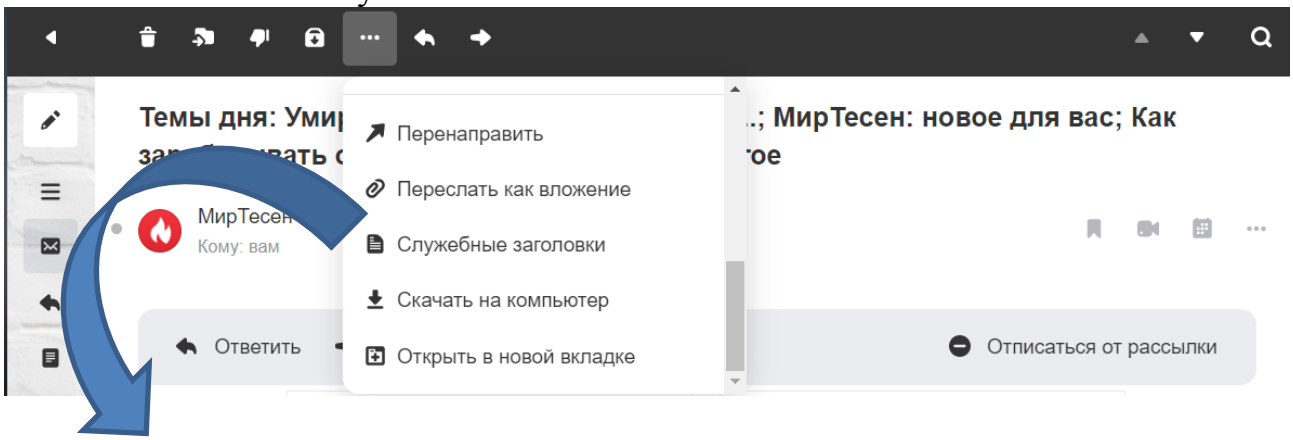
Иногда полезную информацию можно извлечь из IP-адреса электронной почты. Чтобы узнать IP-адрес отправителя, в почтовых сервисах существуют специальные функции:

– Яндекс.Почта.Свойства письма.



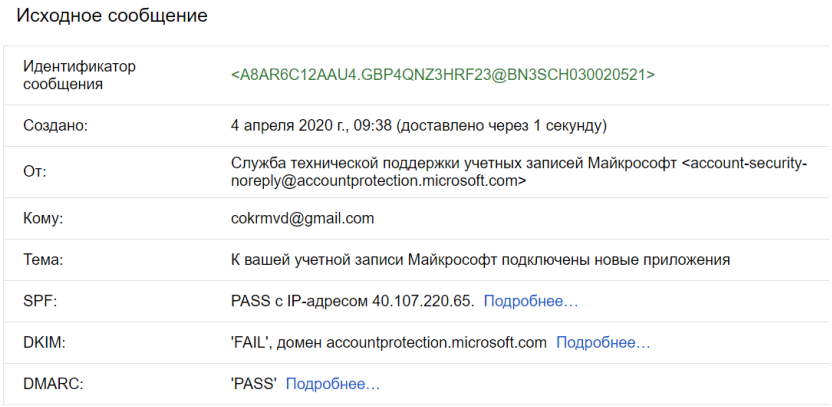

```
Received: from mxfront3o.mail.yandex.net (localhost [127.0.0.1])
        by mxfront3o.mail.yandex.net with LMTP id InF6OWIYjF-Az6167LW
        for <konradmix@yandex.ru>; Tue, 28 Apr 2020 18:42:19 +0300
Received: from 2ip.ru (2ip.ru [195.201.201.32])
        by mxfront3o.mail.yandex.net (mxfront/Yandex) with ESMTP id PZmTmThdJ9-gJkGhcwe;
        Tue, 28 Apr 2020 18:42:19 +0300
```

– Mail.ru.Служебные заготовки.




```
Delivered-To: cokr@mail.ru
Return-path: <no-reply@mirtesen.ru>
Received-SPF: pass (mx49.mail.ru: domain of mirtesen.ru designates 95.131.27.108
Received: from mx1-2.sd37.mtml.ru ([95.131.27.108]:53946)
```

– Google.Почта.Свойства.Еще.Показать оригинал



Исходное сообщение

Идентификатор сообщения	<A8AR6C12AAU4.GBP4QNZ3HRF23@BN3SCH030020521>
Создано:	4 апреля 2020 г., 09:38 (доставлено через 1 секунду)
От:	Служба технической поддержки учетных записей Майкрософт <account-security-noreply@accountprotection.microsoft.com>
Кому:	cokrmvd@gmail.com
Тема:	К вашей учетной записи Майкрософт подключены новые приложения
SPF:	PASS с IP-адресом 40.107.220.65. Подробнее…
DKIM:	'FAIL', домен accountprotection.microsoft.com Подробнее…
DMARC:	'PASS' Подробнее…

Подробную информацию, относящуюся к IP-адресу или доменному имени можно найти на сайте https://2ip.ru.

После подбора сведений, непосредственно характеризующих цель, следует продолжить поиск по связям цели, проанализировать друзей и близких, сообщества и группы по интересам, адреса, автомобили и т.п. Сбор информации в Интернете по конкретной цели можно продолжать до бесконечности, т.к. информационное пространство живет и постоянно пополняется новыми сведениями. Данная статья задает лишь общую модель ведения поиска в Интернете и знакомит читателя с наиболее популярными поисковыми инструментами.

Для дальнейшего совершенствования своих навыков в области интернет-разведки читатель может посетить:

http://iam.ru – персональный сайт одного из ведущих специалистов конкурентной разведки А.И. Масаловича;

http://hrazvedka.ru – блог о разведке в бизнесе и бизнесе как разведке.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Страхов А.А., Анисимова Т.В. Правовые аспекты использования сети Интернет в Российской Федерации // Вестник Московского университета МВД России. 2015. № 11. С. 229–233.

2. Страхов А.А., Анисимова Т.В. Оценка подлинности и достоверности информации в интернет-публикациях // Вестник экономической безопасности. 2016. № 6. С. 129–146.

3. Страхов А.А. Как анализировать интернет-информацию / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 3-й Международной научно-практической конференции (14 октября 2016 г.). – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2017. С. 54–74.

4. Страхов А.А. Социальная инженерия на вооружении у киберпреступности / Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 6-й Международной научно-практической конференции (17 мая 2019 г.). – Белгород: Белгородский юридический институт МВД России имени И. Д. Путилина, 2019. С. 260–264.

УДК 371.311

ОСОБЕННОСТИ ФОРМИРОВАНИЯ АЛГОРИТМИЧЕСКОГО МЫШЛЕНИЯ У КУРСАНТОВ И СЛУШАТЕЛЕЙ

Карпика А.Г.,
кандидат технических наук, доцент;
Лемайкина С.В.
(Ростовский юридический институт МВД России)

Аннотация: статья посвящена вопросу формирования системного подхода к решению профессиональных задач на базе развития алгоритмического мышления у курсантов и слушателей в начальном периоде обучения. Для достижения цели предлагается оптимизировать структуру и содержание дисциплин.

Ключевые слова: алгоритм, мышление, методика, курсант, слушатель, системный подход.

FEATURES OF FORMING ALGORITHMIC THINKING IN CADETS AND STUDENTS

Karpika A.G.,
Candidate of Technical Sciences, Associate Professor;
Lemykina S.V.
(Rostov Law Institute of the MIA of Russia)

Abstract: the article is devoted to the formation of a systematic approach to solving professional problems based on the development of algorithmic thinking in cadets and students in the initial period of training. To achieve this goal, it is proposed to optimize the structure and content of disciplines.

Keywords: algorithm, thinking, methodology, cadet, listener, system approach.

Вызовы, стоящие перед органами внутренних дел, зачастую плохо предсказуемы и отличаются разнонаправленностью. Так, еще в конце 2019 г. проблема пандемии рассматривалась исключительно с точки зрения теории, а вопросы влияния технологий мгновенного распространения информации на массовую аудиторию до 2010 года находились исключительно в плоскости научных разработок и исследований.

Реальность нашего времени такова, что вопрос обучения курсантов и слушателей готовности к тому, «что еще не произошло и, возможно, не произойдет в ближайшее время», достоин отдельного обсуждения вплоть до фор-

мирования соответствующих компетенций и инвестиций, материальных и интеллектуальных, в реализацию этих компетенций.

Основная трудность, с которой сталкивается большинство обучающихся, заключается в приобретенной на этапе получения среднего образования привычке некритично следовать установленным алгоритмам и впоследствии изученным правилам (оформленным нормативными документами). К сожалению, эта система работает исключительно в «мирных» условиях и вызывает замешательство у обучающихся при моделировании абсолютно нестандартной ситуации как на занятии, так и в перспективе служебной деятельности.

В этих условиях во всех отраслях, в том числе и правоохранительных органах, возрастает потребность в сотрудниках, развивших в себе активное комплексное мышление, имеющих прогностический склад ума и способных на этой базе моделировать возможные будущие ситуации. Что необходимо для подготовки сотрудников, обладающих подобными компетенциями? На самом деле, должно быть учтено достаточно много условий и ограничений (объективных и субъективных), но в контексте статьи интерес представляет формирование абстрактного и алгоритмического мышления на этапе обучения курсантов и слушателей.

Формирование нелинейности мышления, предполагающей всестороннее изучение объекта до принятия решения с последующей его корректировкой, несомненно, является необходимым условием (не оформленным ни одной компетенцией) формирования эффективного сотрудника полиции, способного адекватно принимать решения и отвечать за их своевременность и качество.

Одним из известных способов достичь указанного состояния является последовательное формирование алгоритмического мышления, которое позволяет ответить на вопросы, связанные с понятием предпосылок, процессами, вызванными ими, и следствиями возникших процессов независимо от формы исследуемых явлений.

Специфический стиль мышления, такой как алгоритмическое мышление, предполагает заблаговременное формирование не готовых шаблонов действий, а ментальных мыслительных образов – мыслительных схем, содержание которых предоставляет человеку возможность увидеть и осмыслить возникшую проблему целиком, абстрагировавшись от конкретных примеров и несущественных деталей.

При этом алгоритмическое мышление предполагает декомпозицию крупной задачи в отдельные блоки с возможностью дальнейшей стратификации. Подобный алгоритм действий является абстрактным и может быть применен к широкому классу задач, не связанных с конкретной предметной областью. Описанный подход является стандартом для подготовки специалистов в разработке и управлении сложными системами, в том числе и социальными. Кроме этого, алгоритмическое мышление способствует увеличению интеллектуальных способностей личности и его творческого потенциала.

Обучающиеся, особенно сотрудники полиции со стажем практической деятельности и получающие квалификацию «юрист», не всегда понимают, с какой целью они изучают отдельные темы некоторых дисциплин. Так, например, дисциплина «Информатика и информационные технологии в профессио-

нальной деятельности» предполагает изучение тем, в том числе связанных с алгоритмизацией и основами программирования.

Анализ наименования и содержания тем дисциплины позволил изменить наименование тем с целью оптимизации ее содержания и повышения мотивации обучающихся. Изначально предполагалось уменьшение количества тем, обновление их содержания и смещение акцента в сторону понимания целей дисциплины обучающимися, в том числе и в вопросе формирования алгоритмического стиля мышления. Ниже приведена сравнительная таблица тематических планов 2019-2020 и 2020-2021 учебных годов. Вопрос, безусловно, дискуссионный.

Таблица 1. Тематические планы 2019-2020 и 2020-2021 учебные годы

<table>
<tr><td></td><td>2019-2020 учебный год</td><td>2020-2021 учебный год</td></tr>
<tr><td>№ п/п</td><td colspan="2">Наименование разделов и тем</td></tr>
<tr><td colspan="2">Раздел I. Введение в профессиональные информационные технологии</td><td></td></tr>
<tr><td>1</td><td>Тема 1. Базовые понятия и технические аспекты информационных технологий</td><td rowspan="3">Тема 1. Фундаментальные основы компьютерной обработки информации</td></tr>
<tr><td>2</td><td>Тема 2. Вычислительные основы информационных технологий</td></tr>
<tr><td>3</td><td>Тема 3. Программное обеспечение информационных технологий</td></tr>
<tr><td colspan="2">Раздел II. Базовые офисные технологии в профессиональной деятельности (ч. 1)</td><td></td></tr>
<tr><td>4</td><td>Тема 4. Обработка текстовых электронных документов и основы электронного документооборота в профессиональной деятельности</td><td>Тема 2. Базовые технологии электронного документооборота.</td></tr>
<tr><td colspan="2">Раздел II. Базовые офисные технологии в профессиональной деятельности (ч. 2)</td><td></td></tr>
<tr><td>5</td><td>Тема 5. Обработка табличных электронных документов</td><td>Тема 3. Базовые технологии обработки числовых данных</td></tr>
<tr><td>6</td><td>Тема 6. Основы алгоритмизации и программирования</td><td>Тема 6. Основы технологии алгоритмического мышления</td></tr>
<tr><td>7</td><td>Тема 7. Проектирование и обработка баз данных</td><td>Тема 4. Технологии хранения данных</td></tr>
</table>

	2019-2020 учебный год	2020-2021 учебный год
№ п/п	Наименование разделов и тем	
Раздел III. Телекоммуникационные технологии в профессиональной деятельности		
8	Тема 8. Основы телекоммуникационных технологий и локальные сети в профессиональной деятельности	Тема 5. Технологии обмена информацией в локальной и глобальной сети
9	Тема 9. Интернет-технологии	
10	Тема 10. Информационно-аналитическое обеспечение деятельности МВД России	Тема 7. Информационно-аналитическое обеспечение деятельности МВД России
Раздел IV. Мультимедийные технологии в профессиональной деятельности		
11	Тема 11. Основы компьютерной графики в профессиональной деятельности	Тема 8. Основы технологии компьютерной графики
12	Тема 12. Аудио- и видеотехнологии в профессиональной деятельности	Тема 9. Основы Мультимедиа-, кросс- и геоинформационных технологий.
Раздел V. Автоматизированные информационные системы в профессиональной деятельности		
13	Тема 13. Информационные системы сбора, хранения и обработки служебной информации	Тема 10. Информационные системы сбора, хранения и обработки служебной информации
14	Тема 14. Документальные и фактографические информационные системы в профессиональной деятельности	
15	Тема 15. Интеллектуальные информационные системы как системы поддержки принятия решений в профессиональной деятельности	
16	Тема 16. Автоматизированные рабочие места сотрудников как узловые центры единого информационного пространства профессиональной деятельности	

Таким образом, разделы удалены, наименование тем унифицировано, при этом общее содержание дисциплины соответствует примерной программе дисциплины. Номера тем в правой части таблицы расположены не по порядку, но они соответствуют реальной последовательности их преподавания. Видно, что наибольшей трансформации подверглись темы 1, 2, 3, 6, 13-16. Они объединены с целью формирования у обучающихся целостной картины соответствующих предметных областей и системного подхода к их изучению: «Принципы построения и функционирования средств обработки информации», «Алгоритмическое мышление», «Профессиональные информационные системы». Каждая из этих областей прямо или косвенно важна для решения рассматриваемой задачи.

Алгоритмический стиль мышления как основа формирования системного подхода к решению профессиональных задач оказывает существенное положительное влияние на качество освоения новых знаний, способствует использованию их на практике, стимулирует синтез новых знаний на базе приобретенного опыта.

Совместно с другими компетенциями обучение алгоритмическому стилю мышления позволит сформировать у курсантов и слушателей следующие умения:

- декомпозировать задачу на подзадачи;
- планировать время начала и окончания этапов решения подзадач («Тайм менеджмент»);
- оценивать эффективность деятельности по результатам каждого этапа («Обратная связь»);
- использовать источники информации для обеспечения информационной поддержки принимаемых решений;
- приобретать новые знания и распространять их внутри группы;
- мыслить нестандартно, предпринимать нелинейные действия, позволяющие сэкономить временной и материальный ресурсы.

Таким образом, способность мыслить точно, при необходимости абстрагируясь от несущественных деталей, является в современном информационном обществе одним из важных признаков общей культуры человека вообще и сотрудника полиции в частности.

УДК 338:004

ЗАРУБЕЖНЫЙ ОПЫТ УСОВЕРШЕНСТВОВАНИЯ ТЕХНОЛОГИЙ МОБИЛЬНОЙ СВЯЗИ И ИХ ПЕРСПЕКТИВЫ РАЗВИТИЯ В РОССИИ

Данилов Р.М.,
кандидат технических наук, доцент
(Дальневосточный юридический институт МВД России)

Аннотация: в статье рассматривается опыт зарубежных стран в развитии пятого и шестого поколений связи, а также перспективы развития технологий мобильной связи в России.

Ключевые слова: связь, сеть Интернет, интеграция поколение связи, скорость передачи данных.

FOREIGN EXPERIENCE IN IMPROVING MOBILE COMMUNICATION TECHNOLOGIES AND THEIR PROSPECTS FOR DEVELOPMENT IN RUSSIA

Danilov R.M.,
Candidate of Technical Sciences, Associate Professor
(Far Eastern law Institute of the MIA of Russia)

Abstract: the article examines the experience of foreign countries in the development of the fifth and sixth generations of communication, as well as the prospects for the development of mobile communication technologies in Russia.

Keywords: communication, Internet network, integration of communication generation, data transfer speed.

Ни для кого не секрет, что количество абонентов, подключенных к Всемирной паутине связи, с каждым годом увеличивается в разы, соответственно, и требования абонентов к скорости передачи данных возрастают. Так как тенденции развития в области связи и телеком-оборудования набирают обороты, планируется серьезно изменить построение сетей и регламенты взаимодействия, что способствует появлению сети пятого поколения (5G), являющейся уже другим этапом развития сетей четвертого поколения (LTE, 4G).

Высокая скорость передачи данных – одно из главных требований к новому поколению мобильной связи. Большое внимание разработчики уделяют улучшению качества связи при одновременном подключении большого количества абонентов. Таким образом, скорость загрузки данных должна быть 1–2 Гбит/с, а количество одновременно подключенных абонентов – до 1 миллиона на квадратный километр. Например, сеть 4G дает возможность подключить всего до 2000 устройств на таком же расстоянии. Вместе с тем сеть 5G

должна иметь более высокую энергетическую эффективность, а беспроводные гаджеты, использующие мобильную сеть, будут дольше держать заряд батареи, что позволит увеличить срок службы батарей устройств до 10 лет.

У сети 5G увеличиваются радиочастоты с единиц до десятков ГГц, что позволяет увеличить пропускную способность канала и дает возможность использовать многоканальность. Все это дает толчок развитию роботизации в системе связи, а именно позволит различным устройствам непрерывно обмениваться данными без участия человека, а это, безусловно, большой рывок в развитии технологий современного общества.

Южная Корея имеет явное превосходство по отношению к другим странам по внедрению сетей 5G. Сеть 5G была протестирована еще на зимней Олимпиаде в Пхенчхане в 2018 году. А уже с 05.04.2019 в Южной Корее всемирно известная компания Samsung выпустила на мировой рынок первый смартфон, поддерживающий 5G связь. Из некоторых источников известно, что уже 10-миллионный Сеул и еще 85 городов страны готовы к скоростям нового поколения. Однако работами по внедрению 5G-сетей занимается не только Южная Корея, он и США, Швейцарии, Китай, а также Япония. Так, Китай уже в 2020 году планирует покрыть страну скоростным мобильным интернетом. Япония не отстает от передовых государств и неожиданно для всех официально объявила о начале работы над запуском сети шестого поколения (6G) [1, с. 34].

На сегодняшний день в мире пользователей сети Интернет принято считать, что ключевой фактор всех известных «ярусов» G — скорость передачи данных: каждое новое поколение имеет более высокую скорость передачи данных, нежели предыдущее.

Сети пятого поколения являются самыми передовыми на сегодняшний день, так как имеют самую высокую скорость передачи данных 35 Гбит/с. А вот уже сеть 6G, которую разрабатывают японцы, будет иметь самую максимальную скорость из всех поколений связи от 100 Гбит/с до 1 Тбит/с [1, с. 56].

Только с высокой скоростью можно поддерживать технологию виртуальной реальности и передавать большие видеопотоки, а также видео с высоким разрешением. Помимо всего прочего, высокая скорость передачи данных поможет поддержать современные сервисы с той же виртуальной и дополненной реальностью. Однако такого прежде не было, а показатели, которые достигнуты на сегодняшний день, считали предельными, данных показателей удалось добиться с помощью применения сложных алгоритмов детектирования и декодирования сигнала. Показатели, заявленные сейчас просто колоссальны в сравнении с предыдущими. Стоит заметить, что на данный момент скорости передачи данных настолько высокие, текущее поколение сотовой связи на пике запредельных возможностей, то есть, если японцы добьются желаемого результата, то, скорее всего, это будет максимально возможная скорость передачи данных и увеличить ее уже вряд ли получится.

Конечно, японцы громко заявили о запуске сети шестого поколения, но как таковой концепции еще даже не существует, пока что только ведутся раздумья, как создать эту сеть. Но сомнений нет, что новые требования все-таки появятся в ближайшем будущем. Например, чтобы повысить скорость передачи

данных, необходимо делать меньше соты, чтобы расстояние между передатчиками было меньше, а сеть – более плотной [2, с. 12]. Безусловно, сама концепция создания построения этой сети еще будет дорабатываться, а сама сеть 6G будет усовершенствоваться.

На данный момент под руководством самого министра Министерство внутренних дел и коммуникаций Японии формирует экспертное сообщество для подготовки внедрения новой технологии. В рабочую группу уже приглашены ученые из Токийского университета, а также представители технологических гигантов Nippon Telegraph and Telephone и Toshiba [2, с. 76].

Для того, чтобы внедрить и тестировать, Токио готово инвестировать 2,03 миллиарда долларов, также под 6G-связь пообещали создать новые радиочастоты. Возможно, низкие темпы внедрения в стране 5G-связи подтолкнули японские власти на такой шаг. Вероятно, Япония хочет занять ведущее место в развитии следующего этапа технологий связи.

Сети связи 6G будут использовать терагерцевый и субтерагерцевый диапазоны частот и обеспечивать ускорение передачи данных, чем в сетях пятого поколения, работающих в гигагерцевом диапазоне. Вполне возможно, управление сетями будет роботизировано, а на базовых станциях будут использовать радиофотонные цифровые антенные решетки [1, с. 33].

Но усилия Японии не беспочвенны, ведь еще одна ведущая экономика мира – Китай борется за первенство в усовершенствовании скорости передачи данных. Так, в середине января 2020 года Китай вывел коммерческий спутник 5G-связи Yinhe-1 на низкую околоземную орбиту [3, с. 45]. На борту находился спутник Yinhe-1 весом 227 кг, принадлежащий пекинской коммуникационной компании GalaxySpace. Ожидается, что Yinhe-1 будет проводить тестирование связи, однако подробности не уточняются. Galaxy Space планирует создание ведущей в мире широкополосной спутниковой группировки на низкой орбите (LEO) с глобальным покрытием сетью связи 5G. Спутник Yinhe-1 обеспечивает пропускную способность до 10 Гбит/с [3, с. 66].

Как прогнозирует GSMA Intelligence, к 2025 году США, Китай, Южная Корея и Япония станут лидерами по проникновению пятого поколения связи, а Европа и Россия заметно отстанут.

GSMA Intelligence полагает, что в Корее 66% мобильных подключений страны (41 млн) – это подключения к сети 5G, это означает, что Корея будет абсолютным мировым лидером. К 2025 году большая часть всех подключений в США и Японии будут подключения к 5G – 188 млн и 98 млн соответственно. Китай по проникновению сети 5G займет четвертую строчку с 36%, или 600 млн подключений, Европа – на пятом с 30%, или 209 млн подключений. Средний показатель к 2025 году по миру – 18% (1570 млн) подключений. России GSMA Intelligence сулит 19%, или 46 млн подключений к сети 5G в 2025 году [3, с. 69].

Россия закрепила внедрение технологии 5G на уровне государственного стратегического планирования. Федеральный проект «Информационная инфраструктура» национальной программы «Цифровая экономика» к 2024 году наце-

лен обеспечить устойчивым покрытием 5G все крупные города с населением более 1 млн человек.

Сейчас в России заметен некий всплеск, использование сетей LTE 1 по-прежнему продолжает активно эксплуатироваться. Именно от трафика Интернета идет основной поток доходов у большинства наших операторов. В связи с чем им выгодны возможности расширения, ведь они станут доступны с внедрением в стране 5G сети. А на рынке связи идет активная борьба за преобладание.

Так как в России нет свободного радиочастотного ресурса, то это может значительно затруднить развитие 5G сети. Некоторые эксперты говорят, так называемый золотой диапазон от 3,4 до 3,8 ГГц считается самым перспективным для развертывания сетей пятого поколения, поскольку для работы именно в этой полосе в настоящее время создано наибольшее количество абонентских устройств. У нас этот диапазон занят средствами связи различного назначения, в том числе специального [4, с. 20].

Старт активного коммерческого строительства и запуска сетей в 2020–2021 годах.

Доступные РЧ-ресурсы для каждого из операторов:

- 20 МГц в диапазоне 700 МГц;
- 60 МГц в диапазоне 3,4–3,8 ГГц;
- 400 МГц в диапазоне > 24 ГГц.

Оператору единой национальной сети доступно для использования консолидировано:

- 80 МГц в диапазоне 700 МГц;
- 240 МГц в диапазоне 3,4–3,8 ГГц;
- 1600 МГц в диапазоне > 24 ГГц.

К 2027 году достигается 95% покрытия населения сетью 5G в городах с использованием спектра 3,4–3,8 ГГц, в сельской местности и за городом – с использованием 700 МГц, покрытие всех федеральных трасс и порядка 85–90% остальных дорог – с использованием 700 МГц минимум двумя мобильными операторами. Покрытие с использованием 700 МГц подразумевает суммарную фактическую скорость / пропускную способность 5G 70–100 Мбит/с на сектор от базовой станции до абонента (downlink) и до 40 Мбит/с – от абонента до базовой станции при агрегации радиоканалов двух операторов.

Покрытие крупных городов Российской Федерации в 2023 году. Сеть обеспечивает уровень надежности 99,999%. Где необходимо, используется транспортная сеть на базе ВОЛС, а где необходимо и соответствует требуемому уровню качества услуг – радиорелейные линии связи. Курс доллара для моделирования затрат на приобретение оборудования – 78–80 рублей за долл. США. Средняя стоимость базовой станции в трехсекторной конфигурации с Massive MIMO и необходимым ПО – 30 тысяч долларов США.

Моделирование затрат осуществлялось в разрезе двух сценариев роста трафика, приведенных выше, один из которых предусматривал рост в 12 раз к 2027 году, второй – в 21 раз. Не учитываются сценарии использования 5G для строительства сетей фиксированного ШПД, затраты на строительство БС для покрытия внутри зданий и под отдельные клиентские проекты, а также фемтосот.

Оценки по уплотнению сети даны для сценария с более высоким прогнозным уровнем трафика (х21 раз к 2027 г.) в диапазоне:

Max – достижение максимального охвата сетей в городах на базе 3,4–3,8 ГГц без учета возможностей операторов по оптимизации инвестиций в покрытие за счет использования 4.9G или 5G на низких частотах.

Min – с учетом таких возможностей.

Прогнозируется, что более 150 млн абонентов станут пользователями сетей 5G, это значительно больше чем современный 4G. Предполагаемый доход операторов мобильной широкополосной связи достигнет 247 млрд дол. США к 2025 году. Окончательно утвердить стандарт 5G планируется уже в 2020 году [2, с. 79].

Сеть пятого поколения – самая современная сеть, которая не только экологически читая, так и высокоскоростная, но и надежная технология, доступная каждому. Внедрение данного поколения сети произведет не только прорыв в темпах роста потребления трафика и количества конечных потребителей, но и экономический бум.

Основная цель стандарта 5G – обеспечить широким доступом в сеть Интернет каждого абонента в любом месте и в любое время. Второе направление – обеспечение бесперебойной работы удаленного оборудования, третье – использование в автомобильной тематике у «подключенных автомобилей». Четвертой целью стандарта станет медиа-контент, а пятой – более тесная интеграция между человечеством и Интернетом вещей [1, с. 109].

Разбитие сети на сегменты, которые предназначены для каждой цели отдельно, является принципиально важным моментом «пятого поколения». Так, например, рабочий компьютер не требует высокой скорости Интернета в работе, а вот уже просмотр фильма или загрузка какой-либо программы, безусловно, потребует немалых ресурсов. В связи с чем увеличится спрос на современные высокотехнологичные гаджеты.

Благодаря технологиям 5G общество сделает большой рывок вперед в развитии экономики всего мира, а это значит, что мы сможем оснащать датчиками и сенсорами станки, цеха и целые предприятия, реализуя концепцию цифровых фабрик, и еще много другое, о чем сейчас мы даже не догадываемся.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бабков В.Ю., Голант Г.З., Русаков А.В. Системы мобильной связи: термины и определения. – Москва: ГЛТ, 2018. – 158 с.

2. Бабков В.Ю. Сотовые системы мобильной радиосвязи. – Санкт-Петербург: BHV, 2019. – 432 с.

3. Берлин А.Н. Цифровые сотовые системы связи. – Москва: Эко-Трендз, 2019. – 296 с.

4. Берлин А.Н. Сотовые системы связи: учебное пособие. – Москва: Бином. ЛЗ, ИНТУИТ, 2019. – 360 с.

5. Михайлов В.Ф., Мошкин В.Н., Брагин И.В. Космические системы связи: учебное пособие. – Санкт-Петербург: ГУАП, 2019. – 174 с.

УДК 343(575+14) 004.7

ПОЛУЧЕНИЕ ИНФОРМАЦИИ В ИНТЕРЕСАХ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ ДАННЫХ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Молоков В.В.,
кандидат технических наук, доцент
(Сибирский юридический институт МВД России)

Аннотация: в статье рассматривается проблема криптографического закрытия информации в телекоммуникационных сетях в контексте возможности её получения правоохранительными органами в интересах раскрытия и расследования преступлений. Приводятся основания для законного получения криминалистически значимой информации и варианты доступа к ней на ресурсах сети Интернет.

Ключевые слова: Интернет, интернет-коммуникации, криптография, криминалистически значимая информация, раскрытие и расследование преступлений.

GETTING INFORMATION IN THE INTERESTS OF THE CRIME DISCLOSURE AND INVESTIGATION UNDER CONDITIONS OF DATA ENCRYPTION IN THE TELECOMMUNICATION SYSTEMS

Molokov V.V.,
Candidate of Technical Sciences, Associate Professor
(Siberian Law Institute of the MIA of Russia)

Abstract: this paper considers the problem of the information encryption in the telecommunication networks in the context of the possibility of its receiving by law enforcement agencies in the interests of disclosing and investigating crimes. The basic for legitimately obtaining forensic information and the options for accessing it on Internet resources are given.

Keywords: Internet, Internet communications, cryptography, forensic information, crime disclosure and investigation.

Современная преступность все чаще использует новейшие достижения в области информационно-телекоммуникационных технологий для осуществления криминальных замыслов [1]. Интернет-технологии используются для управления организованным преступным сообществом, с их помощью совершаются мошеннические действия, осуществляется незаконный сбыт наркотиков и оружия, происходит легализация денежных средств, добытых противоправной деятельностью, и т.п. И эта тенденция не случайна, так как развитие

интернет-коммуникаций осуществляется в сторону анонимизации личности пользователя и скрытия передаваемой в каналах связи информации. В этой связи актуальными являются меры противодействия подобного рода преступным проявлениям, успешной реализации которым может способствовать возможность документирования информации, передаваемой по телекоммуникационным каналам сети Интернет.

Вопрос анонимности пользователей сети Интернет не раз обсуждался в многочисленных публикациях [2]. В основе этого лежат два механизма обезличивания коммутируемого сетевого устройства – это скрытие IP-адреса и закрытие передаваемой информации средствами криптографии. Для этого используются вполне легальные средства, реализующие одну из обозначенных технологий либо представляющие их гибридное сочетание. Тому примеры: анонимные прокси-сервера, VPN-сервисы, SSH-туннели, децентрализованные сети (Tor, P2P и т.п.). На волне всеобщей конфиденциальности наибольшую популярность завоевали интернет-мессенджеры, открыто декларирующие сквозное шифрование, больше известное как end-to-end. Суть данного метода заключается в организации закрытого взаимодействия между участниками информационного обмена без разглашения данных третьим лицам, включая организаторов сервиса. Поэтому так популярны раскрученные мессенджеры Viber, WhatsApp, Telegram. Не секрет, что на каналах Telegram открыто работают площадки по торговле наркотическими средствами и психотропными веществами.

Современную ситуацию на рынке интернет-коммуникаций можно охарактеризовать тотальным господством криптографии. В чем секрет применения сквозного шифрования? Таким вопросом могут задаться большинство рядовых пользователей Интернета. Скорее, дело не в секрете, а в популярности. Классический алгоритм Диффи-Хеллмана использует систему открытых ключей для генерации закрытого симметричного ключа на противоположных сторонах информационного обмена. И такой механизм не компрометирует секретный ключ. Однако существуют некоторые уязвимости оригинального алгоритма Диффи-Хеллмана, например, атака «человек посередине». Поэтому разработано немало модификаций алгоритма, которые лишены данной уязвимости. На текущий момент можно утверждать, что сам принцип сквозного шифрования является достаточно криптостойким и надежно защищает от перехвата данных в канале связи.

Складывается ситуация, что с повышением уровня защиты информации, хранящейся и обрабатываемой в телекоммуникационных системах, растет степень ее конфиденциальности и анонимности. Безусловно, такая тенденция в условиях цифровизации экономических и иных общественных отношений является предпочтительной и оправданной. Однако, как было обозначено ранее, преступность все чаще использует возможности современных средств сетевой коммуникации, зачастую опережая в технической и технологической оснащенности правоохранительные органы.

Таким образом, для успешного противодействия преступлениям, совершаемым с использованием сети Интернет, необходимы мероприятия, связанные с получением значимой в интересах раскрытия и расследования преступлений инфор-

мации. Обозначим, какими возможностями обладают правоохранительные органы для осуществления документирования фактов преступной деятельности.

Во-первых, в соответствии со ст. 64 Федерального закона № 126-ФЗ «О связи» операторы связи обязаны хранить на территории Российской Федерации данные о фактах передачи информации в течение 3 лет, а сами сообщения и иные пересылаемые данные – в течение 6 месяцев. Это позволяет правоохранительным органам в законодательном порядке запрашивать необходимую информацию у интернет-провайдеров и интернет-компаний, осуществляющих свою деятельность на территории Российской Федерации.

Во-вторых, согласно тому же Закону «О связи» операторы связи должны быть оснащены средствами обеспечения оперативно-розыскных мероприятий. Данные средства позволяют субъектам оперативно-розыскной деятельности осуществлять снятие оперативно значимой информации. Обработка передаваемой по телекоммуникационным каналам информации осуществляется с использованием технологий глубокого анализа трафика, позволяя выделять данные отдельных приложений и абонентов сети Интернет. Вопросы получения оперативно значимой информации в сети Интернет неоднократно обсуждались в контексте противодействия преступлениям в сфере незаконного оборота наркотиков [3].

В-третьих, в связи с принятием Федерального закона от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», больше известного как Закон «О безопасном Интернете», появилась возможность оперативного и эффективного блокирования ресурсов сети Интернет, распространяющих противоправный контент. То есть, операторы связи и интернет-компании, не соблюдающие законодательство Российской Федерации, могут быть блокированы на территории нашей страны.

Получается, что законодательно и технически имеются возможности для получения оперативно и криминалистически значимой информации. Однако это может касаться открытых данных, представленных в виде, удобном для их восприятия и документирования. Имеются проблемы с информацией, закрытой криптографически без возможности расшифровки.

В этих условиях необходимо исходить из уязвимостей, которые обнаруживаются в самих механизмах передачи и трансформации обрабатываемой посредством компьютерных средств информации.

Во-первых, нет необходимости в перехвате шифрованной информации, размещаемой на серверах интернет-компаний, социальных сетей и иных сервисов. Открытую информацию можно законно запрашивать непосредственно у них самих.

Во-вторых, принцип сквозного шифрования в интернет-мессенджерах декларируется исключительно самими разработчиками систем коммуникаций. Непосредственно проверить программный алгоритм на наличие бэкдоров ввиду закрытости исходного кода не представляется возможным. Также странно работает механизм сквозного шифрования на нескольких устройствах, связанных с одной учетной записью. Процесс считывания защищенного кода происходит

однократно, а в дальнейшем передача сообщений дублируется на все устройства. Если постоянно используется один ключ, то это компрометирует его, если сеансовые ключи меняются, то ими управляют. Что также наводит на мысль о необходимости работы по предоставлению значимой информации непосредственно с операторами связи интернет-коммуникаций.

В-третьих, компании, оказывающие услуги связи на территории Российской Федерации, должны соблюдать российские законы, иначе их деятельность может быть ограничена. Соответственно, встает вопрос, как обеспечивается конфиденциальность от правоохранительных органов и специальных служб государства. Значит, необходимо контактировать с такими интернет-компаниями.

В-четвертых, электронное взаимодействие участников пересылки сообщений осуществляется компьютерными устройствами, которые работают с известными и популярными операционными системами типа iOS и Android. При этом сами системы создают резервные копии приложений и данных, сохраняя их на своих облачных серверах. Соответственно, вопрос доступа к информации можно решать через администрации компаний разработчиков операционных систем. Не исключением являются и сами мессенджеры, создающие резервные копии сообщений.

Анализируя представленные доводы, можно сделать выводы относительно предположения, что использование интернет-мессенджерами принципа сквозного шифрования не является безупречным с точки зрения обеспечения полной конфиденциальности сообщений. Правоохранительным органам необходимо в рамках существующего законодательства проводить целенаправленную работу с интернет-компаниями, осуществляющими свою деятельность на территории Российской Федерации, по получению оперативно и криминалистически значимой информации в интересах раскрытия и расследования преступлений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Урбан В.В. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей: общая характеристика и уголовно-процессуальные меры по их противодействию // Вестник Восточно-Сибирского института МВД России. 2019. № 1 (88). С. 55–63.

2. Молоков В.В. Средства противодействия раскрытию преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием сети Интернет / Национальный и международный уровни противодействия наркоугрозе и взаимодействие в сфере реабилитации и ресоциализации наркопотребителей: материалы XVIII международной научно-практической конференции. – Красноярск: СибЮИ ФСКН России, 2015. Ч. 2. С. 56–60.

3. Молоков В.В. Программно-технические системы получения оперативно значимой информации в телекоммуникационных каналах сети Интернет / Актуальные проблемы борьбы с преступностью: вопросы теории и практики: материалы XXI международной научно-практической конференции: в 2-х ч. – Красноярск: СибЮИ МВД России, 2018. Ч. 2. С. 108–110.

УДК 004.382.6

ИССЛЕДОВАНИЕ И ОБОСНОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ «ТОНКИЙ КЛИЕНТ» ДЛЯ ОРГАНИЗАЦИИ ПРОЦЕССА ТЕРМИНАЛЬНОГО ДОСТУПА В УЧЕБНЫХ КЛАССАХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ

Черкасов Р.И.,
кандидат технических наук;
Куриленко Ю.А.,
кандидат юридических наук
(Московский университет МВД им. В.Я. Кикотя);
Деркачев И.С.,
кандидат технических наук
(ФКУ НПО «Специальная техника и связь» МВД России)

Аннотация: в статье рассматриваются вопросы, касающиеся анализа использования технологии «тонкий клиент» в правоохранительных структурах различных государств. Отдельное внимание уделено рассмотрению вопроса внедрения технологии «тонкий клиент» в автоматизированных системы управления органов внутренних дел России.

Ключевые слова: компьютер, терминал, сеть, интернет, система, топология, автоматизация, доступ.

RESEARCH AND JUSTIFICATION OF THE POSSIBILITY OF APPLYING THE THIN CLIENT TECHNOLOGY FOR ORGANIZING THE TERMINAL ACCESS PROCESS IN THE EDUCATIONAL CLASSES OF EDUCATIONAL ORGANIZATIONS OF THE MIA OF RUSSIA

Cherkasov R.I.,
Candidate of Technical Sciences;
Kurilenko Yu.A.,
Candidate of Law
(Kikot Moscow University of the MIA of Russia);
Derkachev I.S.,
Candidate of Technical Sciences
(FKU NPO «Special equipment and communications» of the MIA of Russia)

Abstract: the article discusses issues related to the analysis of the use of thin client technology in law enforcement agencies of various states. Special attention is paid to the consideration of the implementation of the thin client technology in the automated management system of the internal affairs bodies of Russia.

Keywords: computer, terminal, network, Internet, system, topology, automation, access.

В современном мире наиболее важным направлением комплексной системной автоматизации различных сфер деятельности можно считать создание объединенного информационного пространства со взаимодействующими субъектами. Для решения данной задачи в рамках реализации программ создания автоматизированных систем управления МВД России наиболее важное значение имеет информационное взаимодействие комплексов средств автоматизации, созданных различными производителями и разработчиками.

Одной из самых важных задач при реализации программ создания автоматизированных систем управления (АСУ) МВД России является разработка и внедрение автоматизированных рабочих мест, которые должны отвечать следующим требованиям:

- оказание информационной поддержки личному составу при решении задач;
- возможность получения сотрудниками доступа ко всем абонентам сети для обмена информацией (ранжированно), а также к информационным базам данных на различных объектах в соответствии с уровнем доступа и приоритетом информации;
- предоставление общего и мандатного доступа сотрудникам к защищаемой информации, ресурсам в соответствии с определенными для них полномочиями, идентификация и аутентификация всех сотрудников и используемых средств, участвующих в приеме и обработке информации;
- предотвращение несанкционированного доступа (НСД) к хранимой и обрабатываемой информации как защищаемой, так и служебной, несанкционированного использования средств ввода и вывода информации;
- наличие средств восстановления информации в случае информационных атак, а также сбоев в работе программных и технических средств;
- антивирусная защита и организация систем обновления антивирусных баз;
- создание и внедрение средств диагностирования и контроля аппаратной составляющей системы;
- низкая стоимость элементов системы, высокие эксплуатационные характеристики с минимальными затратами на использование;
- возможность простой модернизации системы посредством ресурсов подразделения [1, с. 48].

В качестве решения поставленных задач возможно использовать систему АРМ на базе тонкого клиента с использованием терминальных решений.

Эволюция компьютерных сетей в мировом масштабе происходила главным образом благодаря коренным изменениям двух серьезных технологических направлений коммуникаций и вычислительной техники. Первоначально

организация возможности работы с электронными вычислительными машинами (ЭВМ) двух и более пользователей заключалась в загрузке в мэйнфрэйм (основную ЭВМ) некоторого количества заранее подготовленных пакетов данных, которые однако нуждались в обработке.

Начало развития данной технологии было положено в середине 50-х годов XX века. В то время ЭВМ представляли собой громоздкие, занимавшие порой целые здания машины, на обработку информации у которых уходило значительное время. В то время удобству пользователя отводилось крайне малое место в развитии, основное силы были задействованы на решении задач увеличения вычислительной мощности компьютеров.

На следующем этапе за одну из ступеней развития компьютерных сетей можно принять создание самостоятельных терминалов, которые были снабжены собственными устройствами ввода-вывода и работали напрямую с общим центральным компьютером. Работа с такой ЭВМ для пользователя была более удобной, факт параллельного использования вычислительной мощности другими людьми для него мог быть незаметным. Именно это время можно считать периодом появления первых компьютерных систем, принцип работы которых заключался лишь в простом удалении рабочих станций (терминалов) на определенные расстояния.

С момента появления в 70-х годах XX века более компактных компьютеров, внедрение их смогло позволить себе все большее количество предприятий, необходимость использования средств связи между ними при этом возрастала. Именно тогда и начали возникать близкие к современным способы объединения ЭВМ в сеть, а также организация непосредственно компьютерных сетей в масштабах государства [3, с. 68].

В 1969 году произошло знаковое событие: минобороны США приняло решение об объединении всех основных компьютерных узлов в общую сеть. Передача данных осуществлялась между ними по коммутируемому кабелю, а для ее осуществления были созданы специальные операционные системы и огромное количество сложных сопутствующих протоколов. Впоследствии коммутируемые кабели телефонных сетей станут одним из основных способов передачи данных, вплоть до середины 80-х годов [4, с. 25].

Принцип передачи данных по телефонному кабелю при этом уже в первые годы существования компьютерных сетей претерпел определенные изменения. Так, в отличие от непрерывного потока информации, который мог подвергаться искажениям и мешать другим пользователям работать с сетью, как это бывает со стандартным телефонным сигналом, компьютерные данные отправлялись сразу готовыми закрытыми пакетами, что позволяло одновременно использовать один и тот же кабель множеству пользователей.

Говоря о компьютерных сетях, следует отметить, что сейчас есть две основных их разновидности. Под подключением WAN (Wide Area Network) подразумевают объединение удаленных физически друг от друга компьютеров, а также простой выход в Интернет, в то время как LAN – это закрытая сеть, объединяющая физически близкие компьютеры и способная быть полностью изолированной от каких-либо других соединений.

Однако на ранних этапах развития компьютеров нужды в LAN-сетях не было – их заменяли стандартные комплексы из мейнфреймов и терминалов, хотя удаленная передача данных была крайне важным и приоритетным направлением исследований.

Нельзя не отметить роль персональных компьютеров, благодаря общности оборудования и программного обеспечения, используемых в них. начали появляться первые сетевые протоколы. К концу XX века лидирующие позиции среди них занимал протокол Ethernet, который обеспечивал в ранних вариантах исполнения скорость передачи данных в сети до 10 Мбит/с, в современном варианте данный протокол позволяет довести это значение до 1 Гбит/с.

Историю становления и развития компьютерных сетей в мире можно условно разделить на следующие этапы:

1. 1950–1960 годы – первые попытки объединения мейнфрейма с терминалами.
2. 1969 – появление APRANET и использование телефонных сетей для передачи данных.
3. 1970–1974 гг. – возникновение мини-компьютеров и создание вручную настраиваемых локальных сетей.
4. 1974 г. – появление первой стандартизованной сетевой архитектуры IBM SNA, а также стандартизация X.25.
5. 1980–1985 гг. – возникновение персональных компьютеров, появление Интернета в близком к современности виде. Использование стека TCP/IP на всех узлах. Возникновение стандартных технологий локальных сетевых протоколов Ethernet, FDDI, Token Ring.
6. 1986–1987 гг. – старт коммерческого использования Интернета.
7. 1991 г. – появление протокола Web и первых интернет-сайтов.
8. 1995-2000 гг. – развитие Web и массовая популяризация компьютеров.
9. 2000–2010 гг. – использование беспроводных сетей, снижение стоимости передачи единицы информации сразу в несколько тысяч раз [6, с. 12].

Уровень развития современных компьютерных сетей, а также скорости передачи данных в них позволяют серьезно модернизировать либо полностью менять подход к организации работы на персональных компьютерах сотрудников различных подразделений. В некоторых из них, как, к примеру, в компьютерных классах вузов, целесообразна организация терминального доступа к сети типа «клиент–сервер» или тонкий клиент.

Предвестником возникновения технологии «тонкий клиент» можно считать терминалы первых ЭВМ. Как уже было сказано выше, на ранних этапах развития ЭВМ могли занимать целые комнаты, а процесс ввода–вывода информации производился пользователем на внешних «терминалах» – специальных устройствах, которые состояли из клавиатуры, дисплея (на ранних этапах буквенно-цифрового) и устройства для ввода перфокарт. Терминалы соединялись непосредственно с ЭВМ и сами по себе никаких вычислений не выполняли, а только передавали данные для последующей обработки на центральном устройстве и выводили на дисплей полученный результат. Так как объем необходимых вычислений был довольно велик, данная схема организации давала воз-

можность реализовать весь невысокий вычислительный потенциал первых ЭВМ. В то время, когда пользователь терминала обрабатывал полученные результаты, вносил исправления в программу и заново набивал ее на перфокарту, ЭВМ просчитывала задачу, загруженную из другого терминала.

Терминальный режим в современной интерпретации хоть и схож с принципом терминальных клиентов середины XX, но по сути является технологией совершенно отличающейся как от ранних решений, так и от современных локальных сетей.

Терминальный режим рассчитан на то, что на рабочем месте у пользователя в наличии только «фреймы», то есть изображения результата обработки информации. Весь набор операций по обработке информации и ее хранению осуществляются серверами приложений. Доступ клиентов к приложениям реализуется путем подключения к терминальному серверу через один из известных протоколов терминального доступа [7, с. 22].

Главным объектом в процессе организации рабочего места пользователя можно считать специализированный терминал – тонкий клиент. Данный тип устройств разработан для работы в терминальной сети и имеет возможности для работы у обычного персонального компьютера, при этом пользовательские приложения обрабатываются на сервере. Типовая схема построения терминальной сети состоит из терминального сервера, соединенного непосредственно с серверами приложений и системой хранения данных и опосредованно через коммутатор с терминалами пользователей.

В настоящее время технические решения для реализации проектов компьютерных сетей на базе технологии «тонкий клиент» предлагают все основные крупные производители техники.

Терминал Lenovo ThinkCentre M600 для сетей с использованием технологии «тонкий клиент» изготовлен в виде блока, не имеющего внутри подвижных механизмов (не требуется охлаждение), причем блок может быть установлен как с любым монитором, так и с фирменным, во втором варианте блок будет расположен непосредственно на мониторе с тыльной стороны. Производитель заявляет широкие возможности монтажа, включая поддержку стандартных креплений и конфигураций Tiny-in-One. При этом данный блок поддерживает подключение трех мониторов, работает на базе энергетически экономичных процессоров Intel Celeron с интегрированными видеокартами и оснащен всеми современными интерфейсами.

Тонкий клиент HP t530 построен на основе процессоров AMD со встроенным графическим ядром, рассчитан на выполнение вычислительных операций в облачных сервисах, в качестве носителей памяти используются флэш–накопители, отличающиеся высоким быстродействием. Данный терминал оснащен сетевым контроллером GbE, дополнительным адаптером с поддержкой Wi-Fi и Bluetooth с возможностью подключения внешней антенны для усиления принимаемого сигнала. В качестве операционной системы в случаях, когда работа в облачных сервисах по каким-либо причинам не доступна, предлагается HP ThinPro со Smart Zero Core.

Ведущие аналитические организации отмечают, что рынок аппаратного обеспечения, построенного на технологии «тонкий клиент», от года к году показывает устойчивый рост, прирост составляет в среднем до 20% в год и к началу 2020 года 23 млн устройств. В последние годы отмечено несколько важных событий в развитии технологии: сильно возросла способность сетей пропускать данные, в то же время каналы связи, которые соединяют распределенные информационные сети, стали более защищенными; огромное количество ресурсов информации перемещается из отдельных серверов компаний в единые дата-центры, где они хранятся и обрабатываются; ввиду подорожания некоторых аппаратных и программных частей персональных компьютеров возрастает целесообразность использования аппаратных средств на базе технологии «тонкий клиент» с экономической точки зрения [8, с. 12].

Среди крупных производителей компьютерной техники также произошло перераспределение направлений деятельности и пересмотр стратегий на рынке. В недалеком прошлом лидер рынка фирма IBM практически отошла от производства аппаратных комплексов. В сегменте тонких клиентов лидируют такие компании, как HP, Sun Microsystems и Fujitsu Siemens Computers, развитие направления тонких клиентов которых происходит не в последнюю очередь и за счет небольших российских компаний. Более того, рост продаж аппаратных комплексов на базе технологии «тонкий клиент» отмечается на всех развивающихся рынках мира, в их числе Китай, Индия, Бразилия. На данный момент в Российской Федерации аппаратные комплексы в небольших количествах закуплены такими государственными структурами, как Федеральная налоговая служба, Пенсионный фонд Российской Федерации и т.д.

Также стоит отметить, что использование технологии тонкий клиент должно иметь разумно-достаточный вид для недопущения повторения ситуации конца XX века на фоне увеличения количества внедренных терминальных технологий при недостаточной развитости сетей. Тонкие клиенты можно считать массовым, а не нишевым решением. Ведущими аналитиками отмечается тот факт, что практически все процессы в IT–сфере сейчас возможно выполнять посредством данной технологии, разве что кроме приложений САПР (системы автоматизированного проектирования) [9, с. 8].

Из-за роста производства аппаратных средств на технологии «тонкий клиент» в ближайшие годы стоит ожидать серьезного рывка в разработке программ, предназначенных для работы в открытых средах. Этот скачек обусловлен тем, что производители и интеграторы терминальных аппаратных устройств все чаще обращают внимание на нужды конечных пользователей, которым, если верить ведущим исследовательским организациям в сфере IT технологий, необходимы такие показатели, как стабильность и устойчивость работы; простота администрирования; производительность; функциональность; техническая поддержка в процессе эксплуатации. На данный момент заметно, что экологические вопросы пока что никак не мотивируют конечных пользователей и менеджеров, отвечающих за принятие конечных решений, к интеграции аппаратного обеспечения на базе технологии «тонкий клиент». Рассмотрим срав-

нительную экологическую составляющую тонких клиентов и ПК на примере трехфазной модели информационной системы.

Производство аппаратных средств в мире на данный момент рассредоточено, из-за этого зачастую производство персональных компьютеров и терминалов на базе технологии «тонкий клиент» совмещено. В итоге для создания аппаратных средств на базе технологии «тонкий клиент» потенциально требуется меньшее количество затрат на энергию и материалы, снижаются логистические и транспортные затраты (так как физические размеры терминалов меньше персональных компьютеров), происходит удешевление вторичных производственных процессов. По оценке ведущих аналитических организаций, производство терминалов «тонкий клиент» на 60-65% менее затратное, чем производство обычных ПК [10, с. 12].

Один из важнейших аргументов в пользу аппаратного обеспечения построенного на базе технологии «тонкий клиент» – это энергопотребление, данные по этому параметру приведены в таблице 1.

Таблица 1. Сравнение энергопотребления классической схемы локальной сети и сети с использованием «тонкого клиента»

Параметр	Информационная система	
Состав	1000 ПК	1000 тонких клиентов и 100 терминальных серверов
Расход электроэнергии в год, кВт	156000	14560
Платежи за электроэнергию, тыс. рублей (в среднем по России)	321,4	29,99

Для примера в США на данный момент до 1% расхода электроэнергии приходится именно на ПК, с учетом того что эта цифра ежегодно растёт.

Также необходимо отметить, что терминалы «тонкий клиент» имеют высочайший уровень надежности, но даже в случае выхода их из строя замена терминала не потребует привлечения IT-специалиста предприятия. Организация работы с использованием терминалов «тонкий клиент» практически сводит на нет возможность потери данных.

На данный момент масштаб проблемы утилизации слабо изучен, хотя в Германии уже сейчас утилизируется до 2 млн тонн разнообразных электронных устройств ежегодно, из них 120 тыс. тонн – это отходы сферы информационных технологий. Статистические данные наиболее развитых стран свидетельствуют о том, что один из четырех произведенных ПК отправляется в утилизацию сразу после продажи ввиду высокой скорости устаревания электронных компонентов. В данном случае актуальным становится вопрос не только замены ПК терминалами, но и рационального использования массива ПК в общем.

Технологии «тонкий клиент» свойственны ряд отрицательных черт, так как каждый вариант реализации сети имеет сильные и слабые стороны. Однако стоит отметить, что она отвечает серьезным требованиям, предъявляемым в

АСУ МВД России, таким как многоуровневая комплексная зашита информации, предотвращение несанкционированного доступа к хранимой и обрабатываемой информации, наличие средств восстановления информации в случае совершения на систему вирусных атак и сбоев в работе программных и аппаратных средств, информационная поддержка действий сотрудников, централизация управления, мобильность, снижение издержек.

Также к преимуществам данного решения можно отнести максимально полное использование дорогостоящего серверного оборудования, увеличение надежности и защищенности сетей, сокращение расходов на покупку лицензионного программного обеспечения, а также на администрирование системы.

В случае совмещения процессов внедрения данного типа локальной сети с очередным обновлением аппаратных средств компьютерных классов, а именно замены стандартных персональных компьютеров терминалами доступа, будут исключены дополнительные расходы и получена значительная экономия.

Немаловажными также являются факторы пониженного энергопотребления данным вариантом сети и более высокой, по сравнению с сетью из персональных компьютеров, надежностью системы.

Исходя из вышесказанного, можно сделать вывод, что внедрение технологии «тонкий клиент» является обоснованным для решения вопроса оптимизации IT-инфраструктуры. Переход на тонкие клиенты позволяет решить ряд вопросов касательно информационной безопасности, а также обеспечить непрерывность IT-процессов и более эффективно организовать работу в компьютерной сети.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Сулейманова Л.И Автоматизация рабочих мест на базе тонкого клиента // Автоматизация систем управления. 2009. Вып. 16. С. 48–52.

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации 2006. № 12. Ст. 134.

3. Сергеев Р. Тонкие клиенты на пути к массовости // Журнал сетевых решений. 2008. № 4(141). С. 68–72.

4. Соколов И.А., Сергеев И.В. Перспективы использования компьютерной технологии «тонкого клиента» в информационно-телекоммуникационных системах интегрированного типа / Системы и средства информатики. – Москва: Наука, 2001. Вып. 11. С. 24–37.

5. Карпухин Е.О., Мазепа Р.Б. Использование тонких клиентов с ARM архитектурой и вычислительным кластером при проведении практикума по дисциплинам естественнонаучного и профессионального циклов в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма. 2015. № 25. С. 194–199.

6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. – Санкт-Петербург: Питер, 2010. – 944 с.

7. Ручкин В.Н., Фулин В.А. Архитектура компьютерных сетей. – Санкт-Петербург: Диалог-МИФИ, 2008. – 240 с.

3. Столлингс В. Современные компьютерные сети. – Санкт-Петербург: Питер, 2003. – 783 с.

8. Столлингс В. Компьютерные сети, протоколы и технологии Интернета. – Санкт-Петербург: БХВ-Петербург, 2005. – 832 с.

9. Таненбаум Э. Компьютерные сети. – Санкт-Петербург: Питер, 2007. – 992 с.

10. Куроуз Дж., Росс К. Компьютерные сети. – Санкт-Петербург: Питер, 2004. – 765 с.

УДК 343.132

УГОЛОВНОЕ ДЕЛО В РЕАЛИЯХ ЭЛЕКТРОННОГО СУДОПРОИЗВОДСТВА

Жукова П.Н.,
доктор физико-математических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Золотухина Н.В.,
кандидат юридических наук
(Военный университет Министерства обороны Российской Федерации)

Аннотация: в представленной работе авторы анализируют теоретические, нормативные и практические аспекты внедрения электронного документооборота в процессе предварительного расследования. Изучена следственная и судебная практика с целью выявления пробелов при реализации действующего уголовно-процессуального законодательства, регламентирующего оборот электронных документов, а также сформулированы предложения по его совершенствованию и практическому применению в деятельности следственных подразделений.

Ключевые слова: уголовное судопроизводство, электронные документы, электронный документооборот, электронное уголовное дело.

CRIMINAL CASE IN THE REALITIES OF ELECTRONIC COURT PROCEEDINGS

Zhukova P.N.,
Doctor of Physical and Mathematical Sciences, Associate Professor
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia);
Zolotukhina N.V.,
Candidate of Jurisprudence Sciences
(Russian Defence Ministry military University)

Abstract: the present paper is consider the theoretical, regulatory and practical aspects of the introduction of electronic paperwork during the preliminary investigation stage. Investigative and judicial practice has been analyzed in order to identify gaps in the implementation of the existing criminal procedure legislation regulating the circulation of electronic documents. The proposals are given in the article can used for improvement in the activities of investigative units.

Keywords: criminal proceedings, electronic documents, electronic paperwork, electronic criminal case.

Способы документирования процессуально значимой информации в настоящий момент подвергаются научному и практическому обсуждению, так как наряду с классическими способами (текстовым, техническим, фотографическим, фоноскопическим, аудиовизуальным) стал внедряться электронный способ документирования, законодательное закрепление которого нашло отражение в положениях ч. 6 УПК РФ, где и зафиксированы требования к формуляру – бланкам процессуальных документов.

В ч. 2 ст. 474 УПК РФ «Оформление процессуальных действий и решений на бланках процессуальных документов» указаны способы документирования: типографский, электронный или иной.

Не выдерживает критики упоминание об изготовлении процессуального документа типографским способом (**отметим** – не бланка процессуального документа), поскольку это невозможно – не существует типографского документа, используемого в уголовно-процессуальной деятельности. Следственные подразделения зачастую заказывают в типографии **бланки** процессуальных документов. Но, как видно из содержания указанной статьи, в ней разделены понятия «бланк процессуальных документов» и «процессуальные документы», таким образом здесь закралась явная ошибка, которую необходимо устранить.

Других требований, предъявляемых к бланкам процессуальных документов, уголовно-процессуальное законодательство не содержит.

Деятельность, осуществляемая органами предварительного расследования, связана с принятием решений, как процессуальных, так и организационных, а их качество и эффективность во многом определяется уровнем организации документационного обеспечения.

Хорошо налаженные коммуникационные потоки содействуют обеспечению организационной эффективности, могут перемещаться в горизонтальном или вертикальном направлении. Вертикальное направление, в свою очередь, подразделяется на нисходящее и восходящее.

Обязательным элементом оформления документов является реквизит, виды которых и порядок их проставления на документах определены ведомственными инструкциями по делопроизводству [8]. Состав реквизитов процессуального документа зависит от его вида и назначения, указан в федеральном законодательстве, регламентирующем уголовно-процессуальную деятельность и порядок делопроизводства, и способствует как идентификации документа, так и определению его статуса.

Критически важным для осуществления делопроизводства в электронной форме и определения статуса электронного документа является подтверждение легитимности электронных документов. Так, в п. 1 ст. 6 Федерального закона «Об электронной подписи» [9] закреплено, что «информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью». Таким образом, Федеральными законами «Об информации, информационных технологиях и о защите информации» [5] и «Об электронной подписи» закреплены основы организации делопроизводства в Российской Федерации – документирование информации и использование электронных документов.

Порядок использования электронных документов в уголовном судопроизводстве определён в одноименной ст. 474.1 УПК РФ, в соответствии с которой ходатайство, заявление, жалоба, представление могут быть поданы в суд в форме электронного документа, подписанного электронной подписью, а судебные решения могут быть изготовлены в форме электронного документа, подписанные усиленной квалифицированной электронной подписью, что в соответствии с п. 1 ст. 6 Федерального закона «Об электронной подписи» признается документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Уведомление потерпевшего (или его законного представителя или представителя) по его ходатайству о ходе исполнения приговора может быть направлено в форме электронного документа по электронной почте (ч. 5.1 ст. 42, ч. 5 ст. 313 УПК РФ).

Порядок обращения к исполнению решения суда предусматривает возможность направления судом исполнительного листа судебному приставу-исполнителю в форме электронного документа, подписанного судьёй усиленной квалифицированной электронной подписью.

Электронные носители информации, упоминаются в ч. 4 ст. 81, ст. 81.1, ст. 82 УПК РФ, поименованные наряду с вещественными доказательствами. В ч. 4.1 ст. 164, ст. 164.1, ст. 166 УПК РФ указаны особые правила изъятия электронных носителей информации при производстве следственных действий.

В ч. 7 ст. 185 предусмотрена возможность выемки и осмотра электронных сообщений и иных передаваемых по сетям электросвязи сообщениях по судеб-

ному решению. В настоящий момент остаётся спорным положение о порядке изъятия электронных носителей информации [2, с. 98-99]. В рамках данной работы эта проблема нами исследоваться не будет, так как споров по определению форм материальных носителей здесь не возникает, а только лишь о процессуальном порядке его изъятия как доказательств по уголовному делу.

На территории Северо-Кавказского федерального округа с 2015 по 2019 год апробировался проект «Электронный паспорт уголовного дела», направленный на осуществление своевременного упреждающего ведомственного процессуального контроля хода расследования каждого уголовного дела, находящегося в производстве следователей подразделений на территории СКФО [3, с. 143-146].

Несмотря на развитие корпоративной сети МВД России – интегрированной мультисервисной телекоммуникационной системы органов внутренних дел Российской Федерации, позволяющей соблюдать все требования, предъявляемые к электронным документам и системам электронного документооборота, остаются вопросы информационной безопасности и сохранности персональных данных.

Мы не ставим целью настоящего исследования выступить с аргументами «за» или «против», а предлагаем рассмотреть элементы электронного документооборота, действующие в настоящее время, а также предложить расширить в силу возможных реалий настоящего времени.

В соответствии с инструкцией по организации и осуществлению процессуального контроля в военных следственных органах Следственного комитета Российской Федерации [4, п.п. 4.23.2 «д», 4.24.10 «п», 5.5.6 «б», 5.8.2, 5.10.1] установлен порядок электронного документооборота по пересылке по электронной почте электронных копий докладных записок о результатах осуществления процконтроля.

Кроме этого, электронный документооборот по пересылке электронных копий процессуальных документов активно используется внутри ведомственных подразделений, но редко используется при осуществлении межведомственного взаимодействия. Например, при интервьюировании сотрудников следственных подразделений ими было высказано одобрение законодательного закрепления возможности направления электронных копий процессуальных документов для ведения надзорного производства по уголовному делу.

Одним из направлений, требующих усовершенствования действующего законодательства, является институт уведомления заинтересованных лиц о движении уголовного дела на досудебных стадиях уголовного судопроизводства.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» делопроизводство является единым на всей территории Российской Федерации. Так, п. 1 ст. 11 Закона закрепил возможность установления требований к документированию информации как законодательством Российской Федерации, так и соглашением сторон.

Порядок обмена информацией в электронном виде закреплён в ст. 11.1 рассматриваемого Федерального закона. Так, п. 1 указанной статьи даёт возможность гражданину или организации выбрать, в какой форме они желают

получить ответ от органов государственной власти, органов местного самоуправления или организаций, осуществляющих отдельные публичные полномочия, – «в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе». Пункт 2 той же статьи даёт право организациям и физическим лицам предоставлять документы в указанные органы власти и организации «в форме электронных документов, подписанных электронной подписью».

Положения ч. 2 ст. 188 определяют возможность передачи повестки о вызове лица на допрос с помощью средств связи. Федеральный закон «О связи» [10] среди видов предоставляемых услуг предусматривает рассылку абонентам коротких текстовых сообщений. Возможность использования смс-сообщений предусмотрена и при извещении участников судебного заседания, порядок которого разъяснён в постановлении Пленума Верховного Суда Российской Федерации [6, п. 15.1]. Но, как показывает изучение следственной и судебной практики, смс-сообщения о вызове участников допроса на досудебных стадиях не применяется, несмотря на активное его применение судами различных уровней. Считаем необходимым внедрить в практику следственных подразделений уведомление участников уголовного судопроизводства о приглашении для производства следственных действий путём направления смс-сообщения при наличии их письменного согласия об уведомлении подобным способом.

Внедрение электронного документооборота (с соблюдением режима секретности) должно способствовать повышению эффективности управления, срокам и качеству предварительного расследования за счёт сохранения временного ресурса, упрощения делопроизводства, исполнения поручений и осуществления его контроля.

Целью системы электронного документооборота является не искоренение бумажных документов, а создание эффективной среды управления и функционирования организации. Но нельзя забывать, что деятельность следственных подразделений связана исключительно с «тайной следствия», процессуальной независимостью следователя и потому целесообразно аккуратно подходить к электронному обороту материалов, содержащих сведения, предназначенные исключительно для служебного пользования и содержащие в себе любые виды тайн, охрану которых гарантирует государство.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Двоеносова Г.А. Синергетическая теория документа: автореферат на соискание ученой степени доктора исторических наук. – Москва, 2017.

2. Золотухина Н.В., Жукова П.Н. Проблемные вопросы собирания доказательств по уголовному делу // Вестник Волгоградской академии МВД России. 2019. № 2 (49). С. 94–100.

3. Золотухина Н.В. Качественно или эффективно – к вопросу об оценке деятельности следственных органов / Следственный комитет Российской Федерации: второе десятилетие на службе Отечеству: сборник материалов Между-

народной научно-практической конференции / под общ. ред. А.М. Багмета. – Москва, 2019. С. 143–146.

4. Приказ заместителя Председателя Следственного комитета Российской Федерации – руководителя Главного военного следственного управления от 17.11.2015 № 150 «Об утверждении Инструкции по организации и осуществлению процессуального контроля в военных следственных органах Следственного комитета Российской Федерации» // СПС «КонсультантПлюс».

5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». (ред. от 18.03.2019) // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

6. Постановление Пленума Верховного Суда Российской Федерации от 05.03.2004 № 1 (ред. от 01.06.2017) «О применении судами норм Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс».

7. Основы делопроизводства в органах внутренних дел: учебно-методическое пособие / А.Н. Прокопенко [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2016. – 42 с.

8. Приказ МВД России от 20.06.2012 № 615 «Об утверждении инструкции по делопроизводству в органах внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

9. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс».

10. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СПС «КонсультантПлюс».

УДК 343.72:004.9

НЕКОТОРЫЕ ВОПРОСЫ ОСОБЕННОСТЕЙ ДОКУМЕНТИРОВАНИЯ МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПЕРИОД РАСПРОСТРАНЕНИЯ КОРОНАВИРУСНОЙ ИНФЕКЦИИ

Озеров И.Н.,
кандидат юридических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Озеров К.И.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассмотрены теоретические сведения и практические методики, направленные на повышение эффективности выполнения задач оперативно-служебной деятельности, в том числе оперативно-разыскной, в условиях действия ограничительных мер, связанных с обеспечением санитарно-эпидемиологического благополучия населения.

Ключевые слова: оперативно-разыскная деятельность; ограничительные меры; Covid-19.

SOME QUESTIONS ABOUT THE FEATURES OF DOCUMENTING FRAUD COMMITTED USING INFORMATION AND TELECOMMUNICATIONS TECHNOLOGIES DURING THE SPREAD OF CORONAVIRUS INFECTION

Ozerov I.N.,
Candidate of Law, Associate Professor
(Putilin Belgorod Law Institute of the MIA of Russia);
Ozerov K.I.
(Kikot Moscow University of the MIA of Russia)

Abstract: authors considers theoretical information and practical methods aimed at improving the efficiency of performing tasks of operational and service activities, including operational search, in the conditions of restrictive measures related to ensuring the sanitary and epidemiological well-being of the population.

Keywords: operational search activities; restrictive measures; Covid-19.

С первых дней самоизоляции многие эксперты предрекали и рост преступности, и изменение её структуры. Говорили о снижении числа карманных краж из-за того, что людей в транспорте стало меньше, а театры и другие увеселительные заведения (традиционные места работы «щипачей» и «ширмачей») закрылись. Предрекали нападения на граждан из-за продуктов, массовые драки,

в том числе на межнациональной почве, а также рост бытового насилия. Отмечали, что будет увеличиваться количество мошеннических преступлений, в частности компьютерных. Некоторые прогнозы были сомнительными, другие – авторитетными, но все опрошенные специалисты сходились во мнениях [1].

15 апреля 2020 года МВД России выступило с заявлением [2], в котором утверждалось: «обстановка контролируется, число зарегистрированных убийств и покушений на убийства сократилось на 4,9%, умышленных причинений тяжкого вреда здоровью – на 3,3%. Значительно меньше зафиксировано разбоев – на 22,4% и грабежей – на 8,4%. Отмечено снижение количества фактов присвоения или растраты – на 1,7% и умышленных поджогов – на 1,5%». В январе – марте 2020 года зарегистрировано 510,5 тыс. преступлений, или на 4,0% больше, чем за аналогичный период прошлого года.

И только в самом конце скромно упоминалось, что общее число зарегистрированных преступлений выросло на четыре процента. Тем не менее завершалось заявление словами: «Призываем представителей СМИ при подготовке материалов опираться на объективные показатели официальной статистики и не доверять сомнительным источникам информации» [2].

В тот же день ежемесячный анализ опубликовала Генеральная прокуратура Российской Федерации: «В январе-марте 2020 года в Российской Федерации зарегистрировано 510 510 преступлений, что на 19 590 больше, чем за аналогичный период прошлого года (+4%). В целом по России удельный вес тяжких и особо тяжких преступлений в числе всех зарегистрированных преступлений составляет 27,8% (141 847; 2019 год – 127 169; +11,5%). Количество тяжких преступлений увеличилось на 14,2%. Число зарегистрированных в отчетном периоде особо тяжких преступлений по сравнению с аналогичным периодом прошлого года увеличилось на 3%». На 83,9%, то есть почти вдвое, возросло число преступлений, «совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации», то есть тех самых компьютерных краж и мошенничеств (в цифрах: 101 537). А также зарегистрирован рост террористических (на 13,7%, с 482 до 548) и экстремистских (на 40,9%, с 149 до 210) преступлений [1]. Сегодня вопрос об усилении карантинных ограничений и возвращении режима самоизоляции постоянно обсуждается в нашем обществе. Постоянно принимаются определенные меры организационно-управленческого и рекомендательного характера, в связи с чем задачи самосохранения человека в процессе его производственной и служебной деятельности становятся очень злободневными. Насчитывается более двух тысяч профессий, сопряженных с опасностью быть подвергнутым заражению. В этом случае экономическая, социальная или правоохранительная деятельность неизменно связана с ней. В этих условиях важное значение приобретает использование всех возможностей оперативно-разыскной деятельности, особенно по документированию преступлений, совершаемых с использованием компьютерных телекоммуникаций. Исходя из того, что одной из основных целей осуществления оперативно-разыскной деятельности (ст. 1 Федерального закона «Об оперативно-розыскной деятельности») является защита жизни и здоровья граждан, общества и государства, требуется поиск новых возможно-

стей борьбы с преступностью, в том числе в сложившейся обстановке, при распространении коронавирусной инфекции и вводимых ограничительных мерах.

Этот поиск новых методов, по своей сути, направлен на совершенствование оперативно-разыскной деятельности. Однако он связан с риском как категорией прогнозируемого допущения определённых сопутствующих решению правоохранительных задач негативных последствий.

Ситуация риска в процессе правоприменения возникает при объективно существующей неопределенности. Она выражается в том, что для достижения стоящих перед правоприменителем целей, например, реализация обеспечения субъективного права гражданина, раскрытие преступления или решение вопросов, имеет глобальный характер [3]. Как известно, возник ажиотажный спрос на продукты из-за коронавирусной инфекции. Возросшую нагрузку стали ощущать и российские магазины. Волнение людей было понятно, но необоснованно. Но этим не преминули воспользоваться недобропорядочные граждане. И тут на первые позиции, наряду с другими органами исполнительной власти, вышла правоприменительная деятельность работников оперативных подразделений, напрямую соприкасающихся с криминальным элементом.

Оперативно-разыскная деятельность возникла и существует с целью удовлетворения потребности общества в борьбе с преступностью. Объективная необходимость в оперативно-разыскной деятельности как социальной ценности определяется закономерностями борьбы с преступностью в современных условиях. Во-первых, общественное и техническое развитие общества не позволяет решить задачу борьбы с преступностью исключительно профилактическими и уголовно-правовыми, уголовно-процессуальными средствами, во-вторых, тайный характер действий преступников и закономерности образования информации о лицах, замышляющих и совершающих преступления, делают необходимым применение негласных сил, средств и методов.

Необходимость оперативно-разыскной деятельности выражается в решении задач по раскрытию преступлений, а также вытекает из проявления таких черт преступности, как замаскированный характер значительной части преступлений, наличие активно действующих опытных преступников, хорошо осведомлённых о методах оперативной работы, применение ими тайных способов подготовки, совершения и сокрытия преступлений, различных ухищрений, приемов противодействия, своего рода разведки, контрнаблюдения и т.п. [4].

Сюда же можно отнести рост организованности и повышение преступного профессионализма, характеризующегося устойчивым рецидивом, превращением преступной деятельности в регулярный источник существования, наличием преступных сообществ с замкнутой законспирированной структурой со своими правилами поведения, установками, распределением ролей при совершении преступлений, использованием современной техники [5].

Скрытый характер неочевидных преступлений, организованность и профессионализм преступников, их, по существу, открытое противостояние правоохранительным органам и органам внутренних дел в первую очередь определяют объективную необходимость использования специальных средств и методов, нередко связанных с риском, направленных на выявление преступных на-

мерений и совершенных преступлений, участников преступлений, фактических данных, имеющих доказательственную перспективу.

Однако нельзя забывать как бы о вынужденном, с точки зрения уголовно-правового института, характере оперативно-разыскной деятельности, её обусловленности необходимостью адекватного противодействия негласным, конспиративным формам, методам отбора и проверки информации, которые в современных условиях всё более активно используются в сфере экономического шпионажа, профессиональной преступности, наркобизнеса, международного терроризма, политического экстремизма и т.д. Причём криминогенная сфера применения конспиративных форм и методов отличается тенденцией к расширению, особенно в условиях экономического кризиса и политической нестабильности в стране. Если учесть, что возрастают техническая оснащённость и тактическая изощрённость в применении средств конспирации для сокрытия разведывательно-подрывной и преступной деятельности, а в арсеналах спецслужб, преступных сообществ используются новейшие достижения в области микроэлектроники, компьютерной техники, лазерной физики и т.п., вплоть до космических систем связи и наблюдения, применяемых в сочетании с агентурными методами. Очень трудно возразить против использования адекватных по своему характеру форм и методов, средств оперативного противодействия со стороны отечественных специальных служб и правоохранительных органов – субъектов ОРД. При этом осуществление оперативно-разыскных мер позволяет специально уполномоченным на это органам государства и должностным лицам как можно раньше вмешиваться в развитие событий, ведущих к преступлению, предотвратить наступление общественно опасных последствий [6].

При этом очень серьезная проблема для оперативно-разыскной деятельности – это правомерность, поскольку она является неотъемлемым элементом оперативно-разыскной деятельности и необходимо соблюдать определенный механизм, регулирующий правовой аспект ее проявления. Правомерность определяется оптимальным сочетанием точного следования нормам законности и мер, регламентирующих и обеспечивающих возможность идти на обоснованный риск. Критерием такой обоснованности выступает право, которое закрепляет содержание оперативно-разыскной деятельности, устанавливает задачи, принципы, функции, полномочия, ответственность, а также совокупность ряда показателей – количественных, качественных социально-экономических, уголовно-правовых, нравственно-политических и ряда других.

Нельзя сказать, что данные вопросы в полной мере охватывают все проблемы оперативно-разыскной деятельности в условиях действия ограничительных мер, направленных на обеспечение санитарно-эпидемиологического благополучия населения.

Дифференциацию проблем оперативно-розыскной деятельности в условиях действия ограничительных мер, направленных на обеспечение санитарно-эпидемиологического благополучия населения, можно продолжить, так как каждая из названных имеет различные аспекты его проявления. Так, если взять только группу связанных с подготовкой и проведением оперативно-разыскных мероприятий, можно выделить присущие конкретному мероприятию.

При рассмотрении сущности и характера оперативно-разыскной деятельности становится понятным, что она раскрывается в конечном счете через реализацию функций присущих тому или иному виду деятельности, то есть определенные совокупности действий, приемов, методов, линий поведения. Исходя из этой предпосылки, есть возможность классификацию проблем осуществлять и по функциональному признаку. Такой подход позволил бы адекватно отображать реально существующие действия оперативных работников. Ведь каждый сотрудник занимает определенную должность, для которой характерна соответствующая технология выполнения определенных видов деятельности по функциональному признаку. И, естественно, степень ответственности, его реализация полностью зависит от того, насколько тот или иной сотрудник смог разобраться в конкретной ситуации.

В период коронавирусной инфекции сотрудники оперативных подразделений органов внутренних дел подвергаются риску гораздо чаще, нежели в доэпидемиологическое время, так как, осуществляя свою оперативно-разыскную деятельность, оперуполномоченные сталкиваются с лицами, заражёнными Covid-19, тем самым подвергая не только своё здоровье опасности, но и состояние своих близких, друзей, родственников и коллег по службе. С другой же стороны, сотрудники, осуществляющие оперативно-разыскную деятельность во время действия мер ограничительного характера по причине коронавирусной инфекции, гораздо меньше контактируют с общественностью, применяя дистанционные методы работы, в частности при проведении оперативно-розыскных мероприятий (например, опрос). Меры ограничительного характера влияют на тот факт, что весь арсенал сил, методов и средств оперативный сотрудник не может задействовать, ему приходится ограничиваться в определенных действиях как при выявлении, предупреждении и раскрытии преступлений, так и во время сотрудничества с лицами, оказывающими содействие.

Так, во время тяжелой эпидемиологической обстановки в России отмечается рост преступности. В Кремле признаётся и фиксируется интенсивный рост преступлений. Также Дмитрий Песков добавил: «Правоохранительные органы работают с повышенной нагрузкой, но сгущать краски в связи с данной ситуацией не стоит» [7]. На сегодняшний день, как показывает практика, мы видим, что многие подразделения полиции уходят на карантин в связи с многочисленными заражениями сотрудников органов внутренних дел. И не спроста, пресс-секретарь Президента отметил, что у всех подразделений органов внутренних дел колоссальная нагрузка. Данный факт также пагубно влияет на работоспособность той или иной службы, ведь при нехватке кадров, ограничений в деятельности рост преступности остановить практически невозможно, поэтому следует идти на риск, создавать рискованные ситуации, которые могут привести ещё к большему ухудшению ситуации для правоохранителей, но, с другой стороны, закрыть те «дыры», которые в данный момент создают большую угрозу обществу и государству.

Меры ограничительного характера пагубно влияют практически на все сферы жизнедеятельности, поэтому рост преступных деяний на территории России и во всем мире в целом объясним. Люди теряют работы, лишаются спроса на свою

продукцию и доходят до самого настоящего «финансового голода», в силу этого повышается количество мошенничеств в сфере IT-технологий.

Ко всему этому хотелось бы добавить, что оперативным работникам следует разрабатывать новые методы работы на дистанционном режиме, так как такого рода деятельность достаточно специфична и требует разработки новых методов борьбы с преступностью дистанционно, дистанционного межведомственного взаимодействия и взаимодействия со своими оперативными источниками.

Сегодняшние дни – это век информации и высоких технологий, поэтому стоит принять это за должное и эффективно действовать в непривычное для нас время, перестраиваться, строить новые планы и использовать грамотнее все ресурсы технологического прогресса, которые даны нам в настоящий момент, чем преступное сообщество. Ведь при качественном освоении и правильном использовании всех новшеств можно не просто стабилизировать и замедлить рост преступности во время эпидемии, но и улучшить показатели по раскрываемости и выявлении преступлений любого рода. Никто не знает, насколько долго продержится такая обстановка во всем мире, поэтому нужно суметь перестроиться, правильно выбрать дальнейшую тактику работы и быть готовым к новым, более строгим ограничениям, чтобы они не смогли заставить врасплох ведомства, которые обеспечивают правоохранительную функцию, в частности подразделения, осуществляющие оперативно-разыскную деятельность.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Что происходит с преступностью во время карантина [Электронный ресурс]. – Режим доступа: https://news.rambler.ru/other/44149945/?utm_content=news_media&utm_medium=read_more&utm_source=copylink
2. О состоянии преступности в Российской Федерации в 1-м квартале 2020 года [Электронный ресурс]. – Режим доступа: https://мвд.рф/news/item/19986723/
3. Мамчун В.В. Правоприменительный риск и его ограничительные пределы / Теория и практика ограничения прав человека по российскому законодательству и международному праву: сборник научных трудов. Ч. 1 / под ред. В.М. Баранова. – Нижний Новгород: НЮИ МВД РФ, 1998. С. 261.
4. Ривман Д.В. Сущность, задачи и принципы оперативно-розыскной деятельности органов внутренних дел: лекция. – Санкт-Петербург, 1999. С. 4.
5. Шумилов Н.И. Информационная безопасность: методическое пособие / под ред. И.А. Возгрина. – Санкт-Петербург: СПб А МВД России, 1997. С. 3.
6. Основы оперативно-розыскной деятельности: учебник / под ред. С.В. Степашина. – Санкт-Петербург: Лань, 1999. С. 94–95.
7. https://yandex.ru/turbo/gazeta.ru/s/social/2020/04/13/13047019.shtml

УДК 004

К ВОПРОСУ О РЕАЛИЗАЦИИ СЕМАНТИЧЕСКОЙ ИНТЕРОПЕРАБЕЛЬНОСТИ ПРИ ДАТАЦЕНТРИРОВАНИИ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ БАЗАХ ДАННЫХ, СОДЕРЖАЩИХ СВЕДЕНИЯ ОБ ИНОСТРАННЫХ ГРАЖДАНАХ И ЛИЦАХ БЕЗ ГРАЖДАНСТВА

Вихляев А.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассмотрены основные вопросы, связанные с датацентрированием и обеспечением семантической интероперабельности информационно-аналитических баз данных об иностранных гражданах и лицах без гражданства, функционирующих в системе МВД России; обозначены проблемы, возникающие у операторов и пользователей при работе с большими данными, связанные с их интерпретацией и программно-аппаратной реализацией в процессе семантической интероперабельности информационных систем; предложены пути решения обозначенных проблем.

Ключевые слова: датацентрирование, семантическая интероперабельность, информационно-аналитическая база данных, большие данные, ППО «Территория», ЦБДУИГ.

ON THE IMPLEMENTATION OF SEMANTIC INTEROPERABILITY IN DATA CENTERS IN INFORMATION AND ANALYTICAL DATABASES CONTAINING INFORMATION ABOUT FOREIGN CITIZENS AND STATELESS PERSONS

Vikhlyaev A.A.
(Kikot Moscow University of the MIA of Russia)

Abstract: the article deals with the main issues related to data centering and ensuring semantic interoperability of information and analytical databases on foreign citizens and stateless persons operating in the system of the Ministry of Internal Affairs of Russia; identifies the problems that arise for operators and users when working with big data, related to their interpretation and hardware and software implementation in the process of semantic interoperability of information systems; suggests ways to solve these problems.

Keywords: datacenter, semantic interoperability, information and analytical database, big data, PPO «Territory», CBDUIG.

В последние годы в Российской Федерации происходит активная фаза модернизации процессов получения, обработки и хранения информационных массивов данных.

Прежде всего это связано с активным внедрением в различные сферы жизни, включая экономику и государственное управление, современных информационных технологий, способных накапливать и анализировать различные объемы сведений.

В рамках реализации национального проекта «Цифровое государственное управление», входящего в программу «Цифровой экономики Российской Федерации» до 2024 года, немаловажным обстоятельством является и обеспечение самих условий, способствующих накоплению больших данных на основе кластерной механики.

Указанный функционал в условиях глобальной цифровизации приобретает признаки достаточно трудоемкого и требующего значительных операционных ресурсов процесса.

Подключение новых участников технологического процесса, связанного с обработкой и систематизацией больших данных в единую систему, требует не только слаженности и оперативности в обеспечении непосредственного функционирования самой системы, но и правильного семантического восприятия электронной средой всех вносимых в нее сведений.

Для обеспечения значимой семантической интероперабельности функционирующих систем и надлежащего обобщения сведений в требуемые базы данных необходимо исполнение всех уровней, охватывающих указанный процесс: организационного, семантического и технического.

Правильное построение и структурирование метаданных в системе требует соблюдения точноалгоритмированных последовательностей, позволяющих выстроить не только саму архитектуру и функционал системы, но и произвести построение ее проблемно-ориентированной модели, четко определить профиль интероперабельности и программно-аппаратную реализацию.

Сама программно-аппаратная реализация в подобном случае включает внутрисистемное структурирование и функционал внешней системы, предоставляющей возможность выхода как в локальную, так и во внешнюю сеть.

Если видение указанного вопроса в рамках реализации программ Big Data в сфере предпринимательской деятельности позволяет реализовать полный комплекс мер, направленных на единое восприятие экстраполируемых сведений, вносимых в систему, с использованием как горизонтально-масштабируемых горизонтальных систем, так и специальных инструментов класса Business Intelligence, доступных для широкого круга пользователей, то действие специальных систем баз данных должно, прежде всего, основываться на локально-ориентированные замкнутые сети с высокой степенью защиты интегрируемых сведений.

Далее полагаем остановиться на структурировании процесса обработки и распознавания данных, вносимых в автоматизированные базы данных, содержащие в себе сведения об иностранных гражданах и лицах без гражданства, функционирующие в системе МВД России.

Речь пойдет о прикладном программном обеспечении «Территория» (далее – ППО «Территория») и автоматизированной системе Центрального банка данных по учету иностранных граждан (далее – АС ЦБДУИГ), применяемых подразделениями Главного управления по вопросам миграции МВД России для ведения банков данных об иностранных гражданах и лицах без гражданства, пребывающих на территории Российской Федерации.

Указанные интегрированные системы имеют общие свойства и направлены, прежде всего, на оперативную обработку специализированной информации для правоохранительных органов, содержащей персональные данные иностранных граждан и лиц без гражданства, пересекших границу Российской Федерации в целях туризма, трудоустройства, постоянного места жительства или в транзитных целях, объединенные в единые кластеры с информацией, полученной из интегрированных баз данных учреждений, также занимающихся предоставлением государственных услуг в сфере миграции (например, многофункциональных центров).

Представленные системы ориентированы на использование проприетарного программного обеспечения, исключающего возможность несанкционированного доступа к соответствующим сведениям.

Семантика ППО «Территория» и ЦБДУИГ обеспечивается при помощи использования соответствующих стандартов – языка разметки XML. При этом каждый тип учетных сведений, содержащихся в пакетах должен поддерживать единый формат, коррелируемый с соответствующими кластерами упорядоченных данных.

Использование баз данных обладает обратной совместимостью, что обеспечивает возможность выгрузки сведений из одной базы данных в другую.

При всей визуальной целостности и взаимодополняемости информационных массивов данных следует выделить и некоторые недостатки, которые часто проявляются в процессе фактического использования указанных ресурсов.

Прежде всего, можно выделить непосредственную автоматизацию процесса внесения соответствующих сведений в интегрированные банки данных.

Зачастую сложности в автоматизации и управлении процессами ввода и обработки связывают с рядом факторов: недостаточной квалификацией операторов информационных систем; использованием механического ввода сведений при отсутствии алгоритма предварительной проверки имеющихся данных, что влечет дублирование ранее внесенных в базы сведений, либо внесение сведений идентичного характера при неправильном их распределении по различным информационным кластерам.

Далее следует выделить отсутствие единой системы транскрибирования сведений, вносимых в базы данных, в связи с чем интерпретация символов, некорректно внесенных оператором при вводе сведений об одном и том же лице, может повлечь их распределение неравномерно или неправильно по различным информационным кластерам.

Так, например, некорректное внесение сведений об иностранном гражданине по фамилии «Mukhorgonov» при переводе с английского языка подлежит заполнению, как «Махорджонов». В то время интерпретация указанных сведений операторами, ответственными за ввод информации, как «Мукорджонов» или «Махорчонов» вызовет образование дополнительных кластеров со сведениями об указанном лице, однако идентифицировать его по указанным данным уже будет невозможно. В таком случае при получении сведений из автоматизированных баз данных, связанных с привлечением указанного лица к ответственности за совершение правонарушений, может повлечь невозможность его привлечения к юридической ответственности вовсе в связи с тем, что при расхождении сведений о лице судами его личность будет считаться неустановленной.

Следующим негативным аспектом является, безусловно, отсутствие корректной системы распознавания изображений. Имеющаяся в настоящее время система, коррелирующая с описываемыми платформами, иногда существенно искажает содержащиеся в кластерах фрагменты, что влечет затруднения в идентификации отдельных личностей.

Также фактором, существенно влияющим на семантику при обеспечении интероперабельности ППО «Территория» и АС ЦБДУИГ, безусловно, является отсутствие возможностей автоматизированной корректировки сведений, содержащихся в базах данных, при наличии несистемных ошибок.

Выход в обеспечение семантической интероперабельности при организации датацентрирования сведений в рассматриваемых информационно-аналитических базах данных видится во внедрении и развитии в указанный процесс методов глубокого машинного обучения, способных самостоятельно делать акцент на недочетах и некорректных данных в разметке вносимой информации.

Это позволит своевременно выявлять ошибки операторов ввода метаданных, распределять сведения в соответствии с информационной архитекурой по корректным информационным кластерам. Распределение сведений при реализации семантической интероперабельности информационных систем также позволит получать достоверные сведения о запрашиваемом объекте.

Другой выход видится в автоматизации процесса предобработки метаданных с переходом от механически-операционного в сторону программно-ориентированного. Прежде всего указанный процесс видится во внедрении программного обеспечения, позволяющего с использованием алгоритма на основе символьных лемм моделировать правильное транскрибирование и выражение сведений в единственно-верные структуры.

Данные инициативы позволят в полной мере реализовать потенциал автоматизированных баз данных для пользователей, исключить возможности некорректного толкования информации, привести к структурированности и стабильности их функционирования как самостоятельных систем, так и в рамках семантических взаимодействий друг с другом и иными информационными системами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Приказ МВД России, МИД России, ФСБ России, Минэкономразвития России, Министерства информационных технологий и связи Российской Федерации от 10 марта 2006 г. № 148/2562/98/62/25 «О ведении и использовании центрального банка данных по учету иностранных граждан и лиц без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации» // СПС «Гарант».

2. ГОСТ Р 55062-2012 «Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения». [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200102958

3. Национальная программа «Цифровая экономика» [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/activity/directions/858/

4. Официальный сайт Главного управления по вопросам миграции МВД России [Электронный ресурс]. – Режим доступа: https://гувм.мвд.рф.

УДК 378

ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОЦЕССА ФОРМИРОВАНИЯ ГРАЖДАНСТВЕННОСТИ БУДУЩИХ ОФИЦЕРОВ В ВОЕННОМ ВУЗЕ

Остапенко В.С.,

доктор педагогических наук, профессор

(Центральный филиал Российского государственного университета правосудия);

Юршин А.Д.

(Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина»)

Аннотация: в статье рассматривается актуальная проблема информационно-методического обеспечения процесса формирования гражданственности будущих офицеров в образовательном процессе военного вуза, особенности применения в специфических условиях ведомственного вуза.

Ключевые слова: гражданственность, информационно-методическое обеспечение, процесс формирования, будущие офицеры, военный вуз.

INFORMATION AND METHODOLOGICAL SUPPORT FOR THE PROCESS OF FORMING THE CITIZENSHIP OF FUTURE OFFICERS AT A MILITARY UNIVERSITY

Ostapenko V.S.,
Doctor of Pedaqoqical Sciences, Professor
(Central branch of the Russian state University of Justice);
Yurshin A.D.
(Military Training and Scientific Center of the Air Force «Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin»)

Abstract: the article discusses the urgent problem of information and methodological support of the process of formation of citizenship of future officers in the educational process of a military university, its features of application in specific conditions of a departmental university.

Keywords: citizenship, information and methodological support, the formation process, future officers, military university.

Информационно-методическое обеспечение учебного процесса вуза – это целенаправленный и специально организуемый процесс сбора, накопления и предоставления обучающимся учебной и методической информации, необходимой для подготовки специалистов, способных реализовать полученные знания и навыки в профессиональной деятельности.

Информационно-методическое обеспечение образовательного процесса включает технические средства (компьютеры, ноутбуки и т.п.), библиотечный фонд, электронные учебники и учебные пособия, справочники, энциклопедии, словари, задания контрольных и курсовых работ, методические рекомендации студентам по самостоятельной работе и другие пособия, имеющие не только печатный, но и электронный варианты предъявления и коммуникации [1].

В широком смысле слова любая информация формирует определенное знание, и наоборот, получение знания невозможно без потоков информации. Информацию формируют и передают самые разнообразные средства, но особую роль сегодня приобретают информационно-коммуникационные технологии, которые внедряются и эффективно используются в образовательном процессе вузов [2].

Информационно-методическое обеспечение процесса формирования гражданственности будущих офицеров в военном вузе имеет свои цели и задачи. Основными из них являются:

- сбор и усвоение информации по проблеме гражданственности, которая используется преподавателями и обучающимися при изучении гуманитарных и правовых дисциплин (Основы права, Философия, Социология, Политология и др.);

- использование при проведении воспитательных мероприятий информации по вопросам гражданского общества, прав и свобод личности, гражданской и правовой ответственности;

- сбалансированное распространение учебной информации с целью исключения перегрузки обучающихся сведениями, не являющимися актуальными и значимыми в конкретных условиях;

- разнообразие источников информации по теме и обеспечение свободного доступа к ним не только профессорско-преподавательского состава, но и обучающихся в специфических условиях военного вуза.

Последнее положение требует дополнительного разъяснения. В военных вузах получение и применение определенных видов информации имеет существенные ограничения. Это обусловлено тем, что в целях обеспечения режима ограниченного доступа к источникам информации в военном вузе, использование некоторых средств получения информации запрещено (ноутбуков, смартфонов и т.п.). Например, открытый доступ к Интернету в военных вузах, как правило, запрещен, что обусловлено необходимостью соблюдения режима секретности по определенным направлениям деятельности.

Все это существенно ограничивает свободное получение обучающимися информации о новациях в гражданском обществе, правах и свободах граждан, об изменениях в законодательстве по данной теме, представленных в открытых источниках. Получить такую информацию обучающийся может или в процессе изучения правовых и социально-гуманитарных дисциплин, или при нахождении за пределами военного вуза, что не является по времени длительным и частым ввиду особого распорядка дня в ведомственных образовательных организациях [6].

Цели информационно-методического обеспечения процесса формирования гражданственности будущих офицеров в военном вузе достигаются через решение конкретных задач. Среди них:

- полное и своевременное предоставление информации по вопросам развития гражданственности в процессе учебной и научной деятельности в военном вузе для подготовки докладов, сообщений, научных статей в рамках изучения гуманитарных дисциплин и участия в научно-практических мероприятиях (конференции различного уровня, «круглые столы», научные дискуссии и диспуты и т.п.);

- улучшение доступа, распространения и обмена информацией по теме гражданственности на принципах приоритетно субъект-субъектного взаимодействия, при учете и субъект-объектных отношений субординационного характера, неизбежных в военном вузе;

- совершенствование работы информационных структур и специалистов, ответственных за сбор, хранение и передачу информации потребителям (как обучающимся, так и организаторам процесса формирования гражданственности будущих офицеров в военном вузе).

Цели и задачи определяют основные этапы информационно-методического обеспечения процесса формирования гражданственности будущих офицеров в военном вузе, а также требования, предъявляемые к нему.

Кратко рассмотрим процесс предоставления информации обучающимся на различных этапах формирования рассматриваемого феномена.

Эти этапы условно выглядят следующим образом:

а) сбор, обработка учебной информации и доведение ее до потребителя;

б) непосредственное воздействие информационных потоков на обучающихся;

в) организация обратной связи с целью оценки эффективности процесса усвоения информации.

Получается своего рода модель информационно-методического обеспечения рассматриваемого процесса, что дает возможность выделить два его аспекта: первый – это предоставление обучающимся необходимой информации для достижения максимальной эффективности работы в данном направлении; второй – это управление процессом на основе активного использования информационно-коммуникационных технологий [3].

Информационно-методическое обеспечение формирования гражданственности у обучающихся в военном вузе предполагает формирование единых баз данных и создание интерактивной среды обучения с помощью образовательных сервисов информационно-образовательного портала и сайтов. Это позволяет повысить качество данного процесса за счет предоставления участникам следующих сервисов:

- хранение и доставка учебно-методических ресурсов с использованием интернет-сервисов с учетом существующих ограничений в военном вузе;
- доступ к электронным учебным пособиям и использование обучающих программных средств по изучаемой проблеме, а при необходимости и создание электронных факультативов;
- электронное тестирование уровня сформированности гражданственности в рамках преподаваемых гуманитарных дисциплин;
- оперативный обмен информацией, хранение электронных документов, отражающих работу в данном направлении.

Организация, построение и реализация информационно-методического обеспечения процесса формирования гражданственности будущих офицеров в военном вузе, его рациональное функционирование и эффективное использование могут быть достигнуты при соблюдении определенных принципов. Наиболее значимыми из них будут следующие:

1. Целенаправленность информационно-методического обеспечения рассматриваемого процесса, что означает выбор такой поисковой стратегии, при которой обучающийся в рамках индивидуальной траектории получает информацию, соответствующую не только заданной тематике, но и его индивидуальным запросам и потребностям [4].

2. Актуальность и своевременность информационно-методического обеспечения процесса формирования гражданственности от этапа к этапу, что заключается в предоставлении обучающимся приоритетной информации в установленные сроки в соответствии со спецификой военного вуза.

3. Полнота и надежность информационного обеспечения данного процесса, которые заключаются в предоставлении потребителям (как обучающимся, так и педагогам) всей необходимой информации с учетом требуемых видов оформления и языкового выражения, хронологической последовательности, качества, визуализации подачи материала и т.п.

4. Системность информационно-методического обеспечения, которая проявляется в удовлетворении запросов и интересов обучающихся на всех эта-

пах данного процесса с учетом категорий потребителей, характера их информационных потребностей, специфики решаемых задач.

Исходя из вышеизложенного можно сформулировать теорию информационно-методического обеспечения образовательного процесса в целом и развития качеств личности в частности, в том числе и гражданственности. В рамках такого подхода можно создать информационную инфраструктуру вуза, развивать дистанционные технологии обучения, что позволяет сформулировать приоритетные направления деятельности по рассматриваемой проблеме.

1) это информатизация всех звеньев управления в военном вузе, обеспечивающая повышение качества обучения и воспитания, что способствует не только профессиональному становлению, но и развитию личности обучающихся;

2) это информатизация учебно-методического работы, обеспечивающая эффективность применения информационно-коммуникационных технологий в целях формирования определенных характеристик и свойств обучающихся, в том числе и гражданственности [5];

3) это информатизация научной деятельности, обеспечивающая доступ к различным источникам научной информации и электронным библиотечным фондам, активное участие обучающихся в научно-практических мероприятиях различного уровня как в очной, так и в заочной формах с использованием информационно-коммуникационных технологий [7].

Таким образом, информационно-методическое обеспечение процесса формирования гражданственности будущих офицеров в военном вузе предполагает изучение как теоретических, так и практических аспектов данной проблемы с целью повышения эффективности рассматриваемой работы с учетом ее специфики в ведомственных образовательных организациях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Асмолов А.Г., Семенов А.Л., Уваров А.Ю. Российская школа и новые информационные технологии: взгляд в следующее десятилетие. – Москва: НексПринт, 2010. – 84 с.

2. Воронкова Ю.Б. Информационные технологии в образовании. – Ростов-на-Дону: Феникс, 2010. – 314 с.

3. Гусева Р.П. Методическая готовность преподавателей к созданию комплексного учебно-методического обеспечения образовательного процесса // Среднее профессиональное образование. 2009. № 3. С. 25–33.

4. Информационные и коммуникационные технологии в образовании: монография / под ред. Бадарча Дендева. – Москва: ИИТО ЮНЕСКО, 2013. – 320 с.

5. Кочетов С.И. Комплексное методическое обеспечение учебного процесса средствами обучения. – Москва: Высшая школа, 2011. – 231 с.

6. Тимофеев А.И. Педагогические условия формирования гражданственности курсантов военного вуза: автореф. дис. … канд. пед. наук. – Чита, 2014. – 23 с.

7. Федотова Е.Л., Федотов А.А. Информационные технологии в науке и образовании. – Москва: Форум, 2018. – 256 с.

УДК 004

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ЛАЗЕРНЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Акапьев В.В.
(Балтийский государственный технологический университет
имени Д.Ф. Устинова);
Акапьев В.Л.,
кандидат педагогических наук;
Савотченко С.Е.,
доктор физико-математических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: проведен сравнительный анализ различных средств проведения измерений скорости движения объектов, схем построения приемного блока доплеровских измерительных приборов и представлен математический аппарат для проектирования доплеровского измерителя скорости.

Ключевые слова: лазерные технологии, лидар, доплеровский измеритель скорости, средства измерения скорости, схема приемного блока, математический аппарат.

SOME ASPECTS OF THE USE OF LASER TECHNOLOGIES IN LAW ENFORCEMENT

Akapev V.V.
(Ustinov Baltic state technological University);
Akapev V.L.,
Candidate of Pedaqoqical Sciences;
Savotchenko S.E.,
Doctor of Physical and Mathematical Science
(Putilin Belgorod Institute of the MIA of Russia)

Abstract: a comparative analysis of various means of measuring the speed of objects, schemes for building a receiving unit of Doppler measuring devices, and a mathematical apparatus for designing a Doppler speed meter is presented.

Keywords: laser technologies, lidar, Doppler speed meter, speed measurement tools, receiving block diagram, mathematical apparatus.

В настоящее время радикально изменяется не только психология правоохранителей, определяющая необходимость использования информационных технологий для решения профессиональных задач. Кардинально трансформи-

руется набор технических средств, востребованных в силовых структурах. Не обошли эти тенденции и лазерные технологии.

Развитие лазерных технологий расширяет спектр их применения в правоохранительной деятельности, но при этом сохраняет свою актуальность задача точного измерения скорости движения различных объектов.

Данной проблемой в различные периоды занимались многие отечественные и зарубежные ученые, такие как П.Н. Агалецкий [1], С.А. Валерик, С.Г. Галиенко, С.Г. Губин [2], А.А. Жеребцов, Н.А. Зайцев [3] и многие другие.

Несмотря на то, что эта тема очень глубоко прорабатывалась на протяжении ряда лет различными учеными, сохраняется некоторая неопределенность при выборе методов измерения и технической реализации лазерных доплеровских измерителей скорости.

Для разработки доплеровского измерителя скорости необходимо провести сравнительную характеристику различных существующих средств измерения для выбора наиболее подходящего (см. таблицу 1).

Таблица 1

Сравнительный анализ различных средств измерения

	Радар	**Лидар**	**Сонар**
Достоинства	Бесконтактность, скорость установки, небольшая погрешность измерений, быстрое получение результата	Бесконтактность, высокая точность измерений, широкий спектр измеряемых скоростей, быстрое получение результата, высокочастотный сигнал, низкий уровень шумов	Высокая точность в твердых средах, низкая стоимость, высокая разрешающая способность, высокая скорость обновления информации
Недостатки	Большие габаритные размеры антенн, небольшая дальность эффективной работы, низкая частота рабочего сигнала, высокий уровень помех	Дороговизна, относительная сложность конструкции, требования к точности настройки оборудования, подверженность к внешним факторам	Контактный способ измерения, работа с механическими волнами, низкая эффективность работы в воздухе и вакууме, малая дальность

Из представленных трех основных средств измерения скорости сонар является наименее пригодным для измерения скорости артиллерийского снаряда, так как измерения происходят в воздухе, где механические волны распространяются намного хуже, чем электромагнитные. Также правильной работе сонара

будет мешать шум от выстрелов орудия, из-за которого объективную оценку скорости невозможно получить.

Лидарный и радарные системы основываются на одном и том же принципе измерения скоростей, но работают в разных диапазонах электромагнитных волн. Оптическое излучение имеет более высокую частоту и, следовательно, потенциально высокую точность измерения. Также для генерации оптического излучения используется лазер, который имеет небольшие габаритные размеры и вывод излучения происходит через оптоволокно в отличие от антенных систем в радарах.

Исходя из сравнительной характеристики различных средств измерения скорости, наиболее подходящим является доплеровский лидар, так как точность измерения является одной из важнейших характеристик прибора, и радар уступает в этом лидару.

Следующим аспектом является выбор схемы построения приемного блока доплеровских измерительных приборов, так как существуют различные схемы построения приемного блока измерителей скоростей.

Самой простейшей из них является обычная схема доплеровского измерителя без дополнительных инструментов (см. рис. 1) [4].

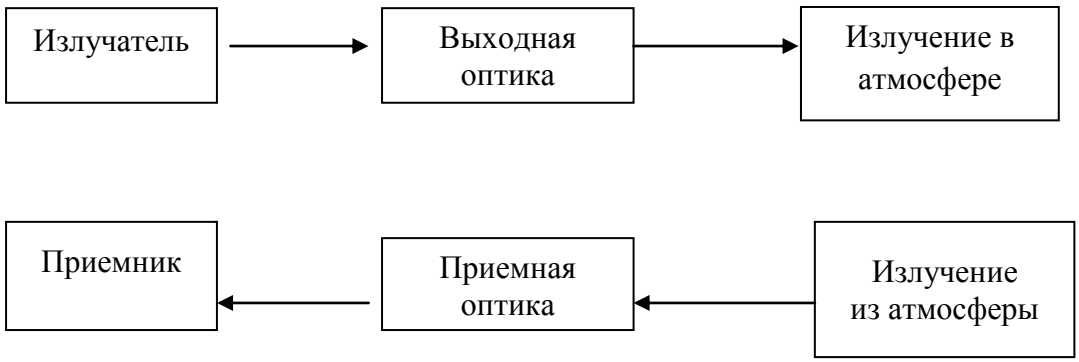


Рисунок 1. Схема доплеровского измерителя скорости

Главным плюсом такой схемы является простота и дешевизна исполнения. Однако у такой схемы есть множество недостатков:

1. Широкий спектр принимаемого сигнала.
2. Низкая точность измерения.
3. Подверженность шумовому загрязнению.

Для устранения большинства недостатков была предложена схема гетеродинного детектирования сигнала (см. рисунок 2). Она основана на дублировании сигнала излучателя и отправке его сразу на приемник, что позволяет определить центральную волну излучения и с большой точностью найти искомый доплеровский сдвиг [5].

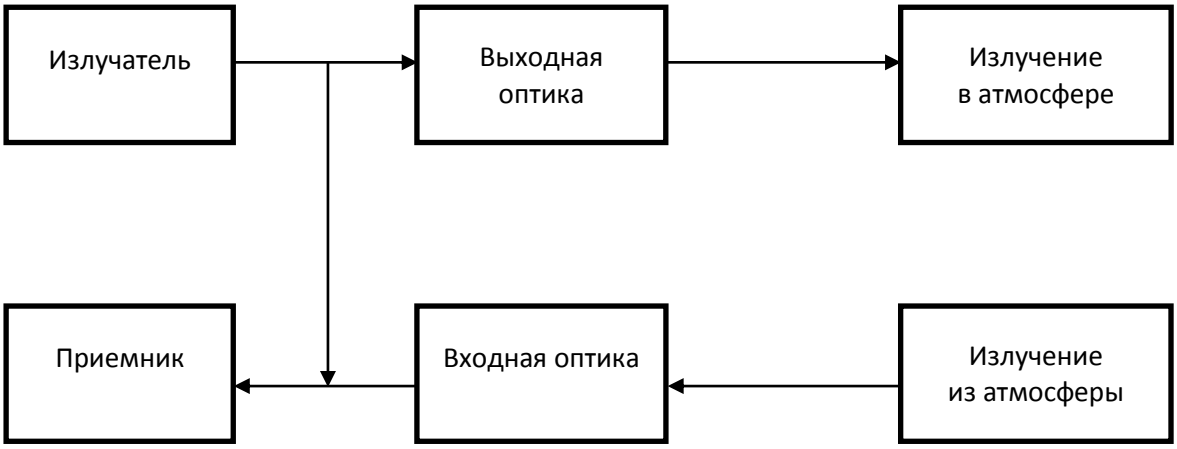


Рисунок 2. Схема доплеровского измерителя скорости с гетеродином

Используя такую схему, можно получить намного более точный результат измерения по сравнению со схемой без использования гетеродина, однако на приемнике остается широкая полоса частот, из-за которой тяжело обработать данный сигнал.

Исходя из требований по точности и быстродействию системы, была предложена схема гетеродинного детектирования с использованием электрооптического модулятора (ЭОМ) (см. рисунок 3).

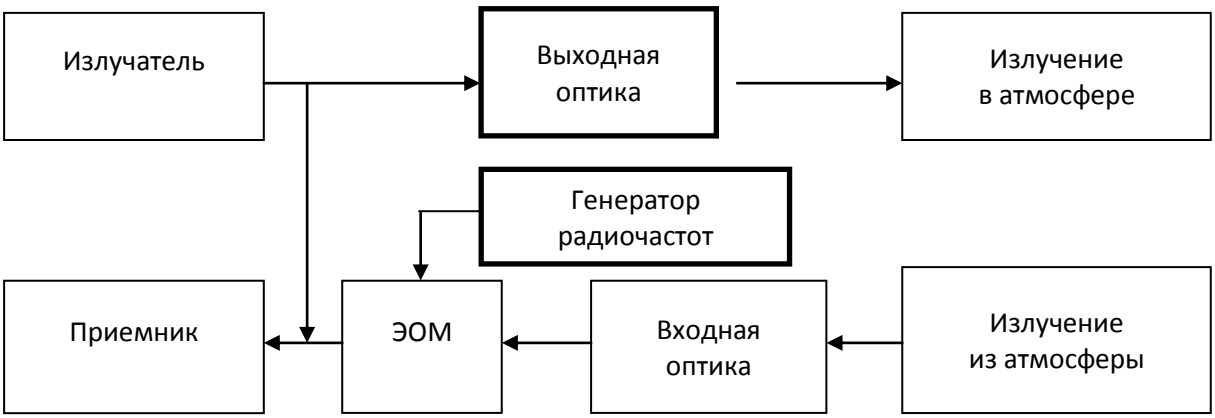


Рисунок 3. Схема доплеровского измерителя скорости с гетеродинным и электрооптическим модулятором

В этой схеме была решена главная проблема, которая заключалась в широкой полосе приемного сигнала. Электрооптический модулятор изменяет частоту принимаемого сигнала до меньших порядков, которые легче обработать. После преобразования принятого сигнала и смешения его с опорным, легко определить искомый допплеровский сдвиг с наивысшей точностью.

И, наконец, ключевым аспектом является математический аппарат для проектирования доплеровского измерителя.

Главным расчетом допплеровского лидара является энергетический расчет, с помощью которого можно определить работоспособность прибора:

$$ED = (4 * E_{las})/(\pi * \Theta * L^2) \quad \textbf{(1)}$$

$$\Theta = M^2 * 1.06 * \lambda/d_t \quad \textbf{(2)}$$

$$E_t = (E_{las} * A * S_{eff} * d_t^2)/(2\pi * \Theta^2 * L^4) \quad \textbf{(3)}$$

$$S_{eff} = S_0 * cos\varphi \quad \textbf{(4)}$$

$$T_{res} = T_{opt} * T_{filt} \quad \textbf{(5)}$$

$$T_{atm} = \exp(-\alpha * R) \quad \textbf{(6)}$$

$$E_r = \left[E_{las} * A * S_{eff} * d_t^2 * T_{res} * \exp(-\alpha * 2L)\right]/(2\pi * \theta^2 * L^4) \quad \textbf{(7)}$$

$$P_{las} = E_{las}/\tau_{las} \quad \textbf{(8)}$$

$$P_\tau = \frac{[P_{las} * A * S_{eff} * d_t^2 * T_{res} * \exp(-\alpha * 2L)]}{2\pi * \theta^2 * L^4} \quad \textbf{(9)}$$

$$P_b(R) = [\pi * P_\lambda * \Delta\lambda * A * \omega_{пр}^2 * d_t^2 * T_{res} * \exp(-\alpha * R)]/16 \quad \textbf{(10)}$$

Основываясь на этих формулах, возможно подобрать комплектующие, а именно, приемник оптического излучения, для обеспечения корректной работы всего измерительного прибора в разных погодных условиях. Основные положения представленной методики могут быть использованы не только для расчета энергетических параметров импульсных измерителей скорости, но и для расчета параметров лазерных локаторов, для которых требование наблюдения цели для наведения на нее локатора не ставится. В этом случае основные соотношения для расчетов остаются справедливыми, но несколько изменяется методика выбора исходных данных. В локаторах могут также применяться специфические методы обработки сигналов, требующие иного подхода к выбору отношения сигнала к шуму, например, при использовании электронно-лучевого индикатора кругового обзора.

Основные принципы методики оценки применимы также к системам, в которых используется непрерывное лазерное излучение. Отличие в этом случае состоит в том, что вместо энергии излучения необходимо пользоваться мощностью излучения, выбирать ширину полосы пропускания DF приемного электронного тракта в зависимости от требований к временной разрешающей способности прибора (к интервалу времени, в пределах которого должна обеспечиваться регистрация изменения мощности сигнала), а также следует иначе подходить к выбору отношения сигнала к шуму: при приеме непрерывного излучения в некоторых случаях могут регистрироваться величины изменения мощности на 5-10%.

Наконец, предложенная методика подхода к оценке мощности излучения обратного рассеяния может быть использована для энергетической оценки лидаров [6], применяемых не только для измерения скорости движущихся объектов, но и для решения широкого спектра других задач, возникающих в ходе осуществления правоохранительной деятельности.

Таким образом, основы представленной методики являются общими для решения существенно более широкого круга задач оптико-электронного приборостроения, не ограниченных узкими рамками дальнометрии и связанных с использованием лазерного излучения в качестве носителя информации для дистанционного измерения параметров удаленных объектов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Способ измерения начальной скорости артиллерийских снарядов: заявка в НКО Лв 4253 (325548) от 02.12.1939.

2. Губин С.Г. Устройства для измерения скорости боеприпасов // Вестник СГУГиТ. 2013 № 4. С. 73–79.

3. Способ измерения начальной скорости снаряда и устройство для его осуществления: патент Российской Федерации № 2250476 от 10.07.2010.

4. Викторов В.А., Лункин Б.В., Совлуков А.С. Радиоволновые измерения параметров технологических процессов. – Москва: Энергоатомиздат, 1989. – 132 с.

5. Патент РФ № 2334995 от 27.09.2008, G01S 13/58.

6. Ким А.А., Елисеев К.В., Акапьев В.В., Акапьев В.Л., Савотченко С.Е., Горлов А.С. Оптимизация параметров газогенераторной и лидарной систем для измерения потоков воздуха при неразрушающем контроле качества охлаждающих микроканалов на малых расстояниях // Письма в ЖТФ. 2020. Т. 46. № 9. С. 20–24.

УДК 378

ВОПРОСЫ ПРЕПОДАВАНИЯ В СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ МВД РОССИИ

Насонова В.А.,
кандидат физико-математических наук, доцент;
Прокопенко А.Н.,
кандидат технических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в работе рассмотрены вопросы дистанционного обучения как альтернативной формы образования в сложной эпидемиологической ситуации, показаны преимущества и недостатки дистанционного обучения, выделены проблемы, на которые стоит обратить внимание при переходе на дистанционное обучение.

Ключевые слова: дистанционное обучение, учебные занятия, проблемы.

THE ISSUES OF TEACHING IN THE DISTANCE LEARNING SYSTEM IN THE EDUCATIONAL ORGANIZATIONS OF THE MIA OF RUSSIA

Nasonova V.A.,
Candidate of Physical and Mathematical Sciences, Associate Professor;
Prokopenko A.N.,
Candidate of Technical Sciences, Associate Professor
(Putilin Belgorod Law Institute of MIA of Russia)

Abstract: the present paper considers the issues of distance education as an alternative form of education in a difficult epidemiological situation, shows the advantages and disadvantages of distance learning, highlights the problems that should be paid attention to when switching to distance education.

Keywords: distance education, training sessions, problems

В современном информационном мире наблюдается глобальная тенденция к исчезновению грани между традиционным образованием и дистанционным, т.к. большинство людей в процессе обучения прибегает к Интернету. В настоящее время в Интернете можно найти огромное количество информации на абсолютно любую интересующую тему, что, в свою очередь, облегчает поиск информации и сокращает время, затраченное на поиск.

Современные студенты являются информационным поколением, т.е. наличие электронных образовательных программ, учебников, заданий не выходит за рамки привычной жизни. Кроме того, в связи с быстрым, стремительным развитием технологий в таких же темпах развиваются и информационные образовательные технологии, в частности, дистанционное обучение[1], которое предлагается как альтернатива традиционному образованию.

Рассматривая историю возникновения ДО, отметим, что история появления дистанционного образования начинается с начала 1700-х годов – обучение стенографии путем обмена письмами с заданиями. В 1960-е годы дистанционное образование получило международное признание и стало активно развиваться при поддержке ЮНЕСКО. Следующим этапом (начало 2000-х гг.) в развитии дистанционного образования является открытие многофункциональных массовых онлайн-курсов (massive open online courses) – это платформы, предлагающие своим слушателям учебные программы разных университетов.

В процессе дистанционного обучения, с которым образовательные организации в системе МВД России, в частности, столкнулись на прямую в апреле 2020 года, наметился ряд проблем, решение которых возможно только с учетом полного погружения в рассматриваемый процесс.

Согласно основным профессиональным образовательным программам образования реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе образовательных организаций активных и интерактивных форм проведения занятий (компьютерных симуляций,

[1] Далее – ДО.

деловых и ролевых игр, разбора конкретных ситуаций, практикумов, психологических и иных тренингов, учений) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся, будущих сотрудников правоохранительных органов. В рамках учебных дисциплин должны быть предусмотрены: встречи с представителями правоохранительных и судебных органов, других органов государственной власти и управления, общественных организаций, участие специалистов в проведении аудиторных и внеаудиторных занятий.

При переходе на ДО существуют проблемы, не позволяющие проводить занятия в полном объеме с методической точки зрения, как общего характера, так и для отдельных видов учебных занятий.

К общим проблемам, безусловно, в первую очередь относится техническая составляющая. Рассмотрим более подробно данный вопрос:

- Использование отечественного лицензионного продукта. Образовательные информационные ресурсы включают в себя несколько составляющих, предназначенных, как для обучающихся, так и для профессорско-преподавательского состава.

Электронная информационно-образовательная среда образовательных организаций системы МВД России в локальной вычислительной сети и сети Интернет основана на базе программного обеспечения «Moodle» и обеспечивает размещение электронных учебных материалов для обучающихся. Программный комплекс дает возможность преподавателям размещать для обучающихся материалы как в текстовом формате, так и в графическом, видео- и аудиофайлы, тестовые задания и презентации. В системе имеется наличие обратной связи с преподавателем через встроенный чат. Доступ к ресурсу обеспечен как и из сети Интернет, так и из локальной сети. Недостатком системы является отсутствие возможности работы в системе при нарушении работы сети. С точки зрения преподавателя недостатками являются:

– отображение всех учебных дисциплин, в том числе тех, которые этому преподавателю не доступны;

– отображение избыточной информации при настройке тестов и вопросов к ним, сложное создание тестовых материалов, проблемы в использовании вопросов, созданных для одного теста в другом (при обычном доступе педагога невозможно, позволено только администратору);

– очень сложная система копирования материалов из одного курса в другой, в результате которой копирование фактически не применяется педагогическим составом.

Указанные недостатки ЭИОС, активно проявившиеся в условиях дистанционной работы, увеличивают время, необходимое для создания учебных курсов преподавателем, а также для проверки успеваемости не менее чем в два раза.

Система видео–конференц–связи TrueConf обеспечивает проведение видеосвязи, видеоконференций, дистанционных лекционных занятий, прием дистанционных зачетов через сеть Интернет. Преимуществом системы является простота в настройке и использовании, возможность отправления текстовых сообщений. Недостатком программного продукта является отсутствие возмож-

ности сохранять в системе идентификаторы конференций, отправлять файлы в конференцию или отдельному контакту, отсутствие возможности сохранения переписки чата при выходе из конференции.

- Недостаточная техническая грамотность педагогического состава. Развитие электронного образования тормозит ситуация с кадрами: одним не хватает педагогических знаний, другим – компетенции в сфере IT. Особенно это касается преподавателей старшего поколения, которые относятся к наиболее квалифицированным кадрам за счет педагогического опыта.

Вторая группа общих проблем возникает в связи с «обезличиванием» обучающихся, к ним относятся:

- Отсутствие широкого академического образования. В рамках преподавания дисциплины, в связи с отсутствием обратной связи с аудиторией в том объеме, который дает «живое» общение, не поступает дополнительная информация об «интересных» взаимосвязях со смежными дисциплинами. Таким образом, происходит узкое изучение дисциплины без ориентирования в каких-либо универсальных основах.

- Нехватка контроля. На любом из видов учебных занятий необходим контроль за обучающимися вне зависимости от уровня их подготовки, для понимания уровня усвоения знаний и навыков, что сложно сделать в рамках ДО, поскольку основной вид контроля приобретает вид тестирования, что ни в коем случае не может заменить «живое» взаимодействие обучающегося и преподавателя.

Лекция является одним из видов учебных занятий и составляет основу теоретической подготовки обучающихся. В перечне видов учебных занятий, которые в совокупности составляют содержание учебной работы по подготовке обучающихся в образовательных организациях системы МВД России, лекция стоит на первом месте. Ее цель – дать систематизированные основы научных знаний по дисциплине, акцентируя внимание на основных и наиболее сложных вопросах темы.

Лекция должна объединять в своем содержании три основных начала: дидактическое, мировоззренческое и методическое.

Методический аспект заключается в нахождении лектором такой соответствующей уровню аудитории и теме лекции формы подачи дидактического и мировоззренческого материала, которая не только обеспечивала бы максимально эффективное усвоение информации в отведенное для чтения лекции время, но и побуждала бы к более углубленному самостоятельному изучению темы.

В режиме ДО объем и качество, включая наглядность материала, излагаемого лектором, может быть увеличено, однако за счет потери «обратной связи» с аудиторией возникают проблемы, описанные выше.

Семинар – это форма организации обучения, заключающаяся в групповом обсуждении обучающимися узловых вопросов раздела или темы определенной учебной дисциплины или курса под руководством и с помощью преподавателя. С позиций теории дидактики высшей школы сущность семинара состоит в такой организации преподавателем работы группы обучающихся, при которой знания, усвоенные на лекции, и результаты индивидуальной самостоятельной

подготовки каждого обучающегося интегрируются в коллективном обсуждении основных вопросов темы непосредственно на самом семинарском занятии, а затем дифференцируются индивидуальным восприятием каждого участника семинара.

Дистанционное обучение в полной мере позволяет проводить данный вид учебного занятия, поскольку вовлеченность аудитории полностью соответствует традиционному обучению. За счет доступности наглядных и теоретических материалов, размещенных в электронном курсе учебной дисциплины, существует возможность расширить проверку знаний по преподаваемой теме. Кроме того, при проведении устного опроса происходит расширение теоретических познаний за счет дополнительной информации по теме, полученной в ходе совместного коллективного обсуждения вопросов.

В образовательных организациях системы МВД России, помимо лекций и семинаров, широко используются практические занятия, проводимые в различной форме в соответствии со специфическими особенностями преподаваемых учебных дисциплин.

Термину «практические занятия» нередко придают очень широкое толкование, понимая под ним все учебные занятия, проводимые под руководством преподавателя и направленные на углубление научно-теоретических знаний и овладение определенными методами работы по той или иной учебной дисциплине. Различные формы практических занятий являются самой емкой частью учебной нагрузки в образовательных организациях системы МВД России.

Практические занятия – метод репродуктивного обучения, обеспечивающий связь теории и практики, содействующий выработке у обучающихся умений и навыков применения знаний, полученных на лекции и в ходе самостоятельной работы.

Практические задания обучающиеся должны выполнять самостоятельно, для чего им разрешается иметь при себе теоретические материалы, обзорно-информационные источники и необходимые пособия. Задача же преподавателя сводится к приданию учебному занятию правильного направления, контролю за результатами выполнения заданий и исправлению ошибок, побуждению обучающихся к нахождению правильных решений.

При проведении практических занятий в системе ДО наблюдаются следующие проблемы:

- **слабая идентификация студента**. При ДО достаточно сложно отследить авторство выполняемых практических заданий, ответов на тестовые вопросы;

- **недостаток форм выражения знаний.** В ДО чаще всего проводится тестирование либо задаются письменные задания, которые не могут в полной мере дать возможность преподавателю оценить уровень сформированности компетенций будущего специалиста;

- **сложности с практикой.** Практические занятия в образовательных организациях системы МВД России могут проводиться как в аудиториях, так и в специальных кабинетах, на местности, на полигонах, в территориальных органах внутренних дел, залах единоборств, оборудованных помещениях для про-

ведения огневой подготовки. В действительности ДО не всегда предусматривает возможность практиковать полученные знания, это видно из перечня аудиторного фонда, используемого при проведении практических занятий.

Исходя из разнообразия обучения, в заключение выделим положительные стороны ДО:

- комфортные условия обучения. Лекционный и другой материал предоставляется обучающемуся в электронном виде, задания могут выполняться в любое удобное время;

- общение в открытых дискуссиях на сайте и широкие возможности сосредоточиться. Предлагается, что возможность поучаствовать в опросах, предложениях, обсуждениях, дискутировать по трудному материалу и т.д. в онлайн-режиме легче для обучающихся. Кроме того, при изучении материала при ДО проще сосредоточиться, потому что не приходится отвлекаться на других обучающихся;

- стимулирование саморазвития. Большую часть учебного материала обучающимся необходимо осваивать самостоятельно, это требует развитой силы воли, ответственности и самоконтроля.

Из вышесказанного следует, что как положительных, так и проблемных качеств при дистанционном обучении немало. В заключение можно утверждать, что проявление ДО как системы образования носит спонтанный характер, который нуждается в более глубокой доработке. Сегодня дистанционное обучение может служить лишь дополнением к традиционной форме, наиболее эффективным внедрением будет сочетание этих двух моделей образования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Жукова П.Н., Прокопенко А.Н., Баранов В.М. О возможности использования для проведения занятий по профессиональной служебной и физической подготовке и морально-психологической подготовке системы дистанционных образовательных технологий / Проблемы информационного обеспечения деятельности правоохранительных органов: материалы III международной научно-практической конференции (Белгород, 14 октября 2016 г.). – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2017. С. 83–86.

2. Частные методики образовательных технологий формирования информационно-технологической компетентности сотрудников правоохранительных органов / С.Е. Савотченко, В.Л. Акапьев, В.А. Насонова [и др.]: учебно-методическое пособие. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2018. – 68 с.

УДК 378

ПРИМЕНЕНИЕ ЭЛЕМЕНТОВ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В БАРНАУЛЬСКОМ ЮРИДИЧЕСКОМ ИНСТИТУТЕ МВД РОССИИ

Кирюшин И.И.,
Сапрыкина Т.П.
(Барнаульский юридический институт МВД России)

Аннотация: статья посвящена вопросам использования дистанционного обучения в БЮИ МВД России. В статье рассматривается применение системы дистанционного обучения «Moodle» в образовательном процессе. Приводится структура учебного электронного курса и его методическое наполнение.

Ключевые слова: дистанционное обучение, система «Moodle», электронный учебный курс, современные информационные технологии, учебный материал.

APPLICATION OF ELEMENTS OF REMOTE LEARNING

Kiryushin I.I.,
Saprykina T.P.
(Barnaul Law Institute of the MIA of Russia)

Abstract: the article is devoted to the use of distance learning in the BYU of the MIA of Russia. The article discusses the use of the distance learning system «Moodle» in the educational process. The structure of the educational electronic course and its methodological content are given.

Keywords: distance learning, Moodle system, electronic training course, modern information technologies, educational material.

С каждым днем растет значимость и актуальность использования электронного обучения, особенно это связано с последними событиями в стране за 2020 год, когда все учебные заведения перешли на дистанционное обучение. Однако стоит обратить внимание, что уровень электронного образования в России, по мнению специалистов, отстает на 5-7 лет по сравнению с другими странами [1].

Система дистанционного обучения «Moodle» (модульная объектно-ориентированная среда) была создана для осуществления самостоятельной подготовки к занятиям и выполнения домашнего задания в период самостоятельной работы как по очной, так и по заочной формам обучения. В связи с последними событиями в России система дистанционного обучения «Moodle» стала использоваться преподавателями БЮИ МВД России для проведения учебных занятий. Более подробно рассмотрим, как используется данный электронный ресурс.

Программное обеспечение, необходимое для функционирования системы «Moodle», выполняет LMS (Learning management system – система управления обучением). LMS – это платформа для развертывания электронного обучения [2].

Дистанционное обучение позволяет не только самостоятельно изучать учебный материал, а также расширять и углублять полученные знания, выполнять практические задания. После перехода на обязательное дистанционное обучение система «Moodle» позволила также проводить и учебные занятия в форме семинаров и практических занятий. Использование системы «Moodle» позволило объективно оценивать степень усвоения учебного материала обучающихся по очной и заочной формам обучения при условии выполнения ими самостоятельно всех заданий, материал которых предусмотрен рабочей программой данной учебной дисциплины. Конечно, нельзя не отметить, что из-за отсутствия аудиторных занятий имеется сложность оценивания качества полученных знаний обучающимися.

В связи с этим при изучении любого курса дисциплины в БЮИ МВД России используется система дистанционного обучения «Moodle».

Дистанционный курс, независимо от изучаемой дисциплины, состоит из следующих блоков:

– новостной блок, состоящий из разделов «Объявления», «Форум» и отдельной вкладки для консультирования, где можно задать вопрос преподавателю. Благодаря данному блоку обучающиеся всегда овладеют необходимой и актуальной информацией;

– в организационном блоке представлены методические рекомендации для изучения дисциплины, планы семинарских и практических занятий, а также немаловажным является расположение в данном блоке рекомендуемой литературы к изучению;

– учебный блок является основным блоком, благодаря которому обучающиеся получают знания, а также совершенствуют полученные навыки. Данный блок, состоит из следующих разделов:

– теоретический материал, наличие которого обязательно и независимо от наличия лекции по той или иной теме. Однако если лекция предусмотрена учебным планом, то при ее изучении происходит оценка получаемых знаний: для перехода от одного вопроса лекции к другому обучающемуся необходимо ответить на предложенный преподавателем вопрос, ответ на который имеется в изученном им разделе лекции. Если обучающийся не может ответить правильно, то система дистанционного обучения возвращает его к прочтению вопроса лекции повторно до тех пор, пока им не будет выбран правильный вариант ответа. По итогам лекции обучающемуся выставляется процент изучения лекции в соответствии с его ответами на предложенные преподавателем вопросы. Также в теоретическом разделе преподаватель может выставить презентацию или видеофрагмент для более наглядного изучения теоретического материала.

Если в соответствии с тематическим планом изучаемой дисциплины по той или иной теме предусмотрено семинарское занятие, то на усмотрение преподавателя оно может пройти в следующих форматах:

– путем обсуждения вопросов, вынесенных рабочим планом семинарских занятий в чате, где происходит активная переписка между преподавателем и обучающимся;

– путем подготовки письменного задания на предложенные преподавателем вопросы семинарского занятия.

Если в соответствии с тематическим планом изучаемой дисциплины по той или иной теме предусмотрено практическое занятие, то на усмотрение преподавателя оно может пройти в следующих форматах:

– решение задач в чате, где происходит активное обсуждение того или иного решения, принятого обучающимся;

– выполнение практического задания каждым обучающимся индивидуально и предоставление результатов выполнения на проверку преподавателю.

По завершении изучения темы каждый преподаватель по своему личному усмотрению может расположить в конце темы тестирование, для проверки и оценки полученных знаний:

– справочный блок содержит в себе справочные материалы для более качественного усвоения учебного материала такие, как словарь терминов, наиболее часто используемых слов;

– завершающим является контрольный блок, который содержит в себе задания для промежуточного и итогового контроля знаний. Задания могут быть представлены в форме теста или выполнения практического задания.

Выполнение заданий, предусмотренных в рамках семинара или практического занятия, возможно только в период их проведения, то есть ограничены по времени, тем самым обучающемуся задаются условия согласно программе обучения. После проведения семинара или практического занятия работа, выполненная обучающимся на занятии, оценивается и преподаватель выставляет оценки в журнал. Также преподаватель комментирует выполненную работу и обосновывает получение обучающимся именно той или иной оценки, в результате чего обучающийся знает свои ошибки и недочеты.

Таким образом, современные методы обучения благодаря новым информационным технологиям позволяют не только повысить качество усвоения учебного материала, а также в сложной обстановке, складывающейся в стране и мире, продолжать процесс обучения дистанционно. Использование в лекциях качественной графики, звука, анимации дает возможность более качественного усвоения обучающимися учебного материала. Преимущество электронного учебного курса также заключается в полноте охвата необходимых областей знаний и их достаточной глубине. При появлении вопросов по изучаемым темам у обучающихся они их могут задать преподавателю, используя разделы информационного блока той лили иной дисциплины. Говоря о необходимости образования и постоянном самообразовании человека в настоящее время, повышении собственной квалификации, подразумеваем обучение, которое может происходить на удаленном расстоянии от образовательной организации без отрыва от выполнения своих должностных обязанностей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Обзор мирового и российского рынка электронного обучения [Электронный ресурс]. – Режим доступа: https://ra-kurs.spb.ru/info/articles/?id=42.

2. MOODLE [Официальный сайт]. – Режим доступа: http://www.moodle.org.

УДК 656

ФАКТОРЫ, ВЛИЯЮЩИЕ НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ

Иванов И.П.,
кандидат педагогических наук, доцент
(Краснодарский университет МВД России);
Осинцева Л.М.;
Кирюшин И.И.
(Барнаульский юридический институт МВД России)

Аннотация: в статье рассматриваются вопросы обеспечения безопасности дорожного движения на территории Российской Федерации и множество факторов, как объективных, так и субъективных, влияющих на ситуацию дорожно-транспортного движения.

Ключевые слова: ДПС, ПДД, ГИБДД, безопасность, дорожное движение, стоп-линия, Глонасс-БДД.

FACTORS INFLUENCING THE ENSURANCE OF ROAD SAFETY

Ivanov I.P.,
Candidate of Pedagogical Sciences, Associate Professor
(Krasnodar University of the MIA of Russia);
Osintseva L.M.;
Kiryushin I.I.
(Barnaul Law Institute of the MIA of Russia)

Abstract: the article discusses the issues of ensuring road safety in the Russian Federation, and many factors, both objective and subjective, that affect this.

Keywords: traffic police, traffic rules, traffic police, safety, road traffic, stop line, glonass-BDD.

В современном мире вопрос, связанный с обеспечением безопасности дорожного движения, актуален как никогда, так как уровень автомобилизации населения за последние годы возрастает стремительно, а вместе с ними и растет количество нарушений, совершаемых с их участием. Наша страна занимает одну из лидирующих позиций в мире по количеству жертв ДТП. Согласно статистике, в среднем в России погибают два человека в час. По данным Росстата и ГИБДД (см. рис. 1), статистика ПДД с начала 2020 года не приводит к положительным тенденциям: аварий на дорогах становится все больше. За январь-февраль 2020 года ДТП произошло на 4% больше, чем за прошедший период прошедшего года, при этом количество погибших возросло на 13,7%, а раненых

соответственно на 3%. Причем, что самое парадоксальное, ДТП возросли по всем направлениям (как по количеству ДТП, так и по смертности и раненым лицам). Органы власти для сохранения безопасности на дорогах используют множество различных видов оборудования и специальных средств. Например, камеры фото-, видеофиксации, устанавливаемые достаточно часто на дорогах, не приводят к улучшению ситуации по снижению количества ДТП.

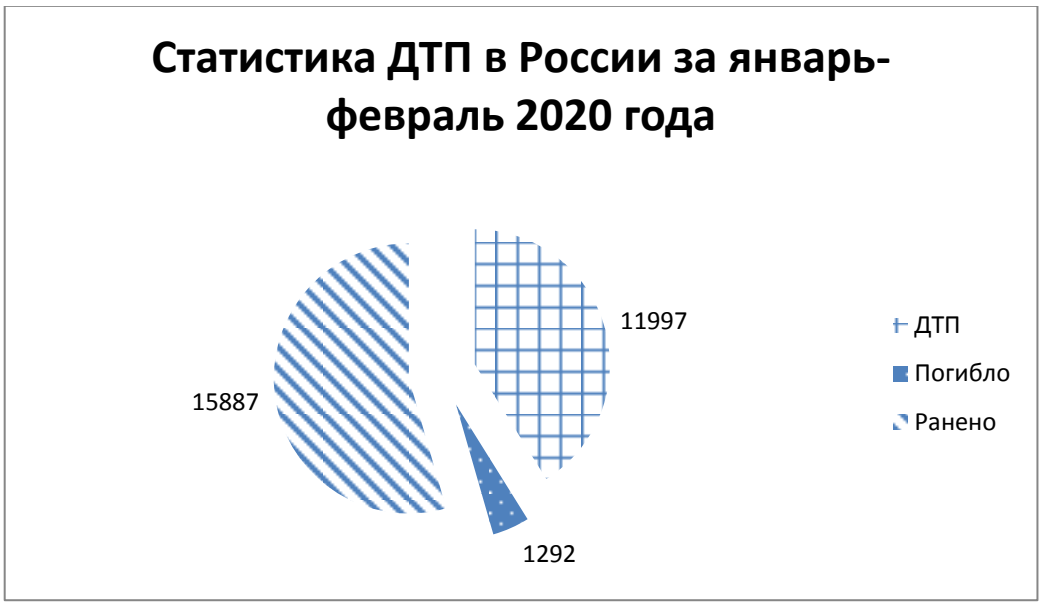


Рисунок 1. Статистика ДТП в России за январь-февраль 2020 г.

Прежде, чем перейти к факторам, влияющим на изменение безопасности дорожного движения, рассмотрим, что скрывается под терминами «безопасность», «дорожное движение» и что скрывается под понятием «безопасность дорожного движения». Так как ответ на эти вопросы позволяет проанализировать влияние устанавливаемых камер видео- и фотофиксации на безопасность дорожного движения. Безопасность – это состояние защищенности личности, общества, государства и среды жизнедеятельности от внутренних и внешних угроз или опасностей»[1]. «Дорожное движение – совокупность общественных отношений, возникающих в процессе перемещения людей и грузов с помощью транспортных средств или без таковых в пределах дорог»[2]. Следовательно, понятие «Безопасность дорожного движения» – это комплекс мероприятий, направленных на обеспечение безопасности всех участников дорожного движения. Светофоры, дорожные знаки, дорожная разметка и другое – все это служит для обеспечения безопасности дорожного движения, но этого недостаточно, так как водители все равно нарушают ПДД.

[1] Безопасность / Гражданская защита: энциклопедия в 4-х т. – Москва: ФГБУ ВНИИ ГОЧС (ФЦ), 2015.
[2] Постановление Правительства Российской Федерации от 23.10.1993 № 1090 (ред. от 26.03.2020) «О Правилах дорожного движения».

В настоящее время большинство водителей, даже самых законопослушных, становятся нарушителями ПДД. И речь идет не о малозначимых проступках, за которые не предусмотрены штрафы, а о достаточно серьезных нарушениях, которые зачастую приводят к серьезным последствиям. Вся проблема заключается в том, что мы не привыкли смотреть на установленные дорожные знаки, особенно если они не запрещающие. Такие знаки, как «въезд запрещен», «ограничение скорости», «обгон запрещен», наше периферическое зрение автоматически их выхватывает, и на эти знаки мы с Вами стараемся реагировать. А вот на другие дорожные знаки, за нарушение требований которых вряд ли лишат прав водителя, как правило, остаются без должного внимания.

Например, ст. 12.12 КоАП РФ нарушение – проезд на запрещающий сигнал светофора. Все знают, что проезд на красный сигнал светофора – это явное нарушение правил дорожного движения, вот только не для всех современных водителей это считается нарушением де факто, и что жёлтый сигнал светофора относится тоже к запрещающим сигналам. Сразу хочется отметить, что в ПДД есть исключение, которое разрешает движение на жёлтый сигнал светофора. В п. 6.14 ПДД сказано, что «водители, которые при включении жёлтого сигнала или поднятии регулировщиком руки вверх не могут остановиться, не прибегая к экстренному торможению в местах, определяемых п. 6.13 правил, разрешается дальнейшее движение». В частности, этим правилом и пользуется большинство современных водителей. Со стороны правоприменительной практики доказать, что водитель имел возможность остановиться, но проигнорировал данное действие, очень сложно. Следовательно, штрафы за проезд на жёлтый сигнал светофора являются большой редкостью, а если и случаются, то чаще всего оспариваются нарушителями в суде.

Еще одной разновидностью частых нарушений является «движение без остановки запрещено», знак 2.5. Знак «Стоп» запрещает движение без остановки перед стоп-линией, а если её нет, то перед краем пересекаемой проезжей части. Согласно Приложению 1 к ПДД «водитель, увидевший знак «Движение без остановки запрещено», обязан остановить свое транспортное средство перед стоп-линией. Вместо нее (или вместе с ней) около знака 2.5 может быть установлена информационная табличка 6.16 («Стоп-линия»). В этом случае прекратить движение необходимо перед воображаемой линией, которая проходит через этот графический объект» [1].

В приведенном случае можно смело утверждать, что если аналогичный знак установлен в глухой местности, перед хорошо просматриваемым перекрестком, то многие водители его просто игнорируют.

С недавнего времени комплексы фото-, видеофиксации на дорогах следят за данным видом правонарушения. Камер слежения на дорогах водители сегодня бояться больше, чем сотрудников ДПС, так как камеры беспристрастны, неподкупны и работают в круглосуточном режиме. Сразу же хочется отметить, что на перекрестках, где устанавливаются такие камеры, нарушителей ПДД становится меньше.

Проведенный анализ эффективности комплексов фото-, видеофиксации нарушений ПДД в регионах Российской Федерации компанией «Глонасс-БДД» показал, что в зоне действия некоторых комплексов фото-, видеофиксации происходит снижение числа ДТП, что составило около 75% нарушений в прошлом году. По словам генерального директора «Глонасс-БДД» Максима Нечеухина: «Статистика нарушений ПДД в местах установки систем фото-, видеофиксации, можно сказать, приблизилась к нижнему порогу: данные за 2019 год свидетельствуют, что под камерами водители в большинстве случаев ведут себя дисциплинированно. Формально камера, установленная несколько месяцев или лет назад, уже не влияет на статистику нарушений. При этом ее польза остается очевидной, так как она продолжает выполнять профилактическую функцию именно на этом участке дороги».

Но как на самом деле камеры фото-видеофиксации влияют на безопасность дорожного движения? Исследование проводилось госкорпорацией «Ростех», которая опубликовала следующие данные: «В ряде регионов положительно на дорожную статистку влияет менее 20% установленных дорожных камер». Всего было проанализировано 15000 комплексов видеофиксации, а также рассчитано их влияние на снижение количества ДТП в 2019 году. При этом учитывалась статистика ДТП с пострадавшими в различных регионах за пять лет. Исследования показали, что количество установленных камер практически никак не влияет на эффективность дорожного движения. Следовательно, процент комплексов, влияющих на улучшение дорожных ситуаций, в большинстве регионах очень низок, а абсолютное множество камер бесполезны с точки зрения безопасности.

Таким образом, на безопасность дорожного движения влияет множество факторов, как объективных (состояние дорог, интенсивность движения, пешеходы, время года и др.), так и субъективных (нарушение правил водителем и пешеходом, состояние водителя и др.). Следовательно, можно сделать вывод, что на безопасность дорожного движения влияет целый комплекс факторов, состоящий из совокупности элементов «человек», «транспортное средство», «дорога», действующих в определенной «среде». Все эти элементы целостной дорожно-транспортной системы существуют в отношениях и связях между собой и образуют единую целостность.

В частности, состояние безопасности дорожного движения в большинстве случаев определяется дисциплиной и профессионализмом водителя. В нашей стране более 85% ДТП происходит по причине нарушения правил водителями транспортных средств. Это подтверждает необходимость комплексного повышения качества допуска водителей к участию в дорожном движении, а именно к качеству подготовки и приема экзаменов. Также хочется обратить внимание на проблему аварийности на пешеходных переходах, которая в основном связана с низкой дисциплинированностью как водителей, так и самих пешеходов. Большинство наездов и пострадавших приходится на нерегулируемые пешеходные переходы. Особо хочется отметить, что доля ДТП при наезде на пешехода на регулируемых пешеходных переходах за последние пять лет возросла более чем в два раза.

По данным, приведенным на сайте Росстата и ГИБДД, вышеобозначенные факты позволяют выделить основные причины ДТП за 2019 год (см. рис. 2):

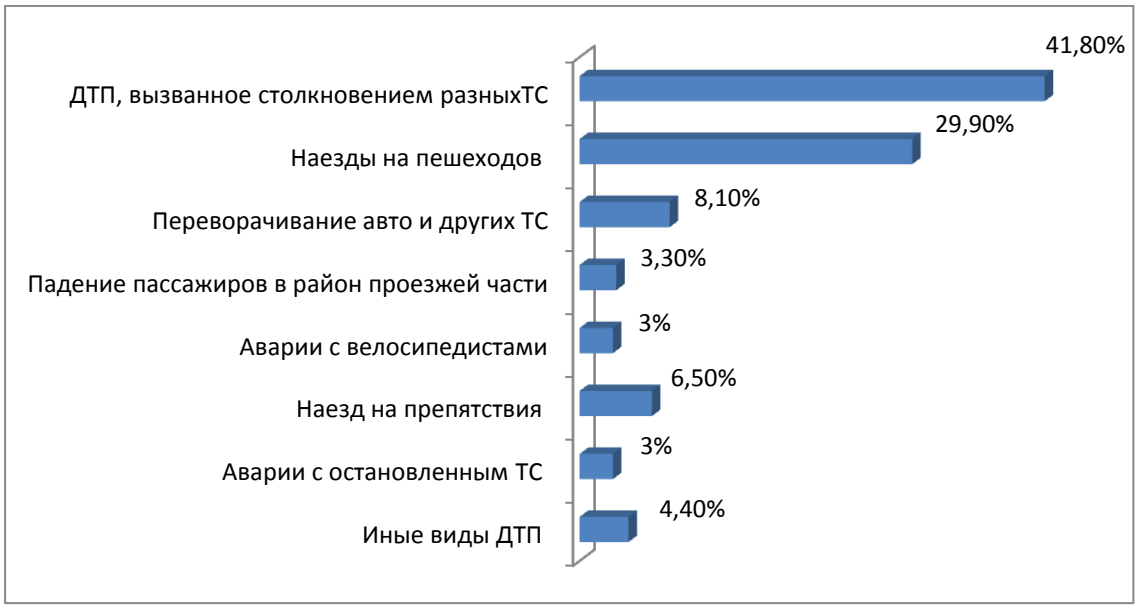


Рисунок 2. Основные причины совершения ДТП в России за 2019 год

Как было уже выше отмечено, что основной причиной дорожно-транспортных происшествий является нарушение водителями ПДД. По данным Росстата, данный показатель составляет 89,23% от общего числа количества дорожно-транспортных происшествий.

Нежелание водителей транспортных средств соблюдать ПДД является первостепенной причиной смертности на дорогах. Также хочется отметить наиболее существенные причины аварийности на дорогах по вине водителей:

- несоблюдение очередности при проезде перекрестков – 20%;
- неправильный выбор дистанции – 10,0%;
- нарушение правил проезда пешеходных переходов – 9,2%;
- выезд на полосу встречного движения – 8,4%;
- несоответствие скорости конкретным условиям движения – 5,8%;
- нарушение требований сигнала светофора – 2,7%;
- превышение установленной скорости движения – 2,3%;
- нарушение правил обгона – 1,3%.

На втором месте, исходя из статистических данных, находится нарушение требований к эксплуатационному состоянию автомобильных дорог и железнодорожных переездов. Этот показатель занимает примерно треть всех ДТП по стране.

Третье место среди причин ДТП занимает нарушение ПДД пешеходами. Доля ДТП от общего числа дорожно-транспортных происшествий, в которых виновником является пешеход, составляет 10,56%, т.е. каждое десятое ДТП происходит по вине пешехода.

Основными причинами ДТП по вине пешеходов являются переход дороги в неустановленном месте, переход дороги на запрещающий сигнал светофора, движение по обочине с правой стороны, несоблюдение требований безопасности при переходе или движении по обочине в темное время суток и многие другие факторы.

Существенной долей ДТП является и эксплуатация технически неисправных транспортных средств. Дорожно-транспортные происшествия, при которых зафиксированы технические неисправности транспортных средств, либо условия, при которых запрещена их эксплуатация, составили 4,14% от общего числа всех нарушений. Основными видами технических нарушения являются: установка на одну ось ТС шин различных размеров, конструкций, моделей, с различными рисунками протектора, а также установка ошипованных и неошипованных шин одновременно, наличие конструктивных изменений по сравнению с серийными транспортными средствами, сведения о которых отсутствуют в регистрационных документах, неисправность внешних световых приборов, а также коэффициент светопропускания стекол менее нормативного.

Подводя итоги, хочется сказать, что независимо от того, какие законы и наказания принимаются для снижения количества дорожно-транспортных происшествий, главным в безопасности движения всегда будет являться человеческий фактор. Прежде всего именно человеческий фактор определяет причины возникновения дорожно-транспортных происшествий и их последствия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баумтрог В.Э., Каширский Д.Ю., Рычкова Н.В., Кирюшин И.И., Осинцева Л.М. Специальная техника в деятельности государственной инспекции безопасности дорожного движения МВД России: учебно-методическое пособие. – Барнаул, 2019.

2. Иванов И.П., Помогалов А.А. Выявление закономерностей и построение математической модели совершения дорожно-транспортных происшествий: научно-исследовательская работа. – Краснодар, 2019.

3. Постановление Правительства Российской Федерации от 23.10.1993 № 1090 (ред. от 26.03.2020) «О Правилах дорожного движения» (вместе с «Основными положениями по допуску транспортных средств к эксплуатации и обязанности должностных лиц по обеспечению безопасности дорожного движения») // СПС «КонсультантПлюс».

УДК 34

ПРАВОВЫЕ И ЭТИЧЕСКИЕ АСПЕКТЫ ЗАИМСТВОВАНИЯ С ТОЧКИ ЗРЕНИЯ НАРУШЕНИЯ АВТОРСКИХ ПРАВ

Акапьев В.Л.,
кандидат педагогических наук;
Гуржий А.А.;
Дрога А.А.;
Савотченко С.Е.,
доктор физико-математических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: проанализированы проблемы списывания и заимствования в научных и учебных учреждениях. В зависимости от целеполагания проблема заимствования разделена на две основных составляющих. Рассмотрены основные проблемы нарушения авторского права в связи активным развитием глобальной компьютерной сети.

Ключевые слова: плагиат, заимствование, авторское право, правообладатель.

LEGAL AND ETHICAL ASPECTS OF PLAGIARISM IN TERMS OF COPYRIGHT INFRINGEMENT

Akapev V.L.,
Candidate of Pedaqoqical Sciences;
Gurzhiy A.A.;
Droga A.A.;
Savotchenko S.E.,
Doctor of Physical and Mathematical Science, Associate Professor
(Putilin Belgorod Institute of the MIA of Russia)

Abstract: the problems of writing off and borrowing in scientific and educational institutions are analyzed. The problem of borrowing is divided into two main components depending on the goal setting. The main problems of copyright infringement in connection with the active development of the global computer network are considered.

Keywords: plagiarism, borrowing, copyright, copyright holder.

В настоящее время проблема плагиата широко распространена в России. Следует отметить, что в последние годы данная проблема встает все острее и не могла не затронуть научное сообщество, что обусловило появление большого количества работ на данную тематику [1-21]. Основной целью данной работы

является выявление правовых и этических проблем заимствований и анализ зарубежного опыта в борьбе с плагиатом.

Проблема плагиатирования разделятся на две основных составляющих с точки зрения целеполагания: 1) плагиат в научных исследованиях и учебных работах с целью присвоения их результатов; 2) плагиат в нарушении авторских прав на произведения с целью извлечения коммерческой выгоды.

Первая составляющая развивается в высших учебных заведениях и научных организациях. Помимо заимствований в квалификационных и научных работах также актуальна проблема заимствований и в форме списывания на экзамене, что влечет к снижению уровня и качества образования и, как следствие, снижению качества работы во всех отраслях деятельности. Следует выделить следующие направления распространения плагиата в вузах: «помощь» на экзамене, плагиат контрольных работ, покупка контрольных работ.

Борьба с плагиатом в текстах успешно решается с помощью современных информационных технологий в форме специальных автоматизированных систем. В настоящее время в российской системе образования активно используется такой продукт, как Антиплагиат.ВУЗ, – система для проверки текста на уникальность, которая чаще других систем используется в вузах. Особенность «Антиплагиат.ВУЗ» – отсутствие доступа к ней у студентов. Доступ (логин и пароль) есть только у преподавателей. Работу на данном сервисе также проверяет преподаватель. В некоторых вузах доступ к системе есть в библиотеке. В случае, если проверить работу с другого IP-адреса (например, компьютер находится за пределами вуза), текст работы может сохраниться в библиотеке и при последующей проверке показать 0% оригинальности. Уникальный текст – это текст, написанный с нуля, без копирований и заимствований. Он такой один. Без копий и повторений. Уникальность измеряют в процентах (%). К примеру, если значение равно 60%, значит 40% статьи скопировано из других источников. Различие систем Antiplagiat.ru (и других систем) и Антиплагиат. ВУЗ состоит в том, что у сервиса «Антиплагиат.ВУЗ» есть множество дополнительных возможностей (модули, коллекции), которых нет в остальных программах. Также сервис использует сразу несколько методов проверки (метод шингла, индексирование), поэтому иногда преподаватели возвращают работу, указывая на то, что процент уникальности невысок, при том, что проверяя текст в системе и других программах, вы получаете от 70% и выше.

Представляется важным отметить, что студентам не разрешается переписывать чужой текст. В случае если студент взял текст из печатного источника или Интернета, то он должен обязательно привести ссылку. При доказанном факте плагиата студент исключается из университета. Данная практика способствует развитию у студента творческого подхода при выполнении заданий. В российских вузах подобная практика была бы весьма полезной.

В [22] были рассмотрены взгляды студентов и преподавателей на обман в обучении. В этом исследовании был проведен опрос, который содержал вопросы на честность. Результаты в дальнейшем оценивались по шкале авторов. Всего было опрошено 220 студентов различных специальностей из трех университетов (66 по специализации психология 154 по специальности менеджмента).

Данные показывают, что 66,4% студентов сообщили, что они списывали в средней школе, колледже. Исследователями в работе был использован метод факторного анализа, благодаря которому была обнаружена корреляция между рейтингами студентов.

Лиз Макдауэл и Салли Браун в своей работе [23] отметили, что в последнее время наблюдается рост беспокойства по поводу обмана и плагиата в научной работе студентов. В анкетировании, проведенном в 1996 г., ученые обнаружили, что значительное число студентов, предпринимали различные формы мошенничества. В работе И. Бернарда и Дж. Витлей приведен обзор результатов 107 исследований распространенности плагиата в образовательных организациях [24].

Вторая составляющая плагиата, связанная с нарушением авторских прав на произведения с целью извлечения коммерческой выгоды, активно развивается в бизнес-индустрии. В условиях глобализации и появления средств распространения информации возникает необходимость охраны произведений, в том числе охраны произведений российских авторов за рубежом. В связи с необходимостью охраны произведений мировое сообщество предпринимает шаги к организации сотрудничества в сфере борьбы с контрафактом.

Рассмотрим международные соглашения по охране авторских и смежных прав. Так, Бернская конвенция по охране литературных и художественных произведений заключена в 1886 г. В 1971 г. в Конвенцию были внесены изменения. Участники данной конвенции создали Бернский союз с целью охраны прав авторов. Административные функции Бернского союза исполняет ВОИС [25]. В 1995 г. Бернскую конвенцию ратифицировала Российская Федерация. Основой Бернской конвенции являются материально-правовые нормы, регулирующие правоотношения, возникающие в связи с передачей и распространением охраняемых произведений и авторов этих произведений. Коллизионное регулирование подразумевает следование нормам права того государства, в котором испрашивается охрана прав автора или закона суда.

Всемирная Конвенция об авторском праве была принята в 1952 г. Цель данной конвенции заключается в том, чтобы дополнить существующие нормы об авторском праве. Данные нормы не должны быть заменены или нарушены Конвенцией. В данной Конвенции множество отсылок к нормам национального законодательства. Материально-правовых предписаний во Всемирной конвенции меньше, чем в Бернской конвенции. На сегодняшний день значение Всемирной конвенции невелико, поскольку большинство стран подписали Бернскую конвенцию.

Всемирная конвенция об авторском праве 1952 г. установила компромисс между формальностями и их отсутствием. Страны, ратифицировавшие конвенции, внесли изменения в законодательство согласно нормам конвенций. В США была отменена необходимость обязательной регистрации авторского права в 1988 г. В Бернской конвенции императивно установлен запрет на формальности при охране авторского права, который распространяется на зарубежных авторов. В странах, в которых формальности необходимы, правообладатель получает определенный объем прав и обязанностей, а также появляется механизм, позволяющий осуществить защиту прав на произведение. Поэтому

литературное создание, основанное на каком-либо из произведений, будет являться объектом авторского права. С принятием Бернской Конвенции необходимость регистрации авторского права с целью его охраны отпала.

В 1996 г. на дипломатической конференции в Женеве был подписан Договор ВОИС в сфере авторского права, которым был установлен новый уровень охраны авторского права, стимулирующий развитие творчества.

Следует упомянуть Мадридскую конвенцию об избежании двойного налогообложения выплат авторского вознаграждения, принятую в 1979 г. Согласно конвенции двойное налогообложение запрещено как в отношении авторских, так и смежных прав. Кроме того, существуют региональные документы. Например, Межамериканская конвенция по охране авторских прав, принятая в 1946 г. Сюда же относятся документы Европейского союза – регламенты и директивы.

Создание произведения порождает права и обязанности для автора данного произведения. Произведения автора подлежат охране, для чего необходимо соблюдение ряда формальностей, несмотря на требование Бернской конвенции.

Можно классифицировать страны по различным типам системы регистрации авторских прав: условно необязательная; необязательная; регистрация, которая применяется в отношении отдельных объектов.

Под условно необязательной системой регистрации понимается система, согласно которой авторские права возникают фактически одновременно с созданием произведения. Регистрация авторского права – это важнейший компонент его защиты. Отсутствие регистрации вызовет негативные последствия для автора [26].

Поэтому, например, национальное законодательство США включает рекомендации по регистрации произведений в бюро авторского права США. Если же автор зарегистрировал произведение до его написания или в первой месяц после написания, то в случае судебного спора об авторских правах автор получит возмещение в большем размере, чем это установлено в законе [27]. Необязательная регистрация распространена более всего. Согласно данной системе защита авторских прав возникает автоматически при создании художественного произведения. Негативные последствия при отсутствии регистрации авторского права отсутствуют. Автор может добровольно зарегистрировать произведение и получить дополнительную его охрану.

Регистрация авторского права в Чили порождает презумпцию авторства. Автором признается лицо, которое депонировало произведение изначально [28].

Также существует вариант регистрации только для отдельных видов произведений. Так, в Российской Федерации по желанию правообладателя регистрируются программы ЭВМ и баз данных. Регистрация других видов произведений возможна при участии общественных организаций.

Акты общественных организаций имеют косвенное значение. Российское авторское общество (РАО) критикует Э.П. Гаврилов [29]. По его мнению, регистрация произведения РАО не входит в его компетенцию и не имеет юридической силы. Такая регистрация подтверждает существование данного произведения, но не подтверждает авторство конкретного лица. Ю.С. Харитонова ука-

зывает на случаи, когда регистрация РАО подтверждала авторство конкретного лица [30].

Депонирование является одним из элементов регистрации. С помощью депонирования возможно объективирование в какой-либо форме произведения. При этом указывается авторство произведения и передача копии произведения в уполномоченный орган на хранение. Кроме охраны авторских прав депонирование выполняет функцию сбережения авторского произведения и передачу его следующим поколениями. Таким образом, выполняется архивная функция. Депонирование осуществляет защиту неимущественных прав автора. Особенно это важно в сети Интернет, носящей трансграничный характер.

В сфере, касающейся сети Интернет, также на сегодняшний день приняты соответственные международные правовые акты. Первый из них был принят в 1996 г. – интернет-договор.

На основании данных договоров национальное законодательство приводится в соответствие с требованиями цифровой эпохи и темпами информационного развития.

В пример можно привести Австралию [31], в которой в 2016 г. депонированию подлежали электронные документы – книги, научные исследования, карты, журналы, сайты, социальные сети и др. В Чехии ситуация аналогична [32]. Депонированию подлежат документы, имеющие цифровую форму. В США депонированием занимается Бюро авторских прав – это федеральный орган власти – федеральный департамент, создан при библиотеке Конгресса – законодательного органа.

Необходимость депонирования можно объяснить тем, что данная процедура является косвенным подтверждением места создания произведения в электронно-цифровой форме. Это может повлиять на выбор наиболее подходящего права при рассмотрении спора. Регистрация и депонирование всех произведений потребует огромных финансовых, энергетических и людских ресурсов.

Таким образом, всеобщая обязательная регистрация авторских прав не может быть императивом (требованием). Это требование противоречит Бернской конвенции.

Рассмотрим особенности защиты произведений в отечественном праве. Предмет административного правонарушения согласно ч. 1 ст. 7.12 КоАП - экземпляры произведений, которые были изготовлены или распространены с нарушением ст. 7.12 КоАП РФ2 [33]. Экземпляр произведения – это копия произведения, которая была изготовлена в материальной форме. Экземпляр фонограммы – это копия фонограммы на материальном носителе, произведенная с фонограммы. Экземпляр включает все звуки, находящиеся на фонограмме. Кроме того, следует отметить, что для программ ЭВМ (баз данных) характерно распространение на магнитных и оптических носителях, а также в форме копии произведения, записанной, хранящейся или воспроизведенной в памяти ЭВМ, которая является экземпляром произведения, с предоставлением доступа к ней сетевым и иным способом (ст. 1 ЗоПОП) [34].

На сегодняшний день с развитием сети Интернет появились новые факты нарушения авторских прав, поскольку размещенный в сети материал часто вос-

принимается как не имеющий авторства [35, 36]. Копирование материала не несет для нарушителей никаких финансовых затрат кроме платы провайдеру. Поэтому на сегодняшний день появляется необходимость охраны авторских прав по всему миру ввиду глобального характера сети Интернет [37].

Правообладатель имеет вариативность в процессе волеизъявления в сфере распоряжения собственными правами. Автор вправе зарегистрировать свое произведение в государственном реестре или заявить отказ от исключительных прав в пользу общественности. Автор вправе заключить договор, заявить публичную оферту и др.

Регистрация произведения является одним из способов защиты авторского права. Существуют различные подходы к регистрации произведений на основании специфики права различных государств. Так, в странах континентальной системы регистрация права производится автоматически без необходимости делать специальное заявление. В странах англо-американской системы зарегистрировать произведение можно было только лишь путем государственной регистрации после специального заявления. Для этого необходимо было: подать заявление; отслеживать срок действия авторских прав; депонировать рукописи; оплачивать государственную пошлину и др.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Благинин В.А. Наукометрические показатели и критерии стимулирования научно-педагогических работников с использованием оценки заимствований // Педагогическая информатика. 2018. № 2. С. 29–33.
2. Бурлакова Е.В., Качалова С.М. Системный подход к формированию контента комплексных информационных образовательных порталов // Педагогическая информатика. 2018. № 2. С. 34–44.
3. Авдеева Н.В., Сусь И.В. Особенности экспертной оценки оригинальности диссертационных работ / Румянцевские чтения-2019: сборник материалов Международной научно-практической конференции: в 3 ч. – Москва: 2019. С. 5–10.
4. Кузьменков В.А. Норма плагиата в российских диссертациях // Abyss (Вопросы философии, политологии и социальной антропологии). 2019. № 2 (8). С. 21–26.
5. Садова Т.С. Текстовые заимствования (плагиат) как предмет лингвистической экспертизы // Acta Linguistica Petropolitana. Труды института лингвистических исследований. 2019. Т. 1. № 15. С. 184–194.
6. Леонтьева И.Н. Плагиат в современном дизайне и айдентике: сборник материалов III Всероссийской научно-практической интернет-конференции с международным участием «Дизайн XXI века». – Тула: Тульский государственный университет, 2019. С. 39–44.
7. Домаков В.В., Матвеев В.В. Реалии плагиата и перлы российского интернет-проекта «антиплагиат» // Национальная безопасность и стратегическое планирование. 2019. № 1 (25). С. 114–126.
8. Гельфанд М.С. Недобросовестные заимствования в диссертационных работах // Образование и наука. 2018. Т. 20. № 3. С. 160–181.

9. Матвейчев О.А. Платон как плагиатор // Миссия конфессий. 2018. Т. 7. № 1 (28). С. 71–83.

10. Попова О.В., Мокрецова Л.А. Плагиат и академическая честность студента: проблемы и пути решения / Современная наука: от плагиата к академической честности: сборник материалов Всероссийской научно-практической конференции. – Курск, 2019. С. 101–112.

11. Евстафьева И.В. О значении понятий «плагиат» и «антиплагиат» в современном российском праве / Юридическая наука и практика: альманах научных трудов. – Самара: Самарский юридический институт ФСИН России, 2019. С. 70–72.

12. Демидова Л.Д. Плагиат как способ сохранения научного результата: неожиданный сюжет из истории дореволюционного изучения русского старообрядчества // Исторический курьер. 2019. № 6 (8). С. 129–136.

13. Лободенко Е.И., Иоголевич Н.И. Размышления об этических проблемах заимствований в высшей школе / Обнаружение заимствований-2018: сборник научных трудов Международной научно-практической конференции. – Уфа, 2018. С. 71–79.

14. Стародубцева А.Д. Заимствование в рекламе / Интеграционные процессы в науке в современных условиях: сборник статей Международной научно-практической конференции. – Уфа, 2019. С. 83–85.

15. Крапивин Ю.Б. Система «плагиатконтроль» как инструмент экспертизы текстовых документов // Информатика. 2018. Т. 15. № 1. С. 103–109.

16. Марков А.В., Миронова Я.С. Анализ использования специализированных программных сервисов для проверки текстовых материалов на объем заимствований в научно-технических проектах // Colloquium-journal. 2018. № 9-1 (20). С. 23–25.

17. Усачева Е.А. К вопросу о допустимости использования системы «антиплагиат» для определения авторства и оценки оригинальности произведения // Образование и право. 2019. № 4. С. 204–210.

18. Левин В.И. Мультиплагиат и будущее российской науки // Ректор ВУЗа. 2018. № 11. С. 50–54.

19. Гореликов С.Ю. «Антиплагиат» – фильтр или тормоз? (критическая статья) // Наука и школа. 2018. № 6. С. 201–204.

20. Большакова В.А. Проблема студенческого плагиата в науке и образовании / Современное образование: актуальные вопросы, достижения и инновации: сборник статей XXVIII Международной научно-практической конференции. – Пенза, 2019. С. 59–61.

21. Хованская Е.А. Значимость соблюдения этических норм в публикационной деятельности // Alma mater (Вестник высшей школы). 2019. № 4. С. 106–111.

22. Examining the Decision Process of Students' Cheating Behavior: An Empirical Study / Richard A. Bernardi1, Rene L. Metzger, Ryann G. Scofield Bruno, Marisa A. Wade Hoogkamp, Lillian E. Reyes and Gary H. Barnaby / Journal of Business Ethics. 2004. Vol. 50. – Режим доступа: https://doi.org/10.1023/B:BUSI.0000025039.47788.c2.

23. Liz McDowell and Sally Brown. Assessing students: cheating and plagiarism / The Higher Education Academy [Электронный ресурс]. – Режим доступа: http://www.ilt.ac.uk/1144.asp (дата обращения: 14.04.2020).

24. Bernard E., Whitley Jr. Factors associated with cheating among college students: A Review // Recearch in Higher Education. 1998. Vol. 39. № 3. P. 235-274. – Режим доступа: https://doi.org/10.1023/A:1018724900565.

25. Бернская конвенция по охране литературных и художественных произведений от 9 сентября 1886 г. [Электронный ресурс]. – Режим доступа: http://www.wipo.int/treaties/ru/text.jsp?file_id=283698.

26. 17 U.S. Code § 410.Registration of claim and issuance of certificate [Электронный ресурс]. – Режим доступа: https://www.law.cornell.edu/uscode/text/17/410 (дата обращения: 14.04.2020).

27. Copyright Basics [Электронный ресурс]. – Режим доступа: https://www.copyright.gov/circs/circ01.pdf (дата обращения: 14.04.2020).

28. Art. 8 de la Ley № 17.336 [Электронный ресурс]. – Режим доступа: https://www.leychile.cl/Navegar?idNorma=28933 (дата обращения: 14.04.2020).

29. Гаврилов Э.П. «Формат» аудиовизуального произведения и некоторые вопросы права интеллектуальной собственности // Хозяйство и право. 2016. № 3. С. 64–79.

30. Харитонова Ю.С. Правовое значение фиксации интеллектуального права с помощью технологии распределенных ресурсов // Право и экономика. 2018. № 1. С. 15–21.

31. Copyright Act 1968 [Электронный ресурс]. – Режим доступа: http://www.wipo.int/wipolex/en/text.jsp?file_id=448217 (дата обращения: 14.04.2020).

32. Consolidated Version of Act № 121/2000 Coll., on Copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act, as amended by Act No. 81/2005 Coll., Act No. 61/2006 Coll. and Act No. 216/2006 Coll.) [Электронный ресурс]. – Режим доступа: http://www.wipo.int/edocs/lexdocs/laws/en/cz/cz043en.pdf (дата обращения: 14.04.2020).

33. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 02.08.2019) // Собрание законодательства Российской Федерации. 2002. № 1 (ч. 1). Ст. 1.

34. Закон Российской Федерации от 07.02.1992 № 2300-1 (ред. от 18.07.2019) «О защите прав потребителей» // Собрание законодательства Российской Федерации. 1996. № 3. Ст. 140.

35. Луткова О.В. Общественное достояние в международном авторском праве // Интеллектуальная собственность. Авторское право и смежные права. 2016. № 3. С. 45–58.

36. Международное частное право: учебник / под ред. Г.К. Дмитриевой. – 4-е изд. – Москва: Проспект, 2016. С. 526.

37. Мирошникова С.Д. Охрана произведений российских авторов за рубежом / Приоритеты развития и ценности экономики и общества: материалы международной научно-практической конференции. – Москва, 2018. С. 85–88.

УДК 378

ОНЛАЙН ОБУЧЕНИЕ – НЕОБХОДИМОСТЬ ИЛИ ЭВОЛЮЦИЯ ОБРАЗОВАНИЯ В ЦЕЛОМ

Епифанцева В.А.,
Хромых А.А.
(Краснодарский университет МВД России)

Аннотация: объектом исследования является организация образовательного процесса с использованием дистанционных цифровых технологий. Предметом исследования является роль функциональных систем для организации веб-конференций в повышении качества обучения. Для достижения высокого уровня образовательного процесса обучающихся необходимо обеспечить возможность приобретения ими глубоких фундаментальных знаний, развития пространственного воображения, стремления к самостоятельному изучению нового материала.

Ключевые слова: дистанционное обучение, онлайн-обучение, учебный процесс, информационные технологии.

ONLINE LEARNING – THE NECESSITY OR EVOLUTION OF EDUCATION IN GENERAL

Epifantseva V.A.,
Khromykh A.A.
(Krasnodar University of the MIA of Russia)

Abstract: the object of research is the organization of the educational process using remote digital technologies. The subject of the research is the role of functional systems for organizing web conferences in improving the quality of training. To achieve a high level of educational process, students must be able to acquire deep fundamental knowledge, develop spatial imagination, and strive for independent study of new material.

Keywords: distance learning, online learning, learning process, information technology.

В реалиях нашего времени становится понятным, насколько необходимым может быть дистанционное обучение.

Идея дистанционного образования появилась не сегодня. В «Великой дидактике», автором которой является Ян Коменский, 350 лет назад обозначено использование системного подхода в образовании [4]. Сегодня благодаря развитию информационных технологий, эта идея дистанционного образования не

только претерпела изменения, но и переросла в стратегически неотъемлемый инструмент образования.

Колоссальный объем информации в онлайн-пространстве дает возможность обучающимся, не выходя из дома, участвовать в образовательном процессе на более высоком уровне.

Результатом процесса информатизации образования становится появление у слушателей способности использовать современные информационные технологии для работы с информацией как в учебном процессе, так и для иных потребностей. Таким образом, у обучающихся происходит формирование информационно-коммуникативной компетентности [2].

Приказ Минобразования России от 30 мая 1997 г. № 1050 «О проведении эксперимента в области дистанционного образования» [6] можно считать официальной датой признания дистанционного образования в качестве реальной технологии образования. Начав путь с высших учебных заведений, дистанционные образовательные технологии пришли в общеобразовательные учреждения, и первая половина 2020 года показала их необходимость. Таким образом, идея дистанционного обучения не только имеет право на жизнь, но и будет развиваться в еще более ускоренном темпе.

Стоит разобраться почему одни курсы называют дистанционными, а другие онлайн? В чем их различия и есть ли они вообще?

Дистанционное обучение. При этой форме обучения «живой» контакт преподавателя и слушателя практически отсутствует. Лишь в форме редких консультаций.

Основной процесс заключается в просмотре записи видеолекций слушателем и предоставлении результатов решений задач преподавателю посредством обратной связи с применением информационных технологий.

Теперь разберем термин «онлайн-обучение».

Онлайн-обучение. В отличие от дистанционного образования основной акцент сделан на получении знаний, умений и навыков в режиме реального времени «здесь и сейчас». Следует заметить, что онлайн-обучение считается логическим продолжением дистанционного.

Во время онлайн-обучения обучающийся изучает лекции, презентации, участвует в решении практических заданий в прямой трансляции, проходит интерактивные тесты, обменивается файлами с преподавателем, общается с другими слушателями и преподавателями в чатах [5].

К общим достоинствам онлайн-обучения и дистанционного образования можно отнести процесс получения новых знаний, навыков и умений вне аудиторий и непосредственного контакта с преподавателями [1], возможность исключить эмоциональное напряжение, пространственные и временные преграды. Доступное образование для любого слушателя.

Недостатками указанных форм обучения является то, что не у каждого слушателя есть возможность пользоваться самыми современными информационными технологиями. Кроме того, не каждый преподаватель имеет достаточный уровень знаний, навыков и компетенций в области информационных технологий, необходимых для реализации онлайн-обучения. Также не все образо-

вательные организации готовы перейти на новый уровень образования и совмещать традиционные формы обучения и дистанционные.

Дистанционное обучение стало популярным с развитием сети Интернет, открыв новые возможности развития для жителей удаленных населенных пунктов [3]. Вначале дистанционное обучение воспринималось лишь как дополнительный способ приобретения знаний или подготовки к экзаменам. Сейчас можно пройти полноценные дистанционные курсы и программы повышения квалификации от передовых университетов, коммерческих и некоммерческих компаний из разных стран, находясь в любой точке планеты.

Информационные технологии становятся основным инструментом, который человек будет использовать не только в профессиональной деятельности, но и в повседневной жизни.

На наш взгляд, комплексное применение традиционных форм обучения и дистанционного образования значительно оживляет процесс объяснения учебного материала и повышает его качество.

Также не следует забывать про требования здоровьесберегающего и эргономического характера, они отвечают гигиеническим нормам и санитарным требованиям работы с информационной техникой.

Основной приоритет в профессии преподавателя – это не останавливаться на достигнутом. Не надо стоять на одном месте, нужно двигаться вперед, совершенствовать приемы и методы обучения, для того чтобы достичь высокого уровня в своей профессиональной педагогической деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Александрова В.Г. Роль инновационного подхода в подготовке молодого учителя // Педагогические науки: журнал. 2016 № 3. С. 45–47.

2. Андриенко Е.В. Конкурс профессионального мастерства как фактор развития конкурентоспособности и инновационной компетентности педагога // Педагогическое образование и наука: журнал. 2016. № 2. С. 28–30.

3. Дистанционное обучение: учебное пособие для вузов. – Москва: Владос, 2018. – 192 с.

4. Коменский Я.А. Педагогическое наследие / сост.: В.М. Кларин, А.Н. Джуринский. – Москва: Педагогика, 1989. – 416 с.

5. Лутфиллаев М.Х., Абдуллаев Э.Н. Некоторый опыт по использованию виртуальных лабораторных работ в дистанционном обучении. – Режим доступа: http://distant. ioso.ru/seminary/09-02-06/lutabd. htm.

6. Приказ Минобразования Российской Федерации от 30.05.1997 № 1050 «О проведении эксперимента в области дистанционного образования» // СПС «Консультант Плюс».

УДК 332.14:316.4

ЦИФРОВИЗАЦИЯ ГОРОДСКОЙ СРЕДЫ КАК ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Тарасенко А.А.,
кандидат педагогических наук;
Озеров И.Н.,
кандидат юридических наук, доцент;
Кириченко Ю.Н.,
кандидат юридических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Озеров К.И.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассматривается роль и анализ в современном мире системы «Умный город».

Ключевые слова: Умный город, цифровые системы, интеллектуальная транспортная система.

DIGITALIZATION OF THE URBAN ENVIRONMENT AS AN ELEMENT OF PUBLIC SAFETY

Tarasenko A.A.,
Candidate of Pedaqoqical Sciences;
Ozerov I.N.,
Candidate of Law, Associate Professor;
Kirichenko Yu.N.,
Candidate of Law, Associate Professor
(Putilin Belgorod Law Institute of the MIA of Russia);
Ozerov K.I.
(Kikot Moscow University of the MIA of Russia)

Abstract: this article discusses the role and analysis of the «Smart city» system in the modern world.

Keyword: smartcity, digitalsystems, intelligenttransportsystem.

Общественная безопасность, представляя собой совокупность урегулированных нормами права общественных отношений в сфере локализации и ликвидации угроз личности, обществу и государству, является составным элементом национальной безопасности. Как и любые другие общественные отношения, общественная безопасность также претерпевает различные изменения и трансформации, соответствующие развитию общества на современном этапе исторического развития.

Современное развитие общества и государства во всем мире имеет тенденцию к цифровизации окружающего пространства: отдельных отраслей, систем производства и целых пластов жизни городской среды. Речь идет о цифровизации как о взаимосвязи комплекса общественных отношений, построенных в цифровой среде. В Российской Федерации на сегодняшний день утверждены и реализовываются две национальные программы по указанному направлению:национальный проект «Жилье и городская среда» и национальная программа «Цифровая экономика» [13].

В рамках указанных программ Минстроем России был разработан проект «Умный город» для цифровизации городской среды. Его идея не является уникальной, это аналог программы «SmartCity», реализованной более чем в 2500 городах по всему миру.

Так, в 2014 году состоялось открытие одного из наиболее ярких представителей эко-инновационных городов – японского города Фудзисава, его строительство началось в 2010 году компанией Panasonic. Указанный город является продуктом реализации программы «SmartCity», экспериментальной площадкой по использованию и созданию технологий «умных городов», таких как запуск беспилотных автомобилей, организация интеллектуальных транспортных инфраструктур, использование солнечной энергии, переработка мусора и прочее [12].

Умный город – это эффективная интеграция физических, цифровых и человеческих систем в искусственно созданной среде с целью обеспечить устойчивое, благополучное и всестороннее будущее для граждан [17].

Проект «Умный город» направлен на улучшение качества жизни населения, прямое и эффективное взаимодействие власти и общества, повышение конкурентоспособности городов, создание безопасных и комфортных условий для жизни горожан. Проект базируется на пяти ключевых принципах:

1) ориентация на человека;
2) технологичность городской инфраструктуры;
3) повышение качества управления городскими ресурсами;
4) комфортная и безопасная среда;
5) акцент на экономической эффективности, в том числе, сервисной составляющей городской среды [15].

Основным инструментом для реализации принципов является максимально возможное внедрение цифровых систем во все сферы жизнедеятельности городских агломератов.

Проект направлен на цифровизацию населенных пунктов с численностью жителей от 100 тыс. человек, а также административных центров федеральных субъектов не зависимо от численности населения. Выбор обусловлен не только с точки зрения экономических факторов, но и с учетом постоянных процессов урбанизации и централизации населения в мире. По оценкам ООН, к 2050 году 68% населения будет проживать в городах. В условиях перенаселения обеспечение личной безопасности граждан, общественной безопасности является трудоемкой и сложной задачей для органов государственной власти. Ввиду этого проект «Умный город» включает в себя 17 компонентов и функциональных областей, которые в своей взаимосвязи образуют новые эффективные технологии

и прикладные решения, позволяющие при грамотном их использовании не просто повысить качество жизни граждан, а выйти на новый уровень комфортности городской среды и безопасности окружающего пространства.

Компоненты и функциональные области проекта «Умный город»:

1. Видеонаблюдение и видеоаналитика. В комплексе система видеонаблюдения и видеоаналитики представляет собой процесс фиксации ряда изображений с его последующим визуальным контролем автоматизированным анализом (автоматическое распознавание лиц, государственных номеров).
2. Камеры видеофиксации.
3. Ситуационные центры, ЕДДС.
4. Система 112.
5. ИТС – интеллектуальные транспортные системы. Интеллектуальная транспортная система – инженерно-технический комплекс, основанный на удаленном управлении городской транспортной системой, включающий в себя инфраструктуру, транспортные средства участников системы и регулирование дорожно-транспортных потоков, с целью обеспечения максимальной безопасности и осведомленности о дорожной ситуации.
6. Безопасность на общественном транспорте.
7. Профессиональная радиосвязь и широкополосный доступ (LTE, 5G).
8. IoT – интернет вещей.
9. Беспилотные автомобили.
10. Биометрия.
11. Обработка неструктурированных данных.
12. Технологии поддержки принятия решений.
13. Дополненная и виртуальная реальность.
14. Распределенные базы данных.
15. Геоинформационные технологии и навигация.
16. Машинное обучение.
17. Облачные/туманные/граничные вычисления [15].

Многие перечисленные компоненты и функциональные области уже были опробованы и интегрированы в городскую среду в процессе реализации функционирования аппаратно-программного комплекса «Безопасный город» в субъектах Российской Федерации. Данный аппаратно-программный комплекс (АПК) предназначен для контроля и фиксации посредством круглосуточного видеонаблюдения нарушений в сфере безопасности дорожного движения, правонарушений и происшествий в общественных местах, а также обеспечения экстренной связи граждан с подразделениями территориальных органов МВД России.

Что касается нашего места пребывания, то Белгород включен в список городов-пилотов по реализации проекта цифровизации городского хозяйства «Умный город». В связи с этим 14 июня 2019 года подписано трехстороннее соглашение между Министерством строительства и жилищно-коммунального хозяйства Российской Федерации, Белгородской областью и городским округом «Город Белгород».

Действует система автоматической фото-, видеофиксации нарушений правил дорожного движения с применением камер видеонаблюдения высокой четкости, установленных с учетом данных об аварийности и потенциальной опасности нарушения ПДД. В 2019 году установлено 120 камер. Работает автоматизированная система управления трафиком на перекрестке ул. Губкина и ул. Магистральной. Это позволило улучшить пропускную способность на дорогах и повысить безопасность дорожного движения.

Направление «Интеллектуальные системы общественной безопасности» предполагает создание системы интеллектуального видеонаблюдения. В 2019 году правоохранительными органами в адрес ЕДДС МКУ «Управление ГОЧС Белгорода» были направлены 250 запросов на предоставление архивной информации и для оперативной работы в режиме реального времени на базе городской системы видеонаблюдения. Действует электронная энциклопедия Службы 112, в которой объединены данные справочников ЕДДС, инструкций и алгоритмов действий.

Проект «Умный город» призван включить в себя и усилить функциональные возможности системы АПК «Безопасный город» тем самым вывести возможности обеспечения безопасности граждан на новый уровень. АПК «Безопасный город» является первой составляющей проекта «Умный город», вторая составляющая – интеллектуальная транспортная инфраструктура. Две эти основные составляющие должны быть модернизированы и расширены, оснащены современными инженерными решениями и цифровым управлением.

При анализе программы по ее составляющим мы видим, что их интеграция откроет новый уровень возможностей для правоохранительных органов по обеспечению личной и общественной безопасности на улицах городов. Технические возможности видеооборудования уже на современном этапе позволяют при необходимости извлекать изображения достаточного качества для проведения портретных экспертиз, при внесении алгоритмов просчитывания возможных вариантов событий видеоряда, передаваемого в режиме реального времени, позволяют правоохранительным органам быстрее реагировать на возможные правонарушения, а при использовании моделей противоправного поведения, аккумулированных криминологической наукой – предупреждать возможные преступления. При использовании криминалистических и оперативных учетов с программным сопоставлением изображений, передаваемых с камер в режиме реального времени или из архива, осуществлять поиск разыскиваемых лиц, идентификацию лиц, представляющих оперативный интерес, и других групп граждан.

Таким образом, мы можем заключить, что система «Умный город» при детальном рассмотрении действительно является современным и необходимым компонентом городской среды, она содержит в себе потенциал, позволяющий повысить качество жизни граждан, обеспечить комфортное и безопасное проживание в городской среде. Однако необходимо детальное согласование возможностей, заложенных в проекте, в рамках каждого отдельного ведомства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ (ред. от 17.10.2015) «О безопасности» // Собрание законодательства Российской Федерации. 2011. № 1. Ст. 2.
2. Федеральный закон от 6 марта 2006 г. № 35-ФЗ (ред. от 18.04.2018) «О противодействии терроризму» (с изм. от 29.03.2019) // Собрание законодательства Российской Федерации. 2006. № 11. Ст. 1146.
3. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 27.10.2019) «О полиции» // Собрание законодательства Российской Федерации. 2011. № 7. Ст. 900.
4. Федеральный закон от 9 февраля 2007 г. № 16-ФЗ (ред. от 02.08.2019) «О транспортной безопасности» (с изм. и доп., вступ. в силу с 06.08.2019) // Собрание законодательства Российской Федерации. 2007. № 7. Ст. 837.
5. Постановление Правительства Российской Федерации от 24 марта 1997 г. № 334 (ред. от 20.09.2017) «О порядке сбора и обмена в Российской Федерации информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера» // Собрание законодательства Российской Федерации. 1997. № 13. Ст. 1545.
6. Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 (ред. от 19.03.2014) «О единой системе межведомственного электронного взаимодействия» // Собрание законодательства Российской Федерации. 2010. № 38. Ст. 4823.
7. Приказ МВД России от 9 декабря 2015 г. № 1149 (в ред. приказа МВД России от 31.12.2016 № 949) «Об организации мероприятий по участию органов внутренних дел Российской Федерации в создании и развитии аппаратно-программного комплекса «Безопасный город»: зарегистрирован в Минюсте России 27 февраля 2015 г., рег. № 36263.
8. Распоряжение МВД России от 10 августа 2016 г. № 1/7891 «О рабочей группе МВД России по созданию и развитию правоохранительного сегмента аппаратно-программного комплекса «Безопасный город» // СПС «КонсультантПлюс».
9. Распоряжение Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р г. «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» // СПС «КонсультантПлюс».
10. Методические рекомендации по вопросам построения, развития и использования сегментов аппаратно-программного комплекса «Безопасный город», затрагивающих компетенцию МВД России 2017 г.
11. https://https://www.panasonic.ru/press_center/news/detail/464650.html (дата обращения: 04.02.2020).
12. http://government.ru/rugovclassifier/614/events.html (дата обращения: 04.02.2020).
13. http://www.minstroyrf.ru/trades/gorodskaya-sreda/proekt-tsifrovizatsii-gorodskogo-khozyaystva-umnyy-gorod.html (дата обращения: 08.02.2020).
14. https:// https://ria.ru/.html (дата обращения: 08.02.2020).
15. https://www.bsigroup.com/ru-RU/.html (дата обращения: 08.02.2020).

УДК 371.3

ПРИЕМЫ ОБУЧЕНИЯ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Корнилова Е.А.,
кандидат педагогических наук, доцент
(ГБОУ БИЮЛИ, г. Белгород);
Корнилова Н.А.
(БГТУ имени В.Г. Шухова)

Аннотация: в данной статье рассматриваются некоторые проблемы и особенности применения информационно-коммуникационных технологий в обучении. Описываются основные приемы такого обучения, а также предъявляемые к ним требования. Говорится тоже и о подсистеме методов и способов обучения с применением информационно-коммуникационных технологий. Также поднимается тема взаимосвязи методов и приемов обучения с применением информационно-коммуникационных технологий. Рассматривается сложная связь между приемами и методами обучения. Происходит деление приемов обучения на определенные категории. Немаловажным аспектом, рассматриваемым в данной статье, являются основные приемы продуктивного и творческого мышления, которыми должен овладеть преподаватель в стенах педагогического вуза.

Ключевые слова: обучения с применением информационно-коммуникационных технологий, методы и приемы обучения.

TEACHING METHODS USING INFORMATION AND COMMUNICATION TECHNOLOGIES

Kornilova E.A.,
Candidate of Pedagogical Sciences, Associate Professor
(GBOU BIULI, Belgorod);
Kornilova N.A.
(BSTU im. V.G. Shukhov)

Abstract: this article discusses some problems and features of the use of information and communication technologies in education. The main methods of such training are described, as well as the requirements for them. We also talk about the subsystem of methods and methods of training using information and communication technologies. The topic of interrelation of teaching methods and techniques with the use of information and communication technologies is also raised. The complex relationship between teaching methods and techniques is considered. There is a division of training techniques into certain categories. An important aspect considered in this

article is the basic techniques of productive and creative thinking, which should be mastered by a teacher in the walls of a pedagogical University.

Keywords: training using information and communication technologies, methods and techniques of training.

Основными проблемами обучения являются: постановка цели обучения (для чего учить?); подбор содержания обучения (чему учить?); выбор формы организации обучения (как организовать процесс обучения?); избрание средств обучения (при помощи чего учить?); отбор методов и приемов обучения (как обучать?). Без принижения значимости какой-либо из приведенных выше проблем следует особенным образом выделить важность подбора методов и приемов обучения. Ведь именно от приемов и методов обучения в итоге и будет зависеть ряд важнейших вещей, включающих в себя качество и количество знаний, навыков и умений учащихся, а также эффективность их познавательной деятельности.

Ко всему вышесказанному следует заметить, что именно подсистема методов, приемов и средств обучения, облекаемая в организационную форму, представляет собой основу любой технологии обучения. Ведь все теоретические положения и примеры из опыта, которые призваны объяснить сущность развивающего обучения, могут оказаться лишенными практического значения, если они не будут связаны с конкретными методами и приемами обучения [1]. Так как именно приемы и методы обучения являют собой средство реализации теории обучения на практике.

Так как противоречия в процессе обучения являются движущей силой развития мышления учащихся, то для их разрешения должны быть найдены соответствующие средства. Как раз такими средствами и являются дидактические методы и приемы. Ведь именно приемы и методы обучения определяют следствия теоретической модели обучения [2]. В педагогической системе обучения с применением информационно-коммуникационных технологий соответствующие приемы должны обусловливать творческий уровень мыслительной деятельности учащихся.

Вообще говоря, считается, что в общем случае приемы обучения входят в структуру метода. Но на самом деле можно сказать, что границы между понятиями «метод» и «прием» очень подвижны и изменчивы. В данной статье под понятием «прием обучения» будет пониматься, что это обусловленные методами конкретные действия преподавателя или учащегося, определяющие их учебно-познавательные операции и приводящие к решению частных содержательных и процессуальных задач обучения.

Переходя конкретно к приемам обучения следует отметить, что их можно подразделить на следующие категории [3]:

- приемы формирования и активизации отдельных операций мышления, внимания, памяти, восприятия, воображения;

- приемы, способствующие созданию проблемных, поисковых ситуаций в мыслительной деятельности учащихся;

- приемы, способствующие разрешению противоречий;

- приемы организации репродуктивного, продуктивного и творческого общения;

- приемы, активизирующие переживания, чувства учащихся, связанные с изучением учебного материала;

- приемы контроля, самоконтроля, самообучения учащихся;

- приемы управления, обусловливающие характер отношений между взаимодействующими сторонами.

Таким образом, прием – это не просто «составная часть или отдельная сторона метода», как считает современная педагогика [4], а именно «обусловленное методом действие...». Из данного тезиса вытекает определяющая сторона метода по отношению к приему. Метод объединяет приемы в целесообразные комплексы, которые призваны решать конкретные цели и задачи конкретной педагогической системы. Практически каждый метод отличается от другого особым сочетанием приемов, среди которых могут быть и доминирующие, определяющие содержательную и процессуальную стороны метода.

Связь между методами и приемами обучения с применением информационно-коммуникационных технологий можно охарактеризовать как достаточно сложную. К примеру, приемы и методы могут сочетаться абсолютно различными способами и применяться в многообразии этих сочетаний, отдельные приемы могут входить в состав различных методов, также один и тот же способ деятельности учащихся в одних случаях может выступать в качестве самостоятельного метода, а в других – как прием обучения. Последнее легко пронаблюдать на примере. Если объяснение или, к примеру, беседа, которые являются самостоятельными методами обучения, эпизодически используются преподавателем в ходе практической работы для привлечения внимания учащихся или же исправления ошибок, то в таком случае они выступают как приемы обучения, входящие в метод упражнения. Метод и прием, таким образом, могут меняться местами.

Анализ содержания учебных программ и учебников, научно-методической литературы, а также опыт работы в системе образования позволяет выделять следующие основные приемы продуктивного и творческого мышления, которыми должен овладеть преподаватель в стенах педагогического вуза:

- умозаключение по аналогии для уяснения проблемы и направления ее решения;

-моделирование объектов и явлений (построение теоретической модели и ее интерпретация);

- экстраполяция и интерполяция;

- интерпретация (раскрытие физического смысла закона, результатов эксперимента и т.п.);

- фантазирование (использование физических знаний в нетрадиционных случаях);

- индукция, дедукция;

- переход от описания к объяснению, от явлений к сущности (анализ структуры исследуемых систем и процессов, переход от одних структурных условий к другим, более глубоким) [5];

- структурно-функциональный анализ (выяснение роли структурных составляющих относительно друг друга после выделения их в системах);

- системный анализ (выявление многообразия связей и отношений исследуемого объекта, имеющих место как внутри этого самого объекта, так и в его взаимоотношениях с внешним окружением, то есть средой);

- выявление межпредметных и внутрипредметных связей;

- выдвижение идей, приводящих к формированию обобщенных теоретических принципов, объясняющих сущность тех или иных явлений [1];

- рефлексия (способность к анализу и самоанализу, самооценка, осознание собственной мыслительной способности);

- абстрагирование (мысленное отвлечение от ряда свойств и отношений между ними и выделение какого-либо свойства или отношения, процесс образования физических понятий; расчленение предмета и выделение в нем существенных сторон, всесторонний анализ их в «чистом» виде);

- определение уровня и степени адекватности отображения оригиналу-объекту (достоверность знания; для теоретического знания – его доказательность, точность и полнота; глубина или существенность отображения оригинала-объекта);

- анализ основной линии в последовательности разработки научных идей, прослеживание тех отрицаний, которым подвергается теория в процессе порождения новой теории;

- анализ конкурирующих аксиоматик различных теорий одной и той же предметной области (механики Ньютона, Лагранжа, Гамильтона);

- анализ расширения области применимости физической теории и тем самым изменение самой теории, зарождение новых методов [6];

- сопоставление и анализ внутренней структуры концептуального аппарата старой и зарождающейся теории (классическая механика, электродинамика и др.);

- анализ идей эволюции и революции в развитии физики;

- прогнозирование за счет использования знания законов физических явлений;

- восхождение от абстрактного к конкретному (теоретическое воспроизведение в сознании целостного объекта, систематическое отображение его в понятиях);

- экспертиза конкурирующих теорий и обоснование выбора теории в физике (раскрытие природы «теоретических наследников» в развитии знаний, анализ принципов развития физических теоретических знаний);

- анализ новых эмпирических результатов, обработанных в рамках известных теорий, но выходящих за пределы объяснимого этими теориями [3];

- анализ тенденций дальнейшего развития, научных теорий;

- изучение средств и методов познания и природы творческого мышления;

- использование генетического исследования природных явлений (установление начальных условий развития; главных его этапов; основных тенденций, линий развития);

- выдвижение гипотез и их проверка путем вывода из них следствий и сопоставление этих следствий с фактами;

- использование диалектики в развитии физических знаний;

- использование приемов доказательства, имеющих целью обосновать истинность или ложность какого-либо утверждения;

- анализ различных типов физических законов (выражающих взаимосвязь между свойствами объекта, самими объектами, системами или между различными их состояниями, различающимися по степени общности и сфере действия, по природе);

- использование идеализации для образования абстрактных объектов (материальная точка, абсолютно твердое тело, идеальный газ и т.п.);

- использование исторического и логического методов для развития физических знаний [6];

- использование обобщения в развитии физических знаний;

- использование анализа структуры и содержания определений физических понятий;

- использование метода дополнительности;

- планирование;

- подбор и использование средств для исследовательской деятельности (приборов, таблиц, материалов и т.д.);

- математическая и графическая интерпретация результатов исследовательской деятельности.

Включение перечисленных приемы продуктивного и творческого мышления в число обязательных элементов усвоения ликвидирует сложившийся в практике обучения физике дисбаланс в распределении учебной нагрузки в сторону усиленного функционирования репродуктивного мышления в ущерб продуктивному. С этой целью в любой крупной теме преподаваемого предмета предлагается выделять такое содержание и такие средства, чтобы они обеспечивали полноценную отработку каждого приема продуктивного и творческого мышления и их сочетаний на все более усложняющемся материале.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Советская педагогика. Межпредметные связи как дидактическая проблема и некоторые аспекты её исследования. 1972. № 8.

2. Зверев И.Д., Максимова В.Н. Межпредметные связи в современной школе. – Москва: Педагогика, 1981.

3. Выготский Л.С. Педагогическая психология: сборник научных трудов. – Москва, 1991.

4. Махмутов М.И. Проблемное обучение: основные вопросы теории. – Москва: Педагогика, 1975. – 368 с.

5. Бабанский Ю.К. Проблемы повышения эффективности педагогических исследований. – Москва: Педагогика, 1982. – 191 с.

6. Журавлев В.И. [и др.] Педагогика: учебное пособие для студентов педагогических вузов и педагогических колледжей / под ред. П.И. Пидкасистого. – Москва: Российское педагогическое агенство, 1996. – 602 с.

УДК 371.3

ОПЫТ ИСПОЛЬЗОВАНИЯ WEBEX ПРИ ДИСТАНЦИОННОМ ОБУЧЕНИИ

Шарпан М.В.,
кандидат физико-математических наук
(Краснодарский университет МВД России)

Аннотация: статья посвящена опыту использования Cisco Webex при дистанционном обучение.
Ключевые слова: дистанционное обучение, Zoom, Skype, Webex.

EXPERIENCE USING WEBEX WITH DISTANCE LEARNING

Sharpan M.V.,
Candidate of Physical and Mathematical Sciences
(Krasnodar University of the MIA of Russia)

Abstract: the article is devoted to the experience of using Cisco Webex for distance learning.
Keywords: distance learning, Zoom, Skype, Webex.

Дистанционное обучение сегодня – это вынужденная необходимость, с одной стороны, это престижно, перспективно и удобно, с другой стороны.

На первый взгляд кажется, что дистанционное и заочное обучение – это одно и то же, но на практике имеются значительные отличия. Так, дистанционное обучение предполагает постоянный контакт с преподавателем, хоть и в режиме «онлайн». И на этом этапе возникает необходимость выбора средства, с помощью которого будет осуществляться такая связь.

Кратко рассмотрим некоторые достаточно распространенные сервисы.

Zoom – это сервис для проведения видеоконференций, онлайн-встреч и дистанционного обучения [1].

Из достоинств следует отметить: организовать встречу может любой, создавший учетную запись; к видеоконференции может подключиться любой, имеющий ссылку, или идентификатор конференции; мероприятие можно запланировать заранее, а также сделать повторяющуюся ссылку.

Недостатками являются: бесплатная учетная запись позволяет проводить видеоконференцию длительностью 40 минут; обучаемые могут только рисовать, на виртуальной доске невозможно ничего передвигать.

Skype – это программное обеспечение для связи с миром, с его помощью миллионы людей и компаний могут совершать индивидуальные и групповые голосовые и бесплатные видеозвонки, а также отправлять мгновенные сообщения и файлы другим пользователям Skype [2].

Достоинствами являются популярность данного сервиса среди пользователей, возможность показа экрана, кроссплатформенность. В качестве недостатков стоит отметить, что обе стороны обязательно должны быть онлайн, низкое качество видео при участии более 5 человек, низкая скорость обмена файлами и огромное количество рекламы.

Webex – это облачный сервис (платформа) для проведения любых web-конференций, позволяющий участникам обмениваться информацией в любой момент времени из глобальной облачной среды, в любом месте, используя компьютер или мобильные устройства [3].

Поскольку на базе нашего университета успешно функционирует академия Cisco было принято решение использовать в качестве средства связи с обучаемыми Webex.

Webex отлично зарекомендовал себя при проведении лекционных, семинарских (одновременно до 35 человек) и практических занятий. Интересными и востребованными оказались такие функции, как возможность отключать звук у всех участников занятия, возможность самостоятельно предоставлять обучаемому роль докладчика (например, при устном опросе), возможность вести аудио- и видеозапись (например, при проведении зачета или экзамена). К сожалению, запись предоставляется не в универсальных форматах, а в собственном формате Webex.

Также полезными функциями оказались возможность предоставлять совместный доступ к контенту как преподавателя (при объяснении нового материала или новых возможностей той или иной программы) и контенту обучаемого (при контроле выполнения практического задания) (см. рис. 1).

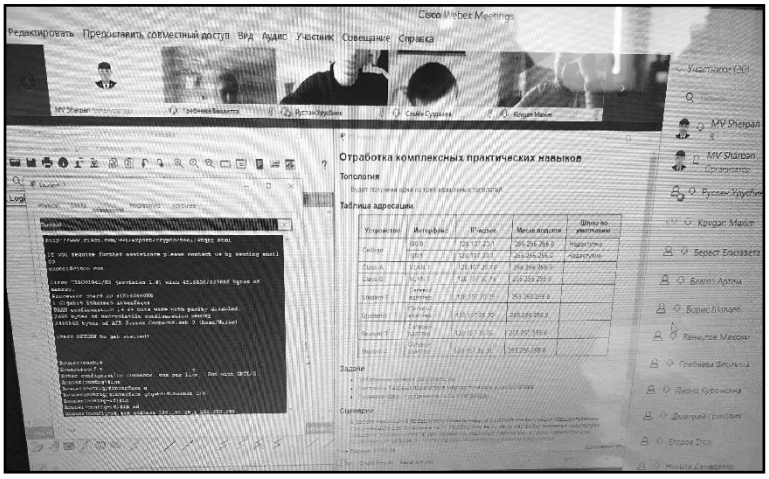


Рисунок 1. Иллюстрация возможности предоставление совместного доступа к контенту

Помимо всего перечисленного также стоит отметить кроссплатформенность, т.е. способность программного обеспечения работать с двумя и более аппаратными платформами и операционными системами (см. рис. 2).

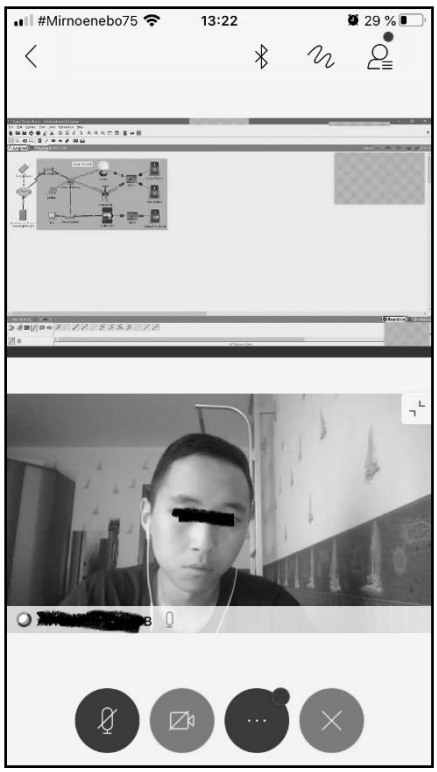


Рисунок 2. Иллюстрация возможности проводить опрос обучаемого с предоставлением совместного доступа к контенту

Единственным существенным недостатком указанного сервиса является то, что он является иностранным программным обеспечением.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://zoom.us/ru-ru/meetings.html (01.05.2020).
2. https://www.skype.com/ru/ (01.05.2020).
3. https://help.webex.com/ru-ru/ (01.05.2020).

УДК 343.9

ФОРЕНЗИКА – КРИМИНАЛИСТИКА В НОГУ СО ВРЕМЕНЕМ

Федосеев А.Э.;
Федосеев А.Э.;
Архипцев И.Н.,
кандидат юридических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматривается аспект появления форензики как подраздела криминалистики, актуальность ее применения, реализация в виде коммерческих продуктов как результат востребованности, их применимость и результативность.

Ключевые слова: извлечение данных, киберпреступность, форензика.

FORENSIC SCIENCE – CRIMINALISTICS IN STEP WITH THE TIMES

Fedoseev A.E.;
Fedoseev A.E.;
Arkhiptsev I.N.,
Candidate of Law
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the article deals with the aspect of the appearance of forensic science as a subsection of criminalistics, the actuality of its application, implementation in the form of commercial products as a result of demand, their applicability and effectiveness.

Keywords: data extraction, cybercrime, forensic science.

Информационные и телекоммуникационные технологии, находя отражение во всех сферах жизнедеятельности человека, являются наиболее быстроразвивающимися и востребованными. Используемые повседневно, они также стали составляющей противоправной деятельности, причем как её объектом, так и инструментом. Удаленный доступ к банковским счетам, «взлом» учетных записей социальных сетей, чтение переписки электронной почты стали более доступными благодаря тому же развитию мобильных гаджетов, которые по производительности электронной начинки далеко опередили стационарное оборудование десятилетней давности. На сегодня разве при совершении преступлений против личности не будут фигурировать гаджеты в качестве инструмента. Такая тенденция привела к появлению термина «киберпреступность» и категорий киберпреступлений [1]. Количественные показатели ценности информации можно измерить в виде экономических потерь. С другой стороны, рост затрат на киберзащиту как крупных компаний, так и государственных структур также можно расценивать в качестве шкалы оценки значимости этого

направления. Все это говорит о необходимости как планирования мер противодействия на информационном поле, так и о технологическом развитии процесса расследования преступлений в киберпространстве. Если противоправная деятельность активно использует современные достижение в области информационных технологий, то и противодействие должно быть организовано при их участии или даже работать на опережение. Связь юридической науки и технических дисциплин привела к появлению термина «форензика» – прикладной науки, являющейся подразделом криминалистики, в области компьютерной информации [2].

Компьютер – как непосредственный носитель таковой информации от момента своего появления до нашего времени трансформировался из громоздкого электронного устройства в карманный гаджет с возможностью хранения много большего объема информации, большей ее разнородности, применимости и возможности ее передачи. Примененный в 1992 году термин «карманный персональный компьютер» трансформировался в современный смартфон – наиболее распространенный проводник человека в виртуальном мире. Мобильный телефон превратился из устройства осуществления голосовой связи в многофункциональное устройство интеграции реального человека с «персонажем» виртуального мира. Современный «телефон», в отличие от ранее использованных соотношений ФИО – абонентский номер, позволяет соотносить лицу такие сведения, как расширенный перечень персональных данных, имена учетных записей различных мессенджеров, социальных сетей, адресов электронной почты и иную информацию, становясь хранилищем структурированных баз данных. Также устройство хранит различную мультимедийную информацию, историю переписки с иными «персонажами» виртуального мира, историю посещенных интернет-страниц, вводимых идентификационных данных, данных геолокации, маршрутов. Использование такой информации преступником позволяет ему качественнее спланировать и легче осуществить свой замысел. И наоборот, знание таких сведений о злоумышленнике повысит качество доказывания противоправности его действий или позволит предотвратить преступный замысел при реализации в качестве оперативной информации.

Получение сведений из гаджета возможно различными способами, реализация которых зависит от возможностей и оснащения извлекающего, от особенностей устройства, временных и других факторов. В 2009 году Сэмом Бразерсом представлена пятиуровневая модель [3] извлечения данных из мобильных устройств. На самом низком уровне представлено ручное извлечение данных, реализуемое без специальных приспособлений, представляющее собой обычный просмотр самого устройства путем открытия соответствующих его разделов и анализа их содержимого.

Последующие уровни, такие как логический уровень, физический уровень, схема памяти и микроуровень, являются технически более сложными, однако их реализация дает более значимый результат как с точки зрения объема и качества информации, так и более «правильный» с точки зрения криминалистики и закрепления доказательной базы. Эти уровни, в соответствии с потребностями на рынке, получили программную, в том числе свободно распростра-

няемую, и аппаратную реализации. Усложнение поставленной задачи вносилось производителями сотовых телефонов за счет разнообразия архитектуры электронных устройств, операционных систем, не позволяя реализовать единый алгоритм извлечения данных. Использование комбинаций имеющихся решений привело к созданию аппаратно-программных комплексов, в которых при реализации разных уровней извлечения данных учитывались различия моделей устройств, необходимость обхода блокировок.

Специальные технические средства, такие как XRY и Cellebrite UFED, получили широкое распространение как в экспертной, так и в оперативной работе. Популярен также и отечественный продукт «Мобильный криминалист», который на фоне законодательно установленного приоритета товаров российского происхождения [4] представляет особый интерес. Его положительной особенностью является возможность обработки и анализа образов, созданных при помощи вышеуказанных иностранных специальных технических средств. Эта функция широко применялась при комплексном использовании различных продуктов. Сегодня «Мобильный криминалист» получил аппаратно-программный вариант реализации, что в совокупности с накопленным опытом, по сведениям разработчика [5], позволяет продукту осуществлять поддержку более 34 тыс. моделей устройств, в том числе заблокированных, более 14 тыс. версий приложений, а также облачных сервисов и иных устройств.

Потребности бизнес-компаний и правоохранительных органов при расследовании компьютерных инцидентов различны. В одном случае достаточно установление факта, в другом необходим определенный порядок документирования. Развитие и усложнение устройств-носителей информации влечет усложнение процедуры извлечения данных не только с точки зрения самого процесса, но и с точки зрения сохранения целостности информации при изъятии и анализе, восстановлении удаленных данных, гарантии её защиты от искажения, в т.ч. непреднамеренного, потери и, как следствие, применимости в качестве доказательной базы. Реалии современной криминалистики и отечественного судопроизводства учитываются при реализации технических решений, позволяя идти в ногу с развитием цифровых технологий при противодействии и профилактике киберпреступности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Преступления, связанные с использованием компьютерной сети / Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями // A/CONF. 187/10 [Электронный ресурс]. – Режим доступа: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf/ (дата обращения: 30.03.2020).

2. Викисловарь статья «Форензика» [Электронный ресурс]. – Режим доступа: https://ru.wiktionary.org/wiki/форензика

3. Brothers S. Cell Phone and GPS Forensic Tool Classification System [Электронный ресурс]. – Режим доступа: https://ru.scribd.com/document/ (дата обращения: 30.03.2020).

4. Постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами» [Электронный ресурс]. – Режим доступа: https://base.garant.ru/

5. Пресс-релиз компании «Оксиджен Софтвер» «Мобильный Криминалист» совершенствует поддержку iOS и Android-устройств! [Электронный ресурс]. – Режим доступа: https://www.oxygensoftware.ru/ru/news/press-releases/230-mk-11-8-1-3 (дата обращения: 19.02.2020).

УДК 004.93

БИОМЕТРИЧЕСКИЕ МЕТОДЫ КОНТРОЛЯ ДОСТУПА, ИХ ДОСТОИНСТВА И НЕДОСТАТКИ

Калашникова А.А.,
Шаблова Е.Д.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье охватываются вопросы использования биометрических систем для контроля доступа, а также изучение работы самых популярных биометрических систем и необходимость их использования. Рассматриваются как положительные, так и отрицательные аспекты.

Ключевые слова: биометрические системы, биометрия, дактилоскопия, защита информации.

BIOMETRIC ACCESS CONTROL METHODS, THEIR ADVANTAGES AND DISADVANTAGES

Kalashnikova A.A.,
Shablova E.D.
(Kikot Moscow University of the MIA of Russia)

Abstract: the article discusses the use of biometric systems for access control, as well as studying the work of the most popular biometric systems and the need for their use. Both positive and negative aspects are covered.

Keywords: biometric systems, biometrics, fingerprinting, information protection.

Сегодня мы живем в информационном обществе, в котором информация является главным ресурсом. Именно поэтому данные о различных процессах деятельности стоят очень дорого и их необходимо постоянно защищать. Существует множество способов защиты данных, таких как программные, законодательные, физические системы и механизмы шифрования. В современных реалиях большое распространение получают биометрические методы защиты данных, в основе которых лежат биометрические характеристики отдельной личности.

Еще с глубокой древности люди идентифицировали друг друга по морфологическим признакам, распознавая по внешнему виду, походке, запаху. Это можно назвать элементарной биометрией. В процессе своего развития человек использовал биометрические характеристики для защиты информации. Сегодня археологи находят глиняные горшки и таблички времен Римской империи, где можно обнаружить рядом с подписью автора еще и отпечаток его пальца.

Первые прототипы биометрических систем контроля доступа появились в конце XX века. Они были похожи на современные аналоги, но отличались излишней громоздкостью, ненадежностью и высокой ценой.

Необходимо отметить, что работа данных систем основывается на безошибочном считывании биометрических характеристик личности.

Биометрические характеристики – это неизменные признаки человека, которые могут успешно использоваться для идентификации его личности. Данные признаки являются статическими и появляются у каждого человека, в основном с рождения. Данные признаки не зависят от временного показателя, однако во многих конкретных системах при регистрации личности измерения проводят несколько раз, чтобы избежать относительных погрешностей.

Также каждому человеку характерны поведенческие биометрические признаки личности. Данный признак основан на бессознательных движениях. Поведенческие характеристики зависят от временного показателя, и при их измерении это следует учитывать. Поэтому при процедуре идентификации личности следует проводить измерения в течение определенного промежутка времени, и при регистрации личности провести несколько раз фиксацию данных для получения средней величины итогового показателя динамической характеристики [1].

Следовательно, современные биометрические технологии можно разделить на статические и динамические.

Статические основаны на существующих антропологических характеристиках личности, которые являются уникальными. К ним можно отнести:

- распознавание по отпечатку пальца;
- распознавание по форме ладони;
- распознавание по сетчатке глаза;
- распознавание по радужной оболочке глаза;
- распознавание по ДНК и т.д.

Динамические же методы основываются на поведенческих показателях, характеризующих личность человека.

- идентификация по рукописному почерку;

- идентификация по клавиатурному почерку;
- идентификация по голосу;
- идентификация по эмоциональным характеристикам;
- идентификация по жестам;
- идентификация по сердечному ритму;
- идентификация по походке и т.д.

Существующие виды биометрических систем имеют как достоинства, так и недостатки. Достоинствами статических характеристик является более удобный процесс измерения, но требующий наличия дорогостоящего оборудования. Биометрические эталоны являются компактными, это связано с тем, что статические характеристики моментные и не требуют хранения данных, собранных за большой промежуток времени. Помимо существующих положительных сторон данной модели, существует значительный недостаток, такой как большая вероятность фальсификации признаков из-за открытости личностных характеристик, что является существенным недостатком для статических биометрических характеристик.

У динамических систем также существуют как положительные, так и отрицательные аспекты. Можно отметить, что их преимуществом является низкая стоимость. Это следствие того, что для идентификации не требуется наличие дорогостоящего оборудования и программного обеспечения. Поэтому можно справиться с использованием стандартных и недорогих мультимедиа (графического планшета, микрофона, звуковой карты). Быстрая смена биометрического эталона является неоднозначным параметром. По сравнению со статическими характеристиками, динамические подвержены изменениям, тем самым повышая возможность фальсификации. Но стоит отметить, что данная вероятность будет невелика. Существенным недостатком является присутствие психофизических факторов. Примером может быть испуг, стресс [2].

Несмотря на многочисленные разновидности биометрических систем, основополагающий принцип работы у всех идентичный. Это регистрация данных, используя идентификатор пользователя, то есть личностные биометрические характеристики. Удобство заключается в том, что от пользователя не требуется наличия посторонних предметов, а он сам является ключом для доступа. Регистрация, как правило, производится несколько раз, чтобы избежать субъективного отклонения. На основе данных образуется массив, из которого выбирается совокупность характеристик и формируется биометрический эталон. Далее происходит аутентификация личности, то есть система сопоставляет биометрические характеристики личности, претендующей на получение доступа к защищаемому объекту, из существующего биометрического эталона. В случае совпадения для лица будет возможен доступ [3, с. 5-7].

В настоящее время популярным способом защиты данных является дактилоскопия. Это связанно с тем, что компании по производству современных телефонов популяризировали данную технологию, используя ее для защиты гаджетов. Для общества это оказалось очень полезным, так как люди хранят в своих смартфонах важную личностную, финансовую информацию.

В мире не менее популярным является защита данных по изображению формы лица. Для существования такой технологии следует собрать все биометрические данные с лица: размер головы, длину бровей, размер носа и глаз. Причем данные должны быть как в двухмерном, так и в трехмерном изображении. Но в представленной технологии существует проблема в том, что учитывать следует множество вариантов, так как при сборе данных с объекта, пытающего получить доступ, будут влиять различные факторы, такие как ракурс, мимика лица, освещение, макияж (у женщин) и иные. Все это должно учитываться при сравнении объекта с биометрическим эталоном. Сейчас благодаря нейросетевым камерам современных гаджетов возможно идентифицировать лицо пользователя. Данная технология распространена не только в сфере защиты мобильных устройств, но и банковской сфере или же в торговой. Нельзя не отметить, что данная технология актуальна не только для защиты информации, но и для охраны общественного порядка и защиты личности. Ярким примером является Китай, где оборудованы все уличные камеры системой распознавания лиц. Также эта страна является лидером по использованию биометрических технологий.

Небольшое распространение имеют распознавание личности по расположению вен на лицевой стороне ладони и рисунка кровеносных сосудов человеческого глаза из-за большой стоимости специализированного оборудования для регистрации информации. Определено, что сканирование рисунка кровеносных сосудов можно заменить на распознавание по глазной радужке, которая у каждого человека уникальна. Для данной системы защиты данных необходима портативная камера, оснащенная специальным программным обеспечением, а дальше происходит стандартная операция по сравниванию полученных результатов с эталоном [4].

Использование динамических биометрических характеристик также является популярным. Примером может быть распознавание человека по его почерку, который может быть как рукописный, так и клавиатурный.

Основа идентификации личности по клавиатурному почерку заключается в анализе конкретной напечатанной фразы. Если подготовленный пользователь будет многократно печатать парольную фразу, то при совершении многократных действий многочисленная часть печати будет проходить на бессознательном уровне. Именно эти бессознательные манипуляции создают клавиатурный почерк. Время нажатия на определенную клавишу t1, t2, t3, …tn является контролируемым показателем, при том что время между нажатием клавиш □1, □2, □3, ..., □n-1 также следует учитывать, потому что оно, как и время нажатия на определенную клавишу, является контролируемым показателем.

Распознавание личности по клавиатурному почерку основано на временных показателях, что позволяет создать временную функцию, отражающую все особенности клавиатурного почерка. Для биометрического исследования очень важно значение вектора V информативных параметров, так как он является решающим для всей процедуры аутентификации. Дальнейшие измерения строятся на основе измерения приближенности данного вектора к вектору эталона $_э$(биометрический эталон, хранящийся в базе данных) [5].

При распознавании личности по рукописному почерку наиболее важным является распознавание по подписи. Данный метод используют многие банки и финансовые компании для защиты личных данных пользователей.

Распознавание подписи может быть как статическое, так и динамическое. Статическое распознавание подписи включает в себя подпись человека на бумажном носителе, которую оцифровали и используют как образец. Динамическая подпись создается в режиме реального времени с помощью графического планшета, при этом регистрируется процесс ее написания и сверка с существующим эталоном.

Нельзя не отметить, что сегодня быстро развивается идентификация по голосу. Существует достаточно много способов построения кода идентификации по голосу, как правило, это различные сочетания частотных и статистических характеристик, поскольку человеческие голоса обладают разной интонацией, высотой тона, модуляцией и пр. Биометрическая система распознает людей по особенностям речи, а чтобы злоумышленники не смогли воспользоваться заготовленными аудиозаписями легального пользователя для получения доступа, системы чаще всего просят произнести случайный набор слов или фраз. Для оцифровки записанной речи в основном используют нейросети. Далее, как и по аналогии с фото- и видеоданными, полученная свертка (код) голосовой записи сравнивается системой с эталоном, хранящимся в базе данных. Данный метод является самым дорогостоящим и в настоящее время он не является максимально удобным и пригодным для повседневной деятельности.

По данным биометрического рынка биометрические системы активно применяются для распознавания и защиты данных (см. рис. 1) [6].

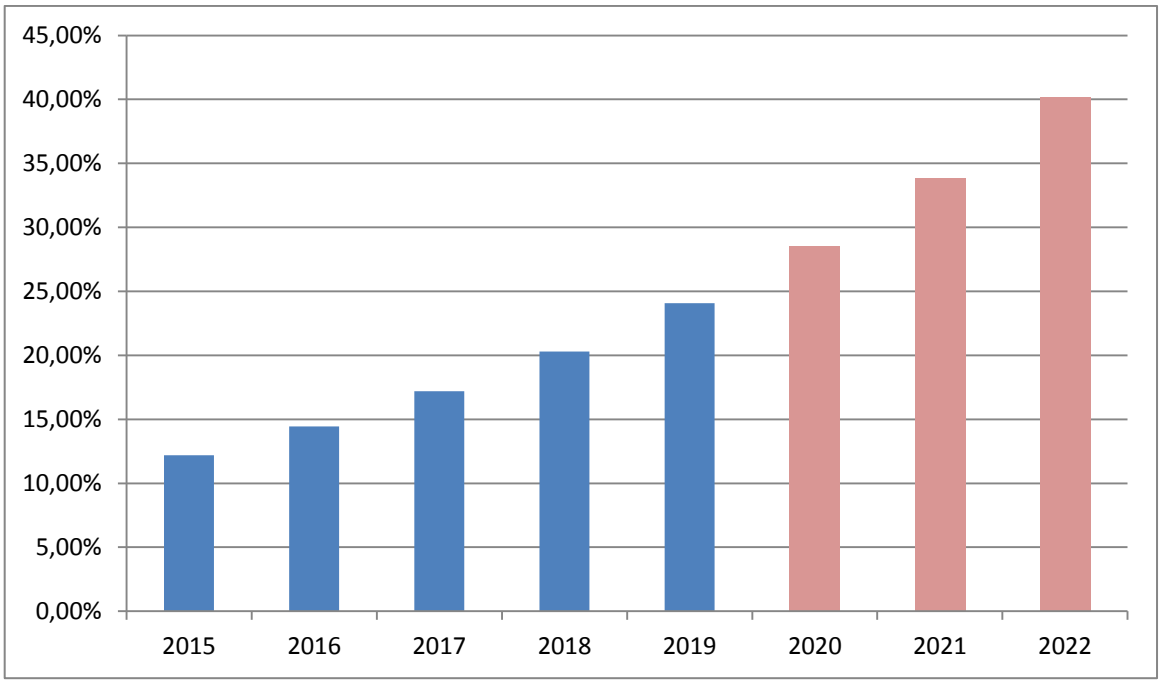


Рисунок 1. Динамика объема мирового рынка биометрических систем 2015-2022 гг.

По представленному графику видно, что прогнозируется рост мирового рынка биометрических систем. Обусловлено это тем, что биометрические системы защиты данных, хоть и имеют ряд недостатков, но являются удобными в использовании и отличаются повышенной надежностью по сравнению с традиционными методами защиты.

Подводя итог, можно сказать, что биометрические системы представляют сложный анализ, но без их использования невозможно представить быстрый и надежный контроль за доступом к информации. Биометрические технологии массово внедряются в общественную жизнь, что приводит к совершенствованию имеющихся на рынке систем и устройств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Брюхомицкий Ю.А Биометрические технологии идентификации личности: учебное пособие. – Ростов-на-Дону: Техносфера, 2017. – 263 с.
2. Болл Р.М.М., Коннел Дж. Х., Панканти Ш., Рахта Н.К., Сеньор Э.О. Руководство по биометрии. – Москва: Техносфера, 2007. – 368 с.
3. Двоеносова Г.А., Двоеносова М.В. Биометрия как наука, метод и способ документирования // Управление персоналом. 2009. № 2. С. 82-86.
4. Двоеносова Г.А., Двоеносова М.В Система аутентификации личности по почерку / Информационная безопасность: сборник трудов научно-практической конференции с международным участием. – Таганрог: ТРТУ, 2002.
5. Международная консалтинговая компании J’son & Partners [Электронный ресурс]. – Режим доступа: https://www.json.ru/ (дата обращения: 08.04.2020).
6. Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации [Электронный ресурс]. – Режим доступа: https://securityrussia.com/blog/biometriya.html (дата обращения: 18.03.2020).

УДК 004

РАЗРАБОТКА ЭЛЕКТРОННОГО ОБРАЗОВАТЕЛЬНОГО РЕСУРСА «РАБОЧЕЕ МЕСТО ТРЕНЕРА»

Захарова Е.А.;
Беляева И.Н.,
кандидат физико-математических наук, доцент
(Белгородский государственный национальный исследовательский университет)

Аннотация: данная статья посвящена разработке электронных образовательных ресурсов на базе CMS Wordpress. Данная система управления содержимым позволяет разработать свой сайт без наличия специальных знаний языков программирования. Внедрение таких ресурсов в образовательный процесс повышает его эффективность и качество образования, а также делает процесс обучения интерактивным.

Ключевые слова: CMS, Wordpress, электронный образовательный ресурс, система управления содержимым, образовательный процесс, разработка сайта.

DEVELOPMENT OF AN ELECTRONIC EDUCATIONAL RESOURCE «TRAINER'S WORKPLACE»

Zakharova E.A.;
Belyaeva I.N.,
Candidate of Physical and Mathematical Sciences, Associate Professor
(Belgorod National Research University)

Abstract: this article is devoted to the development of electronic educational resources based on CMS Wordpress. This content management system allows you to develop your site without special knowledge of programming languages. The introduction of such resources in the educational process increases its efficiency and quality of education, as well as makes the learning process interactive.

Keywords: CMS, Wordpress, electronic educational resource, content management system, educational process, site development.

В современном мире самым распространенным путем получения информации являются интернет-ресурсы. Глобальная паутина становится образовательной площадкой для многих специалистов, стремительно набирающей популярность, и содержит в себе множество сайтов с желаемой информацией, однако не все из них одинаково полезны и достоверны. Разработка линейки электронных образовательных ресурсов для специалистов позволяет увеличить качество образования и повысить его эффективность [2, с. 35].

В настоящее время есть множество путей создания своего собственного сайта. Использование CMS – один из них.

CMS или системы управления содержимым (контентом) – растущая и быстро развивающаяся платформа, позволяющая за небольшой промежуток времени создать с нуля свой собственный сайт [1, с. 333].

CMS не требует от пользователя наличия знаний языков программирования и специальных навыков, благодаря наличию конструктора, позволяющего добавлять необходимые блоки на сайт, наполняя их лишь текстовой, графической информацией или мультимедиа. Помимо этого, CMS содержит в себе все необходимые возможности для сайта: различные фотогалереи, системы комментариев, голосование и другие [5, с. 204].

Одной из самых известных CMS считается Wordpress. Данная система управления контентом предоставляет пользователю большое количество возможностей за счет подключения плагинов и шаблонов. CMS Wordpress позволяет создавать сайты как на удаленном, так и на локальном хостингах, что является плюсом в случае, если сайт не требует срочного размещения в сети. После завершения разработки сайт переносится на удаленный сервер. Официальный сайт Wordpress предоставляет возможность скачать необходимые файлы для корректной работы, а также обладает достаточной справочной информацией по работе с CMS [4, с. 743].

Электронные образовательные ресурсы для специалистов предназначены как для опытных специалистов, позволяя изучать новые методики или размещать собственные наработки, а также предоставляя возможность обмена опытом, так и для студентов или начинающих специалистов с целью использования ресурса как стартовой площадки карьеры.

Электронные образовательные ресурсы требуют соблюдения ряда правил при разработке для повышения эффективности его использования и актуальности. Сюда входят требования соответствия нормативным актам Министерства образования и науки Российской Федерации; удобный интерфейс и структура сайта, его высокая интерактивность и мультимедийность, а также адаптация к наиболее популярным современным техническим платформам [3, с. 256].

Данный электронный образовательный ресурс «Рабочее место тренера» имеет древовидную структуру, которая считается универсальной для web-сайтов. Такая структура позволяет соблюдать логику взаимосвязей всех страниц ресурса, имеет удобную и понятную для пользователя структуру, поскольку пользователь сам может выбрать последовательность перехода между web-страницами, переходя из раздела в раздел.

Электронный образовательный ресурс «Рабочее место тренера» имеет следующую структуру (см. рис. 1):

1. Главная страница, на которой размещены аннотация, актуальные направления деятельности и основная навигация по разделам ресурса.

2. Нормативная база деятельности, в которую входят документы федерального и регионального уровней.

3. Спорт, где собраны документы международного уровня.

4. Деятельность, которая включает стратегии развития и профессиональный стандарт.

5. Методическая копилка, которая включает методические рекомендации, формы и методы работы.

6. Дополнительное меню быстрого доступа «Предметные области», содержащие документы, касающиеся непосредственно тренировочного процесса, соревновательной деятельности, судейской практики и нормативно-правовых основ физкультурно-спортивной деятельности.

Рисунок 1. Электронный образовательный ресурс «Рабочее место тренера»

Внедрение таких электронных образовательных ресурсов в образовательный процесс позволяет повысить интерес к сфере деятельности, раскрываемой в рамках ресурса, а также предоставляет полную информацию о ней, включая наличие нормативных документов, описание различных методик и рекомендаций к ним. Дополнительным преимуществом является возможность обмена передовым опытом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Горнаков С.Г. Осваиваем популярные системы управления сайтом (CMS). – Москва: ДМК Пресс, 2014. – 333 с.
2. Использование электронных образовательных ресурсов нового поколения в учебном процессе: научно-методические материалы / Г.А. Бордовский, И.Б. Готская, С.П. Ильина, В.И. Снегурова. – Санкт-Петербург: РГПУ им. А.И. Герцена, 2015. С. 31–39.
3. Селевко Г.К. Современные образовательные технологии: учебное пособие. – Москва: Народное образование, 2016. – 256 с.
4. Хассей Т. WordPress и создание сайтов для начинающих (+ CD-ROM). – Москва: Эксмо, 2014. – 743 с.
5. Черных А.Ю. Бесплатная система управления сайтом. – Москва: Эксмо, 2017. – 204 с.

УДК 004.056

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МВД РОССИИ

Тимакина Ю.А.,
кандидат экономических наук;
Мхце Э.М.
(Ростовский юридический институт МВД России)

Аннотация: в статье речь идет об аспектах информационной безопасности системы материально-технического снабжения органов внутренних дел Российской Федерации в особых условиях.

Ключевые слова: органы внутренних дел, информационная безопасность, система материально-технического снабжения, особые условия.

PROBLEMS OF COUNTERING THREATS TO INFORMATION SECURITY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Timakina Yu.A.,
Candidate of Economical Sciences;
Mhce E.M.
(Rostov Law Institute of the MIA of Russia)

Abstract: the article deals with the aspects of information security of the logistics system of the internal Affairs bodies of the Russian Federation in special conditions.

Keywords: Internal Affairs agencies, information security, logistics system, special conditions.

Перед Россией сегодня остро стоит ряд различных проблем политического, экономического, социального и духовного характера [7].

Уровень развития демократии определяется не только формальным признанием приоритета прав и свобод человека и гражданина, включая их закрепление в национальном законодательстве и провозглашение общепризнанных норм и принципов международного права в области прав человека частью правовой системы России [5].

В российском обществе должен быть создан эффективно действующий государственно-правовой механизм по обеспечению информационной безопасности страны, позволяющий гражданину России воспользоваться существующими правовыми и организационными процедурами с целью фактической реализации своих прав и свобод [6].

За первый квартал 2020 года в России резко выросло число IT-преступлений. При этом отмечается улучшение в сфере офлайн-криминала. Число убийств, разбоев и грабежей снижается на фоне самоизоляции, сообщает пресс-служба МВД России.

В январе – апреле 2020 года количество IT-преступлений выросло на 83,9%. Их удельный вес достиг 19,9% от общего числа. Из-за этого уровень преступности в стране в целом вырос на 4%.

При этом в России на 4,9% меньше зарегистрированных убийств, на 3,3% – умышленных причинений тяжкого вреда здоровью. Значительно снизилось число разбоев – на 22,4%, грабежей – на 8,4% [9].

Больше всего киберпреступлений в прошлом году было зафиксировано на Ямале. 28,6% преступлений, совершенных в арктическом регионе, были связаны с IT-технологиями, то есть в мошеннических схемах фигурировали компьютеры, разного рода программы, пластиковые банковские карты, электронные падежи и т.п. Примерно такая же доля высокотехнологичных правонарушений приходится на Югру – 27,2%. Помимо этого, верхние позиции рейтинга занимают также Чувашия (26,8%), Коми (23,9%) и Пензенская область (23,1%). Меньше всего киберпреступлений было зарегистрировано на территории кавказских республик: в Чечне – 1,7%, в Дагестане – 3,5%, в Ингушетии – 4,4%. Небольшая доля также в Санкт-Петербурге (4,6%) и Московской области (5,3%).

В целом в 2019 году число зарегистрированных преступлений с использованием информационных технологий достигло 294 тысяч. «По сравнению с 2018-м этот показатель увеличился на 68,5%», - говорится в публикации. Чаще всего это мошенничества (119,9 тысяч эпизодов) и кражи (98,8 тысячи). Кстати, количество афер с использованием карт выросло за год на 280% и составило 16,1 тысяч случаев [11].

Изоляционные мероприятия, введенные в стране, и общее развитие ИТ-отрасли повысили активность мошенников через Интернет. За первые три месяца 2020 года число киберпреступлений выросло на 83,9%.

Общее число мошенничеств в марте 2020 года увеличилось на 48,5%, относительно марта 2019 года, а число преступлений, в которых использовались электронные платёжные средства, увеличилось в два раза. Из-за возросшего

уровня киберпреступности общий уровень преступности в стране увеличился на 4%, а удельный вес киберпреступлений почти достиг 20%.

При этом подобные преступления практически не раскрываются. По словам главы Генпрокуратуры России Игоря Краснова, раскрыть их удаётся лишь в 9% случаев, хотя за пять лет число подобных преступлений выросло с 11 до 295 тысяч. В марте 2020 года Президент России Владимир Путин потребовал от правоохранительных органов и Генпрокуратуры проанализировать ситуацию и выработать комплекс мер по противодействию преступникам [1].

Так, преступная группа, состоящая из более чем 30 хакеров, задержана сразу в нескольких российских регионах. Как сообщает во вторник Центр общественных связей ФСБ России, им вменяется незаконная продажа данных украденных банковских карт через интернет-магазины. По данным следствия, хакеры продавали похищенные данные через Сеть из более чем 90 интернет-магазинов. В итоге средств лишились граждане нескольких государств – точное число пострадавших пока не называется. На средства с похищенных карт интернет-мошенники приобретали дорогостоящие товары в интернет-магазинах [3]. В ходе обысков по 62 адресам изъято более миллиона долларов и 3 миллионов рублей наличными, серверы, поддельные документы, в том числе документы силовых ведомств, а также огнестрельное оружие, наркотики, золотые слитки и драгоценные монеты.

В 2018 году киберпреступники похитили у россиян 2 млрд рублей.

1,5 млрд рублей из них злоумышленники похитили в результате кибермошенничества с использованием интернет-банкинга [4].

В структуре МВД России появились подразделения по борьбе с киберпреступлениями.

Так, 1 ноября сообщалось, что глава МВД России Владимир Колокольцев принял решение о создании в ведомстве подразделения по борьбе с преступлениями в сфере высоких технологий. Отмечалось, что значительно будет увеличен штат Бюро специальных технических мероприятий МВД России и их подразделений на региональном уровне.

В этой связи отметим, что о новом кибероружии рассказала хакерская группа Digital Revolution, которая ранее стала известна взломами предполагаемых подрядчиков ФСБ России. Спецслужба заказала разработку программы «Фронтон», техническую документацию которой хакеры опубликовали 18 марта. Возможно, они получили ее, взломав московскую компанию 0day (ООО «0ДТ»). Один из документов, который стал доступен из-за утечки, был подготовлен по заказу Центра информационной безопасности ФСБ России (войсковая часть № 64829).

ФСБ России заказала разработку программы, которая призвана стать мощным кибероружием. Атакуя серверы через «умные» устройства Интернета вещей, она позволит обвалить сайты соцсетей и блокировать Интернет в небольших странах [2].

Существуют разные версии программы-кибероружия: «Фронтон», «Фронтон-3Д» и «Фронтон-18». С их помощью можно заражать «умные» устройства (от цифровых ассистентов до «умных» домов), объединять их в сеть и «обваливать» серверы. В опубликованной документации говорится, что Интернет вещей защищен гораздо слабее, чем мобильные устройства и серверы. Многие покупатели не меняют логины и пароли, заданные на заводе, поэтому их легко взломать. В подтверждение упоминается опыт Mirai – самой крупной сети зараженных IoT-устройств, насчитывавшей около 600 тыс. ботов. В 2016 году она вывела из строя DNS-серверы американской компании Dyn, интернет-сервисы использовали их для обновления информации в режиме реального времени. Из-за этого от нескольких минут до нескольких часов «легли» сайт Би-би-си, PayPal, Twitter, Netflix и еще около 70 популярных сервисов. Тогда атака шла через принтеры, детские мониторы и IoT-роутеры.

Но «Фронтоном» предлагается заражать IP-камеры и цифровые видеорекордеры. Следы предлагается тщательно запутывать. Запрещено использовать русский язык или кириллицу.

Однако Глава МВД России Владимир Колокольцев сообщил о нехватке бюджетных средств для борьбы с киберпреступлениями. Министерство учитывает стремительно развивающиеся методы киберпреступников, создает программы противодействия, но для их эффективности потребуются новые вложения.

Несмотря на объективные сложности, мы последовательно наращиваем усилия в борьбе с IT-преступностью. Однако, учитывая масштабы распространения киберпреступлений, разнообразие схем и методов их совершения, отсутствие единого алгоритма раскрытия, добиться кардинального улучшения невозможно. Новые подразделения должны быть не только укомплектованы высокопрофессиональными кадрами, но и оснащены современным высокотехнологическим оборудованием. Для чего понадобятся значительные бюджетные средства.

Одно из центральных ежегодных IT-мероприятий в России проводится с 2001 года. И если десятилетие назад проблематика информационной безопасности представляла интерес только для узкого круга специалистов, то сегодня она приобрела государственное значение. Неслучайно, открывая пленарное заседание «Инфофорум-2020», первый заместитель председателя Комитета Госдумы по безопасности и противодействию коррупции, сопредседатель оргкомитета мероприятия Эрнест Валеев призвал всех участников уделить особое внимание выработке единого видения обеспечения информационной безопасности как при рассмотрении традиционных тем, так и при обсуждении совершенно новых вызовов.

В 2019 году в России не допущено крупных компьютерных инцидентов, которые могли бы оказать негативное влияние на систему государственного управления или экономику страны. Хотя такие попытки предпринимались неоднократно. Удалось прекратить деятельность около 12 тысяч зарубежных ресурсов, используемых злоумышленниками для нанесения ущерба нашей стране. Шесть тысяч были заблокированы на территории России по запросам иностранных партнёров.

Кроме того, предотвращены масштабные заражения компьютерными вирусами, которые отмечены в других странах. Это стало возможным благодаря работе, проводимой совместно с российскими операторами связи и компаниями в сфере информационной безопасности, а также с зарубежными партнёрами.

При этом обстановка остаётся напряжённой, угрозы с ростом цифровизации бизнеса и общества продолжают активно эволюционировать.

Сохраняются устойчивые корыстные устремления злоумышленников. Более трети компьютерных атак направлено на получение несанкционированного доступа к финансовым средствам.

Для кражи персональных данных используются практически все известные типы вредоносного программного обеспечения, методы социальной инженерии и мошенничества. Многие пользователи зачастую сами способствуют успеху преступников, проявляя излишнюю доверчивость и пренебрегая методами защиты.

Исследователи выявили очередную уязвимость. Система под названием «умный дом», встроенная в холодильниках, микроволновках, стиральных машинах и прочих приборах быта, является удобной разработкой не только для её владельцев, но и для кибермошенников. По словам экспертов, с 2015 года сохраняется тенденция использования бот-сетей из Интернета вещей (объединённые предметы, оснащённые встроенными технологиями для взаимодействия друг с другом или с внешней средой. – прим. авт.) при осуществлении атак. Домашние устройства – роутеры, веб-камеры, средства контроля самочувствия и многое другое – легко взламываются, так как пользователи уделяют мало внимания их защите. А потом используются для несанкционированного доступа к другим объектам. Совокупная мощность атак через такие бот-сети может быть настолько велика, что способна привести к нарушению работы целого региона.

В 2020 году Национальный координационный центр по компьютерным инцидентам для увеличения защищённости планирует создать специализированный общедоступный ресурс для взаимодействия граждан и организаций с уполномоченными органами. Делается это в целях оперативной передачи данных о противоправных действиях в области IT-технологий, компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем. Такая система обратной связи позволит увеличить скорость реагирования на инциденты и расширит сферу контроля за информационной инфраструктурой.

Также ведомство рассчитывает с начала 2021 года начать опытную эксплуатацию общедоступного антивирусного мультисканера для проверки файлов на наличие вредоносной активности. Это позволит гражданам и юридическим лицам самостоятельно ликвидировать компьютерные инциденты и исключит обращения на зарубежные антивирусные ресурсы.

Статистика 2019-го свидетельствует о том, что государственный сектор вышел на первое место по фактам взлома. В прошлые годы лидировала кредитно-финансовая сфера. Также хакеры охотятся за интеллектуальной собственностью и научными достижениями. В Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации считают, что такая угроза очень ощутима с точки зрения национальной безопасности.

Задача – в короткий период обеспечить рост инфраструктуры, импортонезависимость, гарантировать надёжность и защищённость информационных ресурсов.

Как известно, с 1 июня 2019 года стартовал эксперимент по переводу информационных систем ряда министерств и ведомств в ГЕОП. Его участниками являются Минкомсвязи России, Фонд социального страхования Российской Федерации, Минюст России, Государственная фельдъегерская служба Российской Федерации, Федеральная таможенная служба, Ростехнадзор, Росгвардия, Минтруд России. Итоги будут подведены в декабре.

С момента утверждения четыре года назад концепции перевода обработки и хранения государственных информационных ресурсов произошло существенное развитие облачных технологий. За это время выросли сильные отечественные компании. Принят закон о критической информационной инфраструктуре (КИИ). Она включает объекты энергетики, жизнеобеспечения, системы государственного управления.

Эксперимент может иметь положительный эффект, так как у нас есть возможность отработать все процессы, оценить слабые места, которые будут устранены до масштабного переезда в единую облачную платформу всех организаций. Это обоснованный, логичный и перспективный шаг, своевременная инициатива. Она позволит повысить темпы развития государственных информационных систем за счёт централизованного подхода к защите, хранению и распространению данных.

Флагманами по внедрению решений в сфере IT-безопасности сегодня являются банки, поскольку кибератаки очень легко пересчитываются в денежные потери. Только в 2017-м из российских кредитно-финансовых учреждений и платёжных систем хакеры из группировки «Кобальт» похитили 1,35 млрд рублей. Злоумышленники также ответственны за кражи более 1 млрд евро примерно у 100 банков со всего мира. Мошенники заражали сеть, а затем удалённо посылали банкоматам команду выдавать деньги. Наличные в определённое время собирали специальные группы людей. В начале 2018 года Европол задержал в Испании лидера хакерской группировки. Личность задержанного не раскрывается. Известно только, что он является представителем «русскоязычного мира». После этого есть основания полагать: деятельность группировки прекращена.

В 2019-м более чем в 16 раз по сравнению с 2018 годом сократилось число клиентов кредитно-финансовых организаций, данные которых были украдены. В 2018 году похищенные базы данных содержали информацию почти о 1,4 млн физических лиц. За 2019-й отмечено утечек сведений порядка о 85 тысячах клиентов. Их источниками выступают не столько сотрудники финансово-кредитных учреждений, сколько другие операторы обработки персональных данных. Например, работающие на сайтах интернет-магазинов и объявлений.

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России в первой половине 2019 года обнаружил 13 тысяч объявлений о продаже и покупке персональных данных. Только 1,5 тысячи из них (12%) – это базы кредитно-финансовых организаций.

Более 97% хищений со счетов граждан и 39% юридических лиц было совершено с использованием приёмов так называемой социальной инженерии. Для такого метода необязательны данные, относящиеся к банковской тайне, они лишь уточняют и дополняют необходимую информацию. Мошенникам достаточно владеть сведениями о фамилии, имени и отчестве, а также номере телефона физического лица.

Однако киберсообщества неоднородны.

Есть «кибершпана», которая ворует у бабушек с карты по 1500 рублей, и хакерские группировки, похищающие финансовые средства в крупных размерах. В последнее время появляются и политически мотивированные сообщества, цель которых не монетизация, а получение необходимой информации. Если, скажем, при атаке на банк достаточно быстро преодолевается периметр и злоумышленник дерзко движется туда, откуда можно вывести деньги, то при взломе с целью получения контроля над первыми лицами компаний, госкорпорациями мы сталкиваемся с другим подходом. Это медленные атаки, развивающиеся в течение многих месяцев. Главная задача злоумышленников – не быть скомпрометированными, обнаруженными в этой структуре. Замаскировавшись, они могут жить в системах годами. Обычно такие хакеры используют вредоносное программное обеспечение, специально написанное под конкретную организацию, и стандартные средства защиты от него не спасут. Иногда над созданием «вредоноса» может работать команда до 100 человек. И отсюда возникает вопрос: кто готов инвестировать в атаку такие деньги?

Говоря про новый уровень угроз, считаем, что нельзя им противостоять, продолжая строить статичные системы информационной безопасности. Тратятся огромные ресурсы, при этом мы не становимся более защищёнными. Почему?

Многие руководители организаций считают: достаточно купить побольше дорогой техники, получше её спроектировать и она сама будет оберегать систему. Такой подход в давно поменявшемся мире уже не работает. За технологией должен стоять специалист, который способен вовремя среагировать на угрозу. Ведь злоумышленник может в считаные минуты аккуратно подчистить следы. Нельзя обеспечивать безопасность с 9 до 18 часов. Необходимо находиться постоянно с «открытыми глазами», круглые сутки мониторить ситуацию. Это как боевое дежурство личного состава при возникновении угрозы безопасности государства. Когда у нас речь идёт об обороноспособности страны, не возникает вопроса: а надо ли проводить учения солдат и офицеров? То же самое должно быть и с обеспечением IT-безопасности.

Сегодня по инициативе Минсвязи России и «Ростелекома» создаётся специальный киберполигон – виртуальная страна, где специалисты смогут проводить учения и тренировки, в процессе которых будет моделироваться развитие угроз, отрабатываться ответные действия. На его базе планируется проведение ежегодных федеральных соревнований по информационной безопасности и создание центра тестирования программного обеспечения [8].

У каждой организации есть информация, которая имеет ценность, а значит, притягивает злоумышленников. Причём не только снаружи, но и изнутри. Это могут быть документы под грифом «секретно», клиентская база, особенно-

сти технологических процессов, чертежи – всё, что не хочется дарить конкурентам и жуликам. В принципе, любой работник может являться потенциальным инсайдером и поставить информационную безопасность под угрозу, а также причинить серьёзный ущерб репутации компании. От злого умысла или банальной оплошности не застрахован никто: от низшего звена до топ-менеджмента.

Принцип работы DLP прост и заключается в анализе всей информации, исходящей, входящей и циркулирующей внутри компании. В случае если она критичная или отправляется туда, куда не положено, система блокирует её передачу и уведомляет об этом ответственного сотрудника.

Так, с помощью перехваченных DLP-файлов по ключевым словам в структуре одной из компаний был установлен работник, который выполнял планы продаж, бессовестно обманывая клиентов. Его начальник в связи с этим нес репутационные риски.

В другой организации была обнаружена переписка, где двое сотрудников делились опытом употребления наркотиков. Оперативное выявление противозаконных действий помогло избежать серьёзных проблем.

Система отслеживает не только активные программы на компьютере, но и любую другую работу с информацией: ввод данных с клавиатуры, переписку и передачу файлов по почте, в социальных сетях и мессенджерах, отправляемые на печать документы, время простоя, активность на сайтах и прочее.

Особенно много случайных сливов данных происходит при публикации фотографий в соцсетях с рабочего места, например, во время праздничных мероприятий. Некоторые имеют привычку их писать на бумажке и приклеивать на монитор.

Такая «слежка» вполне законна, так как, подписывая трудовое соглашение, сотрудник обязуется заниматься на рабочем месте только тем, что прописано в должностных инструкциях. О своих намерениях установить систему DLP работодатель должен проинформировать подчинённых.

Итак, технологии защиты становятся всё более совершенными. В МФТИ разрабатывают новый тип биометрии – рефлекторную идентификацию, основанную на индивидуальных особенностях реакции и скорости сужения и расширения зрачка у людей. Техника практически готова создать под неё нейронные сети. Это дело не очень далёкого будущего.

Повысить защищенность собственно электронных компонентов современной техники передачи, накопления и обработки данных от внешних преступных воздействий исключительно сложно.

Будущее России, ее экономики, обороноспособности, благосостояние населения будут определять не только промышленный потенциал и природные богатства, но и современные информационные и телекоммуникационные технологии, информационные ресурсы и услуги, а также способность государства обеспечить необходимую защиту этих ресурсов и технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. В России значительно выросло число киберпреступлений [Электронный ресурс]. – Режим доступа: https://nag.ru/news/newsline/106765/v-rossii-znachitelno-vyiroslo-chislo-kiberprestupleniy.html
2. BBC: хакеры рассказали о новом кибероружии, заказанном ФСБ для атак на соцсети и страны [Электронный ресурс]. – Режим доступа: https://www.znak.com/2020-03-18/bbc_hakery_rasskazali_o_novom_kiberoruzhii_zakazannom_fsb_dlya_atak_na_socseti_i_strany
3. В МВД созданы подразделения по борьбе с IT-преступлениями. [Электронный ресурс]. – Режим доступа: https://iz.ru/973398/2020-02-07/v-mvd-sozdany-podrazdeleniia-po-borbe-s-it-prestupleniiami
4. Долинко В.И. Некоторые аспекты информационной безопасности системы материально-технического снабжения ОВД МВД России в особых условиях // Вестник Московского университета МВД России. 2013. № 7. С. 199-205.
5. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид. наук. – Москва, 2003. – 178 с.
6. Кибербезопасность: как выработать цифровой иммунитет? [Электронный ресурс]. – Режим доступа: https://mvdmedia.ru/publications/shield-and-sword/aktualno/kiberbezopasnost-kak-vyrabotat-tsifrovoy-immunitet/
7. МВД: в России число киберпреступлений подскочило на 80% [Электронный ресурс]. – Режим доступа: https://www.znak.com/2020-04-15/mvd_v_rossii_chislo_kiberprestupleniy_podskochilo_na_80
8. МВД не хватает бюджетных средств для борьбы с киберпреступностью [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/news/505390.php
9. Названы регионы России с высоким уровнем киберпреступности [Электронный ресурс]. – Режим доступа: https://rg.ru/2020/02/10/reg-urfo/nazvany-regiony-rossii-s-vysokim-urovnem-kiberprestupnosti.html

УДК 004.056

ПОДСИСТЕМА, ОБЕСПЕЧИВАЮЩАЯ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В ИСОД МВД РОССИИ

Меняйло Л.Н.,
кандидат политических наук, доцент;
Алексеева П.В.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье рассматриваются ключевые элементы, обеспечивающие информационную безопасность в ИСОД МВД России, делается акцент на угрозах информационной безопасности.

Ключевые слова: информационная безопасность, единая техническая политика, опасность утечки, хищения и модификации, антивирусная защита, криптографическая защита информации.

SUBSYSTEM THAT PROVIDES INFORMATION SECURITY IN THE ISOD OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Menyaylo L.N.,
Candidate of Political Sciences, Associate Professor;
Alekseeva P.V.
(Putilin Belgorod Law Institute of MIA of the Russia)

Abstract: he article discusses the key elements that ensure information security in the ISOD of the Ministry of internal Affairs of Russia, and focuses on threats to information security.

Keywords: information security unified technical policy, risk of leakage, theft and modification, antivirus protection, cryptographic protection of information.

Подсистема информационной безопасности органов внутренних дел представляет собой совокупность правовых, технических и организационных мероприятий, средств и методов защиты, органов управления и исполнителей, направленных на противодействие угрозам информационной безопасности с целью предотвращения или существенного затруднения утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа к ней.

Подсистема информационной безопасности состоит из следующих элементов:

- антивирусная защита;
- анализ защищенности;
- обнаружение вторжений;
- защита информации от несанкционированного доступа;

- криптографическая защита информации;
- управление событиями информационной безопасности;
- ОИБ демилитаризованной зоны (пограничный сегмент, выполняющий функции разделения сети на внешнюю (сети Интернет) и внутреннюю и внутренней (ИМТС) при использовании общедоступных сервисов ИСОД).

Данная подсистема была разработана в обязательном соответствии с требованиями Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю Российской Федерации и решала наиболее значимые задачи обеспечения безопасности как внутри ИСОД, так и при взаимодействии с системами других органов государственной власти. Принимая во внимание все модели возможных угроз и нарушителей, которые были согласованы с ФСБ России и ФСТЭК России, была проведена единая техническая политика, регламентом которой были определены категории должностных лиц, наделенных функциями администраторов доступа к ресурсам либо защиты информации, а также самих пользователей ИСОД.

Угроза информационной безопасности органов внутренних дел выражается в таких условиях и факторах, которые создают реальную или потенциальную опасность утечки, хищения, модификации, искажения, подделки, копирования, блокирования информации и несанкционированного доступа к ней.

При создании довереной программной базы ИСОД МВД России был проведен анализ используемых средств, протоколов и стандартов, на основе которых было создано специальное программное обеспечение прикладных сервисов ИСОД, в том числе и тех, которые были направлены на защиту информации.

В 2016 году началась реализация комплекса поэтапных мер импортозамещения оборудования ИСОД и перевода ведомственной информационно телекоммуникационной платформы на отечественные средства вычислительной техники (СВТ):

- серверы – на базе процессора «Эльбрус»;
- терминальные станции – на базе процессора «Байкал»;
- операционные системы «Эльбрус», «Циркон», «Астра Линукс».

Подсистема обеспечения информационной безопасности ИСОД МВД России включает в себя:

1. Сервис управления доступом к информационным системам и ресурсам ИСОД МВД России (СУДИС). Сервис обеспечивает: управление доступом пользователей в систему; управление доступом пользователей к сервисам ИСОД; управление доступом сервисов ИСОД к другим сервисам ИСОД; единую точку входа в сервисы ИСОД; регистрацию событий безопасности и т.д.
2. Антивирус «Касперский», который надежно обеспечивает защиту от вредоносного программного обеспечения и защиту от почтового спама.
3. ViPNet Client обеспечивает защиту информации при ее передаче по каналам связи и защиту от сетевых атак на уровне АРМ. Он позволяет обмениваться информацией по открытым каналам связи с использованием шифрования. Это специализированный программный комплекс криптографической защиты (СКЗИ) для стационарных и мобильных АРМ, сертифицированный в ФСБ России.

4. КриптоПРО позволяет осуществлять идентификацию пользователей по электронной подписи (доступ в систему, доступ к сервисам ИСОД МВД России) и производить подписание электронных документов в Сервисе электронного документооборота.

В ходе плановых проверок сотрудникам удается выявить различные угрозы информационной безопасности. Большинство из них связаны с несанкционированным доступом к автоматизированным рабочим местам ИСОД устройств доступа к сети Интернет внешних адаптеров (смартфонов, планшетов), съемных носителей информации, которые заражены вирусом.

Актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации. С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации этих новых методов защиты информации. И, конечно, сильным катализатором этого процесса является развитие глобальной компьютерной сети общего пользования Интернет, а также такие нерешенные противоречивые проблемы Интернет, как защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов и т.п.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 25.11.2017) // Российская газета. 2006. № 165.

2. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

3. Распоряжение Правительства Российской Федерации от 20.10.2010 № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011 – 2020 годы)» // Собрание законодательства Российской Федерации. 2010. № 46. Ст. 6026.

4. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

5. Основы информатики и информационных технологий в ОВД: учебное пособие / А.Н. Прокопенко и [др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2016. – 144 с.

6. Информатика и информационные технологии в профессиональной деятельности / И.Ф. Амельчаков, В.Л. Акапьев, А.А. Гуржий, А.А. Дрога, П.Н. Жукова, В.А. Насонова, А.Н. Прокопенко, С.Е. Савотченко, А.А. Страхов: учебник. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2018. – 369 с.

УДК 004.93

ОСОБЕННОСТИ ЭКСПЛУАТАЦИИ СИСТЕМЫ БЕСКРАСКОВОГО ДАКТИЛОСКОПИРОВАНИЯ МАРКИ «ПАПИЛОН»

Чубейко С.В.,
кандидат технических наук, доцент;
Попова Е.В.
(Ростовский юридический институт МВД России)

Аннотация: статья посвящена основным особенностям дактилоскопирования. Рассмотрены бескрасковые устройства считывания информации кожного покрова рук человека, приведены основные задачи таких устройств. Представлены основные проблемные аспекты применения АДИС «Попилон».

Ключевые слова: дактилоскопирование, криминалистика, бескрасковые устройства, автоматизированная информационная система.

FEATURES OF OPERATION OF THE SYSTEM OF COLORLESS FINGERPRINTING OF THE PAPILON

Chubeyko S.V.,
Candidate of Technical Sciences, Associate Professor;
Popova E.V.
(Rostov Law Institute of the MIA of Russia)

Abstract: the article is devoted to the main features of fingerprinting. Colorless devices for reading information from the skin of human hands are considered, and the main tasks of such devices are given. The article presents the main problematic aspects of the use of the Papilon.

Keywords: fingerprinting, forensic science, colorless devices, automated information system.

В век бурного развития различных компьютерных технологий и современных кибернетических устройств в различные сферы человеческой деятельности внедряются новые методы получения той или иной информации. Так, в сфере раскрытия и расследования преступных деяний начали внедрятся современные технико-криминалистические методы и средства, которые применяются для эффективного и быстрого реагирования на совершенные преступления. Как известно, криминалистика состоит из различных разделов, так одна из задач такого раздела криминалистики, как криминалистическая техника, прямо рекомендует применение современных технологий для скорейшего раскрытия и расследования преступления.

Одно из самых распространенных методов и средств технико-криминалистического характера – это дактилоскопирование. Так как практически при совершении любых преступлений лицами, совершающими преступление, остаются объекты дактилоскопии. Как было сказано выше, одной из задач криминалистической техники является применение современных компьютерных и кибернетических технологии, и именно по этой причине отечественные криминалисты разработали совершенно новые автоматизированные дактилоскопические информационные системы, так называемые АДИС, которые на данном этапе являются эффективными помощниками правоохранительных органов. Бескрасковое устройство считывания информации кожного покрова рук человека «ПОПИЛОН» является одной из самых удобных и продвинутых из числа АДИС [1]. В оперативно-служебной деятельности применение данного современного и технологичного устройства позволяет выполнять следующие задачи:

- определять с точностью до 95% папиллярные узоры на пальцах рук человека;
- совершать электронную обработку полученных отпечатков, что позволит в кратчайшие сроки идентифицировать лицо, которому принадлежит данный отпечаток;
- создавать информационную базу отпечатков и следов пальцев рук, которые в значительной степени облегчат поиск нужного отпечатка, с которым необходимо сравнить имеющийся у сотрудников органов внутренних дел образец следа-отпечатка, изъятого из места происшествия, и др.

Все вышеперечисленное свидетельствует о необходимости и целесообразности использования современных технологий в повседневной оперативно-служебной деятельности сотрудников правоохранительных органов. Также на одной из коллегий МВД России Президент России В.В. Путин отметил необходимость дальнейшего совершенствования материально-технической базы структурных подразделений системы МВД России по всей стране [2]. Однако на практике возникают определенного рода сложности при выполнении задачи совершенствования материально-технической базы структурных подразделений системы МВД России, так как представляется крайне сложным повсеместно внедрить современные компьютерные технологии.

Одной из проблем планомерного введения во все структурные подразделения системы МВД России АДИС «ПОПИЛОН» является недостаточная ясность форм и средств проведения дактилоскопии. Вне всяких сомнений, основной нормативный правовой акт, регламентирующий дактилоскопирование на территории Российской Федерации, – Федеральный закон «О государственной дактилоскопической регистрации в Российской Федерации» описывает подробный порядок применения и учета объектов дактилоскопирования, однако, как было сказано выше, имеются недостатки касательно форм и средств проведения этой деятельности [3]. Например, в основном приказе МВД России, регламентирующем деятельность по проведению дактилоскопии, в Приложении № 3, оговорено, что у лица, проводящего дактилоскопирование, должны быть в наличии бланки дактилоскопических карт, черная типографическая краска

высшего качества, валик, металлические пластины для раскатки краски, а также специальный стол для дактилоскопии. Про иные инструменты, которые можно применять в процессе проведения дактилоскопии, не говорится, но п. 30 данного приказа не исключает возможность применения электронных дактилоскопических массивов. Данное положение дел свидетельствует о существовании коллизии в пунктах одного приказа, который регламентирует дактилоскопирование в различных государственных и силовых структурах Российской Федерации (МВД России, МЧС России, Министерство обороны Российской Федерации и др.) [4].

Рассмотрим вопрос о создании в структуре вышеназванного приказа МВД России специальной главы, которая будет содержать определенный перечень предметов, используемых при дактилоскопической регистрации. В нормах приведенного выше Федерального закона № 128-ФЗ данная проблема своего решения не нашла. В ходе проведенного исследования выявлены следующие проблемные аспекты повсеместного применения АДИС «ПОПИЛОН»:

1) чрезмерная дороговизна всей совокупности оборудования, которое составляет электронный сканер «ПОПИЛОН»;

2) на данном этапе чувствуется нехватка профессиональных кадров, способных обеспечивать нормальное функционирование АДИС «ПОПИЛОН»;

3) недостаточная надежность операционной системы, которая не отвечает современным требованиям загруженности компьютерных систем;

4) недостаточная бережность сотрудников органов внутренних дел, использующих данное оборудование в оперативно-служебной деятельности, которая зачастую приводит к поломкам и без того дорогого оборудования.

Резюмируя все вышесказанное, мы можем сказать о все возрастающей необходимости применения бескраскового электронного сканера «ПОПИЛОН» в оперативно-служебной деятельности правоохранительных органов для эффективной борьбы с преступностью. Применение данного оборудования в системе МВД России является той необходимой составляющей технико-криминалистических средств, которые будут способствовать раскрытию и расследованию преступлений по всей стране. Не стоит забывать и о достаточной правовой регламентации применения АДИС «ПОПИЛОН» в системе МВД России, так как отсутствие регламентации какой-либо деятельности ведет к различным негативным явлениям. Также решением проблемы кадрового персонала, который будет профессионально применять вышеназванную систему, является внедрение в программы образовательных организаций системы МВД России учебных занятий по работе с электронным сканером «ПОПИЛОН».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аверьянова Т.В. Криминалистика: учебник / Т.В. Аверьянова, Е.Р. Россинская, Р.С. Белкин, Ю.Г. Корухов. - 4-е изд., перераб. и доп. – Москва: Норма: НИЦ Инфра-М, 2017. – 928 с.

2. Официальный сайт МВД России [Электронный ресурс]. – Режим доступа: http://mvd. ru/news/item/836123/

3. Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» // СПС «Гарант».

4. Приказ МВД России, МЧС России, Минобороны России, Минфина России, Минюста России, Министерства транспорта Российской Федерации, Службы внешней разведки Российской Федерации, Федеральной таможенной службы, ФСБ России, Федеральной службы охраны Российской Федерации, Федеральной службы по контролю за оборотом наркотиков Российской Федерации и Федеральной миграционной службы Российской Федерации от 27 сентября 2010 г. №№ 688/422/1214/110н/235/205/36/1785/456/468/402/299 «Об утверждении Положения о порядке формирования и ведения информационного массива, создаваемого в процессе проведения государственной дактилоскопической регистрации»// СПС «Гарант».

УДК343.13

ИСПОЛЬЗОВАНИЕ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Карагодин А.В.,
кандидат юридических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина);
Карагодина А.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассматриваются актуальные проблемы безопасности жителей городов. Возросший уровень преступности и правонарушений, а также вероятность террористических актов являются одной из проблем для администрации 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.

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

Karagodin A.V.,
Candidate of Law, Associate Professor
(Putilin Belgorod Law Institute of the MIA of Russia);
Karagodina A.A.
(Kikot Moscow University of the MIA of Russia)

Abstract: 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 systemsto help law enforcement agencieswill greatly enhance the effectiveness of their work on crime prevention in the city.

Keywords: police, secure city, assistance of law enforcement agencies, video surveillance, security.

Начать хотелось бы с «громкого» дела, случившегося несколько недель назад. Актер, заслуженный артист России Михаил Ефремов, находясь не в трезвом виде, совершил ДТП, в котором погиб невинный человек.

Авария произошла 8 июня 2020 года вечером в Москве на Садовом кольце напротив здания МИД России. На видеозаписи, которая опубликована в Твиттере центра организации дорожного движения правительства Москвы, видно, как один из автомобилей (предположительно, им управлял Ефремов) движется по внутренней стороне Садового кольца, выезжает на встречную полосу и врезается в легковой фургон, который едет навстречу. Актер в ДТП не пострадал, а водитель, в которого он врезался, был доставлен в тяжелом состоянии в НИИ им. Склифосовского. Утром во вторник в НИИ им. Склифосовского сообщили, что пострадавший скончался.

Ефремов был задержан на месте происшествия и отправлен на медицинское освидетельствование на предмет наличия алкоголя в крови, экспертиза факт наличия подтвердила.

Таким образом, одним из серьёзных и значимых нововведений в профилактике преступности стало внедрение онлайн-съемки улиц города, а именно аппаратно-программного комплекса «Безопасный город», задача которого помогать 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].

На сегодняшний день обеспечение безопасности города намного обширнее, чем просто наблюдение за различными объектами. Современные цифровые системы способны не только обрабатывать видеопоток и передавать его по компьютерным сетям, но и осуществлять интеллектуальную обработку изобра-

жения, идентифицировать 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 связь 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 [2].

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 [3].

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 от-

дельных 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.

Основополагающими 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 [3].

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 безопас-

ности 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, в подъездах, местах скопления людей и проведения массовых мероприятий, на автомобильных магистралях, в государственных учреждениях, на жизненно важных для города объектах. На сегодняшний день более 102 500 камер установлено на только подъездах г. Москвы, более 193 000 камер по всему городу, в том числе камеры внешних систем видеонаблюдения, более 4 000 камер установлено в местах массового скопления граждан, и это далеко не предел.

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 [4].

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 объекты, 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 [5].

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;
- сокращение общего числа правонарушений вследствие осведомленности потенциальных правонарушителей о наличии видеонаблюдения;
- оказание помощи правоохранительным органам в следственно-розыскных 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 [5].

Необходимо выделить функцию выявления противоправных действий, так как с приходом века технологий, фотоснимки или записи, на которых четко видны признаки противоправного деяния, являются неопровержимым источником доказательств. Более 208 000 административных правонарушений зафиксировано в 2019-2020 годах.

Обратимся к ряду примеров, так Верховный суд г. Москвы 10 февраля 2020 г. рассмотрел дело, согласно которому 1 ноября 2018 года в 9 часов 58 минут транспортное средство марки «Toyo1a КАУ4», государственный регистрационный знак <...>, собственником (владельцем) которого является Иванова Е.В., в нарушение требований подпункта 4 пункта 4.4.2.5 Правил было размещено на территории, занятой зелеными насаждениями (травой), чем создано возникновение угрозы причинения вреда зеленым насаждениям, почвенно-растительному слою.

Согласно постановлению административной комиссии № 8 городского округа «Город Хабаровск» от 10 декабря 2018 года указанное административное правонарушение зафиксировано специальным техническим средством, имеющим функции фото- и видеозаписи, ПАК «ДОЗОР-МП», свидетельство о поверке действительно до 15 августа 2019 года.

На основании данных, полученных в результате работы названного комплекса, Иванова Е.В. привлечена к административной ответственности без составления протокола об административном правонарушении [6].

Таким образом, отметим, что аппаратно-программный комплекс «Безопасный город» в настоящее время развит достаточно хорошо, но самое главное, что он продолжает развиваться. 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 в полной мере еще недостаточно хорошо реализован.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галкина А. Интеллектуальное видеонаблюдение // Полиция России. 2014. № 2. С. 18.

2. Подсистемы «Безопасный города» [Электронный ресурс]. – Режим доступа: http://www.mrantenna.ru/stati/bezopasniie-gorod-sredstvo-upravleniya-megapolisom.html.

3. Безопасный город – структура системы [Электронный ресурс]. – Режим доступа: http://www.mrantenna.ru/ stati/bezopasniie-gorod-sredstvo-upravleniya-megapolisom.html.

4. Система видеонаблюдения // Группа компаний «Спецтехника» [Электронный ресурс]. – Режим доступа: http://gkst.org/business/10/.

5. Городская система видеонаблюдения «Безопасный город» / Концерн ПромСнабКомплект [Электронный ресурс]. – Режим доступа: http://www.1avtorem.ru/ pages/b-town.html.

6. Суд. Акт: судебные и нормативные акты РФ [Электронный ресурс]. – Режим доступа: https://sudact.ru/

УДК 343.7

КРИПТОВАЛЮТА КАК СРЕДСТВО И ПРЕДМЕТ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СОВРЕМЕННОМ МИРЕ

Тимакина Ю.А.,
кандидат экономических наук;
Андреева Д.А.
(Ростовский юридический институт МВД России)

Аннотация: в статье рассмотрены вопросы криптовалюты как средства и как предмета совершения преступлений в современном мире. Актуальность данной проблемы заключается в том, что на сегодняшний день криптовалюта – это не просто платежная система, это многомиллионные обороты денежных средств, которые могут попасть мошенникам в руки. Преступность в данной сфере очень высока, т.к. возможность получения огромных сумм заставляет мошенников взламывать криптобиржи. В статье присутствует терминология, сформулированной темы вопроса. Наглядные примеры, приведённые в статье, характеризуют сложившуюся обстановку с криптовалютой в мире в целом, не заостряя внимание на конкретном положении криптовалюты в Российской Федерации.

Ключевые слова: криптовалюта, блокчейн, биткоин, криптобиржа, средство платежа, мошенничество, отмывание денег.

CRYPTOCURRENCY AS A MEANS AND SUBJECT OF COMMITTING CRIMES IN THE MODERN WORLD

Timakina Yu.A.,
Candidate of Economical Sciences;
Andreeva D.A.
(Rostov Law Institute of the MIA of Russia)

Abstract: the article deals with the issues of cryptocurrency as a means and as a subject of crime in the modern world. The relevance of this problem lies in the fact that today the cryptocurrency is not just a payment system, it is a multi – million dollar turnover of funds that can fall into the hands of fraudsters. Crime in this area is very high, because the possibility of obtaining huge amounts of money makes fraudsters hack crypto-exchanges. The article contains the terminology of the formulated topic of the question.

Keywords: cryptocurrency, blockchain, bitcoin, crypto exchange, means of payment, fraud, money laundering**.**

В век распространения инновационных технологий очень распространены платежные средства, которыми можно было бы совершать покупки в электронном пространстве, не требующие выхода из дома и, соответственно, занимающие намного меньше времени. Такие средства очень удобны еще тем, что могут не иметь связи с банком, а быть связаны лишь как продавец-покупатель.

Что же такое криптовалюта? Криптовалюта является одновременно средством платежа и активом в сети Интернет. Благодаря ей можно заказать пиццу, полететь в Париж, отправиться в путешествие на Луну, оплатить билеты в кино. Эта валюта не существует физически, лишь в сети Интернет, однако её можно перевести в рубли и доллары через специальные средства (обменники)[1] Все данные о критовалютах хранятся в виде цепочки блоков на основе технологии Блокчейн. Технология Блокчейн уникальна, она создавалась в течение 10 лет и является безопасной и надежной в использовании. Посмотреть информацию обо всех переводах можно любому желающему, т.е. любой человек может увидеть сколько Вы перевели тому или иному человеку. Каждый новый блок содержит информацию о предыдущих переводах, комиссиях и другую служебную информацию.

Термин «криптовалюта» впервые начали использовать при появлении платежной системы «Биткоин», разработанной в 2009 г. До июля 2013 г. программное обеспечение всех без исключения криптовалют, помимо Ripple, базировалось на открытом исходном коде системы «Биткоин». После июля 2013 г. начали появляться новые платформы, поддерживавшие помимо криптовалюты различную инфраструктуру – мессенджеры, магазины, биржевую торговлю. К числу таких криптоплатформ относят: Nxt, Maastercoin, BitShares и др. [1]

У Блокчейна и Криптовалюты имеется ряд особенностей. Давайте рассмотрим их:

1. Особенность Блокчейна состоит в том, что эта система децентрализована, т.е. не имеет определенного центра, управляют этой системой сами пользователи. Для Криптовалюты не нужен банк, обмен происходит между продавцом и потребителем. К примеру, есть некая организация по предоставлению электроэнергии, которая имеет свою криптовалюту, например PowerCoin. Чтобы получать электроэнергию у этого поставщика вам необходимо иметь его PowerCoin. Вы можете обменивать Вашу криптовалюту на его электроэнергию.

2. Система анонимна. Криптовалюта может храниться на особых кошельках, которые являются безопасными и анонимными о своих владельцах. Есть лишь название кошелька, который представляет собой уникальный набор знаков, который существует в единственном экземпляре. Но с этим иногда происходят проблемы. Название кошелька имеет 33 символа и если пользователь каким-то случайным образом переводит средства на другой кошелек и ошибается на один символ, криптовалюта сгорает и исчезает. То же самое случается, если пользователь забывает имя своего кошелька, все средства, накопленные там остаются «навсегда». Так, британец Джеймс Хауэлс коллекционировал биткоины с 2009 года. Это было просто увлечение, ведь тогда они не имели такой цены, как сейчас. Он скопил около 7500 биткоинов, забыл о них и выбросил свой компьютер на свалку. А когда в 2016 году цены на биткоины возросли в 5 раз, британец понял, какую он ошибку сделал. Он мог заработать приблизительно 20 000 000 долларов.

[1] Данные, взятые с веб-сайта vsdelke.ru [Электронный ресурс]. – Режим доступа: https://vsdelke.ru (дата обращения: 21.05.2020).

3. Простота, но и одновременно скрытность системы. Пользователи могут видеть, что Вы перевели 2 биткоина своему знакомому, но не узнают, сколько биткоинов и другой криптовалюты у вас в кошельке. Система Блокчейна намеренно осложнена.

4. Хранение криптовалюты может быть разнообразным, как на особых кошельках (Matbea, Coinbase). Также есть «Холодные кошельки». Они похожи на флеш-носители и работают лишь при подключении к компьютеру. Еще один способ позволяет офлайн хранить криптовалюту как обычные деньги. Представляет собой похожую на банкноту запись с ключом к кошельку и QR-код. Опасность такого хранения заключается лишь в потере или стирании краски с бумаги.

А теперь немного о видах криптовалюты и ее происхождении.

1. **Биткоин (BTC)** – пожалуй, самая известная криптовалюта на сегодняшний день (и самая дорогая). Биткоин имеет уже устаревший код, и на ее основе сознаются новые криптовалюты, но это не делает ее менее популярной. История биткоина довольно проста. 22 мая 2010 года программист (имя пропущено) заказал себе две пиццы и по прибытию курьера пообедал ими. Ничего удивительного, НО. Эта сделка впервые за всю историю была оплачена криптовалютой, а именно – биткоинами. Эти две пиццы обошлись в 10 000 биткоинов, по 5 000 за каждую, пицца стоила примерно 30 $ на денежный эквивалент. Только представьте, что можно купить сейчас на 10 000 биткоинов по нынешнему курсу этой валюты? Курс биткоина на сегодняшний день 1 BTC = 500 701 рубль.

2. **Эфириум (ETH)** – разрабатывался на основе биткоина русским программистом канадского происхождения Виталием Бутериным. Система Эфириума более продумана, она децентрализована и представляет собой платформу для создания онлайн-сервисов на базе Блокчейна.

3. **Альткоин (ALT)** – криптовалюта, альтернативная биткоину. Если говорить кратко, эта валюта ищет некоторые ограничения и неточности в биткоине и старается их улучшить, сделать совершеннее.

Также существуют и другие виды криптовалют, по данным некоторых сайтов, на 2020 год насчитывается около 4500 криптовалют. Любой пользователь может создать свою криптовалюту, если у него есть достаточно мощное на то оборудование.

Цены на криптовалюту растут. Почему же некогда неизвестный биткоин стал самой дорогой криптовалютой в мире? Если брать один из законов экономики, который гласит «Спрос порождает предложение» и, соответственно, возрастание цен, то можно все понять. Чисто в теории, криптовалюта не имеет инфляции, но цены на нее могут падать. На начало 2018 года некоторые страны признали ее платежным инструментом (Япония, Германия), но не деньгами. В 2019 году некоторые страны разрешили официально выплачивать зарплаты в биткоине. В 2020 году Корея полностью узаконила все операции с криптоденьгами.

В России же еще нет правового регулирования в сфере криптовалюты. Правоохранительная деятельность в этой сфере не реализована, так как зачастую правоохранительные органы не берутся принимать заявления, с этим связанные.

Противники криптовалют часто утверждают, что криптомонеты массово используются в отмывании денег, торговле наркотиками, оружием, финансовых преступлениях и финансировании террористов. В прессе регулярно выходят статьи об очередном взломе криптобиржи или отмывании денег через биткоины. Но стоит задуматься и о том, что такое происходит не только с криптовалютой, но и с обычными электронными деньгами. Ни для кого не секрет, что с появлением какого-либо новшества в сфере информационных технологий, всегда найдутся люди, которые захотят использовать эту новинку в своих корыстных целях. Но давайте рассмотрим наиболее частые случаи, связанные с криптовалютой как предметом преступления в сфере информационных технологий.

Взломы криптобирж. Почему же хакеры взламывают такие биржы чаще, чем обычные кошельки? Это намного легче, и доход от полученного возрастает в разы.

По данным Group-IB, CipherTrace, Carbon Black, хакеры украли в 2018 году криптовалют на сумму от $1.1 до $1.7 миллиарда, из которых $960 миллионов – у криптобирж и платежных систем.

Фишинг. Фишинг – это подделка сайтов известных криптовалют, обменников и кошельков, то есть если пользователь введет на таком сайте свои персональные данные от аккаунта, они сразу попадут в руки к мошенникам, которые, в свою очередь, могут снять имеющуюся криптовалюту у пользователя.

По данным сайта РБК[1]: «27 февраля держатель цифровых денег под ником warith в своем твиттер-аккаунте сообщил, что потерял крупную сумму после того, как установил популярное приложение Coinomi. До этого он распоряжался криптовалютой через кошелек Exodus, но из-за того, что хранилище не поддерживало некоторые активы, переместил средства в Coinomi, используя ту же seed-фразу. Спустя несколько дней warith заметил, что 90% монет были выведены с его Exodus-кошелька на различные адреса. Так пользователь лишился своих биткоинов, ETH, токенов стандарта ERC-20, LTC и BCH, общей суммой в $70 000. В кошельке остались только те активы, которые не поддерживались Coinomi».

Очень много случаев, когда криптовалюта становится средством совершения преступления.

Вымогательство. Вирусы шифруют файлы на зараженном компьютере, после чего требуют выкуп в криптовалютах за ключ дешифровки. Яркие примеры: CryptoWall, Locky, KeRanger, XCodeGhost, WannaCry, NotPetya (общий ущерб составил примерно $325 миллионов).

Отмывание доходов. Обратимся к п. 1 ст. 174 УК РФ: «Совершение финансовых операций и других сделок с денежными средствами или иным имуществом, заведомо приобретенными другими лицами преступным путем, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами или иным имуществом». Но почему это происходит с криптоденьгами? Ввиду того, что система анонимна, ее зачастую обвиняют в отмывании незаконных доходов.

[1] Данные, взятые с веб-сайта [Электронный ресурс]. – Режим доступа: https://rbk.ru/ (дата обращения: 21.05.2020).

По данным Европола и Великобритании, через криптовалюту отмывают $5.5 миллиарда в год. 97% криминальных биткоинов отмывают через биржи со слабой AML-политикой.

Терроризм, незаконная продажа оружия и наркотиков. Из-за того, что система криптовалюты анонимна, зачастую невозможно узнать, кому принадлежит тот или иной кошелек, чем очень пользуются террористы, наркоторговцы и продавцы оружия. Проблема в этом случае приобретает глобальный характер.

Согласно официальным данным, оборот площадки составил около $1,2 миллиарда, доход – $90−$126 миллионов, ее использовали несколько тысяч нелегальных продавцов и более 100,000 покупателей по всему миру.

Согласно данным Фонда борьбы за демократию (FDD), на оборот наркотиков приходится до 90% всех незаконных транзакций с криптовалютами. Годовой оборот такой торговли может составлять $4−$5 миллиардов, доходить до 0.5−1% от общего оборота и охватывать до трети всех покупателей[1].

Что касается терроризма, то, по данным отчета Европола и правительственной комиссии Великобритании, биткоин и другие криптовалюты в последнее время не использовались для финансирования терактов на территории Европы и маловероятно, что ситуация изменится в течение ближайших пяти лет.

Исследование Center of a New American Security говорит о том, что террористы плохо понимают технологию криптовалют и предпочитают наличные и банковские переводы как более удобные и безопасные.

Флипинг криптовалюты. Подобные схемы предлагают быстрое увеличение инвестиций пользователя за определенную плату. В социальных сетях, на специализированных сайтах, размещаются объявления, в которых предлагается «флипнут крипту», т.е. выгодно поменять несколько раз на бирже. Реальное намерение состоит в том, чтобы получить доступ к кошельку и похитить криптоденьги.

Есть значительное число противников и криптовалюты, которые считают, что она способствует увеличению преступлений в сфере информационных технологий. Но, как мы заметили ранее, любая технология может стать предметом или средством совершения преступления. Технологии в современном мире стремительно развиваются и преступность пытается «идти» за ней.

В Российской Федерации необходимо регламентировать все операции с криптовалютой, дабы обезопасить пользователей этой огромной системы от преступных посягательств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шайдуллина В.К. Криптовалюта как новое экономико-правовое явление // Финансы и банковское дело. Вестник университета. 2018. № 2. С. 137–141.

2. Коренная А.А. Квалификация преступлений, совершаемое с помощью криптовалюты // Проблемы экономики и юридической практики. 2018 № 3. С. 220–223.

[1] Данные, взятые с веб-сайта [Электронный ресурс]. – Режим доступа: https://rbk.ru/ (дата обращения: 21.05.2020).

УДК 342.727

ЗАРУБЕЖНОЕ И ОТЕЧЕСТВЕННОЕ ЗАКОНОДАТЕЛЬСТВО, НАПРАВЛЕННОЕ НА БОРЬБУ С НЕДОСТОВЕРНОЙ ИНФОРМАЦИЕЙ В СЕТИ ИНТЕРНЕТ

Нестеров И.А.,
кандидат технических наук, доцент;
Гречко В.А.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье делается обзор отечественного и зарубежного законодательства, направленного на пресечение распространения недостоверной информации в сети Интернет, проводится классификация юридических методов борьбы с фейковыми новостями, а также оцениваются их преимущества и недостатки. Особое внимание в статье уделено конкретным законодательным мерам по предотвращению распространения фейкового контента в различных странах и видам наказания за его распространение.

Ключевые слова: фейковые новости, недостоверная информация, «закон о фейковых новостях».

FOREIGN AND DOMESTIC LEGISLATION AGAINST UNRELIABLE INFORMATION ON THE INTERNET

Nesterov I.A.,
Candidate of Technical Sciences, Associate Professor;
Grechko A.V.
(Kikot Moscow University of the MIA of Russia)

Abstract: the article reviews domestic and foreign legislation aimed at preventing the spread of false information on the Internet, classifies legal methods to combat fake news, and assesses their advantages and disadvantages. Particular attention is paid to specific legislative measures to prevent the spread of fake content in various countries and the types of penalties for its distribution.

Keywords: fake news, false information, «law on fake news».

В нашей стране впервые на государственном уровне вопрос борьбы с недостоверной информацией в сети Интернет был поднят 8 июня 2018 г., когда Комиссия Общественной палаты Российской Федерации по развитию информационного сообщества, СМИ и массовых коммуникаций провела круглый стол «Распространение фейковой информации в сети «Интернет»: проблема, угрозы, меры противодействия». На это мероприятие были приглашены руководители ведущих общественных организаций России (Союз журналистов Рос-

сии, Ассоциация электронных коммуникаций, Mail.ru Group, Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека, Комиссия Общественной палаты Российской Федерации по развитию информационного сообщества, а также многие другие).

Именно на этом мероприятии было сформулировано наиболее полное определение фейковых новостей: «Фальши́вые (подде́льные, «фе́йковые», ло́жные) но́вости – это информационная мистификация или намеренное распространение дезинформации в социальных медиа и традиционных СМИ с целью введения в заблуждение, для того чтобы получить финансовую или политическую выгоду[1]».

Девять месяцев спустя инициатива по борьбе с фейковыми новостями была рассмотрена на самом высоком уровне, вследствие чего Президент Российской Федерации В.В. Путин 18 марта 2019 года подписал ряд федеральных законов о недостоверных новостях. С этого дня в нашей стране за распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях заведомо недостоверной общественно значимой информации под видом достоверных сообщений введено наказание в виде наложения штрафа до полутора миллионов рублей [1].

Спустя год после введения антифейкового законодательства меры пришлось ужесточить. Это в основном связано с распространением недостоверной информации о новой коронавирусной инфекции COVID–19 [2].

Так, по сведениям газеты Коммерсант, глава Государственного центра по информированию россиян о ситуации с коронавирусом Алексей Гореславский сообщил, что ежедневно выявляется пять-шесть кампаний по распространению в Интернете ложных сведений об эпидемии и около 50 сообщений, которые можно назвать фейками [3].

В этой связи был принят Федеральный закон от 01.04.2020 № 100-ФЗ, который внес изменения в административное и уголовное законодательство Российской Федерации, касающиеся установления ответственности за распространение недостоверной информации, в том числе и в сети Интернет. Впервые административная ответственность была введена для юридических лиц с максимальным наказанием в виде штрафа 10 миллионов рублей, а уголовное наказание для граждан стало предусматривать ограничение свободы на срок до трех лет [4].

Стоит отметить, что российское законодательство не является уникальным. Зарубежный опыт борьбы с фейковыми новостями юридическими методами также достаточно обширен, и его можно условно разделить на пять основных направлений:

1. Криминализация процесса распространения фейковых новостей.
2. Стандартизация и кодификация условий распространения информационного контента.

[1] В Общественной палате Российской Федерации обсудили распространение фейковой информации [Электронный ресурс]. – Режим доступа: https://raec.ru/live/branch/

3. Запретительные и ограничительные меры в отношении распространителей фейков.

4. Персонализация и идентификация участников обмена информацией в сети Интернет.

5. Раскрытие информации и предоставление прямого доступа к ресурсам Интернета.

Процесс распространения фейковых новостей в сети Интернет был криминализован (признан общественно опасным деянием) во многих зарубежных странах. Причем в некоторых из них предусмотрены достаточно суровые меры наказания, на их фоне новый российский закон не выглядит столь жёстким.

Например, в Китае с 2 марта 2020 г. на фоне пандемии коронавируса дезинформация в соцсетях была признана уголовным преступлением. По сообщению правозащитной организации Chinese Human Rights Defenders, по меньшей мере 452 интернет-пользователя уже получили наказание за распространение слухов о коронавирусе. Большинство из них были арестованы на срок от 3 до 15 дней, а некоторые отделались штрафами [5].

Аналогично, гражданам Узбекистана может грозить наказание в виде штрафа до 9 тыс. долларов США, обязательные общественные работы до 360 часов, исправительные работы или лишение свободы сроком до трех лет [6].

Согласно закону «Об улучшении правоприменения в социальных сетях» (Net Enforcement Act), принятому парламентом Германии 30 июня 2017 года, за систематическое игнорирование правил по своевременному удалению фейковых новостей в социальных сетях владельцы соцсетей могут быть оштрафованы на сумму до 50 миллионов евро. Данный закон имел огромный резонанс и получил название «Закон о Facebook» [7].

Во Франции были приняты аналогичные законы, среди которых следует отметить Закон от 22 декабря 2018 г. № 2018-1202 «О борьбе с манипулированием информацией» (Relative à la lutte contre la manipulation de l’information). В законе указано, что за недобросовестные публикации, распространение или воспроизведение любым путем ложных, сфабрикованных и фальсифицированных сообщений, вызвавших нарушение общественного спокойствия, предусмотрено наказание в виде штрафа до 135 000 евро [8].

Другие европейские страны также имеют достаточно жёсткое антифейковое законодательство, предполагающее не только штрафы, но и ограничение свободы граждан за распространение лживых новостей в сети Интернет. Так, по сообщению Балканской сети журналистских расследований (BIRN), в течение первых недель марта 2020 года в Турции, Сербии, Венгрии и Черногории за распространение дезинформации о коронавирусе были арестованы по меньшей мере 80 человек, а еще 260 оштрафовано. Некоторые венгерские интернет-страницы и связанные с ними страницы в Facebook, на которых до официального сообщения властей сообщалось о наличии в стране инфицированных и погибших, были закрыты [3].

2 октября 2019 в Сингапуре вступил в силу Закон о борьбе с фейковыми новостями. За распространение ложных сведений грозит до 10 лет тюрьмы и штраф до 1 млн сингапурских долларов, что составляет порядка 738 тысяч американских долларов [9].

По аналогичному пути следует и Малайзия, в парламенте которой 26 марта 2018 года было начато рассмотрение законопроекта о борьбе с фальшивыми новостями. За их распространение предусмотрен штраф до 128 тысяч долларов и тюремные сроки вплоть до десятилетнего заключения [10].

Несколько другим путём идёт законодательство Египта, где 18 августа 2018 года Президентом Египта был ратифицирован Закон «О борьбе с киберпреступностью», согласно которому наказанию подвергаются посетители запрещённых к просмотру сайтов (их в списке более пятисот). Только за одно посещение на пользователя будет наложен штраф в 20 тысяч египетских фунтов (около 6 тыс. американских долларов) или его посадят в тюрьму сроком на один год [11].

Таким образом, процесс распространения фейковых новостей за последние три года был криминализован (признан общественно опасным деянием) не только в России, но и за рубежом. Особенностью этого метода борьбы с фейками является непосредственное воздействие на виновную сторону, а также профилактика совершения новых преступлений.

Другим юридическим методом борьбы с фейковыми новостями является запрещение или ограничение на законодательном уровне тех или иных действий в сети Интернет.

Например, власти Ирана и Шри-Ланки запретили доступ к ряду социальных сетей. Белоруссия, Кыргызстан и Венесуэла заблокировали ряд внешних интернет ресурсов. Аналогично поступила и Украина, где ограничен «доступ сотрудников государственных учреждений, предприятий и организаций к доменным зонам «.ru» и «.ру» с целью предотвращения вреда интересам государства в сфере информационной безопасности [12]».

С марта по май 2020 года в Китае заблокировали более 18 000 аккаунтов за распространение фейковых новостей о коронавирусе [13].

В нашей стране после принятия в 2012 году Федерального закона № 139-ФЗ была разрешена блокировка запрещённых интернет-ресурсов, где имеются призывы к массовым беспорядкам, осуществлению экстремистской деятельности и несогласованным акциям.

Таким образом, меры запретительного и ограничительного характера направлены, прежде всего, на блокировку доступа непосредственно к интернет-ресурсу без подробного анализа всей информации, размещённой на нём. Сами по себе эти меры не налагают на владельцев сайтов иных мер воздействия, кроме блокировки доступа к ресурсу в данной стране.

Наряду с запретами, выраженными в криминализации и ограничении той или иной деятельности в сети Интернет, существуют и иные методы государственного воздействия на процесс обмена информацией. К ним относится законодательное требование к персонализации и идентификации пользователей Интернета.

Например, в Казахстане для того, чтобы сделать комментарий к какой-либо публикации в сети Интернет, пользователь обязан пройти обязательную СМС-идентификацию. При этом владельцы сайтов обязаны хранить данные пользователей не менее трёх месяцев после того, как пользователь расторгнет соглашение [14].

Аналогичное требование действует и в Китае, где 1 октября 2017 года введена обязательная идентификация личности пользователей, пишущих комментарии в Интернете. Однако отправки СМС здесь недостаточно. Нужно ввести свои паспортные данные. Причём процедура привязки паспортных данных пользователя к его аккаунту осуществляется на форумах и других интернет-сообществах [15].

В нашей стране с ноября 2018 года идентификация пользователей мессенджеров происходит при помощи номера телефона. Причём мобильные операторы должны хранить данные о том, в каких приложениях переписываются их клиенты. Иных ограничений, в том числе на обязательную идентификацию при комментировании, пока не введено.

Таким образом, персонализация и идентификация участников обмена сообщениями в сети Интернет ставит своей целью облегчить выявление распространителей запрещённой, в том числе и фейковой, информации.

Довольно радикальным методом по выявлению информации, связанной с противозаконными действиями, в том числе и распространением фейковых новостей, является обязательство интернет-провайдера предоставлять органам власти конфиденциальную информацию о деятельности пользователей.

Например, в Австралии провайдеры обязаны по запросу предоставлять ключи шифрования. Причём за отказ предоставить ключи будет наложен штраф до 7,3 млн австралийских долларов, а также возможно даже тюремное заключение [16].

В нашей стране с марта 2018 года Федеральная служба безопасности Российской Федерации обязала организаторов распространения информации предоставлять в ведомство ключи шифрования в срок до 10 дней со дня получения запроса.

Помимо того, с 1 июля 2018 года в России вступил в силу закон Яровой, который обязывает операторов телекоммуникационных услуг хранить записи телефонных сообщений и интернет-трафик их клиентов на протяжении полугода.

Аналогично, в Китае с 1 ноября 2018 года правоохранительным органам разрешено проведение проверок в компаниях, работающих в сфере информационных технологий, в том числе с правом получать доступ и копировать данные, имеющие отношение к кибербезопасности [17].

Таким образом, прямой доступ к информации позволяет выявлять злоумышленников в процессе расследования преступлений, в том числе и в интернет-пространстве.

Превентивным методом борьбы с фейковыми новостями на государственном уровне является стандартизация и кодификация условий распространения информационного контента.

Например, правительство Великобритании в апреле 2019 г. приняло так называемую Белую книгу «О вреде онлайн», в которую был включен ряд требований к технологическим компаниям по защите интересов пользователей (Duty of care), а также установлена ответственность за информационный контент. В этой связи был разработан комплекс мер против дезинформации «Противодействие» (RESIST), который включает в себя шесть шагов: «обнаружение, ранее предупреждение, ситуационное осмысление, анализ воздействия, стратегическую коммуникацию, отслеживание последствий [18]».

Таким образом, стандартизация на государственном уровне требований к размещаемой в Интернете информации позволяет предотвратить неконтролируемое распространение фейковых новостей.

Подводя итоги анализа зарубежного и отечественного законодательства, направленного на борьбу с недостоверной информацией в сети Интернет, можно утверждать, что к неоспоримым преимуществам юридических методов борьбы с фейковыми новостями можно отнести:

- наличие действенных рычагов наказания за противоправные действия;
- наличие механизмов по прямой блокировке сайтов и соцсетей;
- возможность прямого вмешательства в деятельность интернет-ресурсов и получения необходимой информации.

Слабыми сторонами антифейкового законодательства являются:

- в условиях глобализации фейковые новости могут поступать из-за рубежа, где применить внутригосударственные законы невозможно;
- зачастую источником фейковых новостей является анонимное лицо, идентифицировать которое и применить к нему меры воздействия весьма затруднительно;
- эти методы работают выборочно и требуют отдельного контроля. Другими словами, юридическими методами выявить фейковые новости невозможно. Они работают лишь с уже собранными фактами, а в условиях динамичности интернет-среды их эффективность ограничена.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 18 марта 2019 г. № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СПС «КонсультантПлюс».

2. Разъяснены вопросы разграничения уголовной и административной ответственности за фейки о коронавирусе [Электронный ресурс]. – Режим доступа: https://www.garant.ru/news/.

3. Коваленко М., Беленькая М., Тарасенко П. Вакцина от фейков: как мир борется с дезинформацией о пандемии // Коммерсантъ. 2020. № 57. С. 4.

4. Статья 207.1 УК РФ. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан // СПС «КонсультантПлюс».

5. Замахина Т. Вводится наказание за распространение фейков о коронавирусе // Российская газета. [Электронный ресурс]. – Режим доступа: https://rg.ru/vvoditsia-nakazanie-za-rasprostranenie-fejkov-o-koronaviruse.html

6. Брага К. В Узбекистане ввели уголовную ответственность за фейки о COVID-19 [Электронный ресурс]. – Режим доступа: https://ria.ru/20200326/1569193853.html

7. Маслова В. Штрафной удар: в Германии приняли закон об административной ответственности соцсетей за публикацию фейков [Электронный ресурс]. – Режим доступа: https://russian.rt.com/world/article/404675-feik-novosti-nenavist-socseti-germaniya.

8. Воронко Я. Fake news: как страны борются с недостоверными новостями [Электронный ресурс]. – Режим доступа: https://ilex.by/news/fake-news-kak-strany-boryutsya-s-nedostovernymi-novostyami/.

9. Осипова Т.С. Технологии противодействия fake news в мировой практике // Меридиан. 2020. № 4. С. 31–32.

10. Маркова Н.А. К вопросу об административной ответственности за распространение фейковых новостей // Учёные записки. 2019. № 2. С. 93.

11. Степанова С. Президент Египта ратифицировал закон об интернет-контроле [Электронный ресурс]. – Режим доступа: https://360tv.ru/news/.

12. Рюмин А. Все способы борьбы с фейками в России и за рубежом [Электронный ресурс]. – Режим доступа: http://rapsinews.ru/incident_publication/20181221/292876054.html.

13. Кольцова М. Как борются с фейк-ньюс о коронавирусе: опыт России, Китая и Европы [Электронный ресурс]. – Режим доступа: https://tjournal.ru/internet/.

14. Маляренко В. Власти Казахстана запретили оставлять анонимные комментарии в интернете [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/politics/.

15. Зубарев Д. Китай решил ввести идентификацию по паспортам для комментариев в сети [Электронный ресурс]. – Режим доступа: https://vz.ru/news/2017/8/25/884301.html.

16. Соколов А. Австралия вслед за Россией потребовала предоставить ключи шифрования мессенджеров [Электронный ресурс]. – Режим доступа: https://riafan.ru/1129110.

17. Трепалина Ю. В КНР полиции дали право обыскивать здания провайдеров и копировать их данные [Электронный ресурс]. – Режим доступа: https://nag.ru/news/newsline/.

18. Годованюк К. Кибербезопасность и борьба с дезинформацией: опыт Великобритании // Научно-аналитический вестник ИЕ РАН. 2019. № 4. С. 90.

УДК 004

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБУЧЕНИИ

Дубинина Н.М.,
кандидат юридических наук, доцент
(Московский университет МВД России имени В.Я. Кикотя);
Бубнов В.В.,
кандидат экономических наук, доцент
(Московский авиационный институт»)

Аннотация: в статье рассматривается возможность применения информационных технологий в образовательном процессе.
Ключевые слова: информационных технологии, учебный процесс.

APPLICATION OF INFORMATION TECHNOLOGIES IN TRAINING

Dubinina N.M.,
Candidate of Law, Associate Professor
(Kikot Moscow University of the MIA of Russia);
Bubnov V.V.,
Candidate of Economic Sciences, Associate Professor
(Moscow aviation Institute»)

Abstract: the article considers the possibility of using information technologies in the educational process.
Keywords: information technologies, educational process.

Важнейшим резервом повышения эффективности и качества подготовки высококвалифицированных кадров является внедрение информационных технологий (ИТ) в сферу образования и обучения[1].

В настоящее время информационные технологии являются естественным инструментом познавательной и профессионально-практической деятельности любого специалиста, в том числе и педагога. Поэтому их использование в повышении качества образования и учебного процесса – это не следование модным тенденциям, а осознанная необходимость.

[1] В Федеральном законе «Об образовании в Российской Федерации» под обучением понимается «целенаправленный процесс организации деятельности обучающихся по овладению знаниями, умениями, навыками и компетенцией, приобретению опыта деятельности, развитию способностей, приобретению опыта применения знаний в повседневной жизни и формированию у обучающихся мотивации получения образования в течение всей жизни».

Говоря об информационных технологиях[1], будем подразумевать системно организованную для решения практических задач совокупность методов и средств реализации операций сбора, регистрации, передачи, накопления, поиска, обработки и защиты информации на базе применения развитого программного обеспечения, используемых средств вычислительной техники и связи, а также способов, с помощью которых информация предлагается пользователям. Средства выступают в качестве инструмента, а методы – это правила, приемы, способы манипулирования имеющимися средствами для достижения заданных целей.

Отметим основные свойства, присущие информационным технологиям, которые могу быть полезны для пользователя (педагога, руководителя и т.д.):

– представляют собой наиболее универсальную и надежную форму хранения, передачи и обработки информации;

– благодаря своей универсальности снимают технические ограничения на обмен информацией;

– являются эффективными носителями современных методов решения разнообразных задач практики (образовательных, организационных и др.);

– помогают преодолевать пропасть между сложными явлениями и процессами реальной действительности, формализованными методами их познания.

Таким образом, говоря об информационных технологиях, следует рассматривать две их стороны: определенное научное направление и конкретный способ работы с информацией.

Поэтому информационные технологии можно охарактеризовать и как совокупность знаний о способах и средствах работы с информационными ресурсами, и как способ и средства сбора, обработки и передачи информации для получения новых сведений об изучаемом объекте.

Для эффективного решения образовательных, учебных, научных, производственных, управленческих и других задач должна быть обеспечена возможность передачи во времени и пространстве накопленной информации. Развитие сетевых технологий позволяет обеспечить широкий доступ пользователей к информационным, в том числе и образовательным, ресурсам.

Внедрение информационных технологий в сферу образования и обучения меняет стиль работы педагогов и обучаемых. Обмен данными и файлами, работа с электронной почтой, организация и ведение баз данных делают процесс обучения наглядным, интересным, более эффективным.

Для системы органов внутренних дел появление современных персональных компьютеров, серверов, сетевых технологий и унифицированного программного обеспечения ускорило процесс создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России (продолжение проекта по созданию единой информационно-телекоммуникационной системы органов внутренних дел (ЕИТКС ОВД)).

[1] В Федеральном законе «Об информации, информационных технологиях и о защите информации» определено, что «информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов».

Использование информационных технологий в профессиональной деятельности является одним из квалификационных требований, предъявляемых к сотруднику органов внутренних дел [3]. Всестороннее применение ИТ в процессе подготовки будущих специалистов позволяет повысить уровень информационной культуры и грамотности, снять возможные психологические барьеры, подготовить обучаемых к использованию новых технических возможностей.

Одной из задач образования является не только передача обучаемым определенной суммы знаний, но и формирование у них умений и навыков самостоятельного приобретения знаний. Главным условием успеха в любой сфере деятельности становится умение ориентироваться в потоке информации, выделять главное, обобщать, делать выводы. Поэтому сложно переоценить роль педагога в раскрытии возможностей современных информационных технологий в процессе преподавания естественно-научных и гуманитарных дисциплин.

Не менее важной является проблема подготовки самих педагогов к работе в условиях компьютеризации учебного процесса, поэтому информационная технология обучения (ИТО) представляет собой педагогическую технологию, использующую специальные способы, программно-технические средства для работы с информацией.

Подводя итоги, хотелось бы отметить основную специфику использования информационных технологий в решении практических задач образовательного процесса. Специфика определяется научной постановкой практических задач, которые могут быть решены с использованием информационных технологий; наличием моделей, научно обосновывающих постановку практических задач; использованием методов и алгоритмов решения поставленных задач на основе предложенных моделей; разработкой алгоритмов решения практических задач с использованием вычислительной техники и проведением расчетов; доказательством адекватности поставленных и решенных задач объективной реальности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // СПС «КонсультантПлюс».

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

3. Приказ МВД России от 01.02.2018 № 50 «Об утверждении Порядка организации прохождения службы в органах внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

4. Торопов Б.А., Апульцин В.А. Технологии многокритериального оценивания результатов деятельности территориальных органов МВД России на региональном уровне: учебное пособие. – Москва: Академия управления МВД России, 2016. – 112 с.

5. Информационные технологии в управлении органами внутренних дел: учебник / под ред. И.В. Горошко. – Москва: Академия управления МВД России, 2015. – 156 с.

УДК 344.77

К ВОПРОСУ ПРАВА СОБСТВЕННОСТИ НА КРИПТОВАЛЮТУ (НА ПРИМЕРЕ БИТКОЙН)

Галушин П.В.,
кандидат технических наук;
Филипсон К.Ю.
(Сибирский юридический институт МВД России)

Аннотация: в данной статье рассматривается понятие и принципы функционирования криптовалют, их отличия от традиционных электронных платёжных систем, особенности, затрудняющие законодательное регулирование оборота криптовалют, на примере недавних изменений гражданского законодательства и проекта федерального закона «О цифровых финансовых активах». Авторы показывают, что многие проблемы, связанные с определением и регулированием права собственности на криптовалюту, могут быть трудноразрешимыми при рассмотрении криптовалют самих по себе, но их решение упрощается, если рассматривать реалистичное использование криптовалют, при котором криптовалюта продаётся и приобретается через специальные биржи, не путём майнинга, который является недоступным для большинства лиц применительно к достаточно зрелым криптовалютам.

Ключевые слова: криптовалюта, цифровые права, право собственности, биткойн, блокчейн.

ON THE ISSUE OF CRYPTOCURRENCY OWNERSHIP (USING BITCOIN AS AN EXAMPLE)

Galushin P.V.,
Candidate of Technical Sciences;
Filipson K.Yu.
(Siberian Law Institute of theMIA of Russia)

Abstract: this article discusses the concept and principles of the functioning of the cryptocurrencies, their differences from traditional electronic payment systems, features that complicate the legislative regulation of cryptocurrency circulation, using the example of recent changes in civil law and the draft federal law «On Digital Financial Assets». The authors show that many problems associated with determining and regulating the ownership of the cryptocurrencies can be intractable when considering cryptocurrencies in isolation, but their solution is simplified if we consider the realistic use of the cryptocurrencies, in which cryptocurrency is sold and acquired through special exchanges, not by mining, which is inaccessible to most individuals for fairly mature cryptocurrencies.

Keywords: cryptocurrency, digital rights, ownership, bitcoin, blockchain.

Современное общество характеризуется интенсивным развитием информационных технологий и ростом их влияния на жизнь людей. На первоначальном этапе информационные технологии являлись лишь средством автоматизации привычных видов деятельности, поэтому для них не требовалось особое законодательное регулирование.

Однако со временем развитие науки и техники привело к созданию предпосылок формирования таких общественных отношений, которые идут в разрез с привычными представлениями и попытки их правового регулирования без учёта особенностей их функционирования наталкиваются на серьёзные проблемы.

Одной из подобных информационных технологий являются так называемые криптовалюты – феномен на стыке экономики и компьютерной техники, который в последнее время привлёк к себе существенное общественное внимание. Криптовалюта – это информационная система для обмена имуществом в электронной форме и одновременно единица измерения количества этого имущества. В данной статье рассматриваются принципы функционирования криптовалют и влияние этих принципов на возможность применения концепции права собственности к критповалюте.

Первой криптовалютой был Биткойн (Bitcoin), это название происходит от английских слов bit (бит – минимальная единица количества информации в вычислительной техникие) и coin (монета). Статья [8] с описанием этой системы был опубликована в 2008 году человеком или группой людей под псевдонимом Сатоси Накамото [6].

Термин «криптовалюта» закрепился позже – после публикации статьи о системе Биткойн «Crypto currency» (Криптографическая валюта), опубликованной в 2011 году в журнале Forbes [7]. Сам же автор Биткойн, как и многие другие, использовал термин «электронная наличность» (англ. electronic cash).

Биткойн создавался как децентрализованная альтернатива традиционным электронным платёжным системам с централизованным учётом, основанным, по сути, на доверии участников к организатору системы (государству или юридическому лицу).

Обмен имуществом в электронной форме требует поддержания базы данных, в которой хранилась бы информация о состоянии счетов и транзакциях, а также системы авторизации – проверки права распоряжения счетами (осуществления транзакций). В традиционных электронных платёжных системах указанная база и система авторизации управляется доверенным лицом – организатором данной электронной платёжной системы, который обеспечивает правильность функционирования.

Если же отказаться от наличия доверенного лица, то возникает комплекс вопросов, без ответа на которые функционирование подобной системы невозможно:

– Как проверять право на распоряжение имуществом на счёте?

– Где должна храниться база данных о счетах и транзакциях?

– Как обеспечить невозможность отмены транзакций после её завершения?

Подтверждение права распоряжение счётом осуществляется с использованием несимметричной криптографии, а именно – технологии электронной подписи. Создание счёта в криптовалюте заключается в случайном выборе пароля[1] и построении номера счёта на основании этого пароля[2]. Номер счёта является открытой информацией и играет роль ключа проверки электронной подписи, а пароль необходимо хранить в секрете, так как он используется для простановки электронной подписи.

Для перевода средств со своего счёта на другой счёт владелец просто подписывает (с использованием специализированного программного обеспечения) своей электронной подписью соответствующее распоряжение и отправляет его всем участникам системы. На современном уровне развития науки и техники не существует метода подделки электронной подписи за разумное время, при этом любой желающий может проверить, что распоряжение было действительно подписано владельцем счёта.

В криптовалютах текущее состояние счетов, как правило, вообще не хранится, а определяется по истории транзакций. При этом база транзакций должна храниться у всех заинтересованных участников системы. Это, в свою очередь, требует решения проблемы согласованности баз данных у разных участников и его частный случай – невозможности отмены транзакции после её осуществления.

Обеспечение согласованности основано на технологии блокчейн (англ. blockchain – цепочка блоков). При использовании этой технологии транзакции объединяются в блоки, причём к каждому блоку добавляется некоторая информация о предыдущем блоке – так называемый хэш [1, с. 549-556]. Правила вычисления хэша таковы, что вычислить его для данной информации относительно просто, но определить, какой блок информации заданного размера будет давать заданное значение хэша, можно только путём подбора. Это означает, что внесение локальных изменений в список транзакций невозможно: после изменения даже одной транзакции необходимо внести изменения во все последующие блоки.

Проверкой правильности транзакций и цепочек блоков занимаются добровольцы, которые предоставляют свои вычислительные ресурсы для осуществления указанной выше деятельности, а взамен они получают комиссию от каждой транзакции[3] и право эмиссии новых единиц криптовалюты. Эта деятельность называется майнингом (от англ. mining – добыча полезных ископаемых), а лица её осуществляющие – майнерами.

Так как участие в майнинге вознаграждается получением криптовалюты, а участвовать в нём могут все желающие, то вводится правило, определяющее, кто из майнеров получит вознаграждение, и чья цепочка является правильной.

---

[1] Длина номера счёта выбрана так, что вероятность совпадения номеров пренебрежимо мала.

[2] Заметим, что отсюда следует полная анонимность счетов в криптовалюте: персональные данные владельца счета вообще не фиксируются в системе. Обратной стороной анонимности счетов в криптовалюте является невозможность смены пароля счета или его восстановления в случае утраты.

[3] Размер комиссии устанавливается отправителем, но он может влиять на время, которое уйдёт на включение транзакции в цепочку блоков.

Само по себе добавление блоков в цепочку по правилам, описанным выше, или изменение уже сформированной цепочки не требует большого количества вычислительных ресурсов: необходимость внесения большого количества изменений само по себе не означает, что это займёт много времени при использовании современной вычислительной техники. Поэтому описанная выше технология блокчейна должна быть дополнена специальными правилами, которые делают процесс формирования блоков сложной вычислительной задачей даже для самых мощных компьютеров.

В случае криптовалюты Биткойн и некоторых других криптовалют используется концепция «доказательства выполнения работы», которая требует, чтобы новый блок не только содержал допустимые транзакции (действительно подтверждённые владельцами счетов, с которых производится перечисление, и передающие количество криптовалюты, не превышающее текущий баланс счёта) и хэш предыдущего блока, но и некоторую дополнительную информацию, добавляемую майнером и называемую Nonce. При этом майнер должен подобрать Nonce таким образом, чтобы хеш получившегося блока (список транзакций, информация о предыдущем блоке, временная пометка и Nonce) удовлетворял определённым ограничениям (был меньше заданного числа, определяемого суммарной вычислительной мощностью всех майнеров).

Как уже указывалось выше, не существует быстрого способа определения информации, хэш которой будет иметь заданное значение. Поэтому майнинг действительно оказывается сложной вычислительной задачей. Правила системы таковы, что сложность майнинга возрастает со временем (а объём эмиссии за каждый успешно созданный блок убывает). Это приводит к тому, что на ранних этапах функционирования криптовалюты майнинг возможен на обычных настольных компьютерах, а на поздних – только на специализированных суперкомпьютерах.

Вознаграждение получает тот майнер, которому удалось сформировать новый корректный блок первому, а истинной признаётся та версия цепочки, которая является самой длинной (так как её сложнее всего было получить). При этом остаётся возможность того, что некоторая транзакция будет сначала признана, но потом отменена, но вероятность такого события уменьшается с увеличением количества блоков, следующих за тем блоком, в который входит данная транзакция.

Так как майнингом могут заниматься все желающие, история транзакций в криптовалюте должна быть полностью публичной. Однако, в отличие от электронных платёжных систем, эта публичность не приводит к разглашению каких-либо конфиденциальных сведений, так как счета в криптовалюте являются анонимными.

Федеральная налоговая служба считает криптовалюты «иным имуществом» [3]. Возникает вопрос о праве собственности на это имущество. При рассмотрении криптовалют часто рассуждают о них по аналогии с электронными платёжными системами. Однако электронные платёжные системы и криптовалюты принципиально отличаются. Первые являются централизованными сис-

темами, управляемыми оператором, который может в некоторых случаях, например, по решению суда, применять арест счетов или отменять транзакции.

А в криптовалютах, подобных Биткойн, такие механизмы не предусмотрены принципиально: сделки необратимы, а счётом может управлять только тот, кто знает пароль от него. При этом пароль и счёт связаны друг с другом алгоритмически. Эта связь не устанавливается никакой организацией или органом власти, её невозможно изменить или разорвать. Право собственности становится не причиной, а следствием возможности распоряжения имуществом.

Так называемый Закон «О цифровых правах» ввел в законодательство Российской Федерации принципиально новую конструкцию, когда право может определяться правилами информационной системы: «Если иное не предусмотрено законом, обладателем цифрового права признается лицо, которое в соответствии с правилами информационной системы имеет возможность распоряжаться этим правом. В случаях и по основаниям, которые предусмотрены законом, обладателем цифрового права признается иное лицо» [2].

Однако в соответствии с законом [4] цифровыми правами могут быть: право требовать передачи вещи (вещей); право требовать передачи исключительных прав на результаты интеллектуальной деятельности и (или) прав использования результатов интеллектуальной деятельности; право требовать выполнения работ и (или) оказания услуг.

Существует проект закона «О цифровых финансовых активах» [5], который распространяет подобную конструкцию на право собственности, но на момент написания статьи, он ещё не принят.

В связи с высокой степенью анонимности и неподконтрольности государственным структурам криптовалют, подобных Биткойн, у законодателя может возникнуть соблазн вообще не признавать такие криптовалюты или прямо запретить их. Однако это вряд ли можно признать удовлетворительным решением. Если не признать существование криптовалют, то ситуация де-факто вряд ли изменится, криптовалютами пользовались и до возникновения какого-либо законодательного регулирования.

Если же законом будет признано существование криптовалют, то есть имущества, право собственности на которое определяется правилами информационной системы и знанием определённой информации, то также могут возникнуть новые юридические феномены. Например, необходимость рассмотрения судом соответствия фактического функционирования информационной системы принципам, заявленным её организаторами, или математической корректности алгоритмов, лежащих в основе функционирования криптовалюты.

Так как пароль от кошелька в криптовалюте нельзя изменить, то право собственности фактически не может быть отчуждено. Его нельзя передать, а можно только разделить. Если не брать в расчёт конструкции вида «обещаю забыть пароль», а если брать, то к исполнению этого обещания невозможно принудить.

Однако все сказанное выше относится только к ситуации, когда криптовалюта рассматривается сама по себе. Получение криптовалюты возможно несколькими способами. Во-первых, с помощью майнинга, но для зрелых криптовалют майнинг становится недоступным для физических лиц.

Во-вторых, это так называемое ICO (Initial Coin Offer – первичное предложение монет), в ходе которого создатель криптовалюты продаёт определённое количество криптовалюты за рубли или валюту. Этот метод также плохо подходит для физических лиц.

Наконец, можно обменять своё имущество на криптовалюту, принадлежащую другому лицу. В частности, существуют организации, которые позволяют обменивать криптовалюты на рубли или валюту. Их называют биржи криптовалют или криптобиржи. Официальный курс криптовалют к фиатным валютам, как правило, не устанавливается. На биржах криптовалют устанавливается курс, определяемый балансом спроса и предложения.

Для осуществления операции на криптобирже необходимо указать как счёт криптовалюты, так и счет в фиатных деньгах (например, счет банковской карты или Qiwi-кошелек). Таким образом, криптобиржа имеет возможность связать анонимные счета в криптовалюте с персонифицированными банковскими счетами. А лицо, которое захочет использовать криптовалюту, будет вынуждено купить и/или продать её на криптобирже.

Большинство физических и юридических лиц не сможет получить криптовалюту (за исключением недавно возникших криптовалют) путём майнинга или ICO. Кроме того, криптовалюта сама по себе представляет лишь записи в электронном документе. Таким образом, большинство физических и юридических лиц будет вынуждено прибегать к услугам бирж криптовалюты, что существенно меняет ситуацию.

Предположим, суд принял решение о переходе права собственности на имущество, представляющее собой криптовалюту. В самой криптовалюте нет механизмов обеспечения подобного решения. Это обусловлено самим построением системы. Можно предположить, что законодательный запрет не приведёт к полному отказу от использования подобных криптовалют.

В рамках законопроекта о цифровых финансовых активах существует следующее решение. Обмен криптовалюты на рубли или валюту возможен только через операторов, то есть юридических лиц, которые созданы в соответствии с законодательством Российской Федерации и осуществляют виды деятельности, указанные в статьях 3, 4, 5 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг», или юридические лица, являющиеся организаторами торговли в соответствии с Федеральным законом от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах».

Законодатель мог бы обязать указанных операторов проверять информацию о наличии счетов, оформленных на лицо, указанное в запросе, а также выполнять решения судов о передаче имущества. Если пароль от счёта контролируется биржей, то процедура передачи может применяться к нему немедленно. В противном случае она может применяться при попытке обмена криптовалюты на другой цифровой финансовый актив, рубли или валюту.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кнут Д. Искусство программирования. Т. 3. Сортировка и поиск. – 2-е изд. – Москва: Вильямс, 2007. – 824 с.

2. Федеральный закон от 18.03.2019 № 34-ФЗ О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации // СПС «КонсультантПлюс».

3. Письмо ФНС России от 22.11.2018 № БС-4-11/22635@ «О налогообложении доходов физических лиц» (вместе с Письмом Минфина России от 08.11.2018 № 03-04-07/80764).

4. Федеральный закон от 02.08.2019 № 259-ФЗ О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации // СПС «КонсультантПлюс».

5. Проект Федерального закона «О цифровых финансовых активах» (подготовлен Минфином России) / Федеральный портал проектов нормативно правовых актов [Электронный ресурс]. – Режим доступа: https://regulation.gov.ru/projects#npa=77904 (дата обращения: 25.02.2020).

6. Оригинальное сообщение Сатоси Накомото [Электронный ресурс]. – Режим доступа: https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html (дата обращения: 19.05.2020).

7. Greenberg A. Crypto-currency [Электронный ресурс]. – Режим доступа: https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html (дата обращения 25.05.2018).

8. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. – Режим доступа: https://bitcoin.org/bitcoin.pdf (дата обращения: 19.05.2020).

УДК 378.1

АВТОМАТИЗАЦИЯ ДЕЯТЕЛЬНОСТИ БИБЛИОТЕК НА ОСНОВЕ RFID-ТЕХНОЛОГИЙ

Перепелкин И.Н.,
кандидат физико-математических наук;
Дунаев Р.А.,
кандидат философских наук
(Белгородский государственный институт искусств и культуры)

Аннотация: в статье рассматривается вопрос автоматизации библиотечной деятельности посредством внедрения технологии радиочастотной идентификации. Рассмотрены основные термины и принципы работы систем радиочастотной идентификации. Указаны преимущества RFID-систем, показана их эффективность как в обслуживании читателей, так и в работе персонала. Отмечены преимущества использования технологии радиочастотной идентификации над штрихкодированием.

Ключевые слова: радиочастотная идентификация, RFID-системы, ридер, метка, библиотека, библиотечный фонд.

AUTOMATION OF LIBRARY ACTIVITIES BASED ON RFID TECHNOLOGIES

Perepelkin I.N.,
Candidate of Physical and Mathematical Sciences;
Dunaev R.A.,
Candidate of Philosophical Sciences
(Belgorod State Institute of Art and Culture)

Abstract: the article considers the issue of automation of library activities through the introduction of radio frequency identification technology. The basic terms and principles of the operation of radio frequency identification systems are considered. The advantages of RFID-systems are indicated, their effectiveness is shown both in servicing readers and in staff work. The advantages of using RFID technology over bar coding are noted.

Keywords: radio frequency identification, RFID-systems, reader, tag, library, library stock.

Развитие информационных технологий обозначило некоторые изменения во всех сферах человеческой деятельности: меняются привычные способы взаимодействия между людьми, между человеком и инфраструктурой. Изменения не только внешние, например, Ромбокубооктаэдр библиотеки г. Минск,

библиотека в виде конуса голландского г. Делфта, библиотека-раковина в г. Астане и т.д.), но и высокотехнологичные, полностью автоматизированные (научно-техническая библиотека Сингапура, первая в мире библиотека без бумажных книг BiblioTech (США)). Библиотека сегодня рассматривается как современный информационный центр, а концепция открытого доступа считается одной из инновационных. «Умная» полка, бесконтактная инвентаризация фондов при помощи специализированного оборудования, возможности мобильных устройств и скоростного беспроводного подключения создают определенную комфортную атмосферу, положительно влияют на процессы библиотечной деятельности.

Любая информационная система работает с данными. Одним из условий эффективного внедрения систем является снижение затрат на ввод первичных данных. Воплощение идеи автоматической идентификации объектов посредством радиосигналов начинает свою историю с 40-х годов XX века. Процессы выдачи книг, каталогизация фондов и др. – сегодня основные направления автоматизации. Сокращается время на обслуживание, появляется возможность персонального учета предпочтений. Все это оказывает влияние на удовлетворенность читателей. Если книга находится не на своем месте, то это вызывает недовольство пользователей и может сказаться на репутации библиотеки и ее сотрудников. Для того, чтобы подобные ситуации были единичными в библиотеках внедряются технологии, способные организовать и контролировать процессы, проходящие в современных библиотеках. Внедрение информационных технологий актуально не только для крупных, но и небольших сельских библиотек.

Одним из способов автоматизации библиотечной деятельности является внедрение Radio Frequency Identification (RFID). В аббревиатуре RFID буквы RF означают «радиосигналы», а буквы ID-«идентификацию». По своей сути, RFID аналогичен штрихкоду, который считывается электромагнитным полем, или лазерным лучом. RFID-технология является самой передовой технологией по сравнению с штрихкодированием, постепенно заменяет его или начинает использоваться параллельно [1, с. 53]. При этом имеет ряд преимуществ, а именно: относительно небольшую стоимость меток, отсутствие наличия объекта в прямой видимости, высокую точность считывания, одновременную идентификацию нескольких объектов и т.д.

Системы на базе технологии RFID давно и успешно работают в библиотеках Европы, Америки и Азии. В России более 30 библиотек используют в своей работе RFID-технологию (по материалам компании Bibliotheca, специализирующейся на разработке, производстве, поставке и технической поддержке библиотечных технологических решений).

В настоящее время RFID дает возможность отправить информацию об объекте при помощи радиосигналов и меток на RFID-принимающее оборудование для последующей идентификации объектов. Система радиочастотной идентификации состоит из устройств, которые взаимодействуют между собой для достижения определенной цели, в частности, автоматизации и идентификации [2, с. 87]. Любая RFID-система включает в себя считыватель (ридер) и метку.

Метка представляет собой достаточно сложное устройство, функцией которой является взаимодействие с ридером, который, в свою очередь, управляется компьютером. Управляющий компьютер – это понятие достаточно условное, так как в устройстве самого считывателя, как правило, тоже находится свой компьютер. То же самое можно сказать и о метке, в которой имеется свой компьютер.

Если рассмотреть устройство считывателя, то оно состоит из микропроцессорного блока управления, который, в свою очередь, связан с радиочастотным блоком радиоантенны. Еще как отдельный блок следует выделить интерфейсный модуль связи со внешним компьютером.

Метка, в свою очередь, тоже является достаточно сложным устройством. В ее состав входит блок управления, который можно считать микропроцессором, функцией которого является взаимодействие с радиочастотным блоком [3, с. 66]. Очень важно отметить то, что метка содержит перезаписываемую энергонезависимую память и может содержать в себе некоторое количество данных. Еще одним важным моментом является то, что метка взаимодействует с ридером не путем передачи каких-то сигналов, а путем модуляции электромагнитного поля самого ридера. Во время работы, если метка хочет передать данные для ридера, она по определенной закономерности замыкает антенну. При этом электромагнитное поле нагружается больше замкнутой на «землю» антенной, и сам по себе ридер эти изменения нагрузки улавливает и расшифровывает как некоторые сигналы, которые он получает от метки.

Из 5 существующих диапазонов, в которых работает RFID-оборудование, в библиотеках может быть использовано оборудование в двух диапазонах, исходя из того, что по показателям дальности и проникающей способности они ближе всего к потребностям библиотек: высокочастотный (13,56 МГц) и сверхвысокочастотный (868-960 МГц).

В зависимости от выбора диапазона связь между сверхвысокочастотным (СВЧ) ридером и меткой осуществляется по-разному. Ридер является направленным излучателем, так как длина волны СВЧ-диапазона соизмерима с размерами антенны. По этой причине антенна влияет на распространение волн таким образом, что можно сфокусировать эти радиоволны в определенном направлении. Показатель дальности таких систем значительно выше, чем у ВЧ-систем. При этом сама метка тоже представляет собой антенну.

Если рассмотреть принцип действия ВЧ-систем, то там длина волны значительно больше размеров самого излучателя (примерно 20 м). Подобного размера ридеров не существует, и ридер ведет себя как точечный излучатель. В данном случае нет направленного излучения, а есть излучение во все стороны. Дальность действия таких систем небольшая, обычно до 1 метра. При этом проникающая способность таких радиоволн существенно выше.

В библиотеках RFID система появилась благодаря своим техническим характеристикам и возможностям. В библиотеках давно начали использовать системы, препятствующие воровству книг. Радиочастотная метка позволяет автоматизировать идентификацию пользователей и исключить кражу книг и любых источников информации на твердых носителях. Это оказалось очень удобно, и эти системы начали активно внедрять в библиотеках по всему миру [4, с. 12].

В состав оборудования, используемого в библиотеках, входят, прежде всего, сами ридеры, которые используют сотрудники библиотек для идентификации книг и читателей. Так как идентификация в RFID-системах очень проста, то появилась возможность отдать эту функцию самим читателям через станции самообслуживания. Процесс идентификации читателей настолько упростился, что может происходить автоматически без участия самого читателя. С этим связано появление противокражных функций, и метка, обрабатываемая системой, определяет, может ли читатель выносить книги или не может. Если нет, то система подает сигнал о несанкционированном выносе.

Помимо этого, RFID система позволяет решить очень важную проблему инвентаризации и наведения порядка на стеллажах. Эта задача особенно актуальна для больших библиотек, и ее решение до внедрения RFID-систем требовало значительных временных затрат. Информация, получаемая с помощью RFID-ридера, в автоматическом режиме предается в базу данных и выводится на монитор. RFID-технологии имеют серьезные преимущества по сравнению с штрихкодированием. Информация с метки считывается бесконтактным методом на расстоянии. На метку можно записать большее количество информации, и она может дополняться или изменяться при необходимости [5, с. 18].

К RFID оборудованию, на базе которого строится комплексная библиотечная система, относятся:

- RFID теги (этикетка для маркировки документов и пластиковая карта для идентификации читателей);
- ридеры малой дальности для пунктов комплектования и контроля;
- ридеры средней дальности для пунктов книговыдачи и обработки заказов читателей;
- RFID ворота для контроля перемещения маркированных документов и идентификации читателей;
- мобильные ридеры для автоматизированной инвентаризации библиотечного фонда;
- специализированное оборудование с использованием RFID-технологии – станции самообслуживания, возврата книг, туннельные считыватели, сортировщики, транспортные системы.

Нужно отметить, что на сегодня RFID-метки, по сравнению с другими видами идентификации, такими, как QR-коды, «мягкие» бирки sensormatic softtag (zl) и противокражные метки (EAS), имеют меньшее распространение в силу как специфики применения, так и стоимости. Также помимо электромагнитных систем присутствуют акустомагнитные системы, радиочастотные системы, RFID-системы.

Внедрение RFID-систем в библиотеках позволяет решить актуальную проблему автоматизации библиотечной деятельности. RFID-системы позволяют сотрудникам более эффективно организовать работу с читателями, проводить инвентаризацию и решать проблему сохранности библиотечных фондов, оперативно вносить анализ разнообразной статистики. Это дает возможность вывсти библиотеку на новый, более высокий уровень.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Тимошенко И.В. Библиотечные системы радиочастотной идентификации: возможность создания универсальных систем на основе международных стандартов // Научные и технические библиотеки. 2018. № 4. С. 53–59.
2. Тимошенко И.В. Библиотечное RFID-оборудование и средства поддержки технологии радиочастотной идентификации в составе САБ ИРБИС64 // Научные и технические библиотеки. 2013. № 12. С. 87–94.
3. Абросимова Н.В. Технологии RFID: опыт внедрения и использования // Университетская книга. 2013. № 4. С. 66–68.
4. Андреева Л.Н. Радиочастотная идентификация – средство повышения эффективности работы библиотечного информационно-образовательного центра // Вектор науки Тольяттинского государственного университета. Серия: Педагогика, психология. 2014. № 4 (19). С. 12–14.
5. Зиборов И.А. Применения RFID технологий в деятельности различных субъектов хозяйствования // Молодой ученый. 2009. № 12. С. 17–22.

УДК 323.2

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ В КОНТЕКСТЕ ИНФОРМАЦИОННО-ПРОПАГАНДИСТСКОЙ ДЕЯТЕЛЬНОСТИ

Меняйло Д.В.,
кандидат юридических наук, доцент;
Караулова Е.А.
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в данной статье рассматривается предупреждение и пресечение экстремизма и терроризма путем информирования населения и пропаганды гуманистического принципа существования человека в обществе. Взаимное информирование представителей государственных органов власти, органов местного самоуправления, представителей общественности и в целом граждан и пропаганда нетерпимости к экстремизму и терроризму является одним из действенных способов профилактики и предупреждения терроризма.

Ключевые слова: экстремизм, терроризм, идеология, информационное противодействие, информационно-пропагандистская деятельность, антитеррористическое просвещение.

COUNTERING EXTREMISM IN THE CONTEXT OF ADVOCACY

Menyaylo D.V.,
Candidate of Law, Associate Professor;
Karaulova E.A.
(Putilin Belgorod Law Institute of the MIA of Russia)

Abstract: this article discusses the prevention and suppression of extremism and terrorism by informing the public and promoting the humanistic principle of human existence in society. Mutual informing representatives of state authorities, local governments, members of the public and citizens in general and propaganda of intolerance to extremism and terrorism is one of the most effective ways to prevent and prevent terrorism.

Keywords: extremism, terrorism, ideology, informational counteraction, informational and propaganda activities, anti-terrorism education.

В настоящее время проблема терроризма набирает значительные обороты, так как сопровождается особой жестокостью со стороны преступников. Проблема террористической угрозы является злободневной, к отражению которой необходимо быть готовыми всегда. Существует ряд институтов, которые способствуют предупреждению и предотвращению данной опасности. Таковыми являются различные общественные объединения, научно-исследовательские центры, всевозможные форумы, СМИ и т.д. Основные задачи таких институтов представлены на рис. 1.

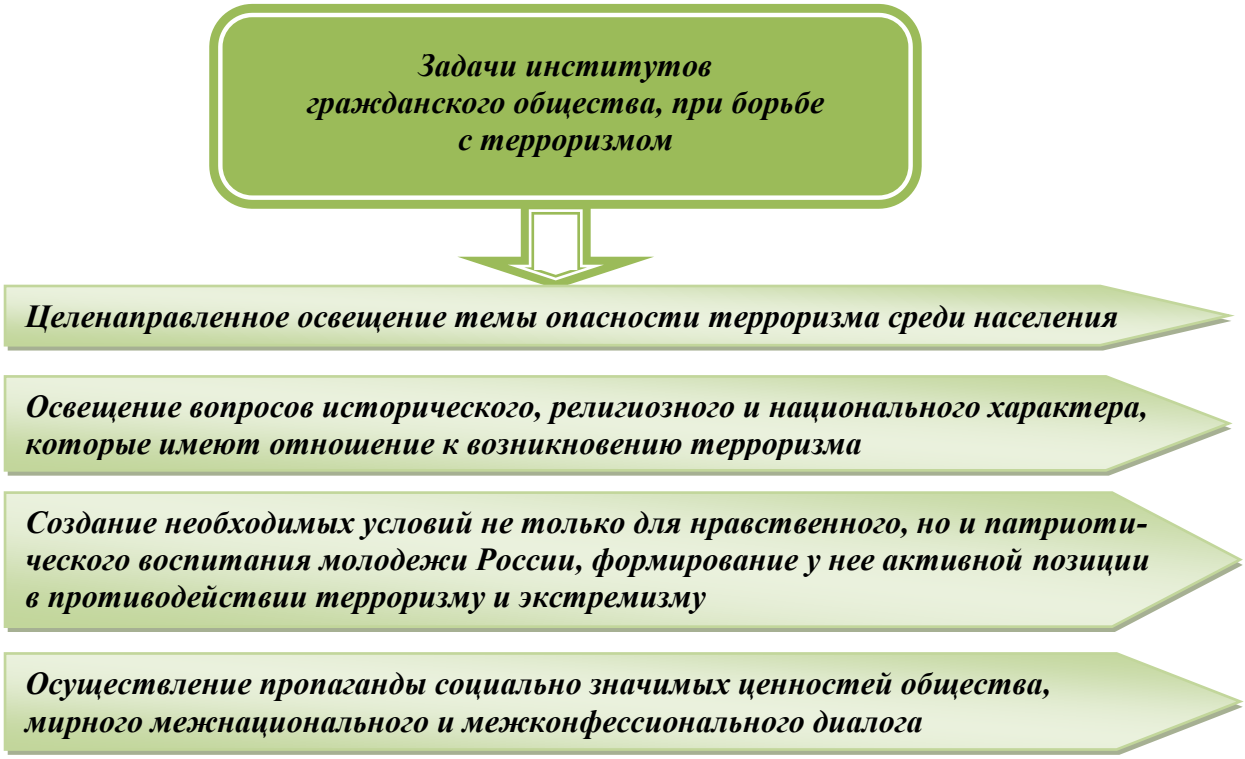


Рисунок 1. Основные задачи гражданских институтов в борьбе с терроризмом

Но следует учитывать, что террористы вырабатывают сотни изощренных, скрытых способов информационного манипулирования над населением [1, 2]. Для этого они используют информационно-телекоммуникационную сеть Интернет, различные личностные и межличностные коммуникации. Терроризм процветает благодаря постоянному материальному обеспечению (финансовому вливанию заинтересованных сторон), данная деятельность оттачивается и совершенствуется с каждым днем. Вырабатываются различные способы укрытия преступников, провоза оружия и боеприпасов через границы. Все это делает терроризм практически не решаемой проблемой человечества.

В связи с этим необходимы глобальные усилия, объединение и солидаризация в сфере информационно-пропагандистской деятельности, которая задействует все население нашей страны. То есть нужно разработать для каждой категории граждан свои эффективные методы и способы информирования и пропаганды против терроризма.

Необходимо выделить общие методы:

- разъяснение сущности терроризма и его общественной опасности;
- формирование стойкого неприятия обществом идеологии насилия;
- привлечение граждан к участию в противодействии терроризму;
- пропаганда социально значимых ценностей;
- создание условий для мирного межнационального и межконфессионального диалога [17].

Рассмотрим конкретные способы информационной пропаганды. Одним из наиболее распространенных является метод информационно-просветительской встречи. При планировании таких встреч в качестве целевой аудитории мероприятий рекомендуется рассматривать школьников старшеклассников и студентов. Сущность этого способа заключается в разъяснении сущности терроризма и его общественной опасности, пропаганда социально значимых ценностей, а также создании условий для мирного межнационального и межконфессионального диалога. В качестве примера можно привести встречи детей и молодежи с представителями антитеррористических комиссий субъектов Российской Федерации или органов местного самоуправления, Национального антитеррористического комитета, ФСБ России, сотрудниками Центра по противодействию экстремизму МВД России, их территориальных органов и т.д. [3]. Также к этой группе следует отнести проведение различных слётов, конференций, организацию дискуссионных клубов.

Еще немаловажным методом является проведение фестивалей и культурно-просветительских мероприятий по антитеррористической тематике. Этот способ направлен на более зрелый возраст. При планировании таких фестивалей и культурно-просветительских мероприятий необходимо обратить внимание на организации и представителей иных народностей и этносов, проживающих в субъекте.

Такой способ, как проведение обучающих программ, требует заблаговременной разработки и реализации обучающих программ. Основной задачей является обеспечение у детей и молодежи стойкого неприятия идеологии терроризма проведением просветительской деятельности. При проведении таких мероприятий необходимо учитывать различные целевые аудитории – от школьников до специалистов органов исполнительной власти. Данный способ заключается в разработке и внедрения специальных дополнительных образовательных программ, методических рекомендаций и учебных пособий.

В условиях осуществления глобализации информационного пространства большое внимание следует уделять информационно-пропагандистскому обеспечению противодействия терроризму во взаимодействии со СМИ.

Следует отметить, что необходимо фильтровать в сети Интернет сайты, пропагандирующие терроризм. Это вызвано тем, что информация, которая выкладывается террористами без какой-либо цензуры, что позволяет обычному гражданину узнать о данной деятельности в полной мере и даже оставить комментарий для вступления в террористическую культуру [1]. Борьба с пропагандой терроризма должна развиваться в рамках безопасности страны, так как информационная безопасность сегодня для многих стран имеет больший приоритет, чем ядерная безопасность. Между тем на современном этапе следует отметить тот факт, что информационная пропаганда является одним из наименее разработанных направлений антитеррористической деятельности как на международном уровне, так и непосредственно в Российской Федерации [15].

Более того, на настоящий момент в официальных источниках не существует строго определенного понятия «информационное пропагандирование», данный термин предполагает лишь на практике реализацию мер, связанных с предупредительным характером.

Главная роль в пропаганде против терроризма отводится сотрудникам органов внутренних дел. Нормативной базой деятельности сотрудников органов внутренних дел является, конечно же, Конституция Российской Федерации, федеральные законы, указы и распоряжения Президента Российской Федерации, постановления Правительства Российской Федерации. Одним из главных нормативно-правовых актов в данной сфере является Федеральный закон «О противодействии терроризму» [15].

Согласно Федеральному закону «О полиции» [16] основными направлениями деятельности органов внутренних дел по профилактике и предупреждению терроризма являются следующие, представленные на рис. 2.

Рисунок 2. Основные направления деятельности сотрудников органов внутренних дел

В компетенцию сотрудников полиции входит предупреждение и пресечение угрозы терроризма. Для создания условий борьбы с данной проблемой появляется необходимость во взаимодействии с другими подразделениями, в полномочия которых входит борьба с терроризмом.

Слаженная работа сотрудников органов внутренних дел и различных ведомств способствует быстрому разрешению в борьбе с терроризмом. Самой сложной формой в предупреждении данной деятельности является пресечение проведения террористического акта. Так как очень сложно предположить, где террорист решит осуществить террористический акт. При поиске заложенных взрывных устройств, используются служебные собаки, а уже для дальнейшего обезвреживания приступают саперы.

Так, на примере Белгородской области можно наблюдать со стороны государства принятие всех необходимых мер для недопущения экстремизма и терроризма. 20 ноября 2008 года на базе Управления по борьбе с организованной преступностью был создан Центр по противодействию экстремизму. Основными задачами, которого являются: мониторинг происходящих процессов в экстремистской среде, профилактика, выявление, пресечение преступлений экстремистской и террористической, а также координация и взаимодействие с

другими правоохранительными органами по линии противодействия экстремизму и терроризму. Данный орган в рамках своей компетенции осуществляет ряд задач. Таковыми являются:

- выявление, предупреждение, пресечение и раскрытие преступлений экстремистской и террористической направленности;

- выявление и установление лиц, их подготавливающих, совершающих или совершивших;

- проведение оперативно-разыскных, профилактических и иных мероприятий, направленных на защиту законных интересов личности, общества и государства в области противодействия экстремизму и терроризму [4].

Кроме того, этот центр осуществляет плотное взаимодействие с подразделениями УФСБ России по Белгородской области.

Так, например, в 2012 году совместными усилиями сотрудников ЦПЭ УМВД и отдела ЗКС и БТ УФСБ России по Белгородской области было раскрыто дерзкое преступление. Бывшая учительница одной из школ города Белгорода из чувства мести и обиды на директора учебного заведения, из которого была уволена, на листах похищенных ею классных журналов писала сообщения о готовящихся актах терроризма в указанной школе и рассылала своим бывшим ученикам. В ходе проведенных совместных оперативно-разыскных мероприятий преступница была изобличена и привлечена к ответственности.

Таким образом, на данном этапе в России существует вполне действенный механизм информационно-пропагандистской деятельности со стороны органов государственной власти, органов местного самоуправления и общественных организаций, выражающийся в разнообразных мероприятиях (тематические встречи в образовательных организациях, научные форумы, публичные акции антитеррористической направленности и т.д.), в рамках которых осуществляется обмен опытом, информацией, вырабатываются конкретные способы решения проблем по профилактике экстремизма и терроризма, создается информационное поле направленное на обеспечение национальной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Меняйло Л.Н., Меняйло Д.В. Распространение экстремистских материалов в сети Интернет / Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты: сборник научных статей 9-й Международной научно-практической конференции. – Курск, 2019. С. 219-222.

2. Гаврилин Ю.В, Смирнов Л.В. Современный терроризм: сущность, типология, проблемы противодействия. – Москва, 2011.

3. Капранова Ю.В. К вопросу о понятиях «экстремизм» и «терроризм» // Противодействие экстремизму и терроризму: философские, социологические и политологические аспекты: материалы IV Международной научно-практической конференции. – Краснодар, 2017. С. 178–182.

4. Подготовка сотрудников органов внутренних дел к обеспечению личной безопасности: учебное пособие / Ю.Н. Кириченко, П.Н. Войнов, В.Л. Михайликов [и др.]. – Курск, 2018. – 124 с.

5. Гончаров С. Актуальные проблемы борьбы с терроризмом / Мировое сообщество против глобализации преступности и терроризма. – Москва: Международные отношения, 2002. – 94 с.

6. Киреев М.П., Баклицкий К. А. Организация предупреждения терроризма и экстремизма в современной России // Пробелы в российском законодательстве. 2008. № 2. С. 439–441.

7. Кудрявцев В.Н. Предупреждение терроризма // Общественные науки и современность. 2004. № 1. С. 89–95.

8. Михеев В.Л., Пиджаков А.Ю., Чибинёв В.М. Современные формы международного терроризма: (правовая основа противодействия): монография. – Санкт-Петербург: Лема, 2011. – 221 с.

9. Патрушев Н.П. О некоторых особенностях современных вызовов и угроз национальной безопасности Российской Федерации // Российское право. 2007. № 7. С. 18.

10. Седых Н. С. Современный терроризм с точки зрения информационно-психологических угроз // Национальная безопасность / nota bene. 2012. № 2. С. 68–75.

11. Синцов Н.В. СМИ в противодействии терроризму: материалы 3-й международной конференции «Терроризм и электронные СМИ» // Официальный сайт Национального антитеррористического комитета [Электронный ресурс]. – Режим доступа: http://www.nak.fsb.ru

12. Современные проблемы гуманитарного образования и науки: материалы II Международной научно-практической конференции (Владивосток, 12 октября 2012 г.) / под ред. В.Ф. Печерицы. – Владивосток, 2012. – 294 с.

13. Трофимов Д.С. Современное состояние борьбы с преступлениями террористического характера. Аналитический обзор. – Саратов, 2013.

14. Чурилов С.А., Быкадорова А.С. О противодействии распространению и профилактике радикальных идеологий в молодежной среде и сети Интернет // Обзор. НЦПТИ. 2016. № 8.

15. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // Российская газета. 2006. № 4014.

16. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // Собрание законодательства Российской Федерации. 2011. № 7. Ст. 900.

17. Письмо Министерства образования и науки Российской Федерации от 21 марта 2018 г. № 09-406 «О противодействии терроризму» // СПС «КонсультантПлюс».

УДК 371.311

К ВОПРОСУ О БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ

Гатаева А.З.;
Карпика А.Г.,
кандидат технических наук, доцент
(Ростовский юридический институт МВД России)

Аннотация: статья посвящена обзору технологий использования банковских карт как инструмента преступлений. Приведены актуальные данные и сформулированы рекомендации, направленные на обеспечение безопасности при проведении операций с банковской картой.

Ключевые слова: банковская карта, персонализация банковской карты, способы незаконного использования банковских карт, «Ливанская Петля», «карта-клон», «фишинг».

ON THE ISSUE OF SECURITY OF USING BANK CARDS

Gadaeva A.Z.;
Carpiquet A.G.,
Candidate of Technical Sciences, Associate Professor
(Rostov Law Institute of the MIA of Russia)

Abstract: the article is devoted to the review of technologies for using bank cards as a tool of crime. Current data is provided and recommendations are formulated to ensure security during operations with a Bank card.

Keywords: bank card, bank card personalization, methods of illegal use of Bank cards, «lebanese loop», «clone card», «phishing».

Интеграция зарубежных платёжных систем в начале 1990-х годов и возникший на них спрос физических и юридических лиц мотивировали российские банки и торговые сети для внедрения безналичного расчёта не только с организациями, но и отдельными гражданами.

Если в период до 2001 года банковские карты в России существовали за счёт небольшой группы клиентов банков, которым было необходимо их использование, например, для поездок за границу, то после 2009 года появились уже так называемые зарплатные проекты, которые успешно работают и в настоящее время.

Вместе с развитием и применением новых платёжных систем на основе банковских карт возник и новый уровень преступлений в этой сфере, направленных на кражу денежных средств посредством этого инструмента. Подделы-

вание банковских карт и их распространение с последующим использованием, а также мошеннические действия, осуществляемые с применением реквизитов карты, составляют лишь малую часть перечня преступлений, которые совершаются в этой сфере.

Анализ информации, представленной в отчётах центра мониторинга и противодействия компьютерным атакам ФинЦЕРТ (структуры Банка России), показал, что по состоянию на август 2019 года большинство признаков несанкционированных операций (8037) пришлось на банковские карты (см. рис. 1).

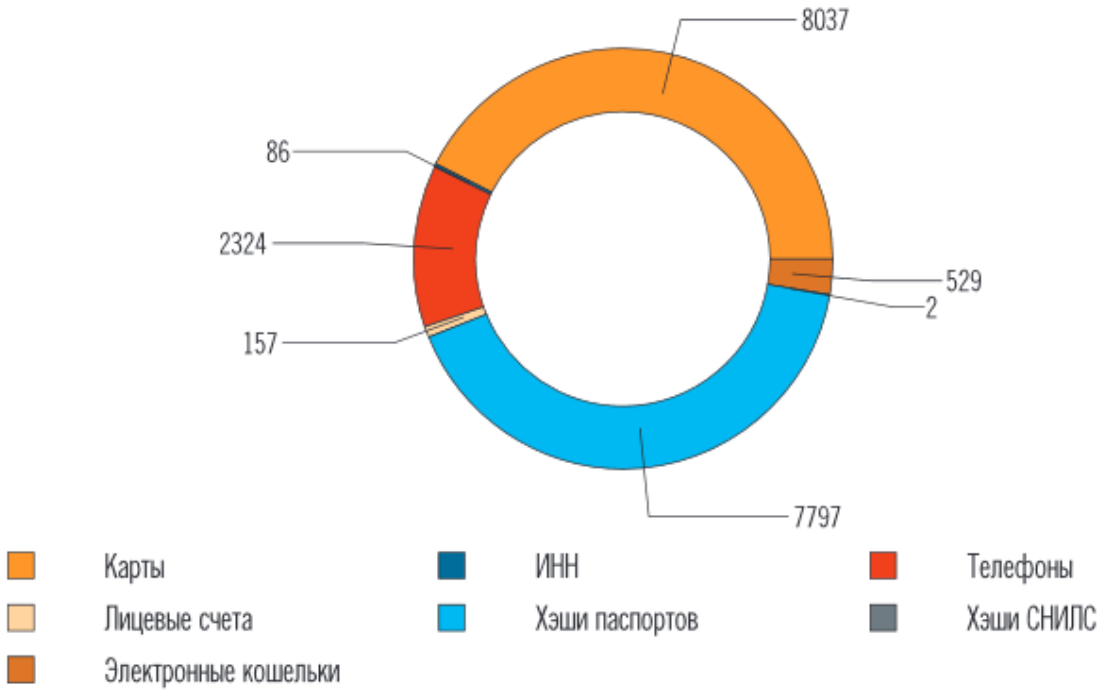


Рисунок 1. Распределение числа сообщений о признаках несанкционированных операций, переданные в ФинЦЕРТ, в период с 31.08.2028 по 31.08.2019

Процесс персонализации банковской карты осуществляется при её выдаче клиенту, так как на карту заносятся данные, с помощью которых возможно идентифицировать как саму карту, так и её «держателя», а также выполнить проверку карты на платежеспособность во время приёма карты к оплате или же при выдаче наличных денег. Также существует понятие «авторизация» – это процесс утверждения продажи/выдачи наличных по банковской карте. Чтобы осуществить авторизацию «точка обслуживания банковских карт» формирует и задаёт запрос платёжной системе о подтверждении полномочий предъявителя банковской карты, а также его финансовых возможностей.

Платежная система, тип карты, технические сопутствующие инструменты, «точки обслуживания карты» влияют на технологический процесс авторизации. Обычно авторизация карты проходит автоматически после помещения ее в терминал для оплаты или же во время прикладывания карты к данному терми-

налу путем считывания данных с карты. Процесс выдачи наличных денег происходит аналогичным с оплатой образом. Разница лишь в том, что денежные средства в автоматическом режиме выдаются банкоматом, который осуществляет авторизацию.

В настоящее время пластиковые карты строятся по принципу «смарт-карт», содержащих чип (интегральную схему). Сам чип встроен непосредственно внутрь карты и имеет видимые металлические контакты для подключения к устройству чтения и последующей аутентификации. Смарт-карты имеют возможность проводить криптографические вычисления. При использовании смарт-карт происходит одно- и двухфакторная аутентификация пользователей, а хранение ключевой информации, а также проведение криптографических операций осуществляется в доверенной среде.

Смарт-карты делятся по способу обмена информации со считывающим устройством на контактные смарт-карты с интерфейсом ISO 7816; контактные смарт-карты с USB-интерфейсом; бесконтактные (RFID) смарт-карты.

Существуют карты, которые включают в себя как контактные, так и бесконтактные интерфейсы.

В настоящее время все кредитные организации предлагают потребителю бесконтактные карты. В банковской сфере это карты с технологией бесконтактной оплаты. Суть данных карт заключается в оснащённости встроенным чипом и антенной, которые передают с помощью радиоканала на бесконтактный терминал информацию о платеже. От простых банковских пластиковых карт такие отличаются возможностью мгновенной оплаты товара при помощи одного касания.

Безусловно, мошенники стремятся получить максимальные знания о технологиях работы с картами и использовать эти знания в преступных целях. В 2017-2019 годах лаборатория «Касперского» выявила компьютерные вирусы, при помощи которых возможна кража денег в банкоматах [1].

Эксперты лаборатории «Касперского» провели исследование, которое показало, что злоумышленники устанавливают в банкоматы компьютерные вирусы для кражи денег. Результаты исследования представлены на рис. 2.

TOP 10 countries by number of unique devices that encountered ATM/PoS malware in 2019

	Country	Devices
1	Russian Federation	2306
2	Iran	1178
3	Brazil	819
4	Vietnam	416
5	India	353
6	Germany	228
7	United States	220
8	Italy	197
9	Turkey	149
10	Mexico	114

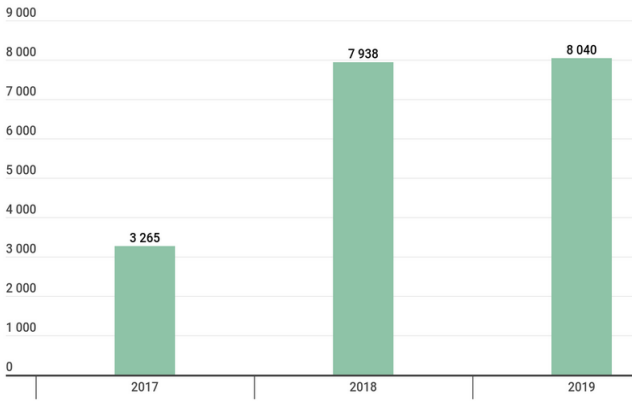


Рисунок 2. Количество зараженных банкоматов в 2019 г.

Помимо внедрения вредоносных программ в устройства работы с банковскими картами злоумышленники активно используют следующие способы:

1. Использование специализированных устройств, устанавливаемых на банкомат с целью получения конфиденциальных сведений доступа к банковской карте путем логирования нажатий кнопок. Способ реализации может предусматривать, например, размещение на клавиатуре банкомата «насадок», которые визуально выглядят и повторяют оригинальные кнопки банкомата. После окончания сеанса владельца карты поддельная клавиатура сохранит последовательность нажатых клавиш, тем самым скомпрометировав конфиденциальные сведения.

2. «Ливанская Петля» – аппаратное устройство, размещаемое в картоприемнике банкомата и выполняющее две задачи: не дать банкомату прочитать параметры карты и воспрепятствовать извлечению ее из банкомата картодержателем. Мошенническая схема состоит в том, что находящийся рядом мошенник предлагает ввести жертве пин-код и нажать кнопки отмены операции. Когда у жертвы ничего не получается и она покидает место преступления, мошенник, обладая достаточной информацией, извлекает «Ливанскую Петлю» вместе с картой, повторно вставляет карту и вводит пин-код жертвы. Результат – хищение денежных средств.

3. Размещение миниатюрных устройств видеосъемки вблизи банкоматов и терминалов оплаты. При этом мошенники, находясь в расположенном вблизи здания автомобиле, видят вводимые держателем карты данные, необходимые для несанкционированного доступа к карте.

4. «Фейковые банкоматы». Размещение «банкоматов», задача которых считать данные банковских карт пользователей.

5. «Клонирование карт». Актуален для карт, не содержащих чипа. Мошенники после получения информации с магнитной полосы карты изготавливают так называемые «белые карты» (кусочки пластика с магнитной полосой, содержащей информацию оригинальной карты).

6. «Фишинг». Получение данных о пластиковой карте от держателя карты. В качестве способа получения используется электронная рассылка на электронные адреса пользователей от имени банка. Содержание письма призвано мотивировать жертву сообщить информацию карты, включая ПИН, или cvc-код, отправив ответное письмо или пройдя на сайт банка-эмитента, заполнив при этом соответствующую анкету. При этом ссылка в письме ведёт не на ресурс банка, а на поддельный сайт, который предназначен для имитации оригинального ресурса.

7. «Социальная инженерия». Реализуется, например, в форме звонка на телефон от лица представителя банка с просьбой погасить задолженность по кредиту. Когда сообщается, что кредит никто не брал, то предлагается уточнить данные пластиковой карты. «Уточнение данных» состоит в получении все тех же конфиденциальных сведений доступа к карте картодержателя.

Перечисленные способы незаконного использования данных карт картодержателей не исчерпывают потенциальные возможности мошенничества в этой области. Вместе с этим, хотелось бы сформулировать некоторые рекомен-

дации, позволяющие снизить возможные риски пользователей банковских карт и способствовать профилактике преступлений в этой области.

Рекомендации:

1. Ответственно относитесь к владению картой. Исключите возможность ее утраты, порчи, копирования данных, несанкционированного, незаконного использования.

2. Запомните, но ни в коем случае не записывайте пин-код карты.

3. Никому не сообщайте пин-код карты, в том числе сотрудникам банков, сотрудникам силовых органов, работникам предприятий.

4. Не передавайте карту другим лицам, в том числе сотрудникам торговых и других организаций.

5. Храните в тайне от других лиц: персональные данные (фамилия и имя) держателя карты, номер и срок действия карты, код проверки подлинности карты CVC 2/ CVV 2, находящийся на оборотной стороне карты на панели для подписи, Ваш ПИН-код, Ваше кодовое слово.

6. Храните в недоступном для других лиц месте копии чеков, билетов и других документов, в которых указаны конфиденциальные данные Вашей карты.

7. Не позволяйте постороннему (в том числе сотруднику банка) выполнять за Вас операции в банкомате, даже если у Вас застряла карточка или возникли проблемы с проведением операции.

8. Не набирайте пин-код на виду у «помощника», не позволяйте себя отвлечь.

9. Если у банкомата за Вами находиться очередь, убедитесь, что никто не может увидеть как Вы вводите пин-код.

10. При вводе пин-кода находитесь как можно ближе к банкомату, вводите код средним пальцем руки, второй рукой закройте клавиатуру.

11. Вводите пин-код только после того, как появится соответствующая запись на экране банкомата.

12. Осуществляйте операции в банкоматах и терминалах, имеющих наклейки с логотипами, соответствующими банковской карте.

13. Старайтесь пользоваться одними и теми же банкоматами, которые Вам хорошо известны.

14. Прежде чем подойти к банкомату, осмотрите окружающее пространство. В случае нахождения поблизости подозрительных людей, воспользуйтесь другим банкоматом.

15. Перед тем как подойти к банкомату, достаньте свою карточку и держите ее в руках. Не открывайте бумажник, кошелёк, сумку, барсетку непосредственно вблизи банкомата или в очереди к нему.

16. Перед использованием банкомата осмотрите его внешний вид. Если Вы обнаружите наличие каких-либо посторонних предметов, проводов, следов конструктивных изменений, воспользуйтесь другим банкоматом.

17. Не применяйте излишнюю физическую силу, чтобы вставить карту в банкомат.

18. Если Вам кажется, что банкомат работает некорректно, отмените осуществление операции, заберите свою карту и воспользуйтесь другим банкоматом.

19. После получения денежных средств, положите наличные денежные средства и банковскую карту в бумажник (кошелек, сумку и т.п.) и только после этого отходите от банкомата.

20. Установите ежедневный лимит снятия наличных денежных средств. Если Вам понадобиться снять сумму, превышающую разрешенную, всегда можно позвонить в банк и изменить лимит.

21. Никогда не отвечайте на телефонные звонки, даже если к Вам обратились по имени, фамилии и отчеству. Перезвоните сами.

Таким образом, понимание угроз, связанных с использованием банковских карт, несомненно, позволит сотрудникам полиции оперативно реагировать на потенциальные угрозы в этой области.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Обзор APT-угроз: тенденции киберпреступности в 2019 году» [Электронный ресурс]. – Режим доступа: https://securelist.ru/story-of-the-year-2019-cities-under-ransomware-siege/95280/ (дата обращения: 24.04.2020).

УДК 004

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ КАК ИНСТРУМЕНТ СОВЕРШЕНИЯ И РАСКРЫТИЯ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ

Орлов А.В.,
кандидат экономических наук, доцент;
Лагунова Е.С.
(Московский университет МВД России им. В.Я. Кикотя)

Аннотация: в данной статье рассмотрены сущность и основная классификация киберпреступлений в сфере экономики, а также место и роль кибертехнологий в противодействии экономическим преступлениям. В статье сделан вывод, что на сегодняшний день целесообразно создание принципиально новой системы криминалистического учета и идентификации на основе электронно-цифрового следа различных технических средств коммуникации (смартфонов, компьютеров или планшетов). Совпадение электронно-цифрового следа с высокой точностью позволит установить личность преступника.

Ключевые слова: киберпреступность, информатизация, кибертехнологии, экономические преступления, экономическая безопасность.

INFORMATION TECHNOLOGIES AS A TOOL FOR COMMITTING AND SOLVING ECONOMIC CRIMES

Orlov A.V.,
Candidate of Economical Sciences, Associate Professor;
Lagunova E.S.
(Kikot Moscow University of the MIA of Russia)

Abstract: this article discusses the nature and main classification of cybercrime in the field of economics, as well as the place and role of cyber technologies in countering economic crimes. The article concludes that today it is advisable to create a fundamentally new system of forensic accounting and identification based on an electronic digital trace of various technical means of communication (smartphones, computers or tablets). The coincidence of the electronic-digital footprint with high accuracy will establish the identity of the offender.

Keywords: cybercrime, informatization, cyber technology, economic crime, economic security.

Благодаря развитию процесса информатизации и компьютеризации в различных сферах всё чаще наблюдается использование так называемых кибертехнологий. Без сомнения, технологии на сегодняшний день являются неотъемлемыми атрибутами нашей жизни. Субъекты экономических отношений на уровне частных физических и юридических лиц активно используют последние разработки в области кибертехнологий в целях извлечения сверхприбылей, зачастую нарушая при этом закон. Именно поэтому на сегодняшний день становится особенно актуальна проблема киберспреступности.

Киберпреступления – это преступления, совершаемые в сфере информационных технологий в киберпространстве. Киберпространство отображает виртуальное пространство, в котором хранятся, обрабатываются и перемещаются электронные данные субъёктов отношений (в том числе и экономических) посредством компьютерных систем или компьютерных сетей.

По статистическим данным Генпрокуратуры России, за январь – ноябрь 2019 года правоохранительные органы зарегистрировали 261 тыс. киберпреступлений, совершенных с применением информационно телекоммуникационных технологий, что на 69,7% больше, чем за аналогичный период прошлого года, и является седьмой частью от общего количества возбужденных за данный период уголовных дел. Прирост по сравнению с 2018 г. достигает 67,1%. Предварительно расследовано менее 60 тыс. Речь идет о правонарушениях, которые совершаются с помощью Интернета, мобильной связи и с использованием банковских карт. Особую озабоченность вызывает то, что раскрываемость киберпреступлений снижается: с 36% в 2016 году до 23% в 2019 г. И это происходит в условиях, когда каждый пятый пострадавший от кибермошенничества даже

не заявляет о произошедшем в полицию в связи с тем, что ущерб незначителен и составляет менее 5 тыс. рублей.

По прогнозам специалистов компании кибербезопасности «Интернет-розыск», к 2023 году удельная доля киберпреступлений может увеличится с 14 до 30% [5]. Этот факт увязывают с достаточно низкой раскрываемостью и слабыми возможностями по идентификации онлайн-мошенников. Современные мошенники применяют технологии, позволяющие скрыть свои реальные данные (VPS/VPN-сервисы для анонимизации интернет-трафика, виртуальные номера сотовых телефонов и адреса электронной почты, неидентифицируемые электронные и криптовалютные кошельки).

Наряду с общим ростом количества киберпреступлений в январе-ноябре 2019 г. преступлений экономической направленности, совершённых в киберпространстве по сравнению с аналогичным периодом 2018 года и выявленных правоохранительными органами, стало меньше на 4,7%. Всего было выявлено 97,1 тыс. преступлений данной категории. Материальный ущерб от указанных преступлений составил 383,3 млрд руб.

Так, в России резко уменьшилось количество киберпреступлений против банков и их клиентов. По результатам анализа компании Group-IB за второе полугодие 2018 г. и первое полугодие 2019 г. их объем составил 510 млн руб., что на 85% меньше, чем за предыдущий год, когда таких преступлений было совершено на 3,2 млрд руб. Финансовые убытки от хакерских атак на российские банки уменьшились в 14 раз до 93 млн руб. Средняя сумма убытков в результате таких целевых атак на банки в России сократилась со 118 до 31 млн руб. Лидерами в сегменте киберпреступлений против банков считаются русскоязычные кибергруппировки Cobalt, Silence и MoneyTaker, а также северокорейская Lazarus и новая группа SilentCards.

Если отдельно говорить о хищениях, произведенных с помощью вирусов для ПК, в этом сегменте объем ущерба уменьшился на 89% до 62 млн руб. Такие преступления традиционно характерны для России. По данным МВД России, хищениями с помощью троянов для ПК в России сейчас активно занимаются две группировки – Buhtrap2 и RTM.

Количество мошеннических схем хищений с помощью троянов для Android продемонстрировало годовой спад на 43% до 110 млн руб. Однако средний размер таких хищений вырос с 7 тыс. до 11 тыс. руб., поскольку мошенники в большинстве своём стали использовать вместо SMS-рассылок кражу средств с использованием переводов card – to – card.

Объем преступлений в сфере кражи данных банковских карт вырос на 33% и до 56 млрд. руб. Количество карт, данные о которых утекли в Интернет, увеличилось на 38% – с 27,1 до 43,8 млн [4]

Ещё одной из наиболее актуальных проблем является хищение денежных средств со счетов организаций и отдельных граждан. Даже в Центробанке по фальшивым платежным документам мошенникам удалось снять со счета, принадлежащего Пенсионному фонду России, 1,25 млрд руб. Заместитель главы МВД России отметил, что по наглости исполнения это преступление может претендовать на «кражу века». И хотя сообщалось, что деньги удалось вернуть,

а возможность совершения этого мошенничества Центробанк объяснил нарушением некоторыми сотрудниками, которые впоследствии были уволены, внутреннего регламента, необходимо признать недостаточность усилий ЦБ России по предотвращению фактов подобного рода.

В целом, необходимо отметить, что количество преступлений в экономической сфере, совершенных с использованием компьютерных и телекоммуникационных технологий, безусловно, влияет на уровень экономической безопасности государства. За 2018 год подразделениями органами внутренних дел было выявлено 8,842 таких преступлений (см. табл. 1), и с каждым годом доля таких преступлений в общем объёме совершённых преступлений только возрастает.

Таблица 1.

Преступления экономической направленности

	Выявлено преступлений (в отчетном периоде)		В том числе			
			сотрудниками ОВД			
	всего	+,- в %	Всего	+,- в %	Всего	+,- в %
ВСЕГО	88341	-5,0	75774	-5,6	26496	1,3
в том числе предварительное следствие по которым обязательно	78819	-5,3	68461	-5,6	24708	1,1
из них:						
коррупционной направленности	20224	4,6	16206	5,9	6282	9,4
совершенных с использованием компьютерных и телекоммуникационных технологий	8842	-16,3	8343	-18,3	1268	-4,7
в сфере экономической деятельности	30579	2,1	27899	1,3	5381	-0,5
в том числе незаконное предпринимательство	272	-18,8	229	-13,6	268	-19,0
изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг	14153	-3,8	14125	-3,5	9	-10,0
производство, приобретение, хранение, перевозка или сбыт товаров и продукции без маркировки и (или) нанесения информации, предусмотренной законодательством Российской Федерации	55	22,2	52	26,8	54	25,6

легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления либо приобретенных другими лицами преступным путем	764	-7,2	685	-9,6	347	1,8

* Количество преступлений, по уголовным делам и материалам о которых не принято решение на начало года или зарегистрированных в отчетном периоде.

Особое место кибертехнологии занимают в проведении оперативно-разыскной деятельности в сфере раскрытия экономических преступлений. Для наиболее эффективной работы оперативным подразделениям и сотрудникам органов внутренних дел необходимо активно и грамотно использовать компьютерную технику, информационно-коммуникационные технологии и ресурсы глобальной сети Интернет.

Следует иметь в виду, что полученная экономическая информация должна быть криминалистически значимой, т.е. содержать сведения о лицах, причастных к подготовке, совершению и сокрытию экономического преступления, или субъектах, знающих что-либо об этом [3]. Именно на основе такой информации дознавателем и следователем выдвигаются следственные версии, устанавливается местонахождение имущества, денежных средств, добытых преступным путем, и принимаются эффективные меры к возмещению ущерба.

На сегодняшний день существующая система информационно-аналитического обеспечения выявления экономических преступлений состоит из двух блоков: информационные ресурсы органов внутренних дел (внутренние), информационные ресурсы иных ведомств и иные информационные ресурсы (внешние).

Необходимо понимать, что, несмотря на достаточно широкий перечень информационных регистров, позволяющих оперативному сотруднику получать интересующую его информацию, Интернет приобретает всё большую значимость. Российский опыт деятельности подразделений органов внутренних дел свидетельствует о тесной взаимосвязи между уровнем информационного обеспечения сотрудников органов внутренних дел и результатами их работы.

В условиях сложной криминальной обстановки в России совершенствование информационного обеспечения подразделений органов внутренних дел России становится одним из главных направлений повышения эффективности правоохранительной деятельности. Актуализирует данную задачу и то, что в условиях, когда использование баз данных для раскрытия интернет-преступлений «Палантир», «Осирис», «Шерлок», «Псков» и других представляется уже недостаточно эффективным, по нашему мнению, требуется создание принципиально новой системы криминалистического учета и идентификации на основе электронно-цифрового следа различных гаджетов. Совпадение электронно-цифрового следа – набора параметров, определяющих конкретный

смартфон, компьютер или планшет с высокой точностью при совершении преступления, будет фактически равно установлению личности преступника [6].

К сожалению, в настоящее время Российскую Федерацию по масштабам киберпреступности и влиянию на мировую экономику включают в первую десятку стран. Российская киберпреступность, исходя из статистических данных, наносит ущерб национальной экономике в объёме около 0,25% от ВВП, что, например, составляет порядка 50% расходов на здравоохранение. Рост числа киберугроз, несомненно, негативно сказывается на развитии экономики России, и задачей сегодняшнего дня является исправление данной ситуации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Козин М.Н. Технологическая модернизация как драйвер развития Российской Федерации // Известия Саратовского университета. Серия: экономика. управление. право». 2012. С. 23–28.
2. Орлов А.В., Орлова О.В. Информатизация экономики в аспекте усиливающейся глобализации / Экономические, правовые и культурные аспекты реализации стратегии пространственного развития России и укрепления (раскрытия) ее человеческого потенциала: сборник публикаций по итогам международной научно-практической конференции. – Москва: Спутник+, 2018. С. 36–41.
3. Михеева М.В. Актуальные проблемы цифровизации российской экономики / Обеспечение экономической безопасности России в современных условиях: сборник статей. – Москва: Московский университет МВД Российской Федерации им. В.Я. Кикотя, 2019. С. 362–372.
4. В России на 85% снизилась киберпреступность против банков [Электронный ресурс]. – Режим доступа: https://zoom.cnews.ru/soft/news/top/2019-11-29_v_rossii_na_85_upala_kiberprestupnost (дата обращения: 15.01.2020).
5. Обзор событий в национальной платежной системе [Электронный ресурс]. – Режим доступа: http://npc.ru/ru/media/pay_news/?id=4997 (дата обращения: 15.01.2020).
6. Сидоренко Е. По цифровым следам: в РФ раскрывается лишь четверть киберпреступлений [Электронный ресурс]. – Режим доступа: https://iz.ru/962966/elena-sidorenko/po-tcifrovym-sledam-v-rf-raskryvaetsia-lish-chetvert-kiberprestuplenii (дата обращения: 15.01.2020).

УДК 37

ИСПОЛЬЗОВАНИЕ ОНЛАЙН-СЕРВИСОВ В СИСТЕМЕ СОВРЕМЕННОГО ОБРАЗОВАНИЯ

Беляева И.Н.,
кандидат физико-математических наук, доцент;
Зернова А.С.
(Белгородский государственный национальный исследовательский университет)

Аннотация: в статье рассматриваются онлайн-сервисы в системе современного образования на примере сервиса WikiWall. В ней затронут вопрос применения сервиса, раскрыты возможности и достоинства сервиса, а также рассмотрен интерфейс и даны рекомендации по использованию. Кроме того, статья даёт представление о современном стандарте образования и изменениях, происходящих в системе образования.

Ключевые слова: онлайн-сервисы, сервис WikiWall, образование, современный стандарт образования, информационно-коммуникационные технологии.

ONLINE SERVICES IN MODERN EDUCATION

Belyaeva I.N.,
Candidate of Physical and Mathematical Sciences, Associate Professor
Zernova A.S.
(Belgorod National Research University)

Abstract: this article considers with the online services in the system of modern education, on an example WikiWall. It addresses the use of the service, reveals the capabilities and advantages of the service, as well as discusses the interface and provides recommendations for use. In addition, the article gives an idea of the modern standard of education and the changes taking place in the education system.

Keywords: online services, WikiWall service, education, modern standard of education, information and communication technologies.

В настоящее время система образования претерпевает огромные изменения. Это связано с информационным развитием общества. Изменились цели, задачи, средства обучения. В рамках современной системы образования обучающиеся должны научиться самостоятельно добывать, анализировать и правильно применять полученную ими информацию. А педагог при этом должен играть роль ментора, наставника и лишь направлять. Современный стандарт ставит задачей развитие творческого потенциала учащихся и умения нестандартно мыслить.

В связи с этим появилась необходимость создания новых образовательных технологий, дающих учащимся возможность самостоятельной деятельности, но при этом ещё отвечающих критериям современного общества [1; 2].

На данный момент многие образовательные организации уже практикуют системы дистанционного, интерактивного обучения, замену текстовых носителей на электронные, использование интернет-сервисов. Наиболее известными онлайн-сервисами являются: Twiddla (многофункциональная и удобная онлайн-доска), WikiWall (онлайн сервис для совместного создания газеты несколькими пользователями), Symbaloo (сервис для создания визуальной коллекции закладок, представляющей собой набор плиток), WebRoom (бесплатный сервис для проведения онлайн-встреч, не требующий регистрации).

В данной статье мы более подробно рассмотрим один из этих сервисов.

Сервис WikiWall – и это один из инновационных онлайн-сервисов, который является частью нового стандарта образования и отвечает его критериям. WikiWall (Вики-стена) первый российский сервис whiteboard. Whiteboard-сервисы (по-другому, виртуальные доски) – это современная альтернатива привычному рабочему пространству. Он даёт возможность одновременно нескольким людям создать проект в режиме онлайн, представить материал в более наглядной форме, при этом затратить меньше ресурсов и времени. Сервис WikiWall может быть использован учащимися для создания тематической газеты или коллективного творческого проекта, классными руководителями в виде памяток, педагогами при объяснении нового материала или может быть размещён дирекцией на сайте учебных заведений для привлечения внимания к какому-нибудь событию.

Можно выделить следующие достоинства данного сервиса:

– простой, понятный интерфейс, подходящий для любой возрастной группы;

– наличие всплывающих подсказок для элементов интерфейса;

– отсутствие обязательной регистрации;

– параллельная работа: группа людей, находящихся даже в разных городах может одновременно вносить изменения в работу;

– наличие чата для общения пользователей между собой;

– возможность создавать рисунки, пометки, добавлять надписи, различные объекты, видео.

Начиная работу с сервисом, необходимо определить цель Вашей работы: хотите ли Вы создать тематическую стенгазету, памятку, презентацию результатов творческого проекта, интерактивный конспект урока или что-то другое. Затем составить примерный план работы, распределить обязанности, ответственных за определённый вид работ. А после этого можно ввести в адресную строку ссылку http://wikiwall.ru/, перейти на сайт, на главной странице сайта нажать кнопку, например, создать стенгазету и начать творить [3].

Работа с сервисом не требует регистрации. Но при желании можно указать своё имя и загрузить фото или картинку на аватар, чтобы другие пользователи имели возможность видеть, кто вносит изменения. Вверху страницы, как показано на рисунке 1, расположена панель инструментов. Первая иконка слева

создаёт новую стенгазету, следующие – блок текст, картинка, видео – создают поля. Каждое поле получает свою нумерацию по порядку создания. Есть возможность менять размер полей, перемещать их, удалять (для этого есть крестик в правом углу каждого поля) и менять цвет (только для текстового).

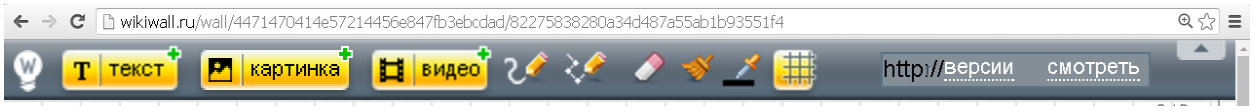


Рисунок 1. Панель инструментов Wikiwall

Далее идёт ряд инструментов для рисования: линия, линия по точкам, ластик, очистить всё, цвет линии и сетка (по умолчанию область рисования размечена, можно убрать её нажатием). Для текстого поля при его создании появляется дополнительная панель. С её помощью можно изменять шрифт и цвет текста, а также на ней указывается номер поля, с которым работает пользователь. В правом верхнем углу расположены кнопки «версии» и «смотреть». В версиях можно изменить название и выбрать версию из уже созданных. А кнопка «смотреть» позволит открыть страницу в режиме просмотра, но при этом редактирование будет недоступно.

Применение сервиса безгранично. Новый стандарт образования требует новых форм и методов объяснения, закрепления и контроля полученных знаний [4]. И сервис WikiWall может в этом помочь как преподавателю, так и обучающимся. Заинтересовать обучающихся – главная цель педагога. Преподаватель может создать с помощью этого сервиса газету, в которой наглядным способом будет отображён весь материал в сжатом виде с использованием опорных схем, картинок. Тем самым новая форма работы заинтересует обучающихся, и представленный таким способом материал станет более понятным. Также при помощи сервиса педагог может осуществлять закрепление знаний в виде домашнего задания (создать стенгазету на заданную тему, отразить в ней основные понятия). Кроме того, Wikiwall можно использовать на внеурочных занятиях или на тематических классных часах. Например, создать презентацию учебных достижений, памятку (правил поведения в компьютерных классах, во время зимних каникул или др.) или для творческих отчётов о проведённом мероприятии (конкурсе, экскурсии, празднике).

Обучающиеся, в свою очередь, могут использовать сервис для представления результатов совместных творческих проектов, создания газет (плакатов), как опору и иллюстрацию слов при ответе на любом предмете.

В заключение отметим, что онлайн-сервисы открывают огромные возможности для педагогов и учащихся и содержат в себе множество достоинств, однако они не должны полностью заменить существующую традиционную систему образования. Онлайн-сервисы можно использовать на занятиях в качестве вспомогательных элементов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Диков А.В. Классные интернет-доски для совместной работы // Известия ПГПУ им. В.Г. Белинского. 2011. № 26. С. 452–462.

2. Михайлов С.Н. Возможности реализации образовательных технологий с помощью интерактивной виртуальной доски // Известия ПГПУ им. В.Г. Белинского. 2015. № 178. С. 124–129.

3. Wikiwall.ru/ [Электронный ресурс]. – Режим доступа: http://wikiwall.ru/ (дата обращения: 29.04.2020).

4. Устинова О.В., Беляева И.Н. Оценка качества электронных образовательных ресурсов // Наука и образование: отечественный и зарубежный опыт: международная научно-практическая конференция (21 декабря 2018 г. Белгород): сборник статей. – Белгород: ГиК, 2018. С. 73–77.

УДК 004:34:374

О НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ[1]

Колесникова Е.А.,
кандидат технических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: в статье обсуждаются некоторые аспекты проблемы противодействия преступности во взаимодействии со средствами массовой информации, связанные с самообразованием, просвещением (посредством зарегистрированного средства массовой информации), источниками информации и предполагающие участие сотрудников органов внутренних дел, педагогических работников, научных работников.

Ключевые слова: компьютерная преступность, внутренняя безопасность, самообразование, рецензирование, проверка источников информации.

[1] Благодарю сотрудников кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Бел ЮИ МВД России имени И.Д. Путилина за участие в обсуждении идеи.

ON THE NEED TO USE THE CAPABILITIES OF THE MASS MEDIA AND ON MEASURES TO IMPROVE THE EFFECTIVENESS OF COUNTERING CRIME

Kolesnikova E.A.,
Candidate of Technical Sciences
(Putilin Belgorod Law Institute of the MIA of Russia)

Abstract: the paper deals with the aspects of the problem concerned with resistance of crime in interaction with the mass media, related to self-education, education (through a registered mass media), sources of information and involving the participation of employees of internal affairs bodies, teachers, researchers.

Keywords: computer crime, internal security, self-education, review, verification of information sources.

Продолжая детальное изучение взаимодействия [1; 2; 3] со средствами массовой информации (далее – СМИ), предполагая возможность повышения его эффективности в свете событий, требующих быстрого принятия решений, становления новой формы социального взаимодействия, отдавая приоритет использованию информационных технологий, возникает вопрос о необходимости расширения использования органами внутренних дел СМИ для правового просвещения граждан Российской Федерации и других лиц о правомерной защите от преступных и иных противоправных посягательств, вопрос об употребляемых понятиях, терминах, определениях. Примером может служить репортаж, подготовленный М. Акинченко, М. Семиным, Л. Зориной, К. Даниловым, в выпуске телепрограммы «Время» от 14.05.2020 на телеканале «Первый канал» (URL: https://www.1tv.ru/n/385859) с информацией о детских пособиях, появившихся «сайтах-ловушках», предложением использовать веб-сервис (Whois.com: [сайт]. URL: https://www.whois.com; Официальный WHOIS сервис. Информация о домене или IP [сайт]. URL: https://whois.ru).

При дистанцировании и, как следствие, самостоятельном поиске и изучении документов важно акцентировать внимание на понятиях, например, «домен», «доменное имя», «унифицированный идентификатор ресурса», «унифицированный указатель ресурса», указав на приоритет использования официальных изданий.

Следует отметить актуальность материалов, при этом подвергнув критике **(не добавляя** цензуру массовой информации) неполноту предлагаемого метода проверки веб-сайта, унифицированного указателя ресурса, доменного имени, описанные на примере федеральной государственной информационной системы (далее – ФГИС) «Единый портал государственных и муниципальных услуг (функций)», а именно:

1) описанная в репортаже ситуация предполагает использование источников информации с доменными именами, составляющими российскую национальную доменную зону[1];

2) следует опираться на официально опубликованные[2] акты, www.gosuslugi.ru[3];

3) следует упомянуть ФГИС координации информатизации, которая обеспечивает формирование единого информационного пространства.

При ограничении в использовании печатных СМИ, учредителем которых является государственный орган, для первичной проверки на фальсификацию начинающим пользователям можно использовать ФГИС «Официальный интернет-портал правовой информации»[4], совокупность систем, зарегистрированных в едином реестре российских программ для электронных вычислительных машин и баз данных[5]: Справочная правовая система (СПС) «КонсультантПлюс», Электронный периодический справочник «Система ГАРАНТ» или другие.

При ознакомлении граждан с телепередачей, в процессе познания, при получении образования в форме самообразования вне организаций, осуществляющих образовательную деятельность, уделяется ли внимание приоритету источников информации?

Ориентируясь на аудиторию СМИ, наряду с использованием сокращений, аббревиатур, коротких фраз, необходимо употреблять полные наименования, например, SMS-сообщение (Толковый словарь Ефремовой. Т. Ф. Ефремова. 2000) или короткое текстовое сообщение, мультимедийное сообщение, сообщение электросвязи (ГОСТ Р 53801-2010. Связь федеральная. Термины и опреде-

---

[1] Приказ Роскомнадзора от 29 июля 2019 г. № 216 «Об определении перечня групп доменных имен, составляющих российскую национальную доменную зону»: зарегистрирован Минюстом России 20 августа 2019 г. // Официальный интернет-портал правовой информации. Дата опубликования: 21.08.2019. – URL: http://publication.pravo.gov.ru/Document/View/0001201908210010 (дата обращения: 06.05.2020).

[2] Указ Президента Российской Федерации от 23 мая 1996 г. № 763 «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти» // Российская газета. 1996. 28 мая.

[3] Приказ Минкомсвязи России от 21 марта 2011 г. № 39 «Об утверждении Административного регламента предоставления Федеральным агентством по печати и массовым коммуникациям государственной услуги "Выдача справок, подтверждающих право на получение льгот, предусмотренных законодательством Российской Федерации для периодических печатных изданий, книжной продукции и полиграфических материалов"»: зарегистрирован Минюстом России 24 мая 2011 г. // Бюллетень нормативных актов федеральных органов исполнительной власти. 2011. № 26.

[4] Федеральный закон от 14 июня 1994 г. № 5-ФЗ «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания»: принят Гос. Думой Федер. Собр. Рос. Федерации 25 мая 1994 г.; одобрен Советом Федерации Федер. Собр. Рос. Федерации 1 июня 1994 г. // Собрание законодательства Российской Федерации. 1994. № 8. Ст. 801.

[5] Единый реестр российских программ для электронных вычислительных машин и баз данных: [Электронный ресурс]. – URL: https://reestr.minsvyaz.ru/ (дата обращения: 06.05.2020).

ления. М., 2011. IV, 26 с.). Сотрудниками органов внутренних дел Российской Федерации через отделы информации и общественных связей МВД России это выполняется с пониманием важности тренировки. Следует заметить, что после получения гражданином Российской Федерации подтвержденной учётной записи вероятность ошибки с доменным именем уменьшается, вероятность ошибки, недоверия может быть высокой в связи с появляющимися сложностями при регистрации учётной записи, возможно с подтверждением учётной записи.

Получение образования гражданами, снижая негативное воздействие на общество, устраняя правовые и социальные дестабилизаторы безопасности, повышая благосостояние, способствует противодействию преступности.

Примеры, приведенные в репортаже, побуждают осветить вопросы развития, качественного наполнения социокультурной среды [3], обратившись к официальным, справочным, информационным изданиям, далее – к научным, научно-популярным, производственно-практическим, нормативно-производственным изданиям, обсудить проблемы организации: методологии, анализа, синтеза, классификации и таксономии, систематизации в целом.

Взаимодействие СМИ и органов внутренних дел может быть более действенным при освещении событий, просвещении, в ходе профилактических мероприятий, в том числе разъяснении гражданам вопросов защиты от преступных и иных противоправных посягательств, при условии очного или заочного консультирования, участия сотрудников в рецензировании материалов или при условии добавления цитат и ссылок на прошедшие рецензирование материалы, ссылок на официальные издания.

В заключение предлагается помимо использования материалов, представленных на сайте МВД России, например, в разделах: «Правовое информирование» или «Ведомственные СМИ», в СМИ, освещающих деятельность органов внутренних дел, размещающих другие материалы в сфере внутренних дел;

1) проверять источники информации во взаимодействии с органами внутренних дел, образовательными организациями, научными организациями;

2) рассмотреть вопрос об активном содействии в области «Средства массовой информации, издательства и полиграфия», участии в работе работников редакции зарегистрированного СМИ сотрудников органов внутренних дел с целью консультирования, вероятного участия в рецензировании неопубликованных материалов о противодействии преступности, о внутренней безопасности;

3) соблюдая полноту, достоверность актуальной информации, способствовать её распространению, акцентируя внимание на официальные издания, пролегомены для последующего краткого, наглядного изложения корреспондентами СМИ[1], специалистами по производству продукции телерадиовеща-

[1] Профессиональный стандарт «Корреспондент средств массовой информации»: утв. приказом Минтруда России от 21 мая 2014 г. № 339н; зарегистрирован Минюстом России 26 мая 2017 г. // Официальный интернет-портал правовой информации. Дата опубликования: 27.05.2017. – URL: http://publication.pravo.gov.ru/Document/View/0001201705260046 (дата обращения: 06.05.2020).

тельных СМИ[1], редакторами СМИ[2], например, участвовать в заседаниях (совещаниях), которые могут проводиться в очной или заочной форме с использованием информационно-коммуникационных технологий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Акапьев В.Л., Дрога А.А., Савотченко С.Е. Профилактическая деятельность органов внутренних дел во взаимодействии со средствами массовой информации // Вестник Воронежского института МВД России. 2018. № 2. С. 146–152.

2. Жукова П.Н., Прокопенко А.Н. Использование социальных сетей в противоправных целях на современном этапе / Белгородские криминалистические чтения: сборник научных трудов. – Белгород: Белгородский юридический институт МВД России им. И.Д. Путилина, 2017. С. 71–81.

3. Тюменцев А.Н. Об особенностях взаимодействия современной российской полиции с населением и средствами массовой информации // Вестник Волгоградской академии МВД России. 2014. № 3 (30). С. 143–150.

[1] Профессиональный стандарт «Специалист по производству продукции телерадиовещательных средств массовой информации»: утв. приказом Минтруда России от 28.10.2014 № 811н; зарегистрирован Минюстом России 15 декабря 2017 г. // Официальный интернет-портал правовой информации. Дата опубликования: 18.12.2017. – URL: http://publication.pravo.gov.ru/Document/View/0001201712180042 (дата обращения: 06.05.2020).

[2] Профессиональный стандарт «Редактор средств массовой информации»: утв. приказом Минтруда России от 4 августа 2014 г. № 538н; зарегистрирован Минюстом России 28 августа 2019 г. // Официальный интернет-портал правовой информации. Дата опубликования: 28.08.2019. – URL: http://publication.pravo.gov.ru/Document/View/0001201908280031 (дата обращения: 06.05.2020).

УДК 662.2

К ВОПРОСУ О МЕТОДАХ СКРИНИНГА ДЛЯ ОБНАРУЖЕНИЯ ВЗРЫВЧАТЫХ ВЕЩЕСТВ

Старостенко И.Н.,
кандидат физико-математических наук, доцент;
Логачева Е.Ю.,
кандидат химических наук
(Краснодарский университет МВД России)

Аннотация: в статье рассматриваются методы и средства выявления наличия взрывных веществ в рамках технологии скрининга. Скрининг-технологии включают использование химических тест-методов или тонкослойной хроматографии и облегчают мониторинг потенциально опасных объектов при возникновении угрозы совершения взрыва.

Ключевые слова: взрывчатые вещества, взрывные устройства, скрининг, терроризм, хроматография, экстремизм.

TO THE QUESTION OF SCREENING METHODS FOR DETECTION OF EXPLOSIVES

Starostenko I.N.,
Candidate of Physical and Mathematical Sciences, Associate Professor;
Logacheva E.Y.,
Candidate of Chemical Sciences
(Krasnodar University of the MIA of Russia)

Abstract: in article discusses methods and means of detecting the presence of explosives in the framework of screening technology. Screening technologies include the use of chemical test methods or thin layer chromatography and facilitate the monitoring of potentially dangerous objects in the event of an explosion hazard.

Keywords: explosives, explosive devices, screening, terrorism, chromatography, extremism.

Борьба с терроризмом и экстремизмом является важной проблемой, остро стоящей перед правоохранительными органами, следственными и судебно-экспертными подразделениями. Анализ статистических данных свидетельствует о постоянном присутствии террористической угрозы. Так, например, на территории Российской Федерации в 2016 году зарегистрировано 2227 преступлений террористического характера, что на 45% выше по сравнению с 2015 годом. В январе-сентябре 2018 года, по официальным данным МВД России, ко-

личество правонарушений, связанных с терроризмом, составило 1341 преступление [1]. Несмотря на тенденцию снижения в динамике террористической активности, предупреждение преступлений террористического характера представляет собой одно из актуальных направлений деятельности подразделений органов внутренних дел, обеспечивающих национальную безопасность. Террористические акты чаще всего совершаются посредством использования взрывчатых веществ (ВВ) и взрывных устройств (ВУ) на их основе в местах значительного скопления людей. К широко распространенным ВВ относятся, например, тротил, гексоген, тетрил, октоген. Данный круг веществ по своей химической природе является органическими ароматическими нитросоединениями. Решение задачи предотвращения террористических актов достигается за счет оперативного выявления наличия ВВ у лиц, готовящихся провести террористический акт, либо своевременного обнаружения опасных веществ в местах готовящихся взрывов.

Для оптимизации оперативно-разыскных мероприятий при борьбе с терроризмом необходимо выполнение комплекса мер, одной из которых является оснащение соответствующих подразделений МВД России современными техническими средствами, с помощью которых в короткие сроки можно обнаружить ВВ и ВУ. Перспективным направлением в решении этой проблемы является развитие методов и средств выявления наличия ВВ в рамках технологии скрининга. В основе методологии скрининга лежат простые методики идентификации веществ, не требующие дорогостоящего оборудования и доступные в использовании для всех сотрудников вне зависимости от их квалификации. Особенность скрининг-технологии заключается в том, чтобы за минимальное время с достаточно высокой чувствительностью выявить из большого круга проб несколько проб, дающих положительную реакцию на искомые вещества, чтобы затем целенаправленно выбрать более сложную и достоверную схему химического анализа для установления их точной структуры. Методология скрининга основана на методах идентификации веществ, допускающих неправильные положительные результаты на присутствие анализируемого компонента и полностью исключающих неправильные отрицательные результаты. Пробы, дающие положительную реакцию, далее изучают с помощью более сложного информативного метода. Скрининг-технологии имеют важное значение для обнаружения взрывчатых веществ вне лаборатории, то есть непосредственно на месте предполагаемого происшествия (так называемые полевые условия). Для обнаружения ВВ в соответствии с технологией скрининга большой интерес представляют химические тест-методы анализа, метод тонкослойной хроматографии, газохроматографический анализ на базе портативных газовых хроматографов.

Под химическими тест-методами понимают простые и дешевые приемы и средства обнаружения веществ с использованием соответствующих простых методик химического анализа, не требующих существенной пробоподготовки и использования сложного лабораторного оборудования, а также подготовленного персонала. Химические тест-методы основаны на индикаторных реакциях взаимодействия искомых веществ с подходящим реагентом с образованием

продуктов реакции, окрашенных в характерный цвет для данного вещества. ВВ способны вступать в реакции с широким кругом реагентов, образуя окрашенные соединения, на твердой поверхности, например, фильтровальной бумаге или ткани. Идентификационным признаком вещества является появляющаяся окраска, которую сравнивают со стандартной шкалой. Изучение условий индикаторных поверхностных реакций ВВ с различными реагентами для наблюдения визуального эффекта легло в основу разработки технических средств экспресс-обнаружения ВВ. Для выявления следовых количеств ВВ, остающихся на различных предметах, руках, одежде лиц, причастных к транспортировке взрывчатки, пробоотбор осуществляется непосредственно на поверхность, на которой далее проводится индикаторная реакция, например, марлевый тампон. Преимуществами химических тест-систем анализа с точки зрения внедрения в практическую деятельность органов внутренних дел являются доступность и простота оборудования, экспрессность, возможность визуальной идентификации, простота интерпретации получаемых данных.

Экспресс-тесты для скрининга взрывчатых веществ, как правило, изготавливают в виде капельниц и аэрозольных баллончиков, содержащих реагенты-идентификаторы ВВ. В качестве пробоотборников используется фильтровальная бумага, тканные и нетканые материалы с липким слоем. Идентификация ВВ осуществляется путем последовательного нанесения реагентов-проявителей на исследуемую поверхность с наблюдением соответствующей цветной реакции.

Для выявления наличия следовых количеств ВВ путем проведения качественных индикаторных химических реакций внедрены в практику комплекты «Антивзрыв», «Лакмус - 2», «Поиск - ХТ», «Вираж - ВВ» [2]. Данные экспресс-тесты позволяют обнаруживать и идентифицировать ВВ по их следовым количествам на поверхностях предметов, одежде и руках человека даже после длительного прекращения контакта (до нескольких месяцев) обследуемой поверхности с ВВ. Пороговая чувствительность (минимальное содержание вещества, которое можно обнаружить в пробе) указанных химических экспресс-тестов находится на уровне $1 \cdot 10^{-5}$ г/см^2.

Процесс исследования является быстрым, наглядным и не требует сложного лабораторного оборудования. Персонал, использующий экспресс-тесты, не нуждается в специальной подготовке. Присутствие следов ВВ определяется по характерному окрашиванию тестовой бумаги с отобранной пробой после ее обработки составами, входящими в комплекты.

Комплекты «Антивзрыв» и «Лакмус - 2» позволяют обнаруживать и визуально подтвердить присутствие следов следующих ВВ и смесей на их основе: тротил, пикриновая кислота, гексоген, октоген, пентаэритриттетранитрат, ВВ на основе нитроглицерина (динамиты, динамоны), дымный порох. Комплект «Поиск - ХТ» позволяет обнаруживать и идентифицировать ту же номенклатуру ВВ, за исключением аммиачноселитровых ВВ и дымного пороха.

Рассмотрим принцип применения тест-систем на примере комплекта «Вираж - ВВ», принятого на снабжение органов внутренних дел Российской Федерации (и включенного в нормы табельной положенности.

Комплект для экспресс-анализа проб на наличие взрывчатых веществ «ВИРАЖ - ВВ» (рис. 1) предназначен для обнаружения и идентификации взрывчатых веществ по их следовым количествам на поверхностях упаковок, на одежде и руках человека, а также на других подозрительных объектах [3].

Рисунок 1. Комплект обнаружения ВВ «Вираж - ВВ»

В состав комплекта входят: три флакона с капельницами с реактивами А, В, С; салфетки из фильтровальной бумаги; пылезащитный корпус; паспорт. Анализ, проводимый с помощью тест-системы «Вираж – ВВ», характеризуется достаточно низкими пределами обнаружения, г: тротил – 10^{-8}, тетрил – 10^{-6}, гексоген – 10^{-6}, октоген – 10^{-6}, пентаэритриттетранитрат – 10^{-5}. Способ применения индикаторов для взрывчатых веществ, входящих в комплект «Вираж – ВВ», включает следующие шаги: обтереть салфеткой исследуемый объект; нанести 1-2 капли реактива А на загрязненную салфетку (появление красно-фиолетового окраса указывает на присутствие тротила и динитротолуола); при отсутствии окраса нанести реактив В и сразу реактив С (при оранжевом окрасе предполагается присутствие тетрила, при розовом окрасе – гексогена, октогена, пентаэритриттетранитрата или нитроглицерина).

Для экспресс-обнаружения ВВ на основе полиароматических соединений на различных поверхностях в работе [4] предложена серия аэрозольных устройств, представляющих собой флаконы с распылителем объемом 120 мл, заполненные индикаторной рецептурой. Методика обнаружения ВВ с использованием данных устройств включает следующие этапы: снять колпачок с насоса-распылителя; поднести аэрозольный флакон на расстояние 10-20 см от контролируемой поверхности; распылить индикаторный раствор многократным нажатием на кнопку насоса; наблюдать за появлением на контролируемой поверхности индикаторного эффекта. О наличии на исследуемой поверхности ВВ судят по появлению пятен соответствующей окраски. При взаимодействии с рецептурой флакона тринитротолуол, тринитробензол и динитротолуол образуют соединения красно-коричневой окраски, тетрил – оранжевой, пикриновая кислота и ее соли – желтой. Испытания показали наглядность индикаторного эффекта на таких поверхностях, как нержавеющая сталь, алюминий, кафель, окрашенные и покрытые нефтепродуктами поверхности, кожа, предметы одежды. Описанное аэрозольное устройство обладает следующими техническими характеристиками: время обнаружения составляет менее 1 минуты, чувствительность методики на

уровне поверхностных концентраций искомых веществ 10^{-2} – 10^{-3} мг/см^2, кратность использования не менее 150 раз, масса флакона 150 г, интервал рабочих температур составляет диапазон от минус 10 до плюс 50 ^{0}С.

Разработан способ обнаружения и идентификации взрывчатых веществ, основанный на визуальном эффекте при взаимодействии ароматических нитросоединений, обладающих взрывчатыми свойствами, с металлорганическим комплексом – цимантреном. Реакция цимантрена и таких нитросоединений, как 2,4-динитротолуол, 2,4,6-тринитротолуол, дает быстрое образование четкого синего окрашивания после кратковременного облучения УФ-светом. Реакция происходит как в растворе, так и на поверхности – ТСХ-пластинке или фильтровальной бумаге. Чувствительность определения на фильтровальной бумаге позволяет обнаруживать нитросоединения в количестве не менее 10^{-5} г. Высокая чувствительность определения тротила (2,4,6-тринитротолуола) позволяет наблюдать визуальный эффект при контакте с поверхностью бумаги, импрегнированной цимантреном [5].

Для экспресс-обнаружения ВВ интерес представляет метод тонкослойной хроматографии (ТСХ). Данный метод перспективен в целях обнаружения веществ, применяемых для изготовления самодельных взрывных устройств. ТСХ-идентификация ВВ основана на разделении анализируемых компонентов в тонком слое сорбента, в результате чего образуются хроматографические пятна веществ, для наблюдения которых используют облучение ультрафиолетовым светом (УФ) или проявление с помощью химических реагентов с получением окрашенных продуктов реакции. В качестве тонкого слоя сорбента используют либо фильтровальную бумагу, либо хроматографические пластинки, представляющие собой слой сорбционного материала, например, силикагеля, нанесенного на металлическую или пластиковую тонкую подложку. Для ТСХ-обнаружения ВВ смесь анализируемых компонентов растворяют в подходящем растворителе, затем наносят на хроматографическую пластинку в месте так называемой линии старта, опускают хроматографическую пластинку в стеклянную камеру, заполненную растворителем-элюентом на время, пока элюент в результате продвижения по слою сорбента не достигнет края пластинки. После чего пластинки высушивают и проявляют зоны искомых веществ, обрабатывая соответствующим реагентом или облучением УФ-светом. Идентификационным признаком ВВ в методе ТСХ является значение R_f, определяемое как отношение расстояния, прошедшего от линии старта идентифицируемым веществом - l_i, к расстоянию, прошедшему элюентом, т.е. расстояние от линии старта до края пластинки - L:

$$R_f = l_i / L$$

Будучи простым и недорогим способом установления природы веществ, ТСХ-идентификация может быть рекомендована для дополнительной проверки результатов поиска ВВ, полученных на основе тест-методов.

Предложена методика ТСХ-исследования таких взрывчатых веществ, как пикриновая и стифниновая кислота и их производные [6]. Указанные вещества активно используются для изготовления самодельной взрывчатки. Идентификацию тринитрофенолов проводили в следующих условиях: в качестве раство-

рителя использовали ацетон, разделение осуществляли на пластинках «Sorbfil», в качестве подвижной фазы выступали системы растворителей ацетон:толуол:гексан (1:1:2) и ацетон:октан (5:2). Для наблюдения хроматографических пятен исследуемых ВВ использовали 5-процентный раствор дифениламина (ДФА) в ацетоне, активацию в УФ-свете, обработку раствором КОН в этаноле, что позволяло наблюдать окрашенные зоны исследуемых ВВ и определять значения R_f. Состав элюентов обеспечил четкое разделение стифниновой кислоты, пикриновой кислоты и ее солей, тринитротолуола. Предложенные в методике способы проявления хроматографических пятен позволили четко визуализировать зоны исследуемых ВВ. При активации хроматографических пятен УФ-светом наблюдали желтое, темно-желтое и оранжевое окрашивание для стифниновой кислоты, пикратов и пикриновой кислоты, тротила соответственно. При обработке ДФА пятна стифниновой кислоты окрашивались в лимонно-желтый цвет, пикриновой кислоты и пикратов – в темно-желтый, тротила в – желто-оранжевый. При обработке раствором КОН наблюдали желтые пятна стифниновой кислоты, желто-оранжевые пятна пикриновой кислоты, темно-желтые пятна пикратов и красно-коричневые пятна тротила.

Перспективным направлением в области технического оснащения антитеррористических служб является использование детекторов паров ВВ – устройств, предназначенных для обнаружения паров ВВ при анализе проб воздуха. Внедрение в практику подразделений органов внутренних дел портативных высокочувствительных газовых анализаторов, реагирующих на ничтожно малые количества взрывчатых веществ в воздухе, значительно расширяет возможности своевременного предотвращения готовящихся террористических актов.

Поиск эффективных мер по усилению безопасности привел к созданию различных портативных газовых хроматографов, адаптированных для выявления источников возможных взрывов. Среди таких разработок известен, например, портативный экспрессный хроматографический обнаружитель взрывчатых веществ ВВ «ЭХО – М» [7] (рис. 2).

Рисунок 2. Высокочувствительный газохроматографический анализатор взрывчатых веществ «ЭХО - М» (с детектором электронного захвата)

Данная хроматографическая система включает скоростные поликапиллярные колонки, узлы сорбционного концентрирования и ввода пробы, дистанционного отбора паров с обследуемых объектов, один из видов детекторов (детектор электронного захвата, фотоионизационный или пламенно-ионизационный), встроенное микропроцессорное управление режимами работы. В хроматографе используется аргон в качестве газа-носителя. С применением предварительного концентрирования предел обнаружения паров тротила составляет 10^{-14} г/см^3, время отбора проб вихревым пробоотборником несколько секунд, время анализа проб занимает 10–20 с. В 1995 г. хроматограф «ЭХО – М» был принят на вооружение МВД России и зарегистрирован в Государственном реестре средств измерений.

Поскольку использование аргона в качестве газа-носителя ограничивало применение прибора в полевых условиях, то впоследствии была разработана модель портативного хроматографа «ЭХО – В», современный образец которой представлена на рис. 3. Высокочувствительный датчик «ЭХО – В» оснащен малогабаритным легкорегенерируемым фильтром для очистки воздуха и газохроматографическим ионизационным детектором перестраиваемой селективности [8], что позволяет использовать воздух в качестве газа-носителя, а не аргон.

Рисунок 3. Высокочувствительный переносной газохроматографический обнаружитель-анализатор взрывчатых веществ

Показанная на рисунке модель характеризуется особенностями, позволяющими осуществлять высокоточный контроль взрывоопасных объектов в потенциальных местах готовящегося теракта. Прибор позволяет проводить экспрессное обнаружение взрывчатых веществ с высокой чувствительностью. Достигаемые пределы обнаружения по тринитротолуолу (тротил) составляют 10^{-14} г/см^3, а время анализа соответствует интервалу 20-120 с. Малогабаритность прибора, простота эксплуатации, низкое энергопотребление, возможность дистанционного пробоотбора обуславливают перспективу создания на его базе мобильной лаборатории. Прибор снабжен программным обеспечением, позволяющим создавать и пополнять базы данных на широкий класс определяемых веществ и вести архивы хроматограмм.

Усовершенствование и развитие технических средств для своевременной идентификации ВВ открывают новые перспективы для борьбы с такими опасными явлениями, как экстремизм и терроризм. Разработка подходов к анализу ВВ является составной частью оптимизации оперативно-разыскной деятельно-

сти в процессе подготовки антитеррористических мероприятий. Методы физико-химического анализа веществ на сегодняшний день выступают мощным средством, позволяющим своевременно выявлять противоправные действия, связанные с организацией террористических актов посредством взрывов. Внедрение в деятельность антитеррористических служб портативных газовых анализаторов, работающих на принципах газовой хроматографии, делают меры по борьбе с терроризмом эффективными, быстродействующими и надежными. Скрининг-технологии, включающие использование химических тест-методов или тонкослойную хроматографию, облегчают мониторинг потенциально опасных объектов при возникновении угрозы совершения взрыва.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Официальный сайт МВД России [Электронный ресурс]. – Режим доступа: https://мвд.рф/reports/iterm/14696015.

2. Сайт компании ООО «Безер-Импер» «Антитеррор» [Электронный ресурс]. – Режим доступа: http://antiterror.com.ru/index.php? news_id= 18&route=information/news.

3. Сайт сообщества криминалистов и экспертов «Криминалисты.ру» [Электронный ресурс]. – Режим доступа: http://kriminalisty.ru/stati/technics/ chemodan-kriminalista/viraz.html.

4. Пашинин В.А. и др. Средства экспресс-обнаружения взрывчатых веществ / В.А. Пашинин, П.Н. Косарев, В.В. Татаринов, Н.Н. Посохов // Технология гражданской безопасности. 2016. Т. 13. № 1. С. 40-43.

5. Способ обнаружения и идентификации взрывчатых веществ. Патент РФ 2336523, Публ. 04.07.2007, МПК: G01N31/22, G01N 21/78.

6. Сайт Федерации судебных экспертов. Исследование бризантных взрывчатых веществ [Электронный ресурс]. – Режим доступа: http://sud-expertiza.ru/library/issledovanie-brizantnyh-vzryvchatyh-veshhestv.

7. Грузнов В.М. и др. Развитие в России методов обнаружения взрывчатых веществ / В.М. Грузнов, М.Н. Балдин, А.Л. Макась, Б.Г. Титов // Журнал аналитической химии. 2011. Т. 66. № 11. С. 1236–1246.

8. Сайт компании «Гранат» [Электронный ресурс]. – Режим доступа: http://granat-e.ru/echo-v.html.

УДК 343

СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВОВОМ ПРОСТРАНСТВЕ. КИБЕРПРЕСТУПНОСТЬ

Цыганкова Я.В.,
кандидат юридических наук;
Смирнов В.М.,
кандидат технических наук;
Киреева Е.В.
(Московский университет МВД России имени В.Я. Кикотя)

Аннотация: в статье рассматриваются правовые аспекты различных способов преступлений, совершенных с использованием информационных технологий. Выявляются основные признаки и способы борьбы с преступлениями, связанными с информационными технологиями.

Ключевые слова: информационные технологии, киберпреступность, киберпреступления, классификация, способы совершения преступлений.

METHODS OF COMMITTING CRIMES USING INFORMATION TECHNOLOGIES IN THE LEGAL SPACE. CYBERCRIME

Tsygankova Ya.V.,
Candidate of Law;
Smirnov V.M.,
Candidate of Technical Sciences;
Kireeva E.V.
(Kikot Moscow University of the MIA of Russia)

Abstract: the article deals with the legal aspects of various types of crimes committed using information technologies. The main signs and methods of combating crimes related to information technologies are identified.

Keywords: information technologies, cybercrime, cybercrime, classification, methods of committing crimes.

Темпы развития научно-технического прогресса и изменения, происходящие в современном обществе, постоянно создают новые, более современные способы совершения преступления. Наиболее значимым примером выступает быстрое развитие сферы информационных технологий, которые проникают почти во все области жизни общества. Это, зачастую, связано с ростом преступной деятельности в данной сфере. Так, достижения в сфере телекоммуни-

каций и массовое внедрение цифровых технологий во все сферы человеческой жизни определяет возникновение новых и развитие уже существующих способов преступлений с использованием информационных технологий, в которых компьютеры и компьютерные сети – это объект киберпреспупности, средство или способ совершения преступления.

В рекомендациях экспертов ООН «киберпреступность» представлена любым преступлением, которое может совершаться благодаря компьютерной системе или сети, в пределах компьютерной системы или сети или против компьютерной системы или сети [4].

Однако более широкое понимание данного термина, которое отражает современные тенденции развития этого явления, дает С.М. Майоров. По его мнению, это «любые преступления, каким-либо образом связанные с компьютерными технологиями и телекоммуникационными сетями, включая закрытые сети, которые не входят в Интернет, а также сети, которые до настоящего дня не введены в эксплуатацию или даже не изобретены» [7].

Применение информационных технологий с целью совершения преступления нужно представлять в качестве способа для совершения преступлений.

Сегодня не выделяют единую классификацию способов совершения преступлений с использованием информационных технологий, поэтому до сих пор в юридической литературе остаются дискуссионные вопросы, которые касаются данной темы.

В Конвенции Совета Европы «О преступности в сфере компьютерной информации» [1] приводится четыре типа компьютерных преступлений, которые представлены:

1. Незаконным доступом (ст. 2 Конвенции Совета Европы).
2. Незаконным перехватом (ст. 3 Конвенции Совета Европы).
3. Вмешательством в данные (ст. 4 Конвенции Совета Европы).
4. Вмешательством в систему (ст. 5 Конвенции Совета Европы).

Представленные виды киберпреступлений представлены собственно «компьютерными», остальные виды являются или связанными с компьютером (computer-related), или совершаемые с помощью компьютера (computer-facilitated) преступления. Такие преступления представлены:

- преступлениями, связанными с нарушением авторских и смежных прав;
- действиями, в которых компьютеры применяются в качестве орудия преступления (электронные хищения, мошенничества и т.п.);
- преступлениями, в которых компьютеры выступают как интеллектуальные средства (к примеру, размещение в сети Интернет детской порнографии, информации, разжигающей национальную, расовую, религиозную вражду и т.д.).

Отечественные исследователи выделяют различные классификации способов совершения преступлений с использованием информационных технологий. Так, Н.И. Шумилов разделяет данные способы на три группы: незаконное изъятие носителей информации; несанкционированное получение информации; неправомерное манипулирование информацией [6]. В.Б. Вехов выделяет два способа: информационные технологии как объект преступного посягательства;

информационные технологии, выступающие в качестве средств совершения преступления [5].

Одной из распространенных классификаций способов совершения преступлений с использованием информационных технологий является классификация, предложенная А.Н. Родионовым и А.В. Кузнецовым, согласно которой они выделяют следующие способы: изъятие средств компьютерной техники; неправомерный доступ к компьютерной информации; изготовление или распространение вредоносных программ; перехват информации; нарушение авторских прав (компьютерное пиратство) [3].

По нашему мнению, такая классификация обладает общим характером, в ней отсутствуют критерии отграничения таких способов. Но при этом они отражают наиболее значимые аспекты данного рода отношений.

В российском законодательстве киберпреступления представлены следующими видами [2]:

1. Мошенничеством с использованием электронных средств платежа и компьютерной информации (ст. 159.3 и ст. 159.6 Уголовного кодекса Российской Федерации).

2. Преступлениями в сфере компьютерной информации (гл. 28 Уголовного кодекса Российской Федерации).

В гл. 28 Уголовного кодекса Российской Федерации предусмотрена ответственность за преступления в сфере компьютерной информации. Но при этом существенный недостаток представлен скудностью закрепленных на законодательном уровне уголовно-правовых норм. Способы совершения преступления в сфере компьютерной информации вообще не предусматриваются уголовным законодательством. Отсутствуют иные нормы, предусматривающие ответственность за незаконные действия в сфере телекоммуникаций и компьютерной информации. Преступления, которые совершаются в сфере телекоммуникаций и компьютерной информации, необходимо относить к преступлениям в сфере высоких технологий.

Вышепредставленные способы совершения преступлений с использованием информационных технологий не являются исчерпывающими, т.к. в связи с постоянно ускоряющимися темпами развития научно-технического прогресса и изменениями, происходящими в современном обществе, возможно появление абсолютно новых видов преступлений, связанных с использованием информационных технологий.

В России за 2019 год зарегистрированы 294,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий, или на 68,5% больше, чем за 2018 г. [9].

Подчеркивается, что доля киберпреступлений среди общего числа правонарушений за 2019 г. выросла с 8,8% до 14,5%. При этом около половины киберпреступлений являются тяжкими и особо тяжкими.

В настоящее время киберпреступления могут совершаться следующими способами: анонимные письма (письма с угрозами); утечка конфиденциальной информации; неправомерный доступ к информации; удаление информации;

мошенничество с помощью ИТ; атаки типа «Отказ в обслуживании» (DoS), в том числе распределенные (DDoS) и др. [8].

Так, фишинг можно считать относительно устаревшим способом мошенничества, но достаточно эффективным. Более современным видом мошенничества является фарминг. Он схож с фишингом, также использует поддельные веб-сайты для кражи личных данных пользователя. Но фарминг не требует от пользователей совершать какие-либо предварительные действия: они перенаправляются на поддельные сайты автоматически без их ведома за счет работы встроенного ранее вредоносного кода-вируса. Хакеры успешно используют эту технику, потому что она позволяет им одновременно проникнуть в огромное количество устройств. В дополнение к этому им не требуется просить пользователей о совершении каких-либо действий, так как этот вредоносный код автоматически загружается без каких-либо сознательных действий со стороны пользователя [10].

Проведенный анализ позволяет сделать вывод, что современные достижения в области интернет-технологий приводят к увеличению способов совершения киберпреступлений, которые в свою очередь не находят отражения в правовом пространстве Российской Федерации. Сегодня государство ведет активную политику в рамках противодействия киберпреступности и преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. Однако на данный момент такие меры не привязаны к конкретным способам совершения преступлений в сфере информационно-телекоммуникационных сетей.

Таким образом, без должного правового регулирования проблему решить невозможно, необходимо повышать ответственность за размещение в сети запрещенного контента, формировать правовые и организационно-технические механизмы противодействия противоправной деятельности на основе конкретных способов совершения преступлений в информационно-телекоммуникационных сетях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конвенция о преступности в сфере компьютерной информации (ETS № 185) (заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003) из информационного банка «Международное право» // СПС «Консультант Плюс».

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020) // СПС «Консультант Плюс».

3. Бочкин Д.В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 40–46.

4. Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // ЮП. 2019. № 4 (91). С. 78–82.

5. Дерюгин Р.А. Киберпреступность в России: современное состояние и Актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2. С. 46–49.

6. Картавченко В.В., Лисун Е.А. Использование высоких технологий в качестве способа совершения преступления / Проблемы и перспективы развития современной юриспруденции: сборник научных трудов по итогам международной научно-практической конференции. – Воронеж, 2015. С. 91–93.

7. Майоров С.М. Киберпреступления: причины, виды, формы, последствия, направления противодействия / Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе: материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. – Самара, 2018. С. 156–160.

8. Сериева М.М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. 2017. № 1(1). С. 104–106.

9. Состояние преступности в России за январь – декабрь 2019 г. / Официальный сайт Генеральной прокуратуры Российской Федерации [Электронный ресурс]. – URL: https://genproc.gov.ru (дата обращения: 12.05.2020).

10. Хусяинов Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве / Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования: материалы всероссийского круглого стола. – Иркутск, 2015. С. 120–125.

СОДЕРЖАНИЕ

НАУЧНОЕ ИЗДАНИЕ

ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Сборник статей 7-й Всероссийской научно-практической конференции

22 мая 2020 г.

Редактор ***Е.А. Олейникова***
Техн. редактор ***И.Ю. Чернышева***

Подписано в печать 2019 г., формат бумаги 60х90/16, 20,0 уч.-изд.л.
бумага офсетная, печать цифровая
Тираж 35 экз., заказ № 57

Отпечатано в отделении полиграфической и оперативной печати
Белгородский юридический институт МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71