Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Всероссийская конференция
(22 апреля 2021 г.)

Сборник научных статей

1 электронный оптический диск (CD-R)
Текстовое электронное издание

Научное электронное издание

Москва
Московский университет
МВД России имени В.Я. Кикотя
2021

ISBN 978-5-9694-1046-6

УДК 004.9
ББК 16.3
И74

Рецензенты:
начальник Центра информационных технологий,
связи и защиты информации ГУ МВД России по г. Москве
А. Ф. Прокопчук; старший научный сотрудник
НИЦ № 2 ФГКУ «ВНИИ МВД России» **Д. С. Горячев**

Составитель *И. С. Мельцева*

И74 **Информационные технологии в деятельности органов внутренних дел**: Всероссийская конференция, 22 апреля 2021 г. : сборник научных статей / [сост. И. С. Мельцева]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2020. – 259 с. – 1 электронный оптический диск (CD-R). – Системные требования: CUP 1,5 ГЦ ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске.

ISBN 978-5-9694-1046-6

В сборнике публикуются статьи авторов – участников Всероссийской конференции «Информационные технологии в деятельности органов внутренних дел», прошедшей 22 апреля 2021 г.

В статьях авторов рассматриваются проблемные вопросы контроля и правового регулирования безопасности государства, анализа угроз обеспечения кибербезопасности страны, а также противодействия преступности в сфере информационных технологий, технологии защиты систем хранения, распространения, обработки и передачи данных, технологий расследования компьютерных преступлений.

Статьи публикуются в авторской редакции. Сборник предназначен для научных и практических работников, участвующих в борьбе с преступностью.

Научное электронное издание

Минимальные системные требования: CPU 1,5 ГГц; RAM 512 Мб;
Windows XP SP3; 1 Гб свободного места на жестком диске

Издание подготовлено
с помощью программного обеспечения Microsoft Word

Корректор *Чамарова Н. В.*
Компьютерная верстка *Чамарова Н. В.*

Подписано к изданию
Объем издания: Кб
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-1046-6

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
https://мосу.мвд.рф, e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Гончар В. В.[1]***,***
заместитель начальника кафедры
информационной безопасности учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

Акиньшин И. С.[2]***,***
заместитель начальника
Московского университета МВД России имени В.Я. Кикотя
по профессиональному обучению, дополнительному
и профессиональному образованию,
кандидат экономических наук

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ В 2020 г.[3]

По итогам 2020 г. наблюдается устойчивый рост количества зарегистрированных преступлений рассматриваемой категории. Сложившиеся обстоятельства социально-экономического характера, обусловленные распространением и преодолением последствий новой коронавирусной инфекции Covid-19, создали дополнительные условия для усиления криминальной активности, связанной с использованием IT-технологий.

В 2020 г. сохранилась динамика значительного роста количества преступлений рассматриваемой категории, уголовные дела о которых находились в производстве правоохранительных органов Российской Федерации – 580,26 тыс., что на 73,4 % превышает показатель предыдущего года (339,3 тыс.), непосредственно в отчетном периоде зарегистрировано – 510,4 тыс. (+73,4 % к АППГ, 294,4 тыс.).

Удельный вес зарегистрированных IT-преступлений увеличился с 14,5 % в 2019 г. до 25,0 % в 2020 г.

Раскрываемость IT-преступлений по-прежнему невысока и по итогам 2020 г. составила 20 % (–10,1 % к АППГ – 22,2 %).

---

[1] © Гончар В. В., 2021

[2] © Акиньшин И. С., 2021.

[3] Термин «киберпреступления», «преступления, совершаемые с использованием информационно-коммуникационных технологий», «преступления в сфере информационных технологий» и другие понятия используются не редко как синонимы. В данном материале подобные преступления будут сокращенно именоваться «IT-преступления».

Анализ информации, поступившей из территориальных органов предварительного следствия МВД России, выявил следующие типичные проблемы в расследовании IT-преступлений:

1. Значительное количество находящихся в производстве уголовных дел и мягкость санкций за данные преступления, что делает такие преступные деяния более привлекательными по сравнению с классическими преступлениями.

2. Отсутствие действенного инструментария быстрого получения от кредитных организаций, интернет-провайдеров, операторов связи, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по уголовным делам (сведений о лице, биллинге, движении денежных средств по лицевым счетам абонентских номеров и др.).

3. Использование преступниками программного обеспечения, позволяющего избежать (или существенно затруднить) их идентификацию, – VPN, TOR, SSL, а также технологий, позволяющих менять IP-адрес пользователя интернетом, создавать динамические или нераспознаваемые IP-адреса, применять технологии «подменных» абонентских номеров посредством IP-телефонии.

4. Несовершенство законодательства. Неопределенность при квалификации хищений по п. «г» ч. 3 ст. 158 УК РФ, ст. 159.3 и п. «в» ч. 3 ст. 159.6 УК РФ. Несмотря на разъяснения, приведённые в постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в данных нормах не учитывается конкретный способ хищения денежных средств с банковских счетов, что вызывает различия в трактовке со стороны следствия, органов прокуратуры и суда.

5. Недостаточная компьютерная грамотность населения. Руководителям следственных подразделений поручено обеспечить принятие действенных мер, направленных на совершенствование методов информирования населения, в том числе с привлечением федеральных и региональных СМИ, социальных медиа о способах совершения IT-преступлений, методах защиты, а также алгоритме действий пострадавшего. Они предупреждены о недопустимости формального подхода к направлению представлений в порядке ст. 158 УПК РФ.

6. Возмещение имущественного вреда, причинённого преступлениями, совершенными в сфере IT-технологий.

В настоящее время действующим законодательством не урегулирована процедура и порядок взыскания денежных средств, арестованных на расчетных счетах, на которые потерпевшие перечислили денежные средства в случае, когда

подозреваемый (обвиняемый) не открывал указанный счет в банковском учреждении, либо его местонахождение не установлено.

7. Не в полной мере сформированы специализированные базы данных. Например, существует единая база данных «Дистанционное мошенничество», где аккумулируется информация о зарегистрированных IT-преступлениях и устройствах, с помощью которых осуществляются хищения денежных средств.

В указанный модуль сотрудниками территориальных органов внутренних дел на региональном уровне вносится актуальная информация о вновь выявленных фактах IT-преступлений.

8. Необходимость увеличения числа государственных специалистов и экспертов, имеющих право проводить соответствующие исследования и компьютерные экспертизы. Сегодня практически отсутствуют ведомственные специалисты, способные идентифицировать компьютерную программу как вредоносную методом обратного реверс-инжиниринга.

Решение данных проблем видится в комплексе законодательных, технических, организационных и научных мер, более детально изложенных в рамках доклада.

Белоусов И. И.[1]***,***
начальник отдела компьютерно-технических
экспертных исследований ГБУ г. Москвы
«Московский исследовательский центр»

АКТУАЛЬНЫЕ ЗАДАЧИ, РЕШАЕМЫЕ ПРИ ПРОВЕДЕНИИ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТНЫХ ИССЛЕДОВАНИЙ

Стремительное развитие микропроцессорной техники, информационных технологий, в частности систем передачи и хранения информации (5G-сети, OneWeb, Blockchain, Big data), обусловливает широкое использование информационных технологий, в том числе и для совершения различных преступлений. Анализ правоохранительной практики показывает, что получение криминалистически значимой информации по делам, связанным с использованием компьютерной техники, невозможно без использования специальных познаний, основной процессуальной формой применения которых является судебная компьютерно-техническая экспертиза.

Для формирования целостного понимания, методических подходов, используемых при проведении компьютерно-технических исследований, следует рассмотреть актуальные для современного уровня развития компьютерной криминалистики задачи, решаемые в рамках проведения судебной экспертизы.

При проведении компьютерно-технических экспертиз и исследований аппаратных объектов, программных объектов, информационных объектов, информационно-телематических объектов решаются две основные группы задач диагностические и идентификационные. Целью решения диагностических задач не только исследование состояния, свойств и функционального назначения объекта, но и анализ процессов, действий пользователя и их последовательности (механизм события), приведших к результатам использования информационно-телекоммуникационных устройств и информации при совершении преступления. Идентификационные задачи имеют целью установить факт индивидуально-конкретного тождества или общей групповой принадлежности представленных объектов экспертизы.

Существенные особенности объектной области и разнообразие видов объектов компьютерно-технических экспертиз и исследований обусловливают доминирующую группу задач, решаемых в рамках данного вида экспертных исследований, – диагностические задачи.

При проведении компьютерно-технических экспертиз и исследований решаются следующие виды задач ***криминалистической диагностики***:

1. *Собственно диагностические задачи*. Определение вида (типа, марки), конфигурации (свойств, функциональных характеристик) и рабочего состояния аппаратных объектов; определение наименования, правообладателя, состава исполняемых модулей, алгоритмов работы, настроек, рабочего состояния и функционального назначения, программных объектов; определение состояния (существующий/удаленный), типа, служебной информации, содержания, функционального назначения файлов (информационных объектов).

2. *Причинно-динамические задачи* решаются с целью определения механизмов, динамики и обстоятельств события (дела), установление причинной связи между объектом исследования и результатами, ставшими следствием его использования; определение механизма и существенных обстоятельств использования аппаратных объектов; установление связи между функциональными возможностями и результатами использования аппаратных объектов; определение механизма и существенных обстоятельств использования программных объектов по результатам их работы; установление связи между функциональными возможностями и результатами использования программных объектов; определение временного периода и последовательности действий с информационными объектами; установление связи между действиями, осуществляемыми с информационными объектами и их следствиями.

3. *Классификационные задачи* решаются с целью установления соответствия между характеристиками объекта и заранее заданным комплексом признаков, для отнесения объекта исследования на этом основании к существующему, строго поименованному, определенному и формально признанному наукой (практикой) классу, включающему бесконечное множество не индивидуализированных объектов:

отнесение аппаратных объектов к определенным классам (IBM-совместимый компьютер, сетевой маршрутизатор, накопитель на магнитных дисках, игровой автомат и т. д.); отнесение программных объектов к определенным классам (операционная система, система управления базами данных, вирусная программа и т. д.); отнесение информационных объектов к определенным классам (исполняемый файл, архивный файл, метаданные EXIF и т. д.).

4. *Задачи по выделению подмножества объектов.* В отличие от классификационных задач, решаются с целью выделения подмножества объектов из значительного (но исчислимого), заранее непоименованного множества существующих, не индивидуализируемых объектов исследования, на основании заданных (в том числе инициатором) признаков, обусловленных исключительно обстоятельствами конкретного дела:

поиск среди программных объектов, содержащихся на представленных носителях информации, тех, которые были установлены в заданный временной период; поиск среди существующих и восстановленных информационных объектов (файлов), тех которые содержат фотографические изображения заданного характера или ключевые слова.

5. *Обеспечение выемки информации.* Данные задачи решаются с целью установления возможности и обеспечения получения криминалистически значимой информации, доступу к которой препятствует техническое состояние устройства, система аутентификации и/или шифрование:

преодоление аппаратного шифрования и восстановление поврежденных носителей информации аппаратных объектов; получение доступа к зашифрованным логическим разделам носителей информации и преодоление парольной защиты программных объектов; восстановление удаленных и поврежденных файлов, получение доступа к содержащейся в них информации.

При проведении компьютерно-технических экспертиз и исследований решаются следующие виды задач ***криминалистической идентификации***:

1. *Задачи индивидуальной идентификации*. Установление тождества между индивидуализирующими обозначениями исследуемого аппаратного объекта и сведениями, отобразившимися в программной среде информационно-телекоммуникационных устройств (при их взаимодействии) или указанными в представленной документации; установление тождества между индивидуализирующими обозначениями исследуемого программного объекта и сведениями, указанными в представленной документации.

2. *Установление групповой принадлежности*. Данные задачи следует рассматривать как незавершенный этап индивидуальной идентификации (в некоторых случаях установления источника происхождения), цель которой – сужение, насколько это позволяют сделать выявленные признаки, группы исследуемых объектов, с учетом безусловной конечности группы, не смотря на её количественный размер. В отличие от классификационных задач, решаются в отношении объектов, предусматривающих возможность индивидуального отождествле-

ния с целью установить их принадлежность (отнесения) к конечной, неклассифицированной группе однородных объектов, ограниченной совокупностью идентификационных признаков, выявленных в объекте исследования:

отнесение индивидуально-определенных аппаратных объектов к носителям информации конкретного типа (HDD, SSD), функционально предназначенным для использования в серверах определенной марки и модели, указанных в обстоятельствах дела, в составе дискового массива; отнесение индивидуально-определенных программных объектов к вирусным программам, функционально предназначенным для выполнения действий, указанных в обстоятельствах дела, с использованием заданных уязвимостей операционной системы конкретной версии, и написанных на определенном языке программирования.

3. *Установление единого источника происхождения*. Данные задачи решаются с целью установления индивидуально-определенных обстоятельств создания (времени, места, автора, программно-технических средств), использования и хранения исследуемых объектов, в том числе выделенных в группу на основании совокупности идентификационных признаков:

установление индивидуально-определенного предприятия, являющегося источником происхождения (создания) выделенной группы исследуемых аппаратных объектов, исходя из выявленной совокупности особенностей аппаратно-программной конфигурации объектов, их индивидуализирующих обозначений, функционального назначения и обстоятельств дела; установление индивидуально-определенного автора программного объекта, исходя из выявленной совокупности особенностей использованных алгоритмов работы программы, структуры её программного кода и языка программирования; установление марки и модели устройства, индивидуально-определенного места и времени создания выделенной группы исследуемых файлов (информационных объектов), исходя из выявленной совокупности, содержащихся в них фотографических изображений, системных свойств и метаданных файлов.

4. *Установление целого по части.* Данные задачи решаются с целью установления принадлежности фрагментированных объектов исследования, к единому целому, индивидуально-определенному объекту. Применительно к компьютерно-техническим исследованиям под «целым объектом» следует понимать как монолитные логические объекты информационной системы (дисковый массив), так и комплексные логические объекты информационной системы, состоящие из множества обособленных, но функционально связанных, логических элементов (совокупность файлов составляющих единую программу):

установление принадлежности выделенной группы исследуемых носителей информации (аппаратных объектов), исходя из выявленной совокупности особенностей их файловой системы и обстоятельств дела, к единому индивидуально-определенному дисковому массиву; установление принадлежности выделенной группы исследуемых файлов (информационных объектов), исходя из выявленной совокупности особенностей структуры программного кода, системных свойств файлов и обстоятельств дела, к единой индивидуально-определенной базе данных.

Сущенко Е. А.[1],
курсант Института подготовки
сотрудников для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ПРОБЛЕМЫ ИНФОРМАЦИОННОГО ХАРАКТЕРА, СВЯЗАННЫЕ С ПРОИЗВОДСТВОМ НЕКОТОРЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ НЕЗАКОННОЙ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Анализ текущего состояния преступности в сфере информационных технологий позволяет сделать вывод о стремительном развитии средств, методов, доступности технологий для совершения противоправных деяний. Так, например, за 2020 г. значительно увеличилось количество преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (в производстве правоохранительных органов Российской Федерации – 580,26 тыс., что на 73,4 % превышает показатель предыдущего года (339,3 тыс.), непосредственно в отчетном периоде зарегистрировано – 510,4 тыс. (+73,4 % к АППГ, 294,4 тыс.)). Удельный вес зарегистрированных преступлений IT-преступлений увеличился с 14,5 % в 2019 г. до 25,0 % в 2020 г.

Актуальная тема информатизации общества – серьёзная проблема, с точки зрения преступности, поскольку злоумышленники используют информатизацию как инструмент для совершения общественно опасных деяний. Правоохранительные органы используют информационные технологии во благо общества, например в ходе следствия в отношении различного вида преступлений, активно используют систему распознавания лиц, анализ больших объемов данных, а также в ходе производства отдельных следственных действий.

---

[1] © Сущенко Е. А., 2021.

В соответствии со статистикой, приведенной Генеральной Прокуратурой РФ на сайте http://crimestat.ru/offenses_chart, уровень зарегистрированных преступлений экономической направленности за период с января по октябрь 2020 г. снизился до 96 154, по сравнению со значениями пятилетней давности: в 2015 г. зарегистрировано преступлений экономической направленности 112 445, также, в сравнении с данными десятилетней давности 2010 г. 276 435 [3].

Незаконная банковская деятельность, предусмотрена ст. 172 УК РФ [4], объективная сторона которой предполагает осуществление банковских операций: открытие и ведение банковских счетов физических и юридических лиц; осуществление переводов денежных средств по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам и т. д. [1]: 1) без соответствующей регистрации; 2) без специального разрешения (лицензии) в тех случаях, когда оно обязательно; 3) с нарушением каких-либо лицензионных требований. При этом условиями привлечения к уголовной ответственности по данной статье выступают: причинение крупного ущерба гражданам, организациям или государству и/или извлечение дохода в крупном размере.

Чтобы качественно и эффективно производить следственные действия в отношении данного преступления, органам предварительного расследования необходимо использовать различные ресурсы информатизации в рамках своей деятельности, для того чтобы заранее определить намерения злоумышленника и вычислить махинации, которые преступники уже разработали в ходе совершения самого преступления, определить способы сокрытия преступления.

При производстве осмотра места происшествия преступлений экономической направленности имеется особенность, заключающаяся в рациональном избрании участвующих лиц в данном следственном действии. Так, в практической деятельности, следователи, расследующие экономические преступления, утверждают, что в большинстве случаев злоумышленники прячут информацию о незаконной экономической деятельности на электронных носителях, т. е. USB-флеш-накопители (флеш-карты), компьютеры, удаленные сервера и др. Поэтому следователь должен работать в команде с IT-специалистом, который грамотно и эффективно проведет необходимые мероприятия по проведению следственного действия в отношении преступлений экономической направленности, изучит электронные носители, технику, поможет правильно изъять и упаковать технические средства, изъятые в ходе проведения ОМП, составить вопросы для проведения соответствующей экспертизы.

Осмотр носителей электронной информации на наличие виртуальных следов. При производстве осмотра места происшествия следователи могут совершить грубую ошибку, а именно пренебречь осмотром информационных объектов. Виртуальные следы не подлежат непосредственному восприятию человеком. Для их восприятия требуются специальное аппаратное и/или программное обеспечение и определённые подготовительные действия [1, с. 101–102].

Чтобы избежать повреждения или полного уничтожения необходимой информации, которая составляет предмет преступления, надо качественно спланировать производство следственного действия, подготовиться, т. е. провести подготовительные мероприятия, например изучить схему расположения удалённых терминалов и сетей и связи между ними, выяснить наличие электронных охранных средств. Часто возникает ситуация, когда у следователя нет необходимых знаний при проведении осмотра, следствием чего может быть утрата важнейшей информации в компьютерном устройстве. Поэтому необходимо привлечение специалиста-программиста, который профессионально произведет работу по извлечению криминалистически значимой компьютерной информации, расшифрует файлы, которые содержат доказательственную базу данных, найти и извлечь виртуальные следы.

Следственные действия – обыск (выемка). Цель обыска (выемки) в том числе – обнаружение и изъятие компьютерной техники, на которой возможно обнаружение информации, свидетельствующей о совершении незаконной банковской деятельности, а также информация о причастных лицах.

Список литературы

1. Агибалов, В. Ю. Виртуальные следы в криминалистике и уголовном процессе / В. Ю. Агибалов. – М. : Юрлитинформ, 2012. – С. 101–102.

2. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 20.04.2021).

3. Портал правовой статистики. – URL: http://crimestat.ru/offenses_chart (дата обращения: 01.03.2021).

4. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 24.02.2021) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_ LAW_110699/ (дата обращения: 20.04.2021).

5. Колмаков, В. П. Следственный осмотр / В. П. Колмаков. – М., 1969.

6. Криминалистика : учебник для бакалавров / под ред. А. Г. Филлипова. – 2-е изд. – М. : Юрайт, 2015.

Бордаченко В. А.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В данной статье рассматриваются вопросы, которые связаны с осуществлением уголовно-правового противодействия по уголовным делам о мошенничестве в сфере компьютерной информации, а также предлагаются способы по разрешению данных дел.

Актуальность данной темы обусловлена тем, что компьютерные преступления в наше время довольно распространены. С недавних пор через интернет совершается большое количество преступлений различной степени тяжести и различного характера. Но в российском законодательстве не было конкретных норм, которые предусматривали ответственность за совершение преступлений в сфере компьютерных технологий. Данная проблема повлияла на принятие Федерального закона от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», который ввел в Уголовный закон ряд экономических преступлений, предусматривающих ответственность за совершение квалифицированных видов мошенничества, в том числе и ст. 159.6 УК РФ, имеющую схожий состав с общественно опасным деянием, предусмотренным ст. 159 УК РФ «Мошенничество», но представляющих меньшую общественную опасность, что влечет менее строгий вид наказания, а также существенно изменил механизм правового регулирования уголовного преследования преступлений.

---

[1] © Бордаченко В. А., 2021.

Включение указанных статей, содержащих преступления в экономической сфере, позволяет конкретизировать компьютерные преступления, однако это порождает ряд проблем.

Для рассмотрения вопросов, связанных с осуществлением уголовно-правового противодействия по уголовным делам, связанных с мошенничеством в сфере компьютерной информации, необходимо рассмотреть характеристику данного общественно опасного деяния.

Статья 159.6 УК РФ состоит из четырёх частей, первая из них раскрывает понятие мошенничества в сфере компьютерной информации, а вторая, третья и четвёртая части данной статьи включают квалифицированные составы данного преступления по следующим признакам:

1. Преступления, совершенные группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, предусмотренного ч. 2 ст. 159.6 УК РФ.

2. Совершение лицом уголовно наказуемого деяния с использованием своего служебного положения; в крупном размере; с банковского счета, а равно в отношении электронных денежных средств, предусмотренного ч. 3 ст. 159.6 УК РФ.

3. Совершение организованной группой либо в особо крупном размере деяния, предусмотренного частями 1–3 настоящей статьи и закрепленного в ч. 4 ст. 159.6 УК РФ.

Компьютерная информация, применительно к ст. 159.6 УК РФ – это информация, зафиксированная на ЭВМ или передаваемая по телекоммуникационным каналам в форме, доступной восприятию. ЭВМ. Её особенность заключается в следующем:

– информация имеет свойство просто и быстро преобразовываться из одной формы в другую;

– при изъятии информации, она сохраняется в первоначальном виде;

– доступ к одному и тому же файлу, содержащему информацию, может одновременно иметь несколько пользователей.

Анализ состава данного преступления позволяет сделать вывод, что общественными отношениями, охраняемыми уголовным законодательством, мошенничества в сфере компьютерной информации одновременно выступают два объекта: компьютерная информация и имущество, что является одним и основных разграничений деяний, предусмотренных ст. 159.6 УК РФ, и иных форм мошенничества.

Объективную сторону составляет хищение чужого имущества или приобретение права на чужое имущество.

Способы совершения преступлений в сфере компьютерной информации:

1. Хаккинг – взлом программного обеспечения с его последующим полном или частичном изменении.

2. Дефейс – тип хакерской атаки, при котором одна страница сайта заменяется другой.

3. Картинг – похищение реквизитов банковских карт через компьютерную сеть, после чего производится незаконное распоряжение денежными средствами.

4. Фишинг – компьютерное преступление, при котором мошенниками получают доступ к конфиденциальным данным пользователя.

5. Крекинг – компьютерное преступление, при котором мошенники снимают встроенную защиту с программного обеспечения с целью его последующего незаконного использования.

6. Нюкинг – компьютерное преступление, при котором мошенники выполняют действия, вызывающие зависание системы.

7. Спамминг – массовая рассылка сообщений рекламного характера.

Рассматривая субъективные признаки преступления, необходимо сказать, что по смыслу ст. 159.6 УК РФ субъектом является физическое вменяемое лицо, достигшее на момент совершения деяния 16-летнего возраста (общий субъект).

Объектом уголовно-правового противодействия мошенничеству в сфере компьютерной информации выступают: 1) уголовно наказуемые деяния; 2) лица, их совершающие; 3) лица с антиобщественной направленностью, не совершавшие преступление, но склонные их совершить; 4) все остальные граждане.

Субъективная сторона преступления выражена умышленной формой вины в виде прямого умысла.

Органы предварительного расследования на различных стадиях уголовного процесса сталкиваются с большими трудностями при раскрытии, расследовании и предупреждении мошенничеств, совершаемых в сфере компьютерной информации. Расследование связано с определенными специальными знаниями, в связи с чем затрудняется обычный порядок предварительного расследования преступлений.

Точность и полнота расследования преступного деяния зависят от правильности выбранного направления следственной работы, которое было составлено при предварительной проверке информации по рассматриваемому делу лицом, осуществляющим предварительное расследование, тщательном анализе и оценке существующей информации, выдвижении версий о подлежащих установлению обстоятельствах преступления.

К основным задачам противодействия преступлениям, связанным с мошенничеством в сфере компьютерной информации следует относить: неотвратимость наступления уголовной ответственности за совершение уголовно наказуемых деяний, правильную квалификацию, вынесение легитимного, мотивированного и объективного приговора. Ученые выделяют три типичные ситуации условий, в которых преступник совершил деяние, предусмотренное рассматриваемой статьи, закрепленной в Уголовном кодексе РФ.

1. Преступление совершенно при известных обстоятельствах потерпевшему, который выявил преступника собственными силами, вследствие чего он был задержан, т. е. в условиях очевидности.

2. Правоохранительным органам известен способ совершения преступления лицом, который скрылся от должностных лиц, но полный механизм совершения преступления неясен.

3. Лицам, осуществляющим предварительное расследование, неизвестен ни механизм преступления, ни лицо его совершившее. Налицо имеется только преступный результат.

В каждой из рассматриваемой ситуации возникают сложности у законодателя в компетентной, подробной и безошибочной квалификации анализируемой статьи, также степень высокопрофессиональной квалификации элементов следствия не постоянно в должной мере соответствует действующим требованиям, что, безусловно, не может не сказаться на качестве предварительного расследования по квалифицированному виду мошенничества.

При рассмотрении данной категории дел можно подвести итог и сказать, что она обладает высокой степенью сокрытия, относится к латентным преступлениям. Причина проблемы расследования, раскрытия и предупреждения компьютерных преступлений – технологический прогресс, обеспечивающий и облегчающий деятельность преступников. Имеющиеся в настоящее время разработанные методики раскрытия и расследования мошенничества в сфере компьютерной информации проявляют второстепенное влияние на качество раскрытия и расследования данных преступлений. Следствие этого – снижение количества раскрытых уголовных дел, связанных с мошенничеством в сфере компьютерной информации и отсутствие должного результата по расследованным и направленным на рассмотрение в суд уголовным делам.

Таким образом, в настоящее время есть потребность в разработке методологий с учетом нынешних достижений в области криминалистики, изменений уголовного и уголовно-процессуального законодательства, а также содержанием в

них криминалистических рекомендаций относительно методики раскрытия, расследования и судебного разбирательства преступлений, связанных с мошенничеством в сфере компьютерной информации.

Список литературы

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 24.02.2021) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.04.2021).

2. Федеральный закон от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс» http://www.consultant.ru/document/cons_doc_LAW_138322/ (дата обращения: 20.04.2021).

3. Фролов, М. Д. К вопросу об ответственности за мошенничество в сфере компьютерной информации / М. Д. Фролов // Образование и право. – 2018. – № 9.

4. Уголовное право Российской Федерации. Общая часть / под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. – 2-е изд. – М. : Контракт; Инфра-М, 2008.

5. Пункты 12–14 постановления Пленума Верховного Суда Российской Федерации от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда Российской Федерации. – 2008. – № 2.

6. Шевелева, С. В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами преступлений / С. В. Шевелева // Вестник Нижегородской академии МВД России. – 2017. – № 4. – С. 229–234.

Грекова М. А.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

МОШЕННИЧЕСТВА, НАПРАВЛЕННЫЕ НА ЗАРАЖЕНИЕ УСТРОЙСТВА ПОЛЬЗОВАТЕЛЯ ВРЕДОНОСНОЙ ПРОГРАММОЙ

В последние несколько лет мошенничество с помощью заражения устройства вредоносными программами очень распространено. Это связано с развитием общества, частым использованием различных гаджетов и других устройств, соответственно, преступления совершаются чаще именно в интернете, становясь большей частью преступности.

Относительно недавно были введены ст. 272, 273, 274.1 УК РФ, ответственность по которым, с совокупностью со ст. 159 УК РФ, наступает за совершение мошенничества посредством неправомерного доступа к компьютерной информации, а равно создания, использования вредоносный компьютерных программ и превышает семи лет лишения свободы [1].

Федеральным законом от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» данные составы преступлений представлены в новой редакции [3]. Эти изменения происходят из-за нескольких обстоятельств. Быстрое развитие информационных и коммуникационных технологий приводит к значительным изменениям в концептуальном аппарате, а уголовный закон должен полностью отражать существующие реалии. Кроме того, увеличение объемов, и разновидностей преступлений в сфере компьютерной информации, диктует

необходимость уточнения объективной стороны составов соответствующих преступлений в уголовном законе, а также дифференциации уголовной ответственности правонарушителей.

Внедрение автоматизированных информационных систем и технологий управления и обработки информации, придающих юридическую силу действиям, осуществляемым с помощью компьютерных программ, создали предпосылки для использования этих процессов для совершения преступных действий, а значит, и необходимость укрепления их защиты, в том числе уголовно-правовым методом. Опасность преступлений в области компьютерной информации в том, что разрушение блокировки, модификация информации важны для действий, связанных с управляющими датчиками сложных компьютерных систем обороны, производства, экономической, банковской и другой сферы, они способны привести к гибели людей, разрушению имущества, нанести вред их здоровью и экономический ущерб в больших размерах. Именно поэтому законодатель отнес гл. 28 «Преступления в сфере компьютерной информации» к разд. IX УК «Преступления против общественной безопасности и общественного порядка» [3].

В примечании 1 к ст. 272 УК РФ дано определение понятия «компьютерная информация»: это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Специфический характер носит деятельность в сфере компьютерной информации, а компьютерные технологии, сети быстро развиваются. Терминология носит технический характер и, соответственно, понятия раскрываются в специальных нормативных актах. Например, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 28.07.2012). В нем информация определяется как сведения в целом, независимо от формы предоставления [2]. Один из видов таких сведений, компьютерная информация, в ст. 272 УК РФ трактуется как информация на машинном носителе, в электронно-вычислительной машине, системе ЭВМ. К ЭВМ помимо компьютера также относятся различного рода гаджеты, банкоматы, бортовые компьютеры, контрольно-кассовые машины. Поскольку это требует особых познаний, для правильной квалификации необходимо назначать соответствующие экспертизы.

Для квалификации по ст. 272 УК РФ надо установить, кто имел доступ к компьютерной информации, а именно, получение возможности ознакомиться с ней и воспользоваться ею. Важно определить, каким образом произошел доступ, например использование специальных технических или программных средств,

которые позволяют преодолеть установленные системы защиты, в том числе незаконного использования действующих паролей или кодов для проникновения в компьютер. Неправомерным доступом признается деяния лица, не обладающего правами на получение и работу с данной компьютерной информацией либо системой, в отношении которых приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ. К информации, которая охраняется государством, относятся служебная и коммерческая тайна, личные данные человека, объекты авторского права и т. д.

Для наступления уголовной ответственности необходимо наступление вредных последствий: приведение информации в непригодное состояние, создание условий ее недоступности, модификация информации (любые изменения компьютерной информации, в том числе внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе) или переноси материала на иной носитель [4].

Для квалификации по ч. 2 ст. 272 УК РФ необходим факт причинения ущерба, который превышал бы 1 млн руб.

Уясним понятие «вредоносная программа». Это такая информация, предназначенная для уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты: вирусы, черви, программы-сканеры, эмуляторы электронных средств защиты, программы управления потоками компьютерной информации, программы-патчеры.

Совершения преступления необходимо создание вредоносной программы, т. е. представление совокупности данных и команд, предназначенных для функционирования информационно-телекоммуникационных сетей, компьютерных устройств, ее выпуск в свет, введение в хозяйственный оборот, а также ее распространение посредством продажи, проката, сдачи внаем, дачи взаймы. Самый распространенный способ распространения – размещение на сайтах в интернете.

Следует учитывать, что деятельность организаций, осуществляющих разработку антивирусных программ и имеющих лицензию, не влечет уголовную ответственность.

На практике это выглядит примерно так: мошенники рассылают с электронных адресов, которые схожи с адресами реальных организаций, сообщения со ссылкой на скачивание какого-либо материала, например открытки, музыки, программы. Скачивание либо запуск данного материала и инициирует установку на устройство вредоносной программы – вымогатель-блокиратор, шифровальщик, троянская программа.

Разберем несколько способов мошенничества с использованием вредоносной программы.

«Троянский конь». Получить его можно по электронной почте или сообщения в мессенджере. Объявление или письмо приходит от неизвестного отправителя. Владелец гаджета открывает соединение, а вредоносное ПО встроено в операционную систему персонального компьютера или мобильного устройства. Когда пользователь входит на официальный сайт банка, в личный профиль ресурса, интернет-магазин вирус троян перенаправляет его на поддельную фишинговую веб-страницу, которая полностью имитирует внешний вид реального сайта. Ничего не подозревающий пользователь вводит свои личные данные, тем самым предоставляя злоумышленникам необходимую информацию. Затем вредоносное ПО просит ввести одноразовый код подтверждения, отправленный банком. И тогда мошенники имеют доступ к счету жертвы, и они могут только переводить деньги на свои счета.

«Мобильный банкинг». С троянскими вирусами атакуют злоумышленники прежде всего банковские мобильные приложения. Троян заменяет исходное окно входа в систему и пароль фишингом, а затем передает данные на сервер злоумышленникам. В этом случае вирус имеет доступ к СМС-сообщениям, из которых мошенник может получить одноразовые пароли, отправленные банком. В этом случае владелец счета может долго не узнать о недостающих средствах, так как у троянца есть возможность скрыть от пользователя сообщения, поступающие на устройство из банка.

«Опасный Wi-Fi». Чтобы свести к минимуму риск мошенничества, нужно не только знать основные правила безопасности, но и соблюдать их ежедневно, а также соблюдать правила личной гигиены. Профессионалы называют правила безопасности кибергигии. К сожалению, на практике три четверти пользователей знают, что они должны выполнять кибергигиену, но не выполняют ее. Более трети имеют по крайней мере одно незащищенное электронное устройство. Многие используют общедоступные беспроводные сети для свободного доступа в интернет и не думают о рисках [5].

Таким образом, необходимо повышать квалификацию сотрудников правоохранительных органов в данной сфере. Ведь расследование таких преступлений требует и теоретических, и практических знаний. Необходимо проводить работу с гражданами, чтобы они знали об угрозах интернет-пространства, тщательно следили за своей деятельностью в сети, личной информацией и персональными данными. Прежде всего надо работать на предупреждение киберпреступлений, так как они сильно подрывают материальное состояние граждан. Несмотря на

постоянное совершенствование систем информационной безопасности самих банковских организаций, правоохранительным органам нужно перенимать опыт гражданских экспертов в области информационной безопасности.

Есть основания полагать, что данный вид преступности стремительными темпами перерастает в международный. Об этом свидетельствует появление международных институтов по кибербезопасности, развитие новых сфер деятельности, противодействующих кибермошенникам. Крайне необходимо налаживать методику взаимодействия с другими государствами в этой сфере, проводить дальнейший системный анализ для успешной борьбы с данным видом преступлений, ведь киберпреступность и кибербезопасность – это две составляющие части глобального интернет-пространства.

Список литературы

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 24.02.2021) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.04.2021).

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 28.07.2012) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 20.04.2021).

3. Федеральный закон от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_122864/ (дата обращения: 20.04.2021).

4. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 20.04.2021).

5. Медиакомпания Зеленоград сегодня. – URL: https://zelenograd-news.ru/news/bezopasnost/moshennichestvo_pri_pomoshchi_vredonosnykh_programm (дата обращения: 20.04.2021).

Глушакова М. А.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя,

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ВОЗМЕЩЕНИЯ УЩЕРБА, ПРИЧИНЁННОГО КИБЕРПРЕСТУПЛЕНИЯМИ

Один из важных аспектов в деятельности предварительного следствия совместно с правоохранительными органами – не только в раскрытии и расследовании преступления, но также и возмещение вреда, который был причинен в ходе преступных деяний. Помимо названных органов одно из направлений деятельности государство – это защита прав и интересов лица, которое подверглось воздействую преступлением.

Киберпреступления – это те преступления, преступный умысел которых направлен на получение денежных средств или иной информации, которая позволит получить доступ к личным данным лица, с помощью разных компьютерных технологий.

Современное общество развивается, и вместе с ним развиваются киберпреступники, они находят все более усовершенствованные и скрытые пути завладения чужим имуществом. Из-за этого существует огромная проблема в нахождение этих преступников, так как большинство из них совершают свои преступные действия удаленно через компьютер, а еще сложнее возмещение вреда, причиненного экономическими преступлениями.

Когда совершается преступление, в том числе киберпреступление, нарушаются права и интересы личности. Для полного их восстановления государству, а также иным лицам, на которых возложена эта обязанность, нужно принять все меры по их обеспечению и защите пострадавшего лица [1].

---

[1]

Согласно одному из важнейшему нормативному правовому акту, а именно ст. 52 Конституции Российской Федерации, права потерпевших от преступлений и злоупотреблений властью охраняются законом. Государство обеспечивает потерпевшим доступ к правосудию и компенсацию причиненного ущерба. Анализируя данную норму, можно сделать вывод, что государство – важный фактор по восстановлению прав потерпевших.

В уголовном судопроизводстве, а именно в процессе расследования преступления, важно обеспечить защиту интересов лица, так как могут ограничиваться их права.

Публичный характер уголовно-процессуальной деятельности и причиняемого в ее сфере вреда предполагает и публичную ответственность государства перед своими гражданами. Российское государство приняло на себя такую ответственность, провозгласив право граждан на возмещение государством вреда, причиненного незаконными действиями органов государственной власти и их должностных лиц.

К видам вреда, причиненного преступлениям относя:

– физический вред определяется вреда жизни и здоровья гражданину;

– имущественный вред, под ним понимается разность между материальным положением лица до и после уголовного судопроизводства, а также неполученные доходы, которые лицо получило бы, не будь незаконных действий органов дознания, предварительного следствия, прокуратуры и суда в отношении гражданина;

– моральный вред, из содержания ч. 1 ст. 151 ГК РФ и руководящих разъяснений Пленума Верховного Суда Российской Федерации «Некоторые вопросы применения законодательства о компенсации морального вреда» от 20.12.94 явствует, что под моральным вредом следует понимать нравственные или физические страдания, причиненные действиями (бездействием), посягающим на принадлежащие гражданину от рождения или в силу закона нематериальные блага либо нарушающими его личные неимущественные права или имущественные права. Моральный вред, в частности, заключается в нравственных переживаниях в связи с утратой близких родственников, невозможностью продолжать активную общественную жизнь, потерей работы, раскрытием семейной, врачебной тайны.

Нормативные правовые акты, которые регулируют возмещение вреда, причиненного преступлением, это, в частности, Гражданский кодекс, Уголовный ко-

декс, а также Уголовно-процессуальный кодекс. Когда нарушаются права и интересы гражданина и ему причиняется любой ущерб, он должен компенсироваться материально [2].

По анализу МВД России всех экономических преступлений за 2020 г. общий ущерб составил 450 млрд руб. Самыми частыми потерпевшими от этих преступлений являются как обычные граждане, так и большие компании.

В связи с тем, что, совершая экономические преступления, материальный ущерб достигает больших размеров. Преступники, совершая преступные деяния, например, хищения, могут причинять вред как самому гражданину, общественным и частным организациям, государству, уклоняются от возмещения вреда и используют его в дальнейшем для своих целей.

Обращаясь к практике, можно сделать вывод, что преступники очень редко возмещают ущерб, который они причинили преступными действиями. Для возмещения вреда необходимо вырабатывать специальные мероприятия, которые возложены на сотрудников экономической безопасности и противодействия коррупции, а также на правоохранительные органы в целом.

Существует несколько способов по возмещению ущерба, причиненного преступным путем:

1. Возвращение похищенного имущества или денежных средств.
2. Компенсация ущерба в денежной форме за счет реализации имущества, на которое налагается арест.
3. Отчисление от заработной платы осужденного.

В настоящее время существует проблема по возмещению ущерба, причиненного преступным путем, потому что конкретизации в нормативных правовых актах нет, а также из-за того, что преступники придумывают наиболее скрытые способы совершения преступления, невозможно найти виновных лиц, с которые должны возмещать ущерб, причиненного преступным путем.

Результат по обеспечению возмещения имущественного ущерба путем хищения, а также других экономических преступлений зависит от многих факторов.

Например, один из главных аспектов – это своевременная фиксация и обнаружение имущества, добытого преступным путем, а также возмещение пострадавшему лицу. В процессе проведения оперативно-разыскных мероприятий сотрудники экономической безопасности и противодействия коррупции должны быть направленны на поиск преступников, установление размера имущественного вреда и пострадавшему лицу.

Немаловажно направление мер, которые направлены на добровольное возмещение подозреваемым или обвиняемым лицом имущественного ущерба, причиненный преступлением.

Таким образом, возмещение имущественного вреда является актуальной темой на сегодняшний день, так как все чаще совершаются экономические преступления, где преступники находят все более скрытые пути их совершения. Из-за этого очень трудно найти лицо, которое совершило преступление, и соответственно взыскать имущественный ущерб.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 (с изм., одобр. в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 20.04.2021).

2. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ / СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 20.04.2021).

3. Гражданский кодекс Российской Федерации : Федеральный закон от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 20.04.2021).

4. СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 20.04.2021).

5. Постановление Пленума Верховного Суда Российской Федерации от 20.12.1994 № 10 «Некоторые вопросы применения законодательства о компенсации морального вреда» (ред. от 06.02.2007) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_5677/ (дата обращения: 20.04.2021).

6. Анисимов, А. Г. Проблемы реального возмещения вреда, причиненного преступлением, в уголовном судопроизводстве России / А. Г. Анисимов, А. И. Цыреторов // Мировой судья. – 2019. ‑№ 5. – С. 164–167.

7. Сычев, П. Г. Имущественный характер экономических преступлений и соответствующие процессуальные последствия / П. Г. Сычев // Имущественные отношения в Российской Федерации. – 2014. – № 12.

Куликова М. А.[1]*,*
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Рассмотрим преобразование криминологической характеристики преступных деяний в отношении собственности за счет популяризация применения электронных расчетных средств и современных способов их воспроизводства, в том числе с использованием информационных технологий, которые постоянно совершенствуются.

На сегодняшний день известны многочисленные способы хищения денежных средств с банковских карт клиентов банка, в том числе с использованием информационных технологий, при этом такие способы постоянно совершенствуются, что не позволяет службе безопасности банков оперативно разрабатывать и внедрять новые методы защиты денежных средств.

Совершение преступлений в информационной сфере требует наличия у лиц особых знаний, навыков в данной области [3]. Совершению непосредственных действий, направленных на хищение денежных средств с электронных счетов населения, предшествует тщательная подготовка. Все это осложняет возможность расследования совершенных преступных деяний, а также своевременного предупреждения и пресечения совершения новых актов преступного посягательства.

За время действия ограничений, связанных с пандемией коронавируса, в России резко выросло число зарегистрированных случаев мошенничества. Об этом

свидетельствует официальная статистика ГИАЦ МВД России. При этом рост данных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, произошел исключительно за счет телефонного и интернет-мошенничества: за 2020 г. зарегистрировано 25 820 число случаев такого мошенничества, сравнительно к аналогичному периоду 2019 г. – 16 119 , т. е. выросло на 60.2 % [1].

Основу осуществления операций в электронной форме составляют отношения, возникающие между банком и клиентом. Такие отношения требуют установления и гарантирования должной защиты получаемых сведений, платежных поручений, соблюдения конфиденциальности таких данных.

Широкая распространенность преступных деяний, направленных на хищение безналичных денежных средств со счетов граждан, определенная специфика преступления, способов и средств его совершения обусловили необходимость выделения такого деяния в самостоятельный состав (ст. 159.3 УК РФ).

Правильное и полное расследование совершенного преступления требует определения всех существенных элементов, обстоятельств, подлежащих установлению. Соответственно, наличие «начальных» данных позволяет следователю, дознавателю сориентироваться на начальном этапе производства по уголовному делу, оперативно организовать и провести необходимые следственные и иные процессуальные действия, позволяющие восстановить обстановку совершенного преступного деяния.

Процент раскрываемости данных преступлений практически не превышает 50 %, а процент привлечения к уголовной ответственности лиц, виновных в совершении данной категории дел, еще более скромен.

К числу факторов, негативно влияющих на своевременность выявления преступлений указанной группы, следует относить:

а) высокий уровень латентности хищений с использованием электронных средств платежа;

б) значительное количество хищений рассматриваемого вида совершается в составе группы лиц по предварительному сговору или организованной группы с четким разделением ролей;

в) большой круг и разнообразие характеристик лиц, имеющих возможности для совершения хищений с использованием электронных средств платежа, которыми могут быть сотрудники банков-эмитентов платежных карт, процессинговых центров; лица, занимающиеся изготовлением в целях сбыта поддельных платежных карт, и др.;

г) межрегиональный и транснациональный характер организованной преступной деятельности, связанной с использованием банковских платежных карт (изготовление поддельных платежных карт может происходить в одной стране, а сбыт – в другой);

д) поверхностные знания оперативных сотрудников об организации оборота платежных карт;

е) ненадлежащее взаимодействие с подразделениями органов внутренних дел, а также субъектами оборота платежных карт [4].

В некоторых случаях при наличии в действиях виновного лица состава мошенничества клиенты стараются обращаться за помощью в банки, клиентами которых они являются, требовать с кредитных организаций возмещения причиненных убытков, нежели обращаться в правоохранительные органы.

Как было указано ранее, совершение мошенничества с использованием электронных средств платежа сопровождается тщательной предварительной подготовкой. В данном случае специфичны и способы сокрытия наступивших преступных последствий. Так, например, получив информацию о реквизитах банковской карты конкретного лица, злоумышленники могут путем введения полученных сведений расплатиться «указанной» банковской картой при оплате товаров. Тогда такое лицо признается владельцем банковской карты, а потому оснований для отказа в совершении соответствующей операции нет.

Специфика следообразования при совершении рассматриваемого преступления сводится к тому, что информация о факте совершенной незаконной транзакции отражается в нескольких источниках – между банками, участвующими в проведении транзакции [2].

Субъектный состав лиц, участвующих в совершении преступного деяния: одно или несколько лиц. Эта разновидность преступных деяний, особенно в период пандемии, приобрела организованный характер. Как правило, такие преступления осуществляются специализированными группами лиц, чья «профессиональная» деятельность базируется в соответствующей сфере, на специфических вопросах (например, путем обзвона клиентов от имени банка в целях получения данных о реквизитах карты либо направления письма для подтверждения совершения определенной операции).

Криминальная специализация в группе такова: одни члены группы осуществляют сбор информации по банковским картам, другие – обрабатывают собранную информацию и передают их тем, кто занимается изготовлением поддельных карт. Подлежат установлению численность и состав организованной группы (преступного сообщества), роль каждого из соучастников [5].

Специфичны и способы совершения мошенничеств с использованием электронных систем. Так, только в период пандемии получили широкое распространение следующие способы:

1. Переход в интернет по ссылкам, содержащим «вирусные» программы. В этом случае установка вирусных программ осуществляется автоматически. Сущность указанных программ сводится к «добыче» персональных данных владельцев банковских карт в результате последующего перехода владельца в личный кабинет банка, а также входа в специальные мобильные приложения, разработанных самими банками и содержащими сведения по счетам владельца (например, приложение СберБанк Онлайн). Например, одна из наиболее распространенных схем мошенничества – предложения по урегулированию взысканий, отсрочке по выплате кредитов или помощи в проведении упрощенной процедуры банкротства за комиссию, предложение зайти по ссылке в личный кабинет банка. При переходе открывается фишинговый (поддельный) сайт банка, на котором жертва вводит свои реальные логин и пароль личного кабинета. Таким образом, эти данные отправляются мошенникам, и они получают к нему доступ. В условиях эпидемии COVID-19 интернет-сайты могут маскироваться под официальные порталы реальных организаций, например, Всемирной организации здравоохранения или Минздрава России, благотворительных организаций, осуществляющих помощь и поддержку граждан.

2. Осуществление рассылки. Как правило, предлагают познакомиться со способами борьбы с возбудителем коронавируса, средствами защиты и т. д. Злоумышленники могут пригласить на осмотр в поликлинику — пройти обследование на коронавирус. Но сначала они просят зарегистрироваться на неизвестном сайте или установить программу на компьютер или телефон. Пользуясь ситуацией на рынке труда, они направляют фейковые предложения об удаленной работе под прикрытием корпоративных рассылок. Такие сообщения имеют вид приглашения принять участие в Zoom-конференции.

3. Продажа товаров путем размещения недостоверных фотографий, изображений товара. Размещаемый товар по фотографии покупатель оценивает по высокой цене с учетом его «качества» и соответствующая сумма денежных средств переводится на счет злоумышленника. Однако в этом случае покупатель либо приобретает товар сравнительно отличающего качества, либо не приобретает никакого эквивалента вообще. В период пандемии мошенники предлагают купить очиститель воздуха, удаляющий возбудителя вируса, маски с фильтром, отсеивающие вирус, или средство от COVID-19 и т. д.

Таким образом, с учетом происходящей в государстве обстановки, вызванной введением режима самоизоляции, злоумышленники разработали новые методы совершения преступлений – мошенничество в области использования электронных средств платежа. А развитие информационных технологий приводит к совершенствованию мошеннических схем, направленных на завладение чужими денежными средствами, содержащимися на банковских счетах. В ходе расследования указанные сведения используют следователь и дознаватель, в частности для выдвижения следственных версий и планирования действий по их проверке, повышения результативности поиска следов преступления, сужения круга подозреваемых.

Список литературы

1. Статистика по данным ГИАЦ МВД РФ // официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://мвд.рф/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen (дата обращения: 25.03.2021).

2. Блашникова, Е. А. Новый этап в борьбе с мошенничеством в информационной среде / Е. А. Блашникова // Наука, образование, культура. – 2019. – № 1.

3. Иванова, Л. В. Хищение с использованием информационных технологий: проблемы квалификации / Л. В. Иванова // Юридическая наука и правоохранительная практика. – 2020. – № 1 (51).

4. Козодаева, О. Н. Способы совершения мошенничества с использованием банковских карт / О. Н. Козодаева // Ученые записки Тамбовского отделения РоСМУ. – 2019. – № 1.

5. Шавалеев, Б. Э. Особенности мошенничества с использованием электронных средств платежа в структуре современной российской преступности / Б. Э. Шавалеев // Ученые записки Казанского юридического института МВД России. – 2020. – № 1 (9).

Самойлова А. К.[1]*,*
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОТДЕЛЬНЫЕ КИБЕРУГРОЗЫ, ПОСЯГАЮЩИЕ НА БАНКОВСКУЮ СИСТЕМУ

Банковская система Российской Федерации занимает отдельное место в развитии экономики страны и ее финансовой системы, кибербезопасность каждой отдельной банковской организации влияет на систему в целом, на безопасность банковского сектора, который обеспечивает движение капитала на территории государства и которому «необходимо обладать устойчивостью и способностью придать импульс для развития экономики в необходимом направлении» [3, с. 404].

В соответствии с Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности» банковская система Российской Федерации включает Банк России, кредитные организации, а также представительства иностранных банков [1].

Центральный Банк Российской Федерации в соответствии со ст. 75 Конституции Российской Федерации наделен особым правовым статусом, обладая исключительным правом на эмиссию денежных средств, а также обязанностью осуществлять защиту и обеспечение устойчивости рубля. Иными словами, Банк России – независимый публично-правовой институт, обладающий правом денежной эмиссии и организации денежного обращения на территории страны.

Банк – это кредитная организация, которая имеет исключительное право осуществлять в совокупности следующие банковские операции: привлечение

во вклады денежных средств физических и юридических лиц, размещение указанных средств от своего имени и за свой счет на условиях возвратности, платности, срочности, открытие и ведение банковских счетов физических и юридических лиц [1].

На сегодняшний день посредством использования новейших информационных технологий многие банки участвуют в различных офшорных схемах, схемах легализации доходов, добытых преступным путем, что снижает спрос на некоторые банковские услуги, а также кибербезопасность во всем банковском секторе страны и влечет неустойчивость каждой отдельной организации. Также необходимо отметить о росте профессиональной киберпреступности в России, создании преступных групп, чья деятельность направлена на дестабилизацию банковских систем. Так, например, осенью 2018 г. были две атаки на банк «Юнистрим», направленные на хищение денежных средств, путем отправки сообщений от имени банка. Далее произошла повторная атака на инфраструктуру банка также путем отправки сообщений, но уже другим, ранее не задействованным организациям. Сумма хищений не разглашалась [7].

Деятельность банков, в виду развития научно-технического прогресса и информационных технологий, связана с ежедневным использованием компьютерных технологий. Аналитические данные, опубликованные компанией BI.ZONE, свидетельствуют, что уровень защищенности внутренней инфраструктуры организации в 91 % случаев оценен как низкий и только в 9 % – как средний [7]. Банковские организации уязвимы для злоумышленников, которые становятся все более приспособленными к преодолению систем защиты, установленных внутри банковских систем.

Гондарь В. В., Зиниша О. С., Шаронова В. А. в своем исследовании выделяют ряд причин кибератак на банковские организации:

– отсутствие должным образом развитого законодательства и единых стандартов безопасности;

– отсутствие финансового обеспечения со стороны самих банков-жертв;

– недостаточное развитие корпоративной культуры в области кибербезопасности внутри банковского механизма [2, с. 180].

Специальное структурное подразделение Банка России Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (далее – ФинЦЕРТ), проанализировав кибератаки на финансовые организации за 2019 г., в своем отчете отметил, что чаще всего совершению преступлений предшествовало:

– нарушение организациями требований федеральных законов, действующих на территории страны, актов Банка России в части обеспечения безопасности информации;

– отсутствие должного контроля поднадзорных организаций к вопросам информационной безопасности;

– недостаточная осведомленность работников поднадзорных организаций об актуальных угрозах информационной безопасности [4].

Проанализировав исследования, представленные компаниями BI.ZONE, Group-IB и «Лабораторией Касперского», определим группы кибератак на банки:

– атаки с использованием минимума инструментов, без создания подозрительных файлов на жестком диске устройства, задействовав уже установленные на компьютере инструменты (чаще всего – инструменты удаленного запуска процессора);

– атаки с использованием физических устройств (флеш-карт, нетбуков и т. д.);

– атаки с использованием вредоносного программного обеспечения (например, использование «денежных мулов», программ-вымогателей и т. д.);

– атаки на клиентов банка, в частности, путем методов социальной инженерии.

Более подробно рассмотрим следующие виды кибератак:

1. Фишинговые рассылки: злоумышленники проникают во внутреннюю сеть банка путем перехода сотрудниками банка по вредоносным ссылкам, замаскированных под легальные, а также путем введения персональных данных или запуска приложения на «зараженном» компьютере. Например, преступная группировка Silence осуществляла атаки на банковские организации России и стран СНГ путем рассылки фишинговых писем с вредоносными программами собственной разработки, используя взломанные инфраструктуры других компаний финансового сектора [6].

2. Атаки на устройства самообслуживания (АТМ), разновидности атак: «blackbox», атаки типа «прямой диспенс» [5]. Обе атаки характеризуются физическим воздействием на банкомат: использование переходника-конвертера в первом случае и нарушение перевода денежных средств через банкомат – во втором.

3. Атаки с использованием вредоносного программного обеспечения заслуживают отдельного внимания, поскольку именно этот вид кибератак самый распространенный на сегодняшний день. На момент 2017–2018 гг. распространение получили атаки с использованием вирусов-шифровальщиков, направленных как на распространение вредоносного программного обеспечения, так и на изучение

внутренней информационной системы банка для осуществления дальнейших манипуляций.

4. Кардинг – неправомерное получение информации о держателях банковских карт, о содержимом их магнитных полос. Специалисты ФинЦЕРТа отмечают, что «текстовые данные собираются с помощью фишинговых сайтов, банковских троянов, разработанных для персональных компьютеров (далее – ПК), операционной системы «Android», банкоматов, а также в результате взломов ecommerce-сайтов. Информацию с магнитных полос банковских карт получают через скимминговые устройства, а также с использованием троянов для компьютеров, к которым подключены POS-терминалы [5].

Кибератаки на банки, как правило, совершают хорошо организованные и подготовленные преступные группы, в состав которых входят люди, имеющие образование в области информационной безопасности или компьютерных технологий, обладающие специальными знаниями интернет-пространства и цифровых технологий, а также действующие или бывшие сотрудники банковских организаций, знающие внутреннюю структуру банковской сети. Данный вид преступлений более уязвим и трудно раскрываем.

Так, П.Д.О и П.Е.О., осуществляя преступную деятельность, обладали специальными познаниями в области компьютерной техники и программного обеспечения, опытом работы в интернете с 2000 г., совершенствовали знания в процессе ежедневного использования ПК, а также имели неоднократный опыт совершения преступлений в сфере компьютерной информации. Полученные знания и навыки П.Д.О и П.Е.О использовали для хищения денежных средств с банковских счетов тех клиентов ПАО «Сбербанк», «ВТБ 24», которые использовали подключенные к интернету ПК и смартфоны для управления своими банковскими счетами в данных кредитных организациях посредством систем дистанционного банковского обслуживания «Сбербанк ОнЛ@йн» ПАО «Сбербанк» и «Телебанк» ПАО «ВТБ 24».

Подводя итог вышеизложенному, дадим определение понятию «киберугроза» – это посягательство на безопасность банковской системы, которые представляют собой сознательное противоправное проникновение или угрозу проникновения во внутреннюю информационно-телекоммукационную систему банка, с целью незаконного получения информации, материальной выгоды, нарушения работы системы и иного противоправного воздействия.

Список литературы

1. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СПС «КонсультантПлюс» – URL:

http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 10.01.21).

2. Гондарь, В. В. Политика Банка России по обеспечению кибербезопасности в банковской сфере / В. В. Гондарь, О. С. Зиниша, В. А. Шаронова // Современные научные исследования и разработки. – 2018. – Т. 1. – № 12 (29). – С. 179–183.

3. Марат, Д. Кибербезопасность в банковском секторе Российской Федерации / Д. Марат // Цифровая экономика и финансы. – 2020. – С. 404–408.

4. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности банка России 1.09.2018–31.08.2019 // Сайт Центрального банка России. – URL: https://www.cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF (дата обращения: 20.11.20).

5. ФинЦЕРТ. Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году // Сайт Центрального банка России. – URL: https://www.cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf (дата обращения: 20.11.20).

6. Исследования. Threat Zone 2018: новые вызовы цифрового мира // Сайт компании BI.ZONE. – URL: https://bi.zone/upload/for_download/BIZONE-annual-report-2018-ru.pdf (дата обращения: 20.11.20).

7. Исследования. Threat Zone 2019: иллюзия безопасности // Сайт компании BI.ZONE. – URL: https://bi.zone/upload/for_download/Threat-Zone_2019_RU.pdf (дата обращения: 16.11.20).

Кушнир В. А.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОСОБЕННОСТИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТКОЙ НАПРАВЛЕННОСТИ, СОВЕРШЕННЫХ В СЕТИ ИНТЕРНЕТ И СОЦИАЛЬНЫХ СЕТЯХ

Наше общество идет в ногу со временем и пример этому развитие технологий. Они упрощают наш быт, повседневные процессы, обучение и выполнение работы. С помощью интернета человек получил доступ к огромному массиву различной информации и возможность общаться и делиться своим мнением с другими людьми, не выходя из дому. Но при использовании интернета и различных социальных сетей, и СМИ, преследуются не только благие цели, но и преступные, – это популяризация ненависти к различным слоям населения, национальностям и действующей государственной власти. Возбуждение данной ненависти в сети и СМИ одна из форм проявления экстремизма, за осуществления которых следует уголовная ответственность. Именно технические возможности использования информационно-коммуникационных технологий позволяют оставаться анонимным и способствуют быстрому распространению необходимой информации. Только за 2019 г. в Российской Федерации зарегистрировано 459 преступлений экстремистской направленности в интернете, а в 2020 г. – 672 таких преступлений [7].

Актуальность темы подтверждают и производимые законодательные изменения, и дополнения. Так, Федеральным законом от 28.06.2014 № 179-ФЗ уго-

ловно-правовые нормы об ответственности за призывы к осуществлению к экстремистской деятельности (ст. 280 УК РФ) и возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ) были дополнены указанием на такой альтернативный способ их совершения, как использование информационно телекоммуникационных сетей, в том числе интернета [3]. Этот же способ, наряду с использованием СМИ или электронных сетей, был включен в качестве квалифицирующего признака в новую статью УК РФ об ответственности за публичные призывы к совершению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 2801 УК РФ) [1].

Развитие уголовного законодательства в данном направлении продолжается. 6 июля 2016 г. Президент Российской Федерации подпал Федеральный закон № 375-ФЗ1, касающийся усиления мер обеспечения общественной безопасности, которым ч. 2 ст. 2052 УК РФ была дополнена указанием на совершение публичных призывов к террористической деятельности или публичного оправдания терроризма с использованием электронных или информационно-телекоммуникационных сетей, в том числе интернета, а также повышена строгость наказания за ряд преступлений террористической и экстремистской направленности [4].

Размещенная информация экстремистского характера находится не в реальном мире, т. е. не материальная и находится в так называемом «киберпространстве». Поэтому для понимания сути положений данной статьи, мы введем данное понятие. «Киберпространство» – это среда, в которой функционируют программы и продукты информационно-коммуникационных технологий, в которых отражается, передается, модифицируется и обрабатывается информация на основе специальных алгоритмов для взаимодействия между агентами (пользователями) как в личных, так и в служебных целях.

Механизм совершения преступлений экстремисткой направленности в интернете, имеет специфические особенности, а именно подготовка непосредственно в процессе совершения преступления и соответственно сокрытии, так как на всех этих этапах используется дистанционный способ осуществления преступных действий с помощью информационно-коммуникационных сетей. Орудие преступления – компьютерная техника и программные обеспечения; информационные ресурсы и сама информация, электронные сообщения; устройства передачи, хранения и приема данных и др.

Следовая картина тоже имеет свою специфику, и традиционные способы их выявления не всегда достаточно эффективны. Так как в таких преступлениях

редко происходит воздействие на внешнюю среду, например при избиении потерпевшего или при тайном хищении имущества, т. е. следы оставленные дистанционным путем нельзя отнести к материальным следам в традиционном их понимании, которые рассматриваются в рамках трасологии, так как они имеют «информационный, виртуальный» характер.

Поэтому для расследования данных преступлений необходим определенный порядок первоначальных действий следственно-оперативной группы.

Для наглядности рассмотрим конкретные действия следственно-оперативной группы на примере следующей судебной практики: «По приговору мирового судьи судебного участка № 344 Бескудниковского района г. Москвы от 26 августа 2013 г. А. признан виновным в совершении преступления, предусмотренного ч. 1 ст. 280 УК РФ. Суд установил, что А., будучи приверженцем радикальных националистических взглядов, принял решение побудить неопределенный круг лиц к выступлению против действующей власти в Российской Федерации. В этих целях он, находясь у себя в жилище и используя принадлежащий ему компьютер, зашел на зарегистрированную на его имя страницу сайта «ВКонтакте» и опубликовал на ней содержащий побуждение призыв к осуществлению экстремистской деятельности, а именно текст, указывающий на то, что необходимо подготовить штурм Кремля, прорвать заслоны ОМОНа, ориентироваться на знамя «Русское подполье» и т. д.» [5].

Для установления лица, разместившего информацию экстремистского характера в сети, используется следующий предложенный алгоритм:

– направляется запрос администратору социальной сети (интернет-ресурса) с постановкой следующих вопросов: в какое время и кем был опубликован материал; во сколько зашел и вышел автор записей; если это социальная сеть с опубликованием материалов в группе(беседе), то каково её название и какой конкретно контент она опубликовала с адресной ссылкой на указанный материал;

– какие данные о личности указаны при регистрации автором материалов (ФИО, электронная почта, год рождения, номер телефона, город и т. д.);

– определить IP-адрес, с помощью направления запроса администрации сайта или социальной сети и с помощью какого браузера был осуществлены данные действия;

– после получения адреса, определить интернет-провайдера, которые предоставляет доступ лицу, который разместил противоправные материалы, например для установление названия компании провайдера можно использовать сервис www.whois-service.ru, которая при вводе IP-адреса выдает данные о провайдере, включая его адрес и т. д.;

– отправить запрос уже самому провайдеру с постановкой следующих вопросов: какому пользователю был выделен указанный в запрос IP-адрес и когда он был зарегистрирован; данные о физическом лиц, который получает услуги провайдера; предоставить номер MAC-адреса компьютера (ноутбука), с помощью которого осуществлялся вход с последующим опубликованием экстремистских материалов; если это было отправлено с телефона, то каков номер отправителя; получить данные о входе и выходе в сеть пользователя, а также историю действии в интернете;

– при использовании преступниками мобильной сети необходимо с санкции суда направить запрос оператору сотовой связи, номер которого был получен от администратора интернет-ресурса или провайдером. Здесь нужно уточнить, каким способом был пополнен баланс (банковские карты, электронные кошельки и т. д.);

– направить запросы с судебным решением в банковские организации, а также компаниям по предоставлению услуг по созданию электронных кошельков, с требованием предоставить персональные данные лица (номер его расчетного счета, номер карты, привязанные телефоны к аккаунту, список транзакций и их детальное описание.

Таким образом, расследование преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей на первоначальном этапе расследования для установления лица, совершившего данное преступление, требует от сотрудников правоохранительных и специальных служб соответствующего уровня правовой и технической подготовки. Данный вид преступлений имеет положительную динамику, что вызвано техническими возможностями использования интернета, поэтому наличие универсальных алгоритмов действий следователя и оперативного сотрудника, позволит успешно и в кратчайшее сроки раскрывать и расследовать такие преступления.

Список литературы

1. Уголовный кодекс Российской Федерации // СПС «Гарант». – URL: https://base.garant.ru/10108000/ (дата обращения: 19.04.2021).

2. Стратегия противодействия экстремизму в Российской Федерации до 2025 г. (утв. Президентом РФ 28 ноября 2014 г., Пр-2753) // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/74094369/ (дата обращения: 19.04.2021).

3. Федеральный закон от 28.06.2014 № 179-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (последняя редакция) //

СПС «Гарант». – URL: https://base.garant.ru/70684696/ (дата обращения: 19.04.2021).

4. Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (последняя редакция) // СПС «Гарант». – URL: https://base.garant.ru/71437612/ (дата обращения: 19.04.2021).

5. Приговор мирового судьи судебного участка № 344 Бескудниковского района г. Москвы от 26.08.2013 // Судебные и нормативные акты. – URL: https://sudact.ru/magistrate/court/reshenya-sudebnyi-uchastok-no-344-timiriazevskogo-sudebnogo-raiona-gorod-moskva/ (дата обращения: 19.04.2021).

6. Власенко, В. В. Квалификация экстремистских преступлений при обеспечении охраны общественного порядка : методические рекомендации / В. В. Власенко. – Ставрополь, 2016.

7. Состояние преступности в России за январь–декабрь 2020 и 2019 годов // Официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 03.04.2021).

Саушкина В. В.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ПРОБЛЕМЫ ВЗАИМОДЕЙСТВИЯ СЛЕДОВАТЕЛЯ С БАНКОВСКИМИ УЧРЕЖДЕНИЯМИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ

Взаимодействие правоохранительных органов с финансово-кредитными учреждениями всегда играло важную роль в обеспечении экономической безопасности государства. При взаимодействии правоохранительных и банковских учреждений повышается не только общий уровень экономической безопасности и благосостояния страны, но и улучшаются результативность, эффективность и действенность раскрытия, расследования, а главное, предотвращение преступлений в сфере экономики.

Практически каждый следователь сталкивается с проблемами подобного взаимодействия по вопросам предоставления в том или ином виде информации, в том числе в соответствии со ст. 857 Гражданского кодекса Российской Федерации (далее – ГК РФ) составляющей банковскую тайну [1].

К банковской тайне ГК РФ относит [1]:

– сведения о вкладах и счетах граждан;

– операций по ним;

– сведения о клиентах.

Банк может предоставить информацию о подобных операциях и заключенных договорах, документы, справки, выписки, а также их копии.

---

[1] © Саушкина В. В., 2021.

Форма запроса не имеет четко установленной формы, но тем не менее наличие таких реквизитов, как относимость к конкретному уголовному делу и согласие руководителя следственного органа, обязательно. Это законодательно закрепляет ч. 4 ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» [2], поэтому отсутствие их даёт право банку оставить запрос следователя без исполнения.

Основная проблема получения необходимой информации от подобных организаций – долгосрочность. Вышеуказанные лица и организации имеют право предоставить ответ на запрос в течение одного месяца со дня получения запроса или в период, указанный следователем. Как правило, предоставление необходимой информации для уголовного дела не позволяет следователю поймать, например, мошенников по «горячим следам», особенно если речь идет о мошенничестве в интернете, где промедление в расследовании даже в пару дней влечет полную нераскрываемость преступления.

Вопросы возникают и при определении объема предоставляемой информации. Следствие интересует информация о движении денежных средств между счетами клиентов**,** с указанием наименования, номеров счетов и ИНН контрагентов, БИК банков контрагентов, расшифровкой назначения платежа. Бывают случаи, когда банк отказывается предоставлять информацию полностью, ограничиваясь только непосредственно информацией о движении денежных средств в виду технических возможностей программного обеспечения в данный момент. Следователю предоставляют выписку в ограниченном виде, что делает подобное взаимодействие практически бесполезным. Ввиду того, что вышеуказанные сведения являются не дополнительной информацией по счету клиента, а обязательным реквизитом платежной операции, лицо, предоставившее подобный ответ на запрос, может быть привлечено к административной ответственности за предоставление информации должностному лицу в неполном объеме.

Такая информация, как правило, предоставляется в виде справок. Но когда следователю требуется истребовать в банке документы, содержащие информацию о счетах и вкладах клиентов, а также денежных переводах, то возникают проблемы. Во-первых, это уже оформляется не просто запросом, а целым следственным действием, что процессуально закрепляется как выемка и требует обязательного вынесения судебного решения. Во-вторых, сам процесс подготовки к данному следственному действию требует качественной подготовки и занимает немало времени. В-третьих, сам факт нахождения правоохранительных органов в банковском учреждении затрудняет его работу и привлекает достаточно много внимания общественности, в том числе СМИ.

Иногда следователи, пытаясь обойти судебное разрешение на производство выемки документов, делают запрос о предоставлении копий документов, содержащих информацию об счетах и вкладах клиентов, завуалировав это под обычное предоставление справки и мотивируя это отсутствием её четко установленной формы.

Отказ банка в предоставлении подобного рода информации в такой форме будет полностью правомерен:

– ни документы, ни их копии не являются справкой и должны предоставляться в рамках отдельного следственного действия;

– к материалам уголовного дела приобщаются либо подлинники документов, либо их заверенные копии, иначе такие доказательства будут признаны недопустимыми;

– понятие банковской тайны относится не к форме документа, а к его содержанию, ввиду постановление следователя о выемке таких документов без судебного решения не имеет законной силы.

Тем не менее, чтобы получить информацию о обстоятельствах, имеющих значение для уголовного дела, не всегда нужно прибегать к помощи банковских учреждений (за исключением информации, содержащей банковскую тайну). При расследовании преступлений экономической направленности правоохранительных органов интересует:

1) Информация о паспортных данных владельца банковской карты.

К персональным данным относится любая информация, относящаяся прямо или косвенно к какому-либо определенному или определяемому физическому лицу. Такие данные получить без согласия владельцев возможно в случаях, если владелец является участником в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах. Запрос в банк можно сделать в том случае, если известен расчетный счет преступника либо сохранился чек платежной операции. Тем не менее анонимность и использование подставных лиц, процветающих в интернете, значительно затрудняют установление личности преступника.

2) Информация о движении денежных средств по банковской карте и местах их обналичивания за последние полгода с указанием точного времени проведения приходных и расходных операций, номера и коды транзакций и др. Проанализировав полученную информацию за последние полгода, можно определить наиболее часто используемые банкоматы, которые, как показывает практика, находятся рядом с домом мошенника или местом частого посещения (работа, торговый центр, адрес родственников и т. д.), информацию о

регулярно оплачиваемых абонентских номерах (личный номер, номер родственников или друзей); а также о торговых точках или интернет-магазинах, на которых совершались покупки. Каждый интернет-магазин предоставит информацию об адресе мошенника, на который почтовым переводом был отправлен приобретенный товар.

3) Информация об абонентских номерах, привязанных к данной банковской карте услугой «мобильного банкинга», где и каким образом они были подключены. Даже не имея на телефоне онлайн-приложения соответствующего банка, клиенты в день могут переводить около 8000 руб. через смс, поэтому получить информацию о банковской карте можно просто по сим-карте. Но многие мошенники принимают денежные средства на счет абонентских номеров. Получить необходимую информацию о расчетных операциях по абонентским номерам «Билайн» можно направив запрос в самому оператору или ЗАО «Национальная сервисная компания», которая и проводит эти расчетные операции.

4) Информация об адресе офиса банка, в котором была открыта банковская карта. Подобную информацию можно узнать и без направления запросов, которые требуют долгосрочного исполнения. Так, при наличии банковской карты на руках у потерпевшего адрес банковского отделения будет закодирован на лицевой части карты в левом нижнем углу (первые четыре цифры обозначают регион, остальные именно код дополнительного офиса). Код полностью вводится в графе «Отделения и банкоматы» на официальном сайте банка, после чего откроется перечень необходимых отделений. Бывают случаи, когда мошенники заведомо сообщают потерпевшему ложные сведения о принадлежности карты к банку. Например, приходит сообщение, что денежные средства необходимо перевести на карту ВТБ, хотя карта по данному расчетному счету выпущена и обслуживается Сбербанком. Чтобы верно направить запрос и не терять драгоценное время в ожидании отрицательного ответа, следует проверять банковские карты на принадлежность. Это можно сделать с помощью БИНа банка, представляющим собой первые шесть цифр номера банковской карты. Существует множество интернет-сервисов, способных определить принадлежность данной банковской карты, например, www.binov.net и www.fraudassets.com.

5) Информация об IP-адресах, использованных для входа в онлайн-сервис по управлению данной банковской картой. Как известно, после любого преступления остаются следы. Так, в большинстве случаев мошенники открывают счета на подставных лиц для дальнейшего их использования в преступной деятельности, но использовать их лично для перевода денежных средств не могут, поэтому используют онлайн-ресурсы на официальном сайте соответствующего банка. При

первом же открытии интернет-страницы компьютеру выдается IP-адрес, уникальный именно для этого пользователя. Это и есть след данного преступления.

Таким образом, взаимодействие следователя с банковскими учреждениями не всегда вызывает необходимость. Обратившись за помощью в подобное учреждение, следователь должен соблюдать ряд требований, обусловливающих необходимость, мотивированность и законность получения информации и документов, имеющих значение при расследовании уголовных дел экономической направленности.

Список литературы

1. Гражданский кодекс Российской Федерации : Федеральный закон от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 20.04.2021).

2. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 20.04.2021).

3. Рудьман, Д. С. Доступ к банковской тайне органов внутренних дел / Д. С. Рудьман // Информационное право. – 2019. – № 1. – С. 14–17.

4. Плыкин, Ю. В. Определение местоположения пользователя по IP-адресу в сети интернет / Ю. В. Плыкин // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений. – Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2020. – С. 173.

5. Ткаченко, М. А. Особенности расследования мошенничества, совершенного в сети интернет / М. А. Ткаченко, О. А. Науменко // Краснодар-2019. АНО «Научно-исследовательский институт истории, экономики и права». – 2020. – С. 138–153.

Орлова А. А.[1]***,***
главный научный сотрудник
НИЦ № 5 ФГКУ «ВНИИ МВД России»,
доктор юридических наук, доцент

К ВОПРОСУ ОБ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Закономерный и неуклонный процесс развития информационно-телекоммуникационных технологий помимо позитивного влияния на все сферы жизнедеятельности общества и государства связан с рисками усугубления криминогенной ситуации ввиду значительного роста числа преступлений, совершаемых с их использованием.

Масштабы явления при неуклонном возрастании уровня преступности[2] на из-за отсутствия надлежащего государственного регулирования и контроля так называемой «виртуальной среды», повсеместного перехода на цифровые средства платежей свидетельствуют о наличии угрозы для государственной и общественной безопасности.

В сфере компьютерной информации или с использованием информационно-телекоммуникационных технологий совершается значительное число преступлений, сосредоточенных как в специальной главе 28 УК РФ, так и регламентированных в других статьях Уголовного кодекса. Это, например, составы преступлений, которые на первый взгляд не связаны с информационно-телекоммуникационными технологиями: склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110.1УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных, иных сообщений (ст. 138 УК РФ), нарушение авторских и смежных прав (ст. 146 УК РФ), вовлечение несовершеннолетних в совершение антиобщественных действий (ст. 151 УК РФ), вымогательство (ст. 163 УК РФ), нарушение правил оборота наркотических средств или психотропных веществ (ст. 228.2 УК РФ).

Согласно сведениям о состоянии преступности и результатах расследования преступлений, представляемым в разделе 11 ежемесячной формы отчетности

---

[1] © Орлова А. А., 2021.

[2] Так, по данным СД МВД России, начиная с 2013 г., уровень преступности в данной сфере увеличился более чем в 20 раз, а в 2019 г. Превысил показатели 2018 г. Почти в 2 раза. Отсутствием каких-либо позитивных изменений в указанной сфере отмечены периоды 20210 г. и первого квартала текущего года.

№ 4 ЕГС, в общей сложности таких составов преступлений насчитывается более 45 [3].

В ходе расследования преступлений в сфере информационно-телекоммуникационных технологий (компьютерной информации) возникают сложностей, обусловленные специфическими особенностями указанных деяний.

Так, значительное число преступлений совершается при отсутствии непосредственного контакта с потерпевшим и в условиях доступности практически неограниченного круга информации о гражданах.

Сложившаяся ситуация требует от органов уголовного судопроизводства поиска новых подходов к оптимизации процедуры раскрытия и расследования преступлений, что возможно только в рамках существующего правового регулирования, а необходимость его совершенствования по целому ряду направлений очевидна.

Решение вопросов о необходимости, целесообразности и содержании предполагаемых изменений уголовного и уголовно-процессуального закона требует взвешенного подхода, основанного на результатах анализа объективно обусловленных неполнотой правового регулирования сложностей правоприменительной практики и причин их возникновения.

Рассмотрим некоторые аспекты.

Например, дискуссионным остается вопрос о целесообразности дополнения ч. 3 ст. 158 УК РФ новым квалифицирующим обстоятельством совершения кражи – с банковского счета, а равно в отношении электронных денежных средств; о включении в ч. 3 ст. 159.6 УК РФ квалифицирующего признака, связанного с совершением компьютерного мошенничества в отношении электронных денежных средств и средств, находящихся на банковском счете потерпевшего [7].

В первом случае кража с банковского счета или в отношении электронных денежных средств с точки зрения общественной опасности по какой-то причине приравнена к краже, совершенной с незаконным проникновением в жилище, из нефтепровода, нефтепродуктопровода, газопровода, в крупном размене, а во втором случае не учтено содержание ч. 1 указанной нормы, а также и то, что ст. 159.6 УК РФ специально посвящена мошенничеству в сфере компьютерной информации.

Тем не менее некоторые проблемы заявили о себе уже с достаточной очевидностью.

Так, в юридической литературе справедливо отмечено, что правоприменитель часто сталкивается со сложностями в квалификации общественно опасных

деяний ввиду отсутствия надлежащего закрепления на законодательном уровне целого ряда понятий [5].

Отсутствие терминологической определенности приводит к необходимости использования в правоприменительной деятельности нормативных правовых актов, содержание которых непосредственно не связано с регулированием правоотношений в сфере уголовного судопроизводства [1]; к многообразию мнений по вопросу о конкретно определенном наименовании преступлений в сфере информационно-телекоммуникационных технологий [8]; к отсутствию унифицированного подхода к содержанию диспозиций уголовно-правовых норм, регламентирующих указанные преступления.

В процессе уголовного судопроизводства в соответствии с УПК РФ специально уполномоченные государственные органы и должностные лица, с одной стороны, доказывают обстоятельства совершения преступлений в сфере информационно-телекоммуникационных технологий (в сфере компьютерной информации), а с другой – используют информационно-телекоммуникационные технологии (компьютерную информацию) в процессе доказывания.

Анализ содержания ч. 2 ст. 74 УПК РФ, конкретизирующей перечень доказательств, в совокупности с содержанием ст. 164, 166, 167, 174, 180, 190, 193, 204, 205 УПК РФ и других свидетельствует о том, что ход и/или результаты процесса собирания доказательств фиксируется в протоколе, постановлении, заключении, ином документе.

Согласно ст. 474 УПК РФ процессуальные документы могут быть выполнены типографским, электронным или иным способом, они могут быть написаны от руки.

В условиях интенсивного развития и применения информационно-телекоммуникационных технологий, законодательная конструкция «электронным или иным способом» применительно к уголовному процессу во избежание расширительного толкования и неоднозначного понимания нуждается в конкретизации.

Практически во всех органах уголовного судопроизводства (за исключением возможно отсталых в техническом оснащении) для изготовления процессуальных документов применяются компьютеры, что свидетельствует об исполнении процессуальных документов электронным способом. Вместе с тем вопрос о том, что может подразумеваться под указанными в ст. 474 УПК РФ дефинициями остается открытым.

Необходимо учитывать, что при определенных условиях электронный документооборот допускается в суде (ч. 2 ст. 393, ст. 474.1 УПК РФ). Однако даже

если судебное решение изготовлено в форме электронного документа, дополнительно изготавливается экземпляр судебного решения на бумажном носителе.

Есть основания полагать, что указание закона об электронном и иных способах выполнения процессуальных документов не может свидетельствовать о возможном отказе от *концептуальных основ уголовного судопроизводства* – концентрации собранных в ходе расследования преступления доказательств (в том числе и с помощью технических средств) в материалах уголовного дела, представленных на бумажном носителе (с приложением фото, видеоматериалов, электронных носителей информации и т. д.).

Указанное обстоятельство представляется значимым во избежание скоропалительных фрагментарных изменений УПК РФ в части внедрения в правовое регулирование уголовного судопроизводства так называемых «электронных доказательств», реализации идей об «электронном уголовном деле» и др.

В сложившейся ситуации российский уголовный процесс не может избежать реформирования, например, в части оптимизации правового регулирования использования информационных технологий в процессе доказывания, расширения сферы действия электронного документооборота.

Назрела необходимость расширения применения и детальной регламентации возможностей видеоконференцсвязи, положительно зарекомендовавшей себя на судебных этапах уголовного судопроизводства (например, в ходе реализации положений ч. 6 ст. 35, ч. 4 ст. 240, ч. 6.1 ст. 241, ч. 1 ст. 293 УПК РФ и др.).

Нуждается в переосмыслении и приведении в соответствие с современными реалиями развития информационно-телекоммуникационных технологий содержание ст. 166 УПК РФ в части правового регулирования порядка составления протокола, применения технических средств и приобщения к протоколу соответствующих объектов.

Показателен и заслуживает внимания опыт США в осуществлении *по судебному решению* таких действий, как электронное наблюдение различных типов коммуникаций: «проводной связи», «устных переговоров», «электронных сообщений», «электронных систем связи» (понятие каждой из которых сформулировано конкретно в нормативных актах); видеонаблюдение в случаях, когда гражданин «рассчитывает на разумное ожидание конфиденциальности» [6].

Подводя итог изложенному, отметим, что развитие информационных технологий оказывает влияние на все сферы жизнедеятельности общества и государства, затрагивает правовые системы в мировом масштабе. При этом использование цифровых технологий в уголовном судопроизводстве различных государств

имеет свои специфические особенности, обусловленные концептуальными основами национального законодательства [6], что также необходимо учитывать при внесении необходимых изменений в законы, регламентирующие уголовное судопроизводство в Российской Федерации.

Список литературы

1. Федеральный закон от 27.07.2006 № 149 ФЗ (ред. от 29.12.2020) «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 20.04.2021).

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 20.04.2021).

3. Приказ Генеральной прокуратуры Российской Федерации от 17.01.2020 № 30 // СПС «КонсультантПлюс». – URL: https://base.garant.ru/73757032/ (дата обращения: 20.04.2021).

4. Гончар, В. В. О важности формирования единообразного понятийного аппарата, необходимого для расследования преступлений в сфере компьютерной информации / В. В. Гончар // Вестник экономической безопасности. – 2018. – № 1. – С. 225–230.

5. Евдокимов, К. Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации / К. Н. Евдокимов // Российский следователь. – 2015. – № 10. – С. 24–29.

6. Информационные технологии в уголовном процессе зарубежных стран : монография / под ред. С. В. Зуева. – М. : Юрлитинформ, 2020. – С. 17–18.

7. Рускевич, Е. А. Об избыточности и пробельности реформирования уголовного законодательства в целях обеспечения защиты цифровой экономики / Е. А. Рускевич // Пермский юридический альманах. – 2019. – № 1. – С. 708–715.

8. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В. С. Овчинский. – М. : Норма, 2017.

9. Федорович, В. Ю. Что такое киберпреступление? / В. Ю. Федорович // Вестник Московского университета МВД России. – 2020. – № 3. – С. 15–17.

Алейник М. В.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ НЕЗАКОННОГО РАСПРОСТРАНЕНИЯ НАРКОТИЧЕСКИХ СРЕДСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Изучение динамики совершенных преступлений, связанных с приобретением и сбытом наркотических веществ с использованием интернета, позволяет сделать вывод, что их количество растет с каждым годом. С развитием информационных технологий появляются все новые и новые способы совершения преступлений, предусмотренных ст. 228.1 «Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества» [1], что делает невозможным полноценно и точно оценить масштаб данных преступных деяний.

Проанализировав формы статистической отчетности, следует вывод, что сегодня они не содержат данных о количестве выявленных преступлений в сфере незаконного оборота наркотических средств с использованием интернета. Это позволяет отнести данные правонарушения к киберпреступлениям, которые имеют характерные особенности:

– в законодательстве отсутствует четкое понятие таких преступлений;

– ущерб, причиненный таким видом деятельности очень велик;

– вероятность вычисления и поимки преступника очень низкая;

---

[1]

– высокая латентность организаторов и администраторов темной стороны интернета;

– преступление может быть совершено в одной стране, а правонарушитель может находиться в другой.

Рассматривая проблемы оборота наркотических веществ в интернете, стало ясно, что имеется множество сайтов, содержащих информацию об обороте и употреблении наркотических средств. Из этого можно сделать вывод, что данные сайты делаться по определенным группам. Например, существуют интернет-страницы, на которых изложены исследовательские работы медицинских учреждений о последствиях употребления наркотических средств. Вторая группа – сайты, владельцы которых продают легальные психоактивные вещества. Их нельзя назвать наркоторговцами, так как они не осуществляют незаконную деятельность, их товар относится к растительным субстанциям (этноботаника), и они преследуют чисто коммерческие интересы. К третьей, самой многочисленной, группе относятся сайты или форумы, на которых люди высказывают свое мнение о наркотических веществах, их употреблении, о своем состоянии во время приема тех или иных психотропных веществ. Четвертой группой, и самой опасной, являются сайты, которые нелегально распространяют и рекламируют наркотические вещества, например интернет-магазин в каталоге которого можно выбрать и заказать запрещенное вещество посредством общения так называемых «покупателя» и «продавца» в онлайн режиме [2].

В настоящее время самой популярной в мире платформой для приобретения и сбыта наркотических веществ является российская «HYDRA». Согласно исследованиям, каждый день в России делаются «закладки» (расшифровка – тайник с наркотическим средством для дальнейшего сбыта) наркотиков на 227 млн руб. Самый пугающий факт – это то, что «кладменами» (расшифровка: люди, делающие «закладки») являются граждане от 17 до 25 лет. Это обусловлено тем, что люди данной возрастной группы проявляют любопытство к наркотикам и в силу несформированности личности оказываются под давлением взрослых, имеют регулярный доступ к интернету и ищут легкий способ заработать денег [3]. Все это привлекает внимание правоохранительных органов. Но расследование преступлений и поимка виновных лиц в данной сфере, пока не дают желаемого результата. Это связанно с отсутствием специализированного ведомственного подразделения, деятельность которого была бы направлена исключительно на раскрытие преступлений, связанных с приобретением и оборотом наркотических

средств в интернете. Острая проблема и постоянное совершенствование информационных технологий, методов и способов совершения преступлений и их сложность.

В практике наиболее часто встречаются:

1. Шифрование и сокрытие электронной информации о предстоящих поставках наркотических веществ. Преступники осуществляют это путем кодирования сообщений, которые содержат координаты мест «закладок», данные банковских счетов, используют неконтролируемые средства связи – факсы, пейджеры, спутниковые телефоны.

2. Отмывание доходов, полученных от продажи наркотических веществ с помощью переводов денежных средств через интернет. Данный способ преступники используют из-за быстроты совершения сделки, свободного доступа и скрытности [4].

3. Противодействие правоохранительным органам при проведении оперативно-следственных мероприятий. Злоумышленники устанавливают на свой компьютер вредоносные программы, при попытке взлома которых происходит ответное хакерство и причиняется ущерб.

Следователи должны учитывать, что эти преступления характеризуются высокой степенью латентности, сложностью в сборе доказательств и поиске преступников. Для выявления и раскрытия преступлений, связанных с распространением наркотических веществ, необходимы специальные навыки и высокий уровень технической оснащенности сотрудников правоохранительных органов. Спецификой расследования данных уголовных дел являются сбор доказательственной базы и проведение оперативно-следственных мероприятий: осмотр, обыск, выемка, экспертиза в кротчайшие сроки. Это обусловлено тем, что при совершении такого рода преступлений злоумышленники используют в качестве орудий телефоны, компьютеры на которых может находиться информация, имеющая доказательственное значение.

Другим важным аспектом для расследования уголовных дел является выявление сайтов, которые размещают информацию о продаже наркотических веществ и способах их изготовления, потому что латентность таких действий очень высока. Самый эффективный способ борьбы с распространением наркотиков через интернет для правоохранительных органов – оперативно-поисковая деятельность, т. е. постоянный мониторинг интернет-пространства, своевременное реагирование на подозрительную активность в социальных сетях среди молодого населения, использование информационных технологий для обнаружения рекламы наркотических средств.

Таким образом, постоянное совершенствование и колоссальные масштабы незаконного распространения наркотических средств с использованием интернета требуют от правоохранительных органов повышения эффективности борьбы с данным видом преступления, подготовки кадров, специализирующихся на киберпреступлениях и своевременного реагирования на действия наркодиллеров в интернет-пространстве.

Список литературы

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (принят Государственной Думой 24 мая 1996 года, одобрен Советом Федерации 5 июня 1996, в ред. от 24.02.2021г.) // СПС «КонсультантПлюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.04.2021).

2. Григорян, Д. К. Актуальные угрозы современной молодежи: новые технологии распространения наркотических средств / Д. К. Григорян // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2015. – № 8 (63). – С. 61–65.

3. Сидоров, П. Г. Распространение наркотических средств среди молодежи высших и средних профессиональных образовательных учреждений: социологическое измерение / П. Г. Сидоров, Н. М. Байков; под ред. Н. М. Байкова, ДВИПК ФСКН России. – Хабаровск, 2012.

4. Киселев, А. В. Социально-информационные аспекты профилактики распространения наркотических средств и психотропных веществ в телекоммуникационной сети Интернет / А. В. Киселев, К. А. Борисенко // Социальные отношения. – 2019. – № 1 (28). – С. 71.

Сумкин Е. А.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Рост информационных технологий как на территории Российской Федерации, так и во всем мире, обусловил не только быстрое развитие и эффективное применение информационных сетей для достижения различных целей, в частности: 1) дистанционный формат обучения; 2) повышение масштабов предпринимательской деятельности; 3) доступ ко всевозможным источникам информации; 4) повышение качества и удобства коммуникаций между людьми и т. д., но и появление новых угроз со стороны киберпреступников. Анонимность пользователей в информационной среде является почвой, которую используют киберпреступники для достижения своего преступного результата.

Информационно-телекоммуникационные технологии в настоящее время стремительно внедряются во все сферы общественных отношений, а законодательные и правоохранительные органы не успевают за таким быстротечным развитием.

В 2020 г. произошла вспышка болезни COVID – 19, и все государства перешли на дистанционный формат деятельности различных предприятий, госучреждений, школ и университетов. В связи с этим информационное пространство стало пополняться различным развлекательным и учебным контентном, но это позволило киберпреступникам совершать еще большее количество злодеяний,

оставаясь не пойманными. Уровень киберпреступности достиг 461 тыс. преступлений, это не окончательно, поскольку большее количество преступлений имеют латентный характер [4].

Проблема киберпреступности имеет два компонента. Во-первых, киберпространство постоянно пополняется новыми видами преступлений, новыми способами совершения уже имеющихся видов преступлений. Во-вторых, в информационном пространстве постоянно совершаются уже криминализированные в Уголовном кодексе РФ: хищения денежных средств, торговля наркотическими и психотропными веществами, торговля оружием и неправомерный доступ к конфиденциальным данным как рядовых граждан, так и государственных корпораций.

Для подробного рассмотрения современных проблем киберпреступности определим понятие данного вида преступлений. *Киберпреступность* – это преступность в киберпространстве. Авторы «модельного закона» о киберпреступности Международного союза электросвязи определяют киберпространство как «физическое или не физическое пространство, созданное или сформированное следующим образом: компьютеры, компьютерные системы, сети, компьютерные программы, данные, движение данных и пользователей». То есть киберпреступность имеет настолько большие масштабы, что позволяет преступникам использовать киберпространство различными методами и способами.

В современных реалиях борьба с киберпреступлениями является ключевой задачей для правоохранительных органов нашего государства, но выполнение невозможно без решения существующих проблем, которые не позволяют правоохранительным органам должным образом бороться с данным видом преступлений.

Среди основных проблем противодействия киберпреступности стоит отметить такие, как [2]:

1. Отсутствие механизмов контроля. Основная и ключевая проблема – анонимность пользователей компьютерными технологиями, что существенно облегчает преступникам совершать киберпреступления и чувствуя себя как «рыба в воде». Имея тенденцию на постоянное совершенствование и проникая во всех сферы общественных отношений, осуществлять контроль и своевременное реагирование на факты киберпреступности остается достаточно сложной задачей.

2. Автоматизация и быстрота использования. Компьютерные данные могут одномоментно быть переданы из одной точки мира до другой, поэтому контролировать передачу данных с учетом их количества и объема практически невозможно.

3. Проблема территориальной юрисдикции в киберпространстве и вопросов сотрудничества между государствами. Расследование преступлений в киберпространстве обычно требует быстрого реагирования со стороны правоохранительных органов, чтобы сохранить весь массив доказательственной базы. Помимо этого, киберпространство требует сотрудничества между различными государствами, которые, например, могут осуществить выдачу преступника или предоставить доказательственную информацию о совершенном киберпреступлении. Но процесс сотрудничества в настоящее время нахождении на низком уровне и существенно влияет на качество и сроки расследования по данным уголовным делам.

4. Слабый уровень технической оснащенности ОВД, критически низкий уровень специалистов в области информационных и телекоммуникационных технологий. Данный аспект существенно влияет на расследование киберпреступлений, поскольку правоохранительные органы нашего государства не имеют достаточно хорошего и своевременного оборудования, компьютерной техники, а также специалистов, имеющих определенные знания в сфере компьютерных технологий, которые позволили бы существенно повысить эффективность расследования, а также эффективно реагировать на данные виды преступлений.

Таким образом, большое количество проблем связаны с противодействием и расследованием киберпреступлений, решение которых возможно лишь с улучшением взаимоотношением Российской Федерации с другими государствами, а также повышением качества рабочих условий в правоохранительных органах, обеспечением своевременными технологиями, которые позволили бы эффективнее расследовать преступления рассматриваемой категории.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изм., одоб. и в ходе общероссийского голосования 01.07.2020) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 20.04.2021).

2. Погебайло, А. Э. Борьба с киберпреступностью : учебное пособие / А. Э. Погебайло. – М. : Ун-т прокуратуры Рос. Федерации, 2019.

3. Карпова, Д. Н., Киберпреступность: глобальная проблема и ее решение / Д. Н. Карпова. – М., 2014.

4. Официальный сайт Генпрокуратуры Российской Федерации. – URL: http://crimestat.ru/offenses_chart (дата обращения: 20.04.2021).

Макаров А. А.[1]*,*
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

НЕКОТОРЫЕ ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ ОРУЖИЯ, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ DARKNET

Актуальность темы данной статьи заключается в том, что вопрос, связанный с незаконным оборотом оружия в нашей стране не теряет остроты уже долгие годы. Конечно, сравнивая современное состояние преступности, например, с периодом конца 80-х–90-х годов прошлого века, и уж тем более с ситуацией конца 40-х годов (т. е. с периодом после окончания Великой Отечественной войны) становится очевидно, что размах преступлений в данной сфере значительно снизился.

Но, несмотря, на то, что объемы оборота нелегального оружия значительно снизились, в данной ситуации есть и обратная сторона. Прежде незаконная торговля оружием происходила примерно по одним и тем же схемам, которые не менялись десятилетия.

Как правило, были три пути поставки оружия:

– поставки так называемого списанного оружия с различных силовых ведомств (армия, ФСБ России, МВД России и т. д.) недобросовестными сотрудниками, ответственными за ликвидацию данного оружия;

– поставки оружия либо с локальных военных конфликтов, либо же из стран «третьего мира», где контроль за оборотом оружия отсутствует;

[1] © Макаров А. А., 2021.

– либо хищение различных деталей оружия с заводов по его изготовлению и последующая его сборка в нелегальных оружейных мастерских, либо создание подпольных оружейных заводов (данный способ встречался довольно редко ввиду у сложности его реализации).

Таким образом, благодаря относительной неизменности способов совершения преступлений сфере незаконного оборота оружия, которые были хорошо известны сотрудникам правоохранительных органов, удалось добиться значительного сокращения незаконного оборота оружия в начале 2000-х годов.

Но в настоящее время складывается ситуация, когда большинство преступлений совершается с использованием интернета, причем не обще пользовательской, а так называемой «темной» стороны мировой паутины, *DarkNet*, что в буквальном переводе означает «темный интернет». И тогда возникают многочисленные сложности с выявлением и расследованием данных преступлений, поскольку сотрудники правоохранительных органов, не располагают ни достаточными знаниями, ни материально-технической базой для выявления и расследования таких типов преступлений.

Что же такое *DarkNet* и как с его помощью совершаются преступления связанные с незаконным оборотом огнестрельного оружия?

Итак, *DarkNet*, также известный как «Скрытая сеть», «Тёмная сеть», «Теневая сеть», «Тёмный веб», – скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов. Анонимная сеть представляет собой систему не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

DarkNet отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства. Именно поэтому даркнет часто воспринимается как инструмент для осуществления коммуникации в различного рода подпольях и незаконной деятельности. В более общем смысле термин «*DarkNet*» может быть использован для описания некоммерческих «узлов» интернета или относиться ко всем «подпольным» интернет-коммуникациям и технологиям, которые связаны с незаконной деятельностью или инакомыслием [1].

Основные проблемы при раскрытии преступлений, совершенных с его помощью, заключаются в том, что сотрудники правоохранительных органов в большинстве случаев даже не подозревают о совершающихся преступлениях, а в тех немногочисленных случаях, когда все-таки имеется оперативная

информация о готовящемся или совершенном преступлении, не в состоянии обнаружить ни отправителя нелегального оружия, ни его получателя. Поэтому для раскрытия подобных преступлений сотрудникам правоохранительных органов необходимо каким-либо образом устранить факт анонимности при совершении сделок по продаже нелегального оружия.

Несмотря на то, что сотрудники правоохранительных органов не способны раскрывать преступления совершаемые в *DarkNet*, все-таки определенные наработки в этой области имеются, например:

1. Постоянный мониторинг интернета средствами поисковых сервисов, осуществляемый оперативными сотрудниками, который позволяет обнаруживать интернет-магазины, осуществляющие незаконный оборот оружия и боеприпасов, затем через электронное обращение направлять материалы в Роскомнадзор и впоследствии блокировать такие ресурсы на уровне провайдеров. Но такой способ трудозатратный, длительный и зависит от человеческого фактора. Поэтому использование автоматизированных систем мониторинга интернет-пространства способствовало бы более эффективному решению обозначенной проблемы. Для блокирования доступа пользователей интернета к противоправному контенту также было бы целесообразным более активное содействие отечественных поисковых сервисов (Yandex, Rambler, Mail).

2. Исключение из выдачи ссылок на ресурсы, содержащие незаконные материалы, были бы профилактическим и подрывающим противоправный бизнес воздействием. Помимо предупредительных и профилактических мер правоохранительные органы реализуют и другие мероприятия по раскрытию преступлений, совершаемых посредством интернета: обнаружение устройств, с помощью которых осуществлялись противоправные действия или которыми пользовались злоумышленники в качестве средств коммуникации. К таким сетевым устройствам относятся мобильные телефоны, смартфоны, планшеты, компьютеры и их периферия, банкоматы и др. Основной идентифицирующий признак устройства в интернете – его сетевой адрес (IP-адрес). Кроме IP-адреса, в основном использующегося для глобальной маршрутизации, сетевой интерфейс имеет физический адрес (так называемый MAC-адрес). IP-адрес назначается сетевому интерфейсу интернет-провайдером абонента, а MAC-адрес производителем оборудования.

Зачастую продавцов оружия находят вне *DarkNet*. Продажу незаконного товара они организовывают через *Tor*, но поиском клиентов они могут заниматься через обычные социальные сети. Полиция находит «пиарщиков», через которых выходит и на торговцев. Помимо этого практикуется и работа под

прикрытием, когда полицейские агенты на время становятся участниками незаконного рынка и втираются в доверие к модераторам сайтов, и массовые DDoSатаки на запрещенные сайты, обеспечивающие взлом данных торговцев. Как итог – массовые аресты участников рынка.

Попытка Роскомнадзора научиться взламывать и блокировать сайты, где осуществляется продажа оружия и боеприпасов в *Tor* – лишь один из методов борьбы с незаконным рынком, который уже сегодня обрел грандиозные масштабы. Однако полностью ликвидировать рынок пока практически невозможно.

Наиболее распространенные криминальные рынки – незаконное производство оружия, а также оборот оружия, ВВ и ВУ через интернет, поэтому необходим комплекс профилактических, технических и оперативно-разыскных мероприятий, направленных на выявление и изъятие из незаконного оборота оружия взрывчатых веществ и взрывчатых устройств совместно с подразделениями МВД России, Росгвардии, ФТС России и ФСБ России [2].

Список литературы

1. Википедия. – URL: https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82 (дата обращения: 20.04.2021).

2. Научная электронная библиотека «КиберЛенинка». – URL: https://cyberleninka.ru/article/n/osobennosti-raskrytiya-prestupleniy-i-vyyavlenie-lits-osuschestvlyayuschih-sbyt-ognestrelnogo-oruzhiya-boepripasov-vzryvchatyh/viewer (дата обращения: 20.04.2021).

Акимов В. Н.[1]*,*
студент кафедры «Цифровые технологии
и информационные системы»
Московского авиационного института
(национальный исследовательский университет)

Максимов Н. А.[2]*,*
доцент кафедры «Цифровые технологии
и информационные системы»
Московского авиационного института
(национальный исследовательский университет)

СИСТЕМА КЛАССИФИКАЦИИ ТРАНСПОРТНЫХ СРЕДСТВ ПО ВИЗУАЛЬНЫМ ХАРАКТЕРИСТИКАМ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ

Классификация объектов всегда была важной задачей во всех областях деятельности, в том числе и в работе органов внутренних дел. Появление камер на улицах, снимающих текущую обстановку на трассах и на улицах городов, привело к возникновению огромного количества визуальной информации, которая для эффективного ее использования требует обработки. Но развитие транспорта привело к их значительному разнообразию не только по видам, но и по моделям. Вместе с тем и возросла потребность в их автоматической классификации.

Рассмотрим разработку интегрируемой в систему компьютерного зрения модели классификации транспортных средств по визуальным характеристикам (цифровым изображениям с видеокамер или спутниковых снимков) на основе алгоритмов глубокого обучения. На вход модели подается одно или несколько изображений любых транспортных средств под любыми углами обзора. На выходе модели нужно определять название предсказанной модели автотранспорта и вероятности принадлежности к каждому известному классу модели. Для решения этой задачи было принято решение разбить этап разработки на несколько этапов:

1. Сбор необходимой выборки для обучения модели нейронной сети.
2. Разработка архитектуры модели и выбор инструментария.
3. Программная реализация архитектуры.

---

4. Обучение модели. Подбор гиперпараметров.

5. Проверка результатов на тестовых данных.

6. Вывод модели в приложение для возможности тестирования в реальном времени.

Этап сбора выборки

При подборе выборки были установлены следующие задачи: количество изображений по каждому классу должно быть приблизительно одинаковым, выборка должна содержать разнообразные фотографии транспортных средств со всех возможных углов, все изображения должны быть корректно размечены.

Для поставленной задачи с открытых веб-ресурсов [1] [2] [3] было собрано 17 882 изображений 91 модели различных транспортных средств, из них: 11402 – обучающая выборка, 2851 – проверочная и 3568 – тестовая выборка.

Разработка архитектуры нейронной сети

В качестве основных технологий использовались: перенос обучения и тонкая настройка сети.

Перенос обучения (*Transfer learning*) [4] – это подраздел машинного обучения, цель которого – применение знаний, полученные из одной задачи, к другой целевой задаче. Данный метод позволяет использовать предварительно обученные на других задачах модели для решения текущих задач.

Тонкая настройка (*Fine-tuning*) [5] – подход, используемый в комбинации с переносом обучения, суть которого заключается в итеративном процессе «размораживания» последних слоев нейронной сети и их обучении.

Процедура тонкой настройки состоит из следующих этапов:

– заморозка всех слоев предварительно обученной модели;

– добавление своих слои к обученной модели;

– обучение добавленных слоев;

– размораживание нескольких верхних слоев;

– обучение этих слоев и добавленной части вместе.

В качестве базовой модели для применения переноса обучения была выбрана архитектура *DenseNet*. Основные особенности данной архитектуры:

1. Сеть состоит из «dense» блоков, представляющих из себя комбинацию из n слоев свертки.

2. В каждом «dense» блоке объединяются карты признаков всех предшествующих слоев блока.

3. Количество блоков свертки k в каждом слое блока называется темпом роста сети *DenseNet* и регулирует, сколько новой информации каждый слой вносит в глобальное состояние сети.

4. Благодаря своей архитектуре сеть имеет вдвое меньше параметров, нежели ее вдохновитель *ResNet*.

Реализация *DenseNet*, используемая в данной работе – *DenseNet-20*, обладает следующими характеристиками:

– состоит из 4 «*dense*» блоков, соединенных переходными слоями;

– темп роста внутри одного «dense» блока – 6, 12, 48 и 32 соответственно;

– количество слоев сети: 707;

– количество обучаемых параметров сети: 18 092 928.

В ходе создания архитектуры сети было принято решение использовать функцию активации из семейства «tanhsoft» [6]:

$f(x; \alpha, \beta, \gamma, \delta) = tanh(\alpha x + \beta e^{\gamma x}) \ln(\delta + e^{x})$

В работе использована следующая функция активации:

$f(x) = x*tanh(\ln(1+e^{x}))$

В итоге разработана следующая архитектура нейронной сети:

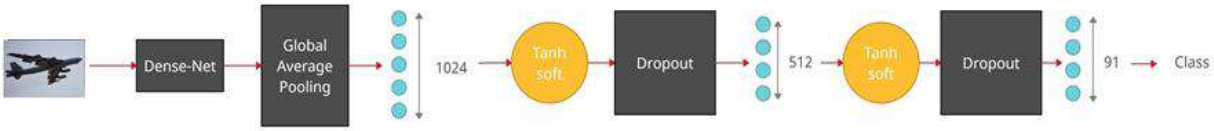


Рис. 1. Архитектура нейронной сети

Архитектура состоит из базовой нейронной сети *DenseNet-201*, входного и среднего слоя из 1024 и 512 нейронов соответственно с функцией активации «*tanhsoft*» и выходного слоя, содержащего 91 нейрон.

На вход модели попадает изображение, которое поступает на вход базовой сети *DenseNet-201*. Значения, полученные на выходе сети преобразуются в одномерный вектор размера 1024 с помощью *Global Average Pooling* и подается на вход первому слою. Сигналы нейронов проходят функцию «*tanhsoft*», после чего происходит исключение (*dropout*) нейронов. Оставшиеся выходы попадают на следующий слой, состоящий из 512 нейронов. Операция повторяется один раз, чтобы получить в итоге 91 сигнал нейронов. Каждому сигналу соответствует свой класс транспортного средства.

Оценка качества модели

В качестве параметра для оценки модели была выбрана средняя точность на тестовой выборке. За начальные параметры были взяты показатели: размер изоб-

ражения, стартовый темп обучения и функция активации. Для сравнения функций активации использовалась функция «*relu*», близкая по форме, но уступающая по многим показателям функции «*tanhsoft*». Время на обработку одного изображения во всех экспериментах составило 0,68 секунды с разницей в сотых долях секунды. Результаты оценки качества приведены в табл. 1.

Таблица 1

Оценка качества модели

Номер эксперимента	**Размер входного изображения**	**Стартовый темп обучения**	**Функция активации полно-связных слоев**	**Средняя точность на тестовой выборке**
1	(256, 256)	10^{-4}	relu	0.8509
2	(256, 256)	10^{-4}	tanhsoft	0.8918
3	(350, 350)	10^{-5}	relu	0.9092
4	(350, 350)	10^{-5}	tanhsoft	0.9233
5	(350, 350)	10^{-6}	tanhsoft	0.9389

Как видно из результатов оценки, на точность модели влияет размер входного изображения и начальный темп обучения, а функция активации «*relu*» уступает выбранной в работе функции «*tanhsoft*».

Программная реализация

Для взаимодействия с моделью был разработан веб-интерфейс, принимающий http-запросы, содержащие одно или несколько изображений и выдающий результаты в режиме реального времени. Это позволяет развертывать систему, как на локальной машине, так и на удаленном сервере. В качестве результатов в теле ответа передается код класса, вероятность принадлежности этому классу и нормализованный коэффициент эксцесса по всем вероятностям, полученным на выходе нейронной сети. Нормализованный коэффициент эксцесса по вероятностям принадлежности позволяет делать более точное суждение о принадлежности транспортного средства определенному классу. Низкое значение этого параметра означает, что среди выходных нейронов модели вместо одного оказалось несколько сигналов высокой силы, что в свою очередь говорит о плохом восприятии сетью подаваемого изображения.

В результате работы была создана модель, осуществляющая распознавание типов транспортных средств в реальном времени. Полученная модель устойчива

к углам съемки и окраске автотранспорта. Достигнутая средняя точность модели на тестовой выборке: 94%. Среднее время распознавания одного кадра – 0,68 сек.

Среди перспектив дальнейшего развития данной системы можно отметить увеличение перечня определяемых классов новыми моделями транспорта, сведение задачи классификации к задаче детектирования и создание трехмерной модели полигона с дальнейшим тестированием системы в виртуальной среде.

Список литературы

1. Airfighters – Military Aircraft Photos. – URL: http://airfighters.com/ (дата обращения: 20.03.2021).

2. Airplane pictures – creative aviation photography. – URL: http://airplane-pictures.net (дата обращения: 21.03.2021).

3. Fine-Grained Visual Classification of Aircraft, S. Maji, J. Kannala, E. Rahtu, M. Blaschko, A. Vedaldi, arXiv.org, 2013. – URL: https://paperswithcode.com/dataset/fgvc-aircraft-1(дата обращения: 24.03.2021).

4. A Comprehensive Hands-on Guide to Transfer Learning with Real-World Applications in Deep Learning. – URL: https://towardsdatascience.com/a-comprehensive-hands-on-guide-to-transfer-learning-with-real-world-applications-in-deep-learning-212bf3b2f27a (дата обращения: 02.04.2021).

5. A Comprehensive guide to Fine-tuning Deep Learning Models in Keras (Part I). – URL: https://flyyufelix.github.io/2016/10/03/fine-tuning-in-keras-part1.html – (дата обращения: 05.04.2021).

6. TanhSoft – a family of activation functions combining Tanh and Softplus. – URL: https://deepai.org/publication/tanhsoft-a-family-of-activation-functions-combining-tanh-and-softplus (дата обращения: 07.04.2021).

Катенко Ю. В.[1]*,*
аналитик ООО «БалтИнфоКом»

ПОДХОД К КЛАССИФИКАЦИИ МЕСТ, ПОСЕЩЕННЫХ АБОНЕНТОМ СОТОВОЙ СВЯЗИ

Система геоинформационного анализа фактографической информации «Следопыт» предназначена для анализа данных, полученных из разных источников, она позволяет извлекать факты из детализаций сеансов абонентов сотовой связи. Запись детализации состоит из идентификаторов абонента и собеседника, идентификаторов и координат базовой станции, даты и времени, типа, направления и длительности сеанса. Такие данные дают возможность выявлять шаблоны в поведении абонента и классифицировать места, которые он посещает.

Кластеризация базовых станций

Базовые станции располагаются недалеко друг от друга, и сеансы, совершенные в одном месте, обрабатываются разными базовыми станциями. Если идентификатор базовой станции используется в качестве идентификатора места, такие сеансы рассматриваются отдельно, что может помешать правильно определить классы мест. Чтобы этого избежать, нужно объединять базовые станции в кластеры, основываясь на расстоянии между ними.

В качестве алгоритма кластерного анализа был выбран DBSCAN (*Density-based spatial clustering of applications with noise*) – метод кластеризации, группирующий такие точки, которые расположены близко друг к другу, и помечает как выбросы точки, находящиеся в областях с малой плотностью [1]. Алгоритм имеет один входной параметр – радиус окрестности точки ε. Точки считаются соседними, если расстояние между ними не больше ε. Расстояние в данной задаче в соответствии с природой данных вычисляется по формуле гаверсина. Для оценки качества кластеризации был использован коэффициент силуэт, который вычисляется по формуле 1 и может принимать значения от –1 (неправильная кластеризация) до 1 (наилучшее разбиение) [2]. В данной работе был достигнут силуэт, равный 0,81.

$$s = \frac{1}{n}\sum_{i}^{n}\frac{b_i - a_i}{max(a_i, b_i)} \qquad (1)$$

где: a_i – среднее расстояние между объектом и другим элементами кластера,

b – среднее расстояние между объектом и всеми элементами ближайшего другого кластера.

---

[1] © Катенко Ю. В., 2021.

Определение классов мест

На первом этапе классификации для всех мест, где совершались сеансы, строится матрица с распределением сеансов по дням. В этой матрице выбирается строка с наибольшим числом ненулевых значений, – она соответствует месту, где сеансы совершались наибольшее количество дней, это место помечается как «Дом». Места, соответствующие строкам с единственным ненулевым значением, получают метку «Единичный визит».

Для оставшихся мест строится матрица с распределением сеансов по часам (пример см. рис. 1). Место, где было совершено больше всего сеансов с 11:00 до 18:00 в разные дни, помечается как «Работа».

hour	11	12	13	14	15	16	17	19	20	21
base_station_id										
GSM;0;0;400;12783	1	4	0	0	0	0	0	0	0	0
GSM;0;0;400;14081	0	0	1	0	0	0	0	0	0	0
GSM;0;0;400;14084	1	3	1	2	0	4	6	3	0	2
GSM;0;0;400;1916	0	0	0	0	2	0	0	0	0	0

Рис. 1. Распределение сеансов абонента по базовым станциям в разные часы

Далее находятся «Транзитные места» – это места, находящиеся в прямоугольной области между домой и работой (см. рис. 2) и посещаемые в утренние и вечерние часы. Остальные места получают метку «Повторяющееся место».

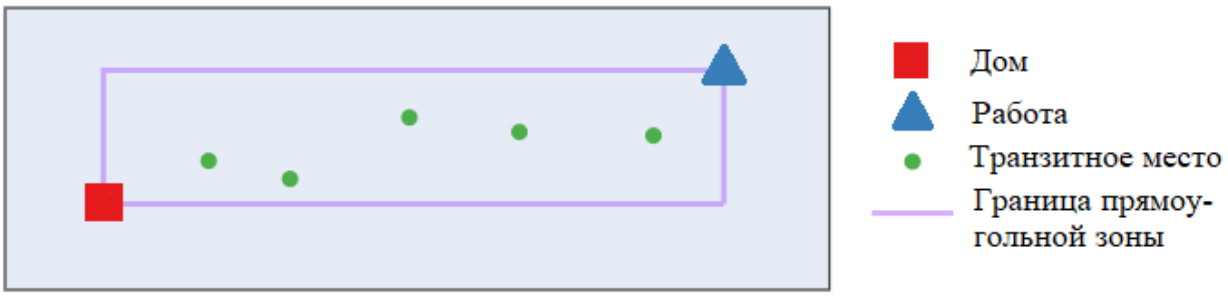


Рис. 2. Расположение «Транзитных мест» относительно «Дома» и «Работы»

Дальнейшая работа по улучшению классификации мест направлена на выявление паттернов в поведении абонента – графиков работы, шаблонов посещения повторяющихся мест. Планируется сопоставить посещаемые места с адресным справочником, что позволит уточнить класс некоторых мест (это касается крупных точек притяжения – университетов, торговых центров, концертных залов и т. д.).

Классификация мест в различные временные промежутки (например, с разделением детализаций по месяцам) позволяет выявлять такие изменения, как переезд абонента или смена работы.

Список литературы

1. Martin Ester, Hans-Peter Kriegel, Jörg Sander, Xiaowei Xu. A density-based algorithm for discovering clusters in large spatial databases with noise // Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96). AAAI Press, 1996. – С. 226–231.

2. Michael R. Brzustowicz. Data Science with Java. O'Reilly Media Publ., 2017. – 236 p.

Бородкина Т. Н.[1]*,*
доцент кафедры предварительного расследования
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ПРОБЛЕМЫ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И ИНФОРМАЦИОННОГО ОБСЛУЖИВАНИЯ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ГРАЖДАН

Информация и научные знания выходят на первый план в системе жизненных ценностей. Создание в пределах большой территории России единой системы телекоммуникационной системы, объединяющей разные информационные технологии, обеспечивая потребителям доступ к информации, способствует решению экономических, энергетических, коммуникационных, управленческих и других задач.

Информационные технологии, выполняя исключительную роль в обеспечении информационного взаимодействия между людьми, являясь составляющими элементами прочих более сложных производственных и социальных процессов, служат для оптимизации в целом информационного пространства.

«Информационные технологии» – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (ст. 2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации») [3].

Процесс собирания, аккумуляции, сохранения, автопоиска, распространения информации осуществляется с помощью информационных систем, банков данных и их сетей. Сведения, используемые в органах внутренних дел, включают данные: о состоянии преступности и общественного порядка; о лицах, совершивших преступления и административные правонарушения; о владельцах огнестрельного оружия; о собственниках авто-, мототранспортных средств; об изъятых вещах, антиквариате, и другие сведения, подлежащие сохранению.

В работе правоохранительных органов применяется как стандартное программное обеспечение, так и специального назначения. Программы специального назначения нацелены на их применение при производстве оперативно-разыскных мероприятий в борьбе, например с киберпреступностью.

Совокупность взаимосвязанных компонентов, таких как информационное (аккумуляция, обработка и направление информации государственным органам и гражданам) и аналитическое обеспечение (исследование преступлений; выявление обстоятельств, влияющих на формирование обстановки; прогнозирование ее изменений), составляет обеспечение информационной работы правоохранительных органов.

Расширился и круг лиц, заинтересованных в истребовании сведений, аккумулирующихся в правоохранительных органах. В настоящее время ее используют органы прокуратуры, сотрудники органов внутренних дел, Федеральная служба безопасности Российской Федерации, финансовые и коммерческие структуры, сотрудники налоговой, таможенной службы, администрации субъектов страны.

Положительное влияние от создания единого информационного пространства очевидно. Как отмечает А. А. Городнова, «информационное общество поможет улучшить администрирование, «транслируя» эффективные методы управления в другие области и города» [1, с. 75].

Андреев Н.С. дает определение термину «единое информационное пространство», которое представляется как «совокупность разнонаправленных информационных потоков государства, … и напрямую зависящих от средств получения, передачи, обработки и хранения информации» [2, с. 14]. Автор рассматривает данное понятие в более широком понимании.

Следует отметить, что многие регионы создают региональные информационные системы, но эти процессы еще не авторизованы в единую систему. Внедряемые системы нередко воплощают собственный язык программирования, потоки и форматы данных; индивидуальные и в то же время разные решения в выборе технических средств. Представляется, что это может создать в будущем проблемы в реализации единого информационного пространства (перебои в работе баз, предоставление недостоверных или не полных сведений и т. д.).

Полагаю, что для обеспечения государственных органов и граждан достоверной и полной справочной информацией, аккумулирующейся в базах правоохранительных органов, необходимо создание единой, созданной на всех уровнях, системы информационного обслуживания.

Список литературы

1. Городнова, А. А. Развитие информационного общества: учебник и практикум / А. А. Городнова. – М. : Юрайт, 2017.

2. Андреев, Н. С. Единое информационное пространство Российского государства: взаимодействие печатных и электронных СМИ : автореф. … канд. полит. наук / Н. С. Андреев. – СПб., 2005.

3. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации» // СПС «КонсультантПлюс». Раздел «Законодательство». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 17.04.2021).

Мокия В. Р.[1]*,*
курсант факультета подготовки
сотрудников полиции по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Смирнов В. М.,
старший преподаватель кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 НА РЕЗКИЙ РОСТ ЧИСЛА КИБЕРПРЕСТУПНОСТИ

В связи с развитием компьютерных технологий, увеличивается количество преступлений в информационной сфере, но в период пандемии COVID-19 количество таких преступлений начало резко расти. Для решения проблемы роста киберпреступности было предпринято ряд мер, одна из них – совершенствования нормативной правовой базы, законов, которые регламентируют общественные отношения в информационной сфере. В настоящее время проходит работа по формированию и развитию национальной защищённости информационной безопасности в России.

Исходя из статистики в период пандемии в Российской Федерации возросла преступность в информационной сфере. В связи с тем, что было принято решение о переводе на дистанционную работу большего числа сотрудников предприятий и целиком организаций, злоумышленникам пошло это на руку. В 2020 г. сотрудники *Microsoft* выявили множество угроз на тему пандемии COVID-19, например:

– выплаты различного характера, тем самым узнавая персональные данные и информацию о банковских картах;

– масочный режим позволил хакерам создать новые сайты, на которых якобы можно приобрести средства индивидуальной защиты;

– письма гражданам на прохождение медицинского обследования, с целью выявления инфекции, в котором указана ссылка для регистрации, а после выпол-

[1] Мокия В. Р., 2021.

нения всех действий посетители данного сайта теряют денежные средства с банковских счетов и многие другие виды, раскрывающие сущность преступлений в информационной сфере.

Пандемия COVID-19 значительно повлияла на киберпреступность. Злоумышленники быстро смогли подстроиться под ситуацию в мире и использовать информационные технологии в преступной деятельности, тем самым значительно снизилась эффективность информационной безопасности. В мире произошли колоссальные изменения.

Киберпреступность – это преступность в виртуальном пространстве, с помощью информационных систем.

К видам данного мошенничества относят:

1) кардинг – оплата производится посредством банковских карт;

2) Крекинг – исследование программного обеспечения с целью выявления слабых мест в защите программы, и последующей эксплуатации этих мест с целью получения бесплатной регистрации программного продукта;

3) спаминг – массовая рассылка сообщений пользователям, не дающим согласие на их получение;

4) фарминг – это процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого используется навигационная структура (файл hosts, система доменных имен (DNS))[1];

5) фишинг – получение идентификационных данных пользователей;

6) нюкинг – действия, вызывающие «отказ в обслуживании» удаленным компьютером, подключенным к сети, говоря на «компьютерном» языке, происходит «зависание» ПК;

7) хакинг – внесение изменений в программном обеспечении, для достижения определенных целей, отличающихся от целей создателей программ, очень часто изменения вредоносны. Хакинг подразделяется на 3 вида, такие как:

a) кракеры (повреждают программные защиты от серийных номеров до аппаратных ключей);

b) фрикеры (занимаются расшифровкой спутниковых сигналов, взломом АТС, «переадресацией» мобильных телефонов с целью их бесплатного использования);

c) сетевые хакеры (их цель – глобальные и локальные сети).

Исходя из статистики Российская Федерация занимает второе место по киберпреступности. Таким образом, требуется направить все силы на повышение

[1] https://ru.wikipedia.org/wiki/Фарминг.

уровня защиты от угроз в информационной сфере. Глобальная проблема современного общества, киберпреступность, требует усиления защиты информационных данных от мошенников.

Законодательная база Российской Федерации полностью не отражает потребности в обеспечении информационной безопасности. Проблема осложняется, когда мошенники не попадают под юридическую ответственность государства.

Преступниками в сфере информационных технологий считаются лица, которые совершают преступления в виде взлома паролей, распространение противоправной информации (например, клевета, материалы, провоцирующие межрелигиозную вражду и т. д.).

Понятие «кибербезопасность» сформировалось в 1989 г., после создания рабочей комиссии по совершенствованию системы национальной безопасности. 5 марта 1992 г. был принят закон «О безопасности», в котором закреплены правовые основы обеспечения информационной безопасности. В соответствии с законом выделяют три принципа обеспечения безопасности информации, к ним относят целостность, конфиденциальность и доступность. Целостность характеризуется тем, что должна соблюдаться защита от несанкционированных изменений. Конфиденциальность – это создание мер защиты информационных данных, обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [2]. Доступность – это обеспечение пользователями нужной им информации.

На протяжении 2020 г. прослеживается рост информационных преступлений, фишинг и вишинг. Исходя из статистики GERT-GIB заблокировал 14 802 фишинговых ресурса, которые стремились к виртуальной краже денежных средств, а также персональной информации посетителей данных сайтов. Распространенный способ мошенничества – звонок, якобы от службы безопасности данного банка. Злоумышленники в этом виде использовали технологии, которые позволяли изменить номер, а также SIP-телефонию, которая не нуждается ни в телефоне, ни в сим-карте.

Что собой представляют фишинг и вишинг? Фишинг – это вид информационного мошенничества, получение конфиденциальной информации пользователей.

Национальная безопасность в Российской Федерации имеет обширный спектр обеспечения. Уровень проблемы обеспечения национальной безопасности не соответствует требованиям времени. Существует много проблем, ко-

торые не дают эффективно обеспечивать информационную безопасность. Таким образом, киберпреступность распространяется не только в период обычной жизни, но и во время пандемии, когда рабочий процесс переведён на дистанционную деятельность.

Кроме того, что до пандемии использовалось, например, кража денежных средств, а также информации, которую можно продать, появились ещё получение сообщения о штрафе за нарушение масочного режима, появление различных сайтов с оформлением фальшивых курьерских служб, а также мошеннические рассылки сообщений различных сервисов видеоконференций.

За время пандемии число DDoS-атак выросла на 15 %, с помощью фишинга произведены атаки на сотрудников различных компаний достигло – 10 %.

За преступление в сфере компьютерной информации наступает уголовная ответственность, которая регламентируется следующими статьями:

– статья 272 «Неправомерный доступ к компьютерной информации» [3], в которой говорится о неправомерном доступе к компьютерной информации;

– статья 273 «Создание, использование и распространение компьютерных программ» [5]. В ней пишется о распространении вирусов с помощью каких-либо изменений в действующие программы. Данный вирус считается опасным, так как может привести к дезорганизации системы компьютерной информации. А также вирус является одной из причин происшествий в области компьютерной информации, как государственная безопасность, способы борьбы с преступность и т. д.;

– статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» [6].

Информационная безопасность ОВД – это состояние защищенности информации, информационных ресурсов и информационных систем ОВД, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования.

Таким образом, в связи с пандемией COVID-19 возросла преступность информационных технологий, появились новые способы мошенничества. В современном мире для безопасности информационных ресурсов требуется создание специальных подразделений, которые должны проследить за обеспечением защиты компаний.

Список литературы

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 19.04.2021).

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 19.04.2021).

3. Приказ Министерства внутренних дел Российской Федерации от 14.03.2012 № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» // опубликован не был.

4. Статья 272. Неправомерный доступ к компьютерной информации УК РФ (в ред. Федерального закона от 07.12.2011 № 420-ФЗ) (см. текст в предыдущей редакции) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/ (дата обращения: 19.04.2021).

5. Статья 273. Создание, использование и распространение вредоносных компьютерных программ УК РФ (в ред. Федерального закона от 07.12.2011 № 420-ФЗ) (см. текст в предыдущей редакции) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/ (дата обращения: 19.04.2021).

6. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей УК РФ (в ред. Федерального закона от 07.12.2011 № 420-ФЗ) (см. текст в предыдущей редакции) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/ (дата обращения: 19.04.2021).

Богданов Д. С.[1]*,*
преподаватель кафедры
информационной безопасности
Краснодарского университет МВД России

Горюн К. Н.[2]*,*
преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

Макуха М. Ю.[3]*,*
преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

ПРЕДЛОЖЕНИЯ ПО ОПТИМИЗАЦИИ ИСПОЛЬЗОВАНИЯ ПАМЯТИ ПОСТОЯННЫХ ЗАПОМИНАЮЩИХ УСТРОЙСТВ СЕРВИСА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ИСОД МВД РОССИИ

В данной статье рассматривается способ оптимизации использования памяти постоянных запоминающих устройств сервиса электронного документооборота ИСОД МВД России. Предлагается отказаться от хранения данных в форматах *pdf и заменить его на более упрощенные варианты хранения информации в форматах *json или *xml, а также использовать эталоны позиционирования реквизитов при отображении хранимых документов сервиса электронного документооборота на серверах департамента информационных технологий, связи и защиты информации.

В настоящее время для обеспечения бесперебойной работы сервисов ИСОД департамент информационных технологий, связи и защиты информации (далее – ДИТСиЗИ) вынужден достаточно часто производить закупки жестких дисков для хранения данных. Прежде всего это связано с большими объемами данных, порождаемых существующими сервисами. Одним из наиболее требовательных

сервисов к объемам постоянных запоминающих устройств (далее – ПЗУ) является сервис электронного документооборота (далее – СЭД). По статистике ДИТСиЗИ данным сервисов в среднем за сутки накапливается 1,2 ТБ информации.

Повышенные затраты памяти постоянных запоминающих устройств в первую очередь связаны с использованием в СЭД типов файлов с расширением *pdf. Документы, сохраненные в данном формате, имеют по умолчанию большой объем, который можно сократить и оптимизировать процедуру хранения документов. Использование расширений *doc или *docx не изменит ситуации радикально в лучшую сторону в силу наличия в рассматриваемых типах файлов избыточной разметки, которая не несет полезной нагрузки для СЭД ИСОД МВД России.

Для решения существующей проблемы предлагается в архитектуре СЭД для хранения документов и внутреннего ознакомления использовать формат расширяемой разметки *xml или текстовый формат обмена данными *json.

Заполнение подобного рода документов будет происходить в HTML форме средствами веб-интерфейса СЭД. Сотруднику, заполняющему документ, будет предложено выбрать вид заполняемого документа, после чего система сгенерирует требуемое количество полей для обязательного заполнения, (на примере рапорта: наименование документа, текст документа, адресат, подпись, дата и т. д.). После завершения подобной процедуры СЭД произведет генерацию json или xml файла (в зависимости от реализации).

Просмотр подобного типа документов будет так же реализован в СЭД. Для отображения содержимого *xml или *json файлов в СЭД требуется предварительно задать эталоны позиционирования реквизитов, которые будут зависеть от типа документа, который указал сотрудник при его разработке. После определения типа документа и подбора соответствующего эталона СЭД произведет генерацию файла документа на веб-странице, исходя из данных, хранимых в файлах *xml или *json для последующего просмотра конечным пользователем. В случае необходимости может быть предусмотрена процедура генерации привычных *docx или *pdf файлов на основе данных, хранимых в файлах с расширениями *xml или *json.

```
[
    {
        "Документ №921": {
            "Тип": "Рапорт",
            "Адресат": "Начальнику...",
            "Наименование документа": "Рапорт",
            "Текст документа": "Докладываю на ваше решение...",
            "Подпись": "Инспектор...",
            "Дата": "20.03.2021"
        }
    }
]
```

Рис. 1. Образец json-файла для хранения информации о реквизитах

```
<?xml version="1.0" encoding="UTF-8" ?>
<root>
    <Документ №921>
        <Тип>Рапорт</Тип>
        <Адресат>Начальнику...</Адресат>
        <Наименование документа>Рапорт</Наименование документа>
        <Текст документа>Докладываю на ваше решение...</Текст документа>
        <Подпись>Инспектор...</Подпись>
        <Дата>20.03.2021</Дата>
    </Документ №921>
</root>
```

Рис. 2. Образец xml-файла для хранения информации о реквизитах

Информация, необходимая для заполнения эталонов позиционирования может быть помещена в контейнеры *json (рис. 1) или *xml (рис. 2) и имеет соответствующий вид.

В случае успешной реализации данного предложения за счет использования эталонов позиционирования теоретически можно уменьшить объем занятого пространства на ПЗУ более чем в 20 раз. При успешной реализации данного предложения индексация хранимых в СЭД документов будет производиться намного быстрее, что позволит осуществлять поиск документов в сервисе с наименьшими затратами временных ресурсов.

Список литературы

1. Сухов, С. Н. Сервисы Единой Системы Информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России) / С. Н. Сухов, А. В. Макаров, С. А. Смирнов. : Нижегородская академия МВД России, 2016.

2. Семенов, Е. Ю. Перспективы Развития ИСОД МВД России / Е. Ю. Семенов // Научный вестник Орловского Юридического Института МВД России имени В.В. Лукьянова. – 2017. – № 3 (72). –С. 135–137.

Ивличев П. С.[1]*,*
доцент кафедры
экономической безопасности Рязанского филиала
Московского университета МВД России имени В.Я. Кикотя,
кандидат физико-математических наук, доцент

ОСНОВНЫЕ ТЕНДЕНЦИИ ИСПОЛЬЗОВАНИЯ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ

Одна из основных служб интернета – служба WWW, которая обеспечивает размещение и просмотр на серверах сети гипертекстовых страниц, определяет концепции развития интернета.

На первоначальном этапе развития сайты интернета представляли собой совокупность статичных веб-страниц, на которых просто размещалась определенная информация для предоставления ее пользователь.

Развитие службы гипертекстовых страниц привело к появлению интерактивных сайтов, для функционирования которых потребовался принципиально иной подход к созданию, размещению и управлению сайтами.

В рамках нового подхода, потребовалась разработка средств создания сайтов, появились языки программирования, заточенные для создания интернет-ресурсов, а также фреймворки и иные средства разработчика. Особенность создаваемых сайтов не только выдача информации по запросу пользователя, но и прием и обработка информации от пользователя. Многообразие средств взаимодействия неизбежно повлекло появление в программных продуктах уязвимостей, которые позволяли недобросовестным пользователям вызывать нештатную реакцию системы и использовать эту реакцию для неправомерных действий с информацией.

Причинами появления таких уязвимостей следует считать изначальную неподготовленность средств разработчика для обеспечения информационной безопасности, недооценка квалификации злоумышленника, а также свободный характер передачи информации в инструментах разработчика.

В целях противодействия угрозам информационной безопасности, выявления уязвимых технологий и методов передачи информации, организация OWASP с 2003 г. осуществляет публикацию бюллетеней безопасности, которая содержит перечни наиболее опасных угроз веб-приложениям [1].

---

[1] © Ивличев П. С., 2021.

При оценке угроз OWASP анализирует степень простоты реализации сценариев атаки, распространенность угроз, сложность обнаружения атак, а также технические последствия для информационных систем. Ранжирование по местам носит субъективный характер, поскольку оценить такие параметры, как последствия для владельцев сайта (экономические, репутационные и т. д.), случае не представляется возможным.

Тем не менее бюллетени OWASP позволяют понять основные тенденции в развитии сферы информационной безопасности, а также сконцентрироваться на разработке методам противостояния наиболее опасным и актуальным угрозам.

Первый бюллетень, содержащий сравнительную и аналитическую информацию, был выпущен в 2004 г.

Наиболее опасной угрозой этого года было обозначено отсутствие контроля над входными данными информационной системы. Данная угроза носит общий характер и в дальнейшем во всех бюллетенях отсутствовала это отсутствие связано с тем, что с 2007 г. все атаки такого типа классифицировались по типу внедрения некорректных данных злоумышленниками [2].

Второе место по степени опасности в 2004 г. заняли ошибки контроля доступа. К таким ошибкам следует отнести уязвимости, которые позволяют получить неавторизованный доступ к страницам, требующим авторизации. Как правило, такой способ связан с манипуляцией URL в строке браузера или изменением параметров GET и POST. Как правило, программное обеспечение сайта обрабатывает лишь стандартные, запрограммированные методы перехода и не рассчитано на прямое изменение адреса. Даже если разработчик предусмотрел проверку авторизации на каждой странице, при использовании прямых ссылок есть возможность обойти обязательную авторизацию.

Такой способ получения несанкционированного доступа к приватным страницам сайтов получил развитие, и в 2007 г. OWASP разделило эту уязвимость на две: небезопасные прямые ссылки и ошибки ограничения доступа по URL. В первом случае, пользователи, уже прошедшие авторизацию, путем изменения URL могли получить доступ к страницам других пользователей, а во втором случае некорректная обработка URL позволяла злоумышленникам получить привилегии пользователей или администраторов без авторизации.

Эксплуатация этой уязвимости не требует от злоумышленника наличия специальных навыков, в связи с чем такие атаки прочно заняли свое место среди наиболее популярных. В 2007 г. это были четвертое и десятое места, в 2010 – четвертое и восьмое, в 2013 – четвертое и седьмое [3].

Однако с развитием программного обеспечения баз данных и генерацией страниц с помощью скриптов, сложность эксплуатации данной уязвимости снизилась и в 2017 г. OWASP поместил ее на пятое место.

Третье место в 2004 г. заняла уязвимость, эксплуатирующая некорректную аутентификацию и управление сессией.

Причинами, способствующими эксплуатации данной уязвимости, были отказ от использования хеширования пароля, уязвимые процедуры восстановления пароля, отображение идентификатора сессии в URL, отсутствие сертификатов TLS, смены идентификатора сессии после аутентификации, отсутствие ограничения по времени для сессии пользователя.

Анализ степени опасности этой угрозы показывает, что к настоящему времени решена только проблема использования сертификатов TLS, в силу чего в 2010 году данная уязвимость также была на третьем месте, а в 2013 и 2017 гг. – на втором. Временное отступление данной уязвимости в 2007 г. на седьмое место, по-видимому, объясняется появлением в 2007 г. большого количества новых методов несанкционированного доступа к информации.

Дополнительной проблемой, которую необходимо решать в настоящее время для устранения данной уязвимости, является проблема проведения автоматизированных атак по подбору пароля и проблема использования ненадежных паролей.

Четвертое место в 2004 г. заняли атаки межсайтового скриптинга. Возможность выполнения скриптов с ресурсов злоумышленников была явно не предусмотрена, поскольку OWASP отмечал, что уязвимость к межсайтовому скриптингу имеют абсолютно все информационные системы.

Как следствие этого просчета, в 2007 г. межсайтовый скриптинг занял первое место, что заставило разработчиков сайтов и браузеров искать методы противодействия.

Пристальное внимание к проблеме межсайтового скриптинга, повышение контроля над вводимыми пользователем данными, дополнения к браузерам привели к тому, что в дальнейшем опасность межсайтового скриптинга неуклонно снижалась. В 2010 г. межсайтовый скриптинг занял второе место, в 2013 – третье, а в 2017 – седьмое.

Учитывая, что разработчиками накоплен опыт в борьбе с другими типами скриптовых атак, есть основания полагать, что в дальнейшем положительная динамика продолжится [4].

Пятое место в 2004 г. заняли атаки типа переполнения буфера, связанные с использованием устаревших языков программирования, которые не имели достаточной «защиты от дурака» и позволявшими злоумышленникам добиваться нештатной реакции системы на некорректные данные. Развитие новых сред программирования позволило в дальнейшем полностью ликвидировать эту угрозу.

Шестое место в 2004 г. заняли инъекции. Причем первоначально это понятие применялось исключительно к языку SQL и реляционным базам данных, однако впоследствии злоумышленниками были разработаны механизмы использования регулярных выражений и для баз знаний и для объектно-ориентированных моделей.

Как следствие число инцидентов начало расти и в 2007 г. инъекции заняли второе место, а с 2010 г. стабильно возглавляют рейтинг уязвимостей.

Такая высокая оценка обусловлена не только распространенностью данной угрозы, но и ее многообразием, а также тяжелыми техническими последствиями. Результатом применения успешных инъекций являются манипуляции со всем массивом хранимой информации.

Учитывая, что базы данных составляют непременную основу современных информационных систем ожидать снижения количества инцидентов, связанных с применением инъекций, не приходится.

Седьмое место в 2004 г. заняла неправильная обработка ошибок. Такая обработка ошибок, по сути, является «защитой от дурака», в связи с чем необходимо не только реализовать эту защиту, но и обеспечить ее корректное функционирование. После устранения уязвимостей, связанных с ошибкой переполнения буфера, злоумышленники переключились на эксплуатацию уязвимостей системы защиты, в силу чего в 2007 г. данная уязвимость заняла шестое место.

По мере развития стандартных библиотек интерфейсов и ужесточения контроля за действиями пользователя, данная уязвимость с 2010 г. перестала быть актуальной.

Восьмое место в 2004 г. заняло небезопасное хранение данных. Важность криптографической защиты в то время недооценивали, что привело к тому, что уязвимости шифрования стали использоваться злоумышленниками не только при атаке баз данных, но и при атаке каналов передачи информации.

В 2007 г. ошибки шифрования заняли восьмое и девятое места, в 2010 г. – седьмое и девятое, в 2013 – шестое место.

К сожалению, пристальное внимание к криптографической защите проявляют не только специалисты по информационной безопасности, многие алгоритмы шифрования подвергнуты криптоанализу, но не заменяются на новыми, в силу чего в 2017 г. эта уязвимость заняла третье место.

Девятое место в 2004 г. заняли атаки на отказ в обслуживании. Однако достаточно оперативно были разработаны механизмы противодействия таким атакам, и в дальнейшем их опасность никогда высоко не оценивалась.

Десятку наиболее опасных уязвимостей в 2004 г. заняли ошибки системы конфигурации, которые позволяли злоумышленникам получить доступ к незащищенным объектам системы, в качестве которых могли выступать страницы входа, консоли администрирования, процедуры и функции библиотек.

Такие объекты довольно часто присутствуют в системе, поскольку дополнительные консоли входа часто используются при отладке, консоль администратора нередко имеет простую функцию восстановления пароля, а в качестве библиотек используются открытые библиотеки, информационная безопасность которых, очевидно, недостаточна [5].

В дальнейшем отмечался рост инцидентов, связанных с эксплуатацией этой уязвимости. В 2010 г. уязвимость заняла шестое место, в 2013 г. – пятое, в 2017 – шестое.

В 2007 г. в списке уязвимостей появились две новые, опасность которых сразу же была оценена очень высоко.

Третье место заняла уязвимость, позволявшая выполнять на атакуемом сервере вредоносные файлы. В дальнейшем, с ужесточением политики администрирования, эта угроза была сведена на нет.

Пятое место в этом году заняла уязвимость, связанная с межсайтовой подделкой запросов. К эксплуатации этой уязвимости привел недостаточный контроль над аутентификацией пользователя, который не препятствовал выполнению действий от авторизованного пользователя на постороннем сайте.

С вводом многофакторной аутентификации опасность таких атак в настоящее время оценивается невысоко, хотя в 2010 г. они занимали пятое место, а в 2013 – восьмое.

В 2010 г. в списке уязвимостей появилась эксплуатация непроверенных ссылок. Такие ссылки позволяют злоумышленнику перенаправлять пользователей с атакуемого сайта на сайт злоумышленника, приводя, фактически, к неработоспособности атакуемого файла. Эта уязвимость в 2010 г. заняла десятое место, то же место она заняла в 2013 г., однако в дальнейшем в связи с ужесточением контроля над URL ссылок ее опасность была сведена на нет.

В 2013 г. в список уязвимостей была включена эксплуатация небезопасных компонентов. Как правило, уязвимости отдельных компонентов в первую очередь обнаруживаются злоумышленниками, что позволяет им захватить стратегическую инициативу. В 2013 и 2017 гг. эта уязвимость заняла девятое место и есть основания полагать, что в дальнейшем ее опасность останется на том же уровне.

В 2017 г. в списке опасных уязвимостей появились три новые категории: внедрение XML-сущностей, небезопасная десериализация и недостатки мониторинга. Первая уязвимость является разновидностью атак на внедрение кода, вторая связана с развитием идентификации сессии с помощью куки, которые появились для того, чтобы повысить безопасность управления сессией и предотвратить ошибки контроля доступа.

Появление этих уязвимостей наглядно показывает, что замена одних технологий на другие также трансформирует и сферу преступности, поэтому необходимо обращать внимание на потенциальную уязвимость всех внедряемых технологий.

Список литературы

1. OWASP Top 10: Sensitive Data Exposure Security Vulnerability Practical Overview // Официальный сайт компании ImmuniWeb. – URL: https://www.immuniweb.com/blog/ OWASP-sensitive-data-exposure.html (дата обращения: 17.04.2021).

2. Ивличев, П. С. Обеспечение информационной безопасности в условиях современной криминальной среды: учебное пособие / П. С. Ивличев, Н. А. Ивличева. – Рязань : Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2018.

3. Ивличев, П.С. Анализ актуальных механизмов неправомерного доступа к компьютерной информации: учебно-практическое пособие / П. С. Ивличев, Н. А. Ивличева, М. Н. Трофимов. – Рязань : Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2019.

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

5. Чернов, С. Б. Обеспечение безопасности данных в условиях цифровой экономики / С. Б. Чернов, О. С. Новикова // Экономические науки. – 2020. – № 189. – С. 104–109.

Данилова Е. А.[1]*,*
курсант факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Плотников Г. Г.[2]*,*
профессор кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя

ПРОБЛЕМА ИМИТОЗАЩИЩЕННОСТИ В ОБЕСПЕЧЕНИИ ЦЕНТРАЛИЗОВАННОГО ОХРАННОГО МОНИТОРА

Актуальность темы исследования обусловлена наличием проблем в обеспечении информационной безопасности в технических системах охраны.

Имитозащита представляет собой защиту канала шифрованной связи от навязывания ложных данных, ложной информации, появляющийся из-за действий противника. Это проявляется в воздействие на информацию, передаваемую по каналу связи, а также на «пустой» канал.

Для реализации имитозащиты важно, чтобы у преступника не было возможности создавать подходящие сообщения, а точнее сообщения, которое приемное устройство определит как истинные.

Для обеспечения имитозащиты используется криптографическая контрольная сумма, зависящая от открытого текста и ключа.

Действия преступника при навязывании информации, путем воздействия на «пустой» канал заключаются в том, что правонарушитель внедряет в канал связи некоторое шифрованное сообщение, после этого данные приходят получателю. Лицо, получившее сообщение, может заметить ложное сообщение, а может и не заметить, и нанести ущерб, действуя в соответствии с этим сообщением.

Для преступника важно максимизировать вероятность навязывания ложных данных при случайном ключе. Получатель, знающий о возможных действиях преступника, будет выбирать такой шифр, чтобы уменьшить максимально возможное значение вероятности навязывания.

Действия преступника при навязывании информации, путем знания открытого текста заключаются в том, что есть возможность того, что преступник обладает дополнительной информацией, например знание открытого текста, и тогда преступник стремится увеличить вероятность навязывания сообщения, а сторона получатель старается уменьшить возможность навязывания ложных данных.

Имитозащита реализуется с помощью добавления к сообщению дополнительного кода, имитовставки, она известна только отправителю и получателю.

В ГОСТ 28147—89 определяется процесс выработки имитовставки, который единообразен для любого из режимов шифрования данных.

Имитовставка – это определенный набор специальных символов, которые добавляются к сообщению, она вырабатывается перед шифрованием всего сообщения либо параллельно с шифрованием по блокам. Имитовставка предназначен для обеспечения целостности данных и аутентификации источника данных.

Стоить отметить, что существует два класса имитовставки:

– MDC (*modification detection code*) – код, осуществляющий проверку целостности данных. При отправке данных добавляется значение хеш-функций. На приемной стороне также вырабатывается хеш от полученного сообщения. Далее происходит проверка целостности сообщения, если хеш выработанный на приемной стороне и на стороне отправителя совпадают, то данные дошли без изменений.

– MAC (*message authentication code*) – код аутентификации сообщения, позволяет верификаторам определить была ли изменена информация в сообщении, а также код аутентификации сообщения предназначен для защиты данных от фальсификации.

В современном мире существует высокая планка к обеспечению информационной безопасности, поэтому существует проблема в навязывание ложных данных в датчиках технических систем охраны.

Основное направление навязывания ложных данных в технических системах охраны проявляется в несанкционированном замене датчика охраны, например: датчика движения и камер видеонаблюдения, подставным элементом, который предназначен для предоставления системе охраны ложных данных.

Для решения задачи противодействия несанкционированной подмене датчиков в охранных систем используются два основных метода:

1. Применение определенной системы шифрования передаваемых данных, в которой подмененный датчик по определению не сможет работать.

2. Обеспечение незамедлительной реакции технических систем охраны на несанкционированное размыкание линии передачи данных, возникающее в момент подмены датчика охранной сигнализации.

В настоящее время для охраны объектов широко используются беспроводные автоматизированные системы охраны. Основной фактор нарушения целостности данных – навязывание ложных данных в пульте централизованного наблюдения, который устанавливается в пункте централизованной охраны.

В пульте централизованного наблюдения осуществляется хранение базы ключей от охранных извещателей, функционирующих в системе, необходимые для вычисления имитовставок.

Варианты имитационного воздействия на автоматизированные системы охраны:

1. Получение данных от охранного извещателя, не входящего в базу данных охранных извещателей. В данном варианте преступник пытается выпасть подставное устройство, под устройство зарегистрированного в базе данных, для навязывания ложных данных.

2. Отрицательный результат проверки значения электронной подписи.

В целях контроля подлинности поступивших данных охранными извещателями. Пункт централизованного наблюдения проверяет электронную подпись поступивших данных.

Существуют определенные изобретения передачи извещений для систем централизованной охраны, которые минимизируют возможность навязывания ложных данных.

1. «Abstract». Изобретение, главной задачей которого является повышение защищенности доступа. Данное устройство дополнительно передает имитовставку и ссылку на ключ для ее генерирования на пункте централизованной охраны. Устройство не позволяет не включенным в список обслуживания клиентам передавать свои данные на ПЦО. Это повышает надежность защиты от несанкционированного подключения неавторизованных абонентов.

2. «Description». Устройство обеспечивает повышение защищенности доступа. Это осуществляется тем, что имитовставку генерируют на пункте централизованной охраны и сравнивают с переданной в составе сообщения, а также формируют последовательный двоичный код извещения с известным количеством разрядов, передают на пункт централизованной охраны данные необходимые для работы, например: номер абонентского блока, основной блок данных.

Список литературы

1. Информационная безопасность и защита информации. Лекция. Контроль целостности данных. Хеш-функции. Имитовставка. ЭЦП // Система управления курсами Moodle. – URL: https://moodle.kstu.ru/mod/page/view.php?id=9315 (дата обращения: 18.04.2021).

2. Гавришев, А. А. К вопросу о защите датчиков технических систем охраны от навязывания ложных данных / А. А. Гавришев, В. А. Бурмистров, Д. Л. Осипов // Сборник научных трудов ставропольского научно-исследовательского института животноводства и кормопроизводства. – 2013. – № 6. – Т. 3. – С. 350–353.

3. Орлов А. В. Имитозащита беспроводных автоматизированных систем охраны режимных объектов / А. В. Орлов, Е. В. Мельников, О. А. Финько // Научная электронная библиотека «КиберЛенинка» – URL: https://cyberleninka.ru/article/n/imitozaschita-besprovodnyh-avtomatizirovannyh-sistem-ohrany-rezhimnyh-obektov (дата обращения: 18.04.2021).

4. Описание изобретения к Евразийскому патенту. Изобретатель Юрий Адольфович Попов. EA019227B1.pdf (storage.googleapis.com) // Google.Patents. – URL: https://patents.google.com/patent/EA019227B1/ru (дата обращения: 18.04.2021).

Бороздина В. Н.[1]***,***
курсант факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Плотников Г. Г.[2]***,***
профессор кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя

СРАВНЕНИЕ СИСТЕМ КОНВЕКЦИОННОЙ И СОТОВОЙ СВЯЗИ В РЕШЕНИИ ЗАДАЧ ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЫ

Средства связи правоохранительных органов – набор аппаратного и программного обеспечения, используемого для генерации, доставки, приема, обработки и хранения сообщений. Правовые отношения в области связи в Российской Федерации регулируются: Конституцией, федеральными законами «О связи» от 07.07.2003 № 126-ФЗ и «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ.

Радиосвязь осуществляется путем модуляции колебаний несущей частоты, которая колеблется от единиц килогерц до сотен мегагерц и более. Конвенциональная радиосвязь – считается классическим типом беспроводной связи, которая реализуется радиостанциями, не объединенными в какую-либо техническую систему, обеспечивающую управление ресурсами, сигнализацию и другие координирующие операции. Сегодня во всем мире используют тысячи конвенциональных радиосистем. Составными частями конвенциональной системы радиосвязи являются центральная радиостанция и абонентские радиостанции. Руководство исполняет диспетчер – передача и прием уведомлений абонентов. Помимо этого, взамен диспетчера могут применяться системы с автоматическим ретранслятором.

Радиосети с ретрансляторами. Каждая конвенциональная радиосистема выстраивается на базе применения ретрансляторов. Для этого нужно наличие двух частот (дуплексной пары) – двух направлений. Первый фактор использования ретранслятора – вероятность существенно повысить расстояние радиосвязи.

Объединить 2 радиостанции при отсутствии ретранслятора допустимо на расстоянии нескольких километров, в то время как ретранслятор позволяет увеличить дальность связи до десятков километров. Самая простая аналоговая конвенциональная система связи – ретранслятор + 2 радиостанции представлена на рис. 1.

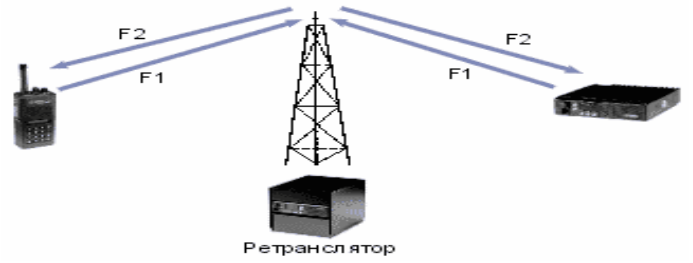


Рис. 1

На данном рисунке связь обеспечивается на двух частотах (F1 – частота приема, F2 – частота передачи), создавая один канал связи.

Отличия и качества конвенциональных портативных (носимых) систем связи: ручной выбор канала; небольшой радиус действия; возможность дозвониться до абонента; прямое общение между абонентами; работа группы абонентов на одной частоте; быстрое установление канала связи; небольшое количество абонентов; слабая защита канала от прослушивания; минимальные затраты; отсутствие доступа к телефонной сети. Основным преимуществом конвенциональной техники является возможность организации собственной системы связи, не требующей подключения к сети какого-либо другого оператора, из чего следует то, что не нужно оплачивать его услуги.

Системы сотовой связи основываются на принципе предоставления услуг связи в относительно малых зонах обслуживания. Такой принцип позволяет, с одной стороны, использовать приемо-передающую аппаратуру менее затратную в виду не высоких требований к передатчику и антенно-фидерному тракту, а с другой – позволяет использовать повторяющиеся частоты в разных зонах обслуживания. Важным преимуществом систем сотовой связи является возможность использования множества сервисов, одним из которых является сервис по определению местоположения устройства.

Построение специальной сети радиосвязи для системы позиционирования чрезвычайно дорого, и это может быть экономически оправданно только в случае небольших территорий, поскольку стоимость создания сетевой инфраструктуры растет прямо пропорционально размеру территории и количеству контролируемых объектов. Лучший вариант – создание крупных систем позиционирования, в которых зона покрытия будет охватывать город или регион, а количество контролируемых объектов также будет расширяться в больших пределах.

Технологии позиционирования в сотовых сетях. Решение проблемы позиционирования радиотелефонов в сотовых сетях возникло из простого метода, он называется Cell ID. Этот метод основан на установлении местоположения абонента, имея точность, которая доходит до сотых долей, определяется путем фиксации радиотелефонного сигнала базовой станцией, а при приеме несколькими станциями определением амплитуды сигнала, которая будет достигать максимума. Территория нахождения абонента указывается при использовании секторных антенн. В этом случае при приеме сигнала несколькими базовыми станциями вычисляются направления его прихода. Погрешность определения местоположения при таком способе довольно мала и может достигать 30 км. Самая элементарная идентификация местонахождения абонента с точностью до определенной базовой станции (речь идет о уже известном нам методе Cell-ID), будет основой при задержании злоумышленника.

На основе вышеизложенного можно сделать вывод о том, что конвенциональную систему радиосвязи обширно применяют: МЧС России, МВД России, ОАО «Российские железные дороги», охранные службы, скорая медицинская помощь, так как системы данного типа всегда пользовались наиболее большим спросом из всех типом систем наземной подвижной радиосвязи, но для того чтобы без ограничений пользоваться конвенциональной системой, нужно получить разрешение на использование частотного диапазона, исходя из этого пользоваться конвенциональной системой в основном могут только корпоративные пользователи, что насчет мобильных средств конвенциональной радиосвязи, они как часть экипировки применяются в основном в силовых структурах борьбы с терроризмом, патрулирования, при проведении спец операций. Без применения спец средств связи не проводиться не одна войсковая или контртеррористическая операция, позволяя наладить управление и осуществлять постоянный контроль над меняющейся ситуацией. Зная номер мобильного телефона системы позиционирования, которая основана на использовании только сетевого оборудования, данные о местонахождении абонента могут выдаваться непрерывно и без его уведомления.

Применение средств связи невозможно без соблюдения стандартов безопасности и требований к средствам связи. Данные требования разрабатываются в Департаменте информационных технологий, связи и защиты информации МВД России.

Список литературы

1. Николаев, В. П. Местоопределение абонентов в сетях сотовой связи / В. П. Николаев // Сайт Ассоциации охранных предприятий «Георгий Победоносец» – URL: http://www.vrsystems.ru/stati/mestoopredelenie_abonentov_v_setyax_sotovoi_svyazi.htm (дата обращения: 15.04.2021).

2. Конвенциональные системы связи. Особенности частотного обеспечения, проектирования и строительства систем подвижной радиосвязи // Портал студенческих и научных материалов Ozlib.com – URL: https://ozlib.com/858080/tehnika/konventsionalnye_sistemy_svyazi (дата обращения: 15.04.2021).

Ермаков С. В.[1]*,*
заместитель начальника кафедры
предварительного расследования
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

РАБОТА СЛЕДОВАТЕЛЯ С ЭЛЕКТРОННЫМИ ДОКАЗАТЕЛЬСТВАМИ

При совершении, традиционных преступлений и с использованием информационно-телекоммуникационных технологий, человек оставляет следы в цифровом пространстве.

Например, работая на компьютере, пользуясь сотовой связью, общаясь в мессенджерах, отправляя письма по электронной почте, попадая в роле зрения различных видеокамер, делая фотоснимки на сотовый телефон, расплачиваясь кредитной картой, заказывая такси через приложение, снимая наличность в банкомате и т. д.

Цифровые следы остаются на различных носителях, сохраняются как на устройствах злоумышленника, так и на внешних ресурсах. При этом преступники предпринимают меры по сокрытию, шифрованию, уничтожению цифровых следов преступления, сохранению анонимности работы в интернете. Что из цифровых следов станет доказательством и как будет использовано в процессе доказывания, зависит от знаний, умений и навыков работы следователя с такими следами. В последнее время возросла потребность у сотрудников следственных органов в дополнительных знаниях [2, с. 178].

Как обнаружить, изъять, исследовать и использовать в качестве доказательств такие следы? Работа следователя в данном направлении достаточно разнообразная. Так, средством получения цифровых следов, хранящихся на внешних ресурсах, является направление запросов в различные организации: сотовой связи, интернет-провайдеру, кредитные, электронной коммерции, электронных платежных систем и прочие. Следователя интересует «привязка» мобильного устройства, которым пользовался в тот или иной момент преступник, к базовым станциям сотовой связи, IP-адрес устройств, выходящих в интернете, время активности в цифровом пространстве. Именно через данные следы можно приблизиться к раскрытию преступления, установлению лица его совершившего.

В каждом случае получения необходимой информации встает вопрос о соблюдении требований УПК РФ законодательства о связи, о банковской тайне, получение судебных решений и пр. Следователю необходимо уметь определять четкий круг сведений, которые необходимо и возможно получить от организаций по запросу. Следственная и оперативная работа в данном направлении не отличается стремительностью. Подготовив, согласовав, получив судебное решение в необходимых случаях и направив запросы, следователь находится в режиме ожидания ответа. Теряются быстрота и наступательность в расследовании, сроки расследования продлеваются. В это время преступники продолжают заниматься противоправной деятельностью.

Качество взаимодействия между органами предварительного расследования и кредитными организациями, операторами сотовой связи, электронными платежными системами нельзя признать удовлетворительным, что проявляется в общих ответах на запросы, в которых часто следователь не может найти важной для расследования информации (обезличенные счета, широкий круг обслуживаемых адресов провайдеров, идентичные IP-адреса), а иногда и в отказе предоставления информации. Повышение качества такого взаимодействия возможно путем перевода данного информационного обмена в цифровой формат, упрощения правовых процедур, автоматизации процессов передачи-получения данных.

Следственные действия не предполагают удаленное получение компьютерной информации с компьютерных систем и сетей. Поэтому в ходе предварительного расследования следователь вправе дать поручение органам дознания, в арсенале которых имеется право на проведение оперативно-разыскных мероприятий, в том числе «получение компьютерной информации». После представления результатов оперативно-розыскной деятельности следователю цифровые носители информации могут быть приобщены в качестве вещественных доказательств.

Большой блок работы следователя связан с получением записей с камер видеонаблюдения (городская система видеонаблюдения, камеры организаций, банков, патрульных машин и т. д.). В данном направлении работы следователь дает поручение органу дознания на обнаружение камер видеонаблюдения и изъятие записей. После процессуального оформления, осмотра видеозаписей возможно назначение судебно-портретной экспертизы по цифровым изображениям для идентификации подозреваемого и лица, запечатленного на цифровой видеозаписи.

Немаловажное значение имеет тактически грамотное изъятие компьютерной техники, сотовых телефонов, флеш-карт и прочих накопителей у подозреваемых,

в ходе производства обыска, выемки осмотра места происшествия и других следственных действий. В дальнейшем следователь должен произвести их осмотр, а в необходимых случаях назначить компьютерные экспертизы с целью получения интересующей информации и данных о работе на данных устройствах.

В условиях бумажного формата уголовного дела в ходе осмотра телефонов и компьютерной техники следователи применяют различные приемы: фотографирование экрана, снятие электронных копий экранов (скриншотов). Непосредственная фотосъемка мобильного устройства представляется «двойной» работой, – необходимо одновременно и искать переписку, продвигать ее вниз при помощи сенсорного экрана смартфона, и наводить фотокамеру на нее и изготавливать фотоснимки. Гораздо проще выглядят скриншоты экранов, которые создаются при помощи функциональных возможностей смартфона, но и они в дальнейшем чаще всего являются лишь частью фототаблицы к протоколу осмотра предметов. Таким образом, ввиду отсутствия электронной формы уголовного судопроизводства, установленных мест хранения электронных доказательств следователи вынуждены заниматься технической работой по переводу цифровых следов в бумажный формат.

Немаловажный аспект связан с техническим оснащением органов предварительного расследования. В работе следователя необходимы современные технические средства для изъятия и хранения информации, объемы которой могут быть значительными.

Итог работы следователя с цифровыми следами – использование их в качестве так называемых «электронных доказательств», которые представляют собой информацию, представленную в цифровой форме, которая способна устанавливать обстоятельства, подлежащие доказыванию по уголовному делу, хранящуюся на электронном носителе информации и/или представленную независимо от него. Такая информация может рассматриваться в статусе вещественных доказательств и иных документов в зависимости от ее (информации) оформления, хранения, использования в совершении преступлений [1, с. 48].

В процессе производства допросов, осмотров, формулировании обвинения следователь должен уметь использовать в доказывании полученные сведения – цифровые следы, указывая IP-адреса, файлы с данными, используемые программы, адреса переписки по электронной почте. В итоговом документе расследования – обвинительном заключении, следователь должен отразить соответствующие электронные доказательства, хранящиеся на различных носителях, например: DVD-R-диски с видеозаписями с камер наблюдения, ноутбуки, НЖМД (накопители на жестких магнитных дисках) и пр.

В настоящее время даже обычный следователь территориального ОМВД должен обладать компетенциями по работе с цифровыми следами, навыками установления цифровой картины совершенного преступления. Привлечение следователем специалиста к работе с цифровыми следами должно быть вызвано лишь объективной необходимостью, либо требованием законодательства.

В зависимости от сложности уголовного дела, решения типовых следственных задач должны определяться необходимые навыки следователя для работы в IT-сфере. Целесообразно разработать систему определения «цифровой квалификации сотрудников» путем тестирования следователей и специалистов. По результатам тестирования можно определить уровни квалификации: минимальный, базовый, продвинутый, что позволит ОВД эффективно использовать силы и средства для противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

Список литературы

1. Зуев, С. В. Электронные доказательства в уголовном судопроизводстве: понятие и значение / С. В. Зуев // Правопорядок: история, теория, практика. – 2020. – № 3 (26) – С. 46–51.

2. Семикаленова, А. И. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики / А. И. Семикаленова, И. А. Рядовский // Актуальные проблемы российского права. – 2019. – № 6. – С. 178–185.

Минаев В. А.[1]*,*
профессор кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор

КИБЕРБЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ ПРОБЛЕМЫ РОССИЙСКОГО ОБЩЕСТВА

Кибербезопасность – это системное сочетание различных современных технологий и процессов, предназначенных для защиты информационных сетей, устройств и данных от атак или несанкционированного доступа.

К 2025 г., из-за роста киберпреступности, возникнет острая потребность в защите информационных ресурсов государственных структур и коммерческих компаний.

Справочно:

– В 2020 г. объем рынка обеспечения кибербезопасности составил около 160 млрд долл. США, к 2025 г. он достигнет 350 млрд долларов, при среднегодовом темпе роста – 14,5 %. Очевидно, что тенденции интернета вещей, разработок в сфере искусственного интеллекта и машинного обучения продолжат расти.

– Киберпреступления, которые включают повреждение и уничтожение данных, кражу денежных средств и интеллектуальной собственности к настоящему времени обходятся миру более $ 2/3 триллиона ежегодно, составляя почти 1% мирового ВВП.

– Расширение M2M (межмашинного взаимодействия), IoT-соединений стимулируют рынок обеспечения кибербезопасности, ориентируя новые бизнес-модели и приложения на снижение затрат и рост числа подключенных устройств (автомобилей, счетчиков, бытовой электроники и др.).

– К 2025 г. в мире будет около трех десятков умных городов, половина из которых расположится в Северной Америке и Европе, что потребует принятия эффективных мер по кибернадежности.

Вспышка коронавирусной пандемии привела к росту использования платформ видеосвязи по всему миру. По данным компании *Checkpoint Security*, с начала пандемии зарегистрировано около 2 тыс. новых доменов. При этом зарегистрирован огромный рост фишинга, распространения вредоносного ПО, атак

---

[1] © Минаев В. А., 2021.

на инфраструктуры удаленной работы с использованием приманок на тему COVID-19.

Пока специалисты по безопасности рекомендуют использовать различного рода биометрическую идентификацию для входа в компьютерные системы, более 80 % компаний продолжают использовать только имена пользователей и пароли.

Росту рынка обеспечения кибербезопасности способствуют:

– быстрое развертывание веб- и облачных приложений;

– растущая потребность предприятий в снижении рисков и строгом соблюдении нормативных требований производства;

– увеличение частоты кибератак.

С развитием технологий блокчейн, онлайн-транзакций, обмена цифровыми файлами киберугрозы постоянно растут. Согласно отчету компании *Verizon* об утечке данных, опубликованному в прошлом году, 86% всех нарушений совершено на финансовой почве, 22 % – с фишингом.

В связи с возросшим числом вирусных атак, киберпреступлений и сетевых угроз, государства и крупные корпорации стали уделять повышенное внимание защите данных и конфиденциальности. Правительства и регулирующие органы установили новые правила (Общий регламент защиты персональных данных в ЕС, Закон о конфиденциальности потребителей в Калифорнии, Акт о мобильности и подотчётности медицинского страхования, Закон о конфиденциальности электронных коммуникаций и защиты данных). Компании, не соблюдающие такие правила, могут столкнуться с серьезными штрафами и риском серьезных репутационных потерь.

Некоторые тенденции

COVID-19 изменил способ ведения бизнеса и осуществления государственных операций.

С февраля 2020 г. компания IBM X-Force зафиксировала рост спама на тему коронавируса на 4300 %.

Прогноз о том, что к 2026 г. более 90 % населения в развитых государствах и почти 70 % – в странах с развивающейся экономикой будут использовать интернет, только усилит мотивацию киберпреступников. При этом атаки на критически важные секторы экономики в скором времени станет очень серьезной проблемой, если не будут приняты адекватные меры по обеспечению кибербезопасности.

Значительный рост кибербезопасности, по мнению мировых экспертов, ожидается в сегментах аэрокосмической и оборонной промышленности, поскольку системы навигации и наведения самолетов очень уязвимы для кибератак.

Компьютеры и сети для всех наземных и воздушных операций будут нуждаться в сильной инфраструктуре безопасности для противодействия кибертерроризму.

По данным *International Data Corporation* затраты на системы ИИ в глобальном масштабе составили в 2020 г. $ 25 млрд. В 2021 г., как ожидается, отрасль вырастет на 44 %. В результате объём мирового рынка ИИ достигнет $ 36 млрд, что положительно скажется на рынке кибербезопасности.

Объем рынка продуктов и сервисов кибербезопасности в России в 2019 г. превысил 17 млрд руб., что составляет около 1 % глобального рынка.

По прогнозам, в период до 2025 г. российский рынок будет расти на 3 % ежегодно и достигнет в 2025 г. 21 млрд руб. Есть и негатив в развитии российского рынка в этой сфере: темпы роста российского рынка в рублевом выражении будут почти в 4 раза ниже темпов роста глобального рынка в валютном выражении. В частности, негативное влияние на количественное и качественное развитие рынка средств обеспечения кибербезопасности окажет задержка в развертывании сетей 5G и сервисов, ориентированных на индустриальные применения. Эти цифры отражают необходимость коренных изменений на российском рынке кибербезопасности, в том числе в области его регулирования. На фоне быстрой трансформации глобального рынка отставание России в области защиты от кибератак выглядит тревожно.

Основные драйверы быстрого расширения функционала, производительности и проникновения средств обеспечения кибербезопасности, реализованных как в виде аппаратно-программных устройств, так и в виде виртуальных функций и облачных сервисов, являются:

1. Рост объема обрабатываемых и хранимых на всех видах компьютерных устройств данных.

2. Преимущественно распределенный характер новых видов приложений: клиентская и серверная часть приложений территориально распределены.

3. Рост разнообразия киберугроз и их тотальный характер, определяемый, в первую очередь, бурным ростом облачной модели совершения преступлений.

Выводы

1. Рост числа киберугроз предприятиям и государственным структурам, усиление тенденций интернета вещей, использование смартфонов, интернет-банкинга, облачных технологий являются ключевыми драйверами роста рынка кибербезопасности России и во всем мире.

2. По данным *Cybersecurity Ventures*, ущерб, нанесенный киберпреступностью в 2021 г., может обойтись мировой экономике в 6 трлн долл. в США. В 2015 г. эта сумма составила только 3 трлн долл. в 2 раза меньше.

3. По прогнозам той же компании, в период 2017–2021 гг. мировые корпорации потратят более 1 трлн долл. на продукты и услуги в области кибербезопасности. К 2021 г. для обеспечения кибербезопасности будет создано 3,5 млн рабочих мест по сравнению с 1 млн в 2014 г.

4. Очевидно, что и в России будут наблюдаться подобные тенденции, которые повлекут совершенствование информационно-технологической базы в системе МВД России и существенное усиление подготовки специалистов для сферы обеспечения кибербезопасности.

Клочкова Е. Н.[1]*,*
доцент кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя

ИНТЕРНЕТ И ПРИВАТНОСТЬ: КАК ЗАЩИТИТЬ СЕБЯ И СВОИ ДАННЫЕ

Сложная эпидемиологическая обстановка в мире, сложившаяся из-за распространения коронавирусной инфекции, привела к ограничению передвижения огромного количества людей, и произошел массовый переход на удаленный режим работы сотрудников коммерческих и государственных организаций. Переход на удаленный режим работы заставил в ускоренном темпе осваивать современные информационные технологии людей, которые еще совсем недавно не думали об этом. Люди вынуждены использовать интернет для решения рабочих и бытовых вопросов. Государственные учреждения расширяли спектр предоставляемых дистанционно услуг. Значительно увеличился объем интернет-покупок с организацией доставки, т. е. за последний год количество активных пользователей сети значительно возросло. При этом далеко не все из них имели представление о том, какие угрозы безопасности в сети существуют и как защитить себя и свои данные.

Проведенные исследования показали, что самая уязвимая категория, наиболее страдающая от мошенников в интернете, это молодежь. При всей гибкости, легкости освоения современных технологий молодые люди оказались более склонными к рискованным действиям, а как следствие чаще теряют деньги, доверяя мошенникам.

Рассмотрим основные простейшие приемы обеспечения безопасности данных. Начнем с защиты своих данных. Защита информации требуется, если она хранится на технических устройствах, и если осуществляется ее передача.

Развитие технических средств привело к тому, что для работы, отправке сообщений, общения в социальных сетях, совершения финансовых операции нет необходимости использовать привычные стационарные компьютеры или ноутбуки. Фактически все операцию можно осуществлять с телефона или планшета, что значительно проще и удобнее. Но использование мобильных

устройств привело к появлению новых угроз, связанных с необходимостью их физической защиты.

Если стационарные компьютеры расположены в помещениях, где отсутствует доступ посторонних или сильно ограничен, то ноутбуками пользуются уже как дома, так и в общественных местах, а мобильными телефонами и планшетами, так и вообще повсеместно. Как следствие увеличивается вероятность кражи или утраты устройств. При этом такие технические средства содержат в своей памяти не только большое количество персональных данных, но на них зачастую установлены приложения, дающие доступ к финансовым счетам пользователя. Именно поэтому необходимо для таких устройств устанавливать дополнительные защитные элементы, блокирующие доступ посторонних к информации, размещенной на устройстве.

Если физическая защита устройства обеспечена, то уже можно говорить о защите информации, которую пользователь передает или получает через интернет. Прежде всего необходимо помнить о том, что каждый раз, посещая какой-либо сайт, вы оставляете там свои данные. В некоторых случай вас об этом могут информировать, но зачастую вы можете даже и не подозревать об этом.

При работе в сети надо убедиться, что установлено безопасное соединение. Если доступ к интернету осуществляется с домашнего компьютера, с использованием Wi-Fi, то перед началом работы нужно настроить пароль для доступа к сети. Требования к такому паролю такое же, как и к любому другому. Он должен быть достаточно надежным, чтобы злоумышленнику было сложно его подобрать, иначе, получая доступ к сети пользователя, злоумышленник получает доступ ко всей его информации.

Если же доступ осуществляется с применением Wi-Fi соединений, предоставляемого в общественном месте, то такое соединение нельзя использовать для обмена информацией конфиденциального характера или перевода денежных средств.

Используя информационные ресурсы сети, пользователей зачастую просят пройти регистрацию. Активное использование сети приводит к тому, что пользователь имеет десятки различных логинов и паролей, которые открывают ему доступ на интересующие его сайты, в социальные сети, в электронную почту и т. д. Проходя многочисленные регистрации, мы зачастую начинаем использовать пароли, легкие для запоминания или даже одинаковые, забывая о том, что если злоумышленник получит ваш логин и пароль, то он получит доступ фактически ко всей вашей личной информации, размещенной в сети.

Еще одна угроза безопасности информации связанна с излюбленной тактикой злоумышленников, заключающейся в том, чтобы заставить пользователя загрузить программное обеспечение, содержащее вредоносные коды.

Способов, с помощью которых такое программное обеспечение может попасть на компьютер, великое множество, но причиной всегда становится безалаберность самого пользователя. В поступившем на электронную почту письме от неизвестного источника, содержащем интересующую информацию, содержится ссылка, переход по которой может привести к загрузке вредоносной программы. Переход на интернет-странице по ссылке на загрузку интересующего контента, вместо требуемого приложения грузится вредоносное программное обеспечение. Такие программы могут маскироваться под любой контент, требующей загрузки на компьютер пользователя.

Для безопасной работы в сети желательно использовать сайты с протоколом HTTPS. Такие сайты используют протоколы SSL и TSL для шифрования соединения.

Ограничения, наложенные пандемией, на перемещения и очные встречи заставили значительную часть общества перейти для общения в социальные сети. Такое безобидное время препровождение также может представлять определенную угрозу. Мошенники часто создают поддельные профили, чтобы вступить в переписку с доверчивыми пользователями. Используя методы социальной инженерии, выступая в роль внимательного и сочувствующего слушателя киберпреступники выманивают у пользователя сведения конфиденциального характера.

Злоумышленнику иногда даже нет необходимости вступать в переписку с заинтересовавшим его лицом, чтобы получить необходимые данные. Используя социальные сети, пользователи часто даже не имеют представление о том, что отображаемую в сети информацию можно настраивать, ограничив доступ посторонних к персональным данным. Информацию, которая необходима мошеннику, пользователи обычно сами и публикуют, например, когда заполняют данные о себе при регистрации в социальных сетях. Эти опубликованные данные содержат достаточно большое количество реальных сведений о пользователе (имя, фамилия, дата рождения и т. д.).

Размещая информацию в интернете, нужно помнить, что интернет – это публичное место и любой может увидеть, что там опубликовано. Один раз размещенная информация, фотография остается там навсегда. Не используя специального программного обеспечения, а пользуясь стандартными поисковыми системами можно получить огромное количество данных конфиденциального харак-

тера о пользователях сети. Основной принцип защиты заключается в простой рекомендации – тщательно выбирать информацию, которая планируется к опубликованию. Информация, опубликованная в сети, может быть использована против ее владельца в реальной жизни.

В данной статье нами были рассмотрены основные угрозы безопасности информации, с которыми сталкиваются пользователи сети Интернет. Соблюдение простейших правил поведения в сети и обращения с информационными ресурсами позволят обезопасить работу в интернете и защитить свои данные.

Список литературы

1. Как защитить себя в интернет // Личные инвестиции и финансы. – URL: https://invlab.ru/texnologii/kak-zashhitit-sebya-v-internete/ (дата обращения: 20.04.2021).

2. Цена приватности в интернете: готовы ли пользователи рисковать личными данными? // Официальный сайт компании «Лаборатория Касперского». – URL: https://www.kaspersky.ru/blog/privacy-report-2019-summary/22730/ (дата обращения: 20.04.2021).

3. 12 способов как защитить себя в интернете // Официальный сайт компании «Лаборатория Касперского». – URL: https://www.kaspersky.ru/resource-center/threats/internet-and-individual-privacy-protection (дата обращения: 20.04.2021).

Крылова С. В.[1]***,***
курсант факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Клочкова Е. Н.[2]***,***
доцент кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя

АУДИТ КАК СПОСОБ КОНТРОЛЯ И ПРОВЕРКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация с каждым годом приобретает все большую ценность. Развитие современных информационных технологий привело к тому, что для доступа к информации теперь нет необходимости находиться в непосредственной близости от нее. Зачастую доступ к ней осуществляется с использованием дистанционных технологий. Для обеспечения безопасности своей информации органы государственной власти, правоохранительные органы, коммерческие организации создают различные системы защиты информации. Для поддержания их в актуальном состоянии надо регулярно осуществлять контроль и проверку информационной безопасности. В настоящее время аудит большими темпами набирает популярность.

Аудит информационной безопасности – мероприятия по оценке состояния информационной безопасности информационной автоматизированной системы и разработки рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных ресурсов информационной системы от угроз ИБ [1].

Аудит информационной безопасности проводится с целью оценки защищенности объекта. Аудит обычно включает в себя серию тестов, которые гарантируют, что информационная безопасность соответствует всем ожиданиям и требованиям, предъявляемым либо нормативными документами, либо руководством организации.

Аудит информационной безопасности позволяет учитывать все технические и организационные аспекты при проектировании системы защиты информационной безопасности в организации, в соответствии с требованиями законодательства. Аудит систем информационной безопасности может проводиться как в виде внутреннего аудита – проводится собственными специалистами по защите информации, так и внешнего – например с участием представителей органов по аттестации. Аудит может включать в себя анализ документов в области информационной безопасности и организационных аспектов, для его проведения может использоваться специальное программное обеспечение.

Проведение аудита – один из методов, позволяющих выявить существующие проблемы информационной безопасности, однако и он имеет недостатки. Одной из типичных ошибок при проведении аудита является то, что при проверке зачастую нет четкого понимания цели и результата, который необходимо получить. Не всегда руководитель подразделения, где проводится аудит, понимает и формулирует цели и задачи для исполнителя. Тогда аудитор должен сформулировать вопросы, которые предполагают конкретный ответ, т. е. по итогу должен получиться перечень узких областей, на которые будет обращено особое внимание.

Для выявления таких направлений целесообразно проводить беседы с сотрудниками, которые непосредственно работают в данной области и имеют представление о том, какие уязвимости имеются и могут быть выявлены в процессе деятельности организации. Не обсуждение с аудитором цели и результатов проведения аудита приводит к тому, что по итогу заказчик не получает желаемого результата. Необходимо показывать уровень решаемых проблем.

При возможном появлении новых угроз возникает необходимость корректировки требований к процедурам и критериям безопасности, что существенно осложняет формирование итогового отчета при оценке рисков. При этом возникают требования по составлению методики практического анализа, опирающегося на специфику объекта исследования. Для этого можно использовать комбинированный анализ рисков и стандартов информационной безопасности, соблюдая такое условие, что эти стандарты актуальны, т. е. существуют и применяются в подразделениях. Это поможет сузить поле применения методик анализа рисков и расширить поле анализа на основе аудита рисков.

Одним из основных правил для проведения аудита является понимание, как выглядит «нормальное» поведение системы и какие сведения в ней обрабатываются. Именно здесь вступает в силу установление базовой линии безопасности. Для его построения можно воспользоваться существующими нормативными документами и опытом внутренних специалистов.

Сведения, необходимые для оценки рисков безопасности, часто разбросаны по нескольким консолям управления информационной безопасностью. Отслеживание всех этих деталей – это довольно трудоемкая задача, поэтому важно централизовать права доступа к данным, выявить основные объекты, которые подлежат защите.

При проведении аудита возможно возникновение сложностей, связанных с созданием и использованием специализированных стендов для проведения тестирования на устойчивость системы, учитывающих специфику технологических сетей подразделений.

Тестирование проводится путем наблюдения за работой исследуемого объекта при конечном наборе определенных специалистом ситуаций. При составлении плана тестирования учитываются требования, связанные с проверкой на стенде устойчивости компонентов системы:

– проверка надежности обеспечения работоспособности интерфейсов и терминалов защиты;

– управление техническими процессами и устройствами нижних уровней системы управления с возможными в последующем критическими повреждениями (например, модификацию блокировок или передачу недокументированных и запрещенных команд) [3].

Оценка безопасности системы и подготовка к аудиту могут потребовать много усилий. Чтобы немного упростить процесс проведения аудита, предлагается небольшой список простых задач, которым стоит уделять внимание:

Документирование текущей политики и процедур безопасности.

Анализ журналов действий, для проверки выполнения требований политики и процедур безопасности.

Отбор сотрудников, которым требуется обучение или повышение квалификации по направлению информационная безопасность.

Создание внутренних правил информационной безопасности, включающее как издание необходимых нормативно-методических документов, так и изучение ее сотрудниками.

Проведение самотестирования имеющегося программного обеспечения, предназначенного для выявления уязвимостей любого рода.

Проверка порядка хранения и обращения со сведениями конфиденциального характера.

Использование при необходимости методов шифрования.

Анализ существующих беспроводных сетей, проверка их безопасности, идентификация каждой точки доступа к сети, отбор и деактивация сетей, в которых нет необходимости.

Обеспечение резервирования значимой информации. Одним из возможных решений для информации, не составляющей государственную тайну, может стать использование облачных сервисов. В отличие от физических средств хранения информации, здесь отсутствуют угрозы, связанные со скачками напряжения, пожарами, стихийными бедствиями, воровством.

Анализ журналов событий, для сведения к минимуму ошибок, происходящих из-за человеческого фактора.

Протоколирование деталей аудита, включая кто проводит аудит, и какая сеть подвергается аудиту, для обеспечения своевременного и легкого доступа к этой информации.

Для успешного проведения аудита информационной безопасности необходимо:

– активное участие руководства организации в проведении проверок;

– независимость и объективность аудиторов (экспертов), их высокая профессиональность и компетентность;

– четко определенная структура проведения проверки;

– использование разработанных мер обеспечения защиты информационной безопасности.

Результатом выполненного аудита информационной безопасности становится документ, содержание которого включает следующую информации:

– об обнаруженных рисках информационной безопасности;

– о выявленных уязвимостях объекта аудита;

– об опасности, возможной при найденных уязвимостях;

– о последствиях в случае осуществлении угроз;

– рекомендации по устранению уязвимостей [4].

После проведения аудита информационной безопасности и предложенных рекомендаций, создается грамотная и надежная система безопасности, которая минимизирует возможные риски информационной безопасности и повышает защищенность системы.

Таким образом, аудит как способ контроля и проверки информационной безопасности – одно из важнейших мероприятий при создании и оценки функционирования системы защиты объекта информатизации.

Каждый системный администратор должен замечать и реагировать, если безопасность его ИТ-инфраструктуры находится под угрозой. Проведение периоди-

ческих аудитов поможет выявлять слабые места на ранней стадии и устанавливать соответствующие исправления. Также аудит даст возможность установить базовый уровень безопасности, который можно использовать регулярно, чтобы увидеть, какие есть улучшения в защите информации и какие области все еще могут быть подвергнуты опасности.

Проведение аудита безопасности подразделения позволит:

– сформировать единую политику и концепцию безопасности информации;

– рассчитать, согласовать и обосновать необходимые затраты на защиту информации;

– объективно и независимо оценить уровень информационной безопасности;

– эффективно создавать и использовать профили безопасности конкретного подразделения на основе качественных и количественных методов многократного тестирования и корректировки, используемых для оценки информационной безопасности [5].

При проведении аудита информационной безопасности возникает немало затруднений. Важно не пренебрегать правилами проведения и более тщательно и требовательно относиться к описанию и определению практик проведения аудита каждой рассматриваемой области.

Список литературы

1. Аверичников, В. И. Аудит информационной безопасности органов исполнительной власти : учебное пособие / [В. И. Аверичников и др.]. – М. : Флинта, 2011.

2. Баймакова, И. А. Обеспечение защиты персональных данных / И. А. Баймакова. – М. : Изд-во 1С-Паблишинг, 2010.

3. Покровский, П. Оценка информационных рисков / П. Покровский. – 2004. – № 10.

4. Efsol. – URL: https://efsol.ru/promo/info-security-audit.html (дата обращения: 14.04.2021).

5. ЦЛС Прогресс. – URL: https://licenziya-fsb.com/aktivnyiy-audit-informatsionnoy-bezopasnosti (дата обращения: 15.04.2021).

Лустин В. И.[1]*,*
старший преподаватель кафедры информационной
безопасности учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя

ОТДЕЛЬНЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Вопросы информационной безопасности являются приоритетными направлениями развития государственной политики страны современного мирового сообщества. Широкое использование и развитие информационных технологий ведут к дальнейшему нарастание угроз информационной безопасности в России и во всем мире. В целях недопущения потери информационного суверенитета государства необходимо эффективно противостоять таким угрозам на основе комплексных эффективных скоординированных мер по всем направлениям проведения политики информационной безопасности.

Как показало исследование по данным Positive Technologies, общее количество киберинцидентов в 2020 г. выросло на 51 % по сравнению с 2019 г. Семь из десяти атак носили целенаправленный характер. Больше всего злоумышленников интересовали государственные учреждения (19 %), промышленные компании (12 %) и медицинские организации (9 %) [3].

31 декабря 2015 г. Указ Президента Российской Федерации В. В. Путина № 683 утвердил действующую и в настоящее время Стратегию национальной безопасности Российской Федерации. Предшествующий этому период характеризуется укреплением России на фоне новых угроз национальной безопасности, сопровождающийся ростом глобальной и региональной нестабильности. Западные страны, воплощая политику сдерживания России, оказывают политическое, экономическое, военное и информационне давления, используя такие меры воздействия, как «гибридные войны», информационные войны, идеологические и кибердиверсии диверсии, что ведёт к угрозам информационному суверенитету нашей страны [1].

Основные положения Стратегии национальной безопасности 2016 г. применительно к информационной политике России уточнены и развиты во второй,

действующей в настоящее время, Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 5 декабря 2016 г. № 646 [2].

Использование информационных технологий во всех сферах общественной жизни предоставляет возможность человечеству реализовать свои потребности, минуя территориальные границы государств. Такой процесс глобализации возможен на основе унификации и стандартизации всех задействованных информационных процессов. Однако возникает для отдельных стран и регионов существенная опасность утраты своей автономности, основ самобытности.

Развитие информационного общества возможно при наличии противоположных факторов:

1) усложнение общественной организации и, следовательно, возрастании неустойчивости;

2) укрепление внутренней устойчивости путем совершенствования различных форм управления.

Данные противоречия связаны с новыми свойствами информационного общества: быстросменяемые события вследствие трансграничного характера информации, существующей реальном и виртуальном пространстве. Немаловажное значение имеет сочетание неограниченного, даже избыточного роста объёма информации с запаздыванием её освоения и применения, что ведёт к нарушению равновесия информационного общества. Поэтому для устойчивого и поступательного движения системы требуются развитие существующих и разработка новых методов и способов сохранения информационной безопасности.

Характерное отличие информационного общества в том, что информационное пространство встраивается между человеком и общественными институтами, а взаимоотношения людей все большей степени опосредуются информационной средой. В итоге отношение человека к информации выходит на первый план в общественной жизни, а на второй план – социальные связи, выраженные в символике и нормах культуры, местных обычаях и традициях.

Межличностные отношения в информационном обществе становятся все менее устойчивыми, а виды связей, существующие в обществе, можно разделить на следующие категории:

– кратковременные контакты;

– среднесрочные (дружеские, соседские, профессиональные);

– длительные (родственные, семейные).

По мере развития информационного общества кратковременные модульные отношения функционального характера занимают ведущее место. При этом каждый из участников таких взаимоотношений становится взаимозаменяем, увеличивается риск расхождения индивидуальных и групповых ценностных ориентаций, что порождает резкий рост субкультур и может увеличить степень противоречивости самого общества.

Одной из особенностей современного этапа является отставание реакции общества от поступательного развития информационной среды. С учетом этого информационную безопасность необходимо рассматривать как одну из главных составляющих формирования и развития информационного общества в стране.

Проводимые научные разработки по решению проблем в области информационной безопасности концентрируются на технической составляющей защиты информации от искажения, уничтожения, утечки и т. д. Важнейшая задача национальной безопасности России заключается в комплекс вопросов, требующих концептуально-мировоззренческого, научного и правового обеспечения. Для этого требуются выявление глубинных причин возникновения данных проблем, определение конкретных факторов и источников, которые обеспечивают – субъективно и объективно – воспроизводство и развитие такой ситуации. А основным «объектом», ответственным за безопасность, является способность системы порождать обратные связи – средство, которое как раз и обеспечивает дистанцию между системой (параметрами ее настройки и функционирования) и средой.

Именно в этом методологическом требовании видится основание стабилизации общества, различных его подсистем. Другими словами, система самовоспроизводит саму себя в виде совокупности элементов, в создании коммуникаций и формировании смыслов.

Развитие информационных технологий оказывает влияние на все сферы жизнедеятельности общества и государства, затрагивает правовые системы в мировом масштабе. При этом использование цифровых технологий в правовых системах различных государств имеет свои специфические особенности, обусловленные концептуальными основами национального законодательства, что также необходимо учитывать при внесении необходимых изменений в нормативную базу, регламентирующую обеспечение информационной безопасности в Российской Федерации.

Список литературы

1. Стратегия национальной безопасности Российской Федерации // Официальный сайт Президента России. - URL: http://www.kremlin.ru/acts/bank/40391/page/1 (дата обращения: 20.04.2021).

2. Доктрина информационной безопасности Российской Федерации // Официальный сайт Президента России. – URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 20.04.2021).

3. Официальный сайт компании Positive Technologies. – URL: www.ptsecurity.com/ru-ru/about/news/positive-technologies-chislo-atak-na-promyshlennye-kompanii-vyroslo-na-91-po-sravneniyu-s-2019-godom (дата обращения: 20.04.2021).

Макуха М. Ю.[1]*,*
преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

Богданов Д. С.[2]*,*
преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

Горюн К. Н.[3]*,*
преподаватель кафедры
информационной безопасности
Краснодарского университета МВД России

ПРЕДЛОЖЕНИЯ ПО СОВЕРШЕНСТВОВАНИЮ ПОРЯДКА ПРЕКРАЩЕНИЯ ДОСТУПА К СЕРВИСАМ ИСОД МВД РОССИИ

В статье описан регламентированный порядок прекращения доступа к ИСОД МВД России сотрудников МВД России после их увольнения из органов внутренних дел, приведена блок-схема данного процесса. Описан способ совершенствования порядка прекращения доступа к ИСОД МВД России и приведена блок-схема предложенного порядка.

Сервисы ИСОД на сегодняшний день предоставляют широкий спектр возможностей для сотрудников органов внутренних дел. Каждый из существующих сервисов выполняет свои функции соответствующим образом и способствует эффективному и своевременному решению сотрудниками служебных задач.

Для получения доступа к сервисам ИСОД сотрудник должен иметь учетную запись в системе управления доступом к информационным системам и ресурсам ИСОД МВД России. Управление учетными записями сотрудников МВД России при предоставлении им доступа к сервисам ИСОД МВД России осуществляется в соответствии с «Регламентом управления учетными записями сотрудников МВД России при доступе к сервисам единой системы информационно-аналитического обеспечения деятельности МВД России».

В случае увольнения сотрудника из органов внутренних дел учетная запись соответствующего сотрудника в системе управления доступом к информационным системам и ресурсам ИСОД МВД России подлежит блокировке. В рамках прекращения доступа к сервисам ИСОД МВД России существует регламентированный порядок полного блокирования учетной записи:

1. В течение трех рабочих дней сотрудники кадрового подразделения уведомляют администратора (оператора) доступа подразделения, в котором проходил службу сотрудник, о факте увольнения, направляя ему на служебный почтовый адрес посредством сервиса электронной почты МВД России сообщение с указанием номера и даты приказа об увольнении и о необходимости полного блокирования учетной записи.

2. После получения информации о необходимости полного блокирования учетной записи администратор (оператор) доступа производит временное блокирование учетной записи, оформляет заявку на изменение учетных записей пользователей и в срок не более одного дня отправляет ее в единый центр эксплуатации ИСОД МВД России с помощью сервиса электронной почты МВД России для полной блокировки учетной записи.

3. Оператор единого центра эксплуатации регистрирует заявку и сообщает администратору (оператору) доступа уникальный идентификатор заявки. В срок не более одного рабочего дня выполняет полное блокирование учетной записи.

4. О результате полного блокирования учетной записи посредством сервиса электронной почты МВД России администратору (оператору) доступа поступает подтверждение.

5. Получив подтверждение, администратор (оператор) доступа с использованием сервиса электронной почты МВД России уведомляет сотрудников кадрового подразделения, в котором проходил службу пользователь, уволенный из органов внутренних дел [1, с. 22–24].

Блок-схема процесса полной блокировки учетных записей сотрудников, уволенных из органов внутренних дел представлена на рис. 1.

В связи с человеческим фактором и неотлаженном взаимодействии сотрудников кадровых подразделений и администраторов (операторов) доступа процесс полной блокировки учетной записи системы управления доступом к информационным системам и ресурсам ИСОД МВД России может протекать некорректно, что может повлечь возникновение высокой вероятности угрозы несанкционированного доступа к учетной записи после увольнения сотрудника, в случае если учетная запись не была своевременно заблокирована.

Во исполнение поручения Министра внутренних дел Российской Федерации генерала полиции В.А. Колокольцева по докладной ДИТСиЗИ МВД России от 07.11.2020 № 9/10016 Департаментом государственной службы и кадров

МВД России проведен анализ активности учетных записей ИСОД МВД России в результате которого выявлены множественные случаи несанкционированного использования учетных записей уволенных сотрудников для доступа в ИСОД МВД России. В целях противодействия риску возникновения описанных фактов ДГСК МВД России запланированы работы по организации информационного взаимодействия сервиса обеспечения кадровой деятельности (СОКД) и сервиса управления доступом к информационным системам и ресурсам (СУДИС) ИСОД МВД России в части автоматизированного уведомления СУДИС об увольнении сотрудника при внесении соответствующей информации в СОКД для блокировки его учетной записи.

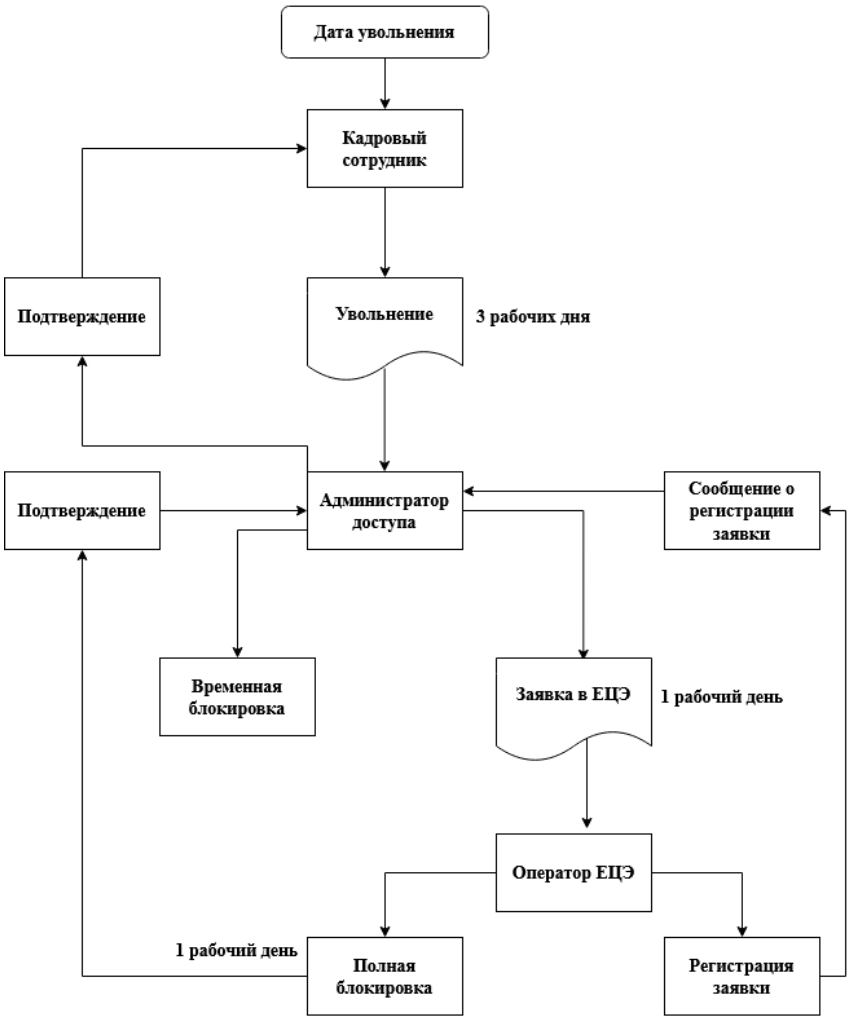


Рис. 1. Блок-схема процесса полной блокировки учетных записей

В контексте совершенствования порядка прекращения доступа к ИСОД МВД России ключевое значение имеет тот факт, что сотрудники кадрового подразделения помимо уведомления администратора (оператора) доступа также вносят информацию об увольнении сотрудника в подсистему «электронное личное дело сотрудника» сервиса обеспечения кадровой деятельности. Учету в сервисе обес-

печения кадровой деятельности подлежит информация об объектах учета сотрудников, проходящих или проходивших службу в органах внутренних дел Российской федерации [2, с. 5].

Объектами учета сервиса обеспечения кадровой деятельности являются:

– послужной список;

– карточка полномерного учета;

– служебная карточка;

– выданные, сданные, утерянные и уничтоженные служебные удостоверения МВД России, а также использованные бланки служебных удостоверений МВД России;

– и др. [2, с. 5].

В целях совершенствования порядка прекращения доступа к ИСОД МВД России предлагается модифицировать процесс проверки статуса учетных записей сотрудников посредством автоматизированных запросов со стороны единого центра эксплуатации к базе сервиса обеспечения кадровой деятельности. В случае если в базе сервиса обеспечения кадровой деятельности сотрудник числится уволенным, а единый центр эксплуатации не имеет информации об этом, то оператор единого центра эксплуатации производит временную блокировку учетной записи системы управления доступом к информационным системам и ресурсам ИСОД МВД России.

В случае истечения пяти рабочих дней с момента временной блокировки, если в единый центр эксплуатации не поступит заявка на изменение учетных записей пользователей, оператор единого центра эксплуатации ИСОД МВД России производит полную блокировку учетной записи системы управления доступом к информационным системам и ресурсам ИСОД МВД России с последующим уведомлением администратора (оператора) доступа подразделения, в котором проходил службу сотрудник, о факте полного блокирования учетной записи, направляя ему на служебный почтовый адрес сервиса электронной почты МВД России сообщение.

Блок-схема процесса полной блокировки учетных записей сотрудников, уволенных из органов внутренних дел, с учетов предложений представлена на рис. 2.

Предложенный порядок позволит предотвратить нарушения сроков блокировки учетных записей и исключить возможность использования учетных записей сотрудников после их увольнения из органов внутренних дел, что приведет к минимизации угроз несанкционированного доступа к сервисам ИСОД МВД России.

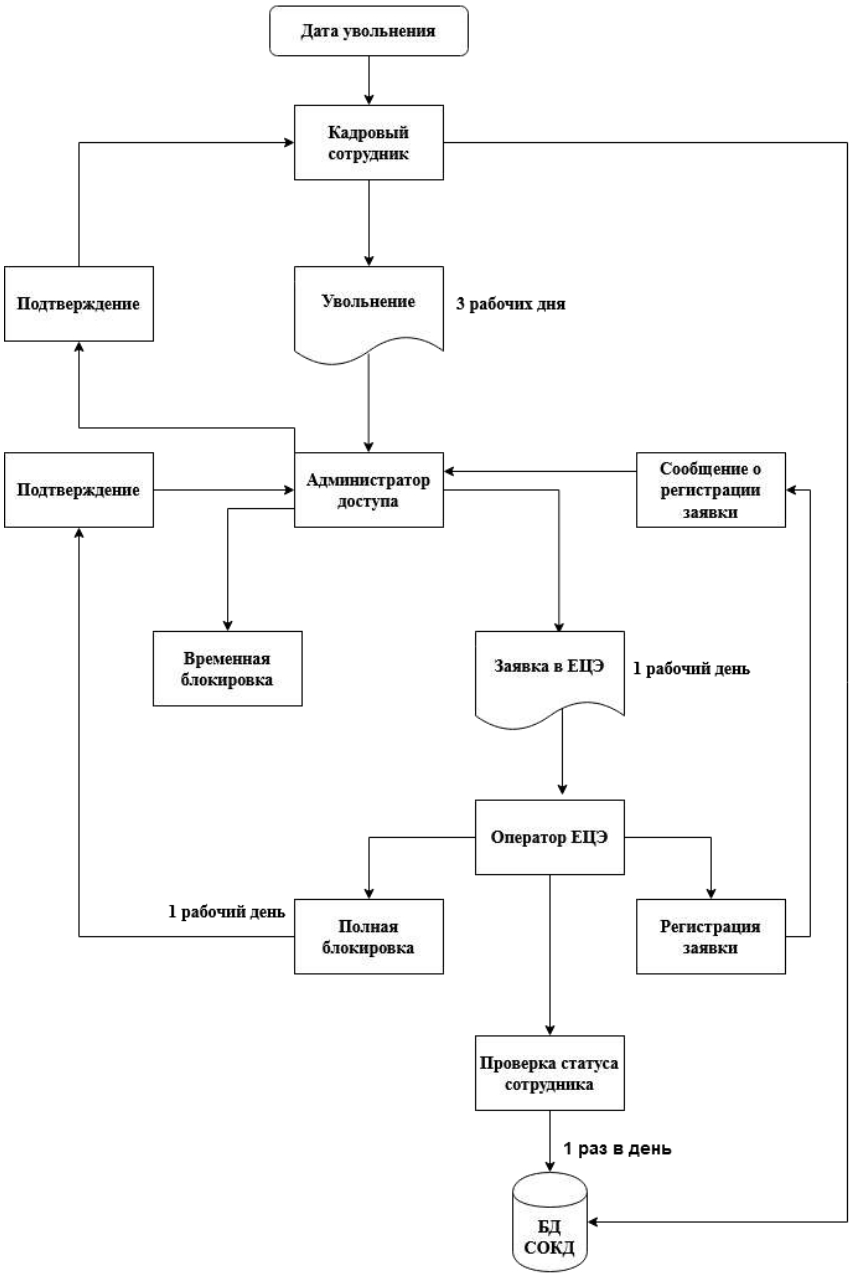


Рис. 2. Блок-схема процесса полной блокировки учетных записей, с учетом предложений

Список литературы

1. Регламент управления учетными записями сотрудников МВД России при доступе к сервисам единой системы информационно-аналитического обеспечения деятельности МВД России. – М., 2018.

2. Приказ МВД России от 28.06.2016 № 349 «Вопросы эксплуатации программного обеспечения для реализации Сервиса обеспечения кадровой деятельности» // опубликован не был.

Шадский В. В.[1]*,*
адъюнкт
Краснодарского высшего военного училища

Чекмарев М. А.[2]*,*
адъюнкт
Краснодарского высшего военного училища

Дудко А. Л.[3]*,*
сотрудник
Краснодарского высшего военного училища

Сизоненко А. Б.[4]*,*
сотрудник
Краснодарского высшего военного училища,
доктор технических наук, доцент

МЕТОДИКА ОПРЕДЕЛЕНИЯ АРХИТЕКТУРЫ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ СЕМАНТИЧЕСКОГО ПОИСКА С ИСПОЛЬЗОВАНИЕМ МЕТОДА АНАЛИЗА ИЕРАРХИЙ

Вопросам систематизации, структурирования и поиска информации в любой организации уделяется большое внимание. Это связано с тем, что информация стала важным ресурсом, оперативное извлечение которой влияет на успешность ее функционирования в целом. Практически в каждой организации циркулируют персональные данные, большое значение уделяется коммерческой тайне. Кроме того, существуют и другие виды конфиденциальной информации, от которых также зависит повседневная жизнедеятельность. Поэтому успешное решение задачи своевременного и оперативного поиска такой информации для принятия решений, а также для реализации других целей становится жизненно необходимым.

Реализуя данное требование, предлагается прибегнуть к методам машинного обучения, положительно зарекомендовавших себя и показывающих в настоящее

время достаточно высокие результаты в сфере информационного поиска [1], способных выдать пользователю наиболее релевантные запросы, учитывая его предпочтения и, порой, некорректные формы выражения мысли.

Взяв во внимание специальные области научных знаний, следует отметить, что для достижения этих целей необходимо обучить нейронную сеть на наборах данных, которые, к сожалению, отсутствуют в достаточном количестве. В связи с этим необходимо прибегнуть к ряду мер, позволяющих улучшить качество обучения при фиксированном объеме обучающих данных. К одной из таких мер можно отнести выбор оптимальной архитектуры нейронной сети. При этом стоит отметить, что подбор архитектуры нейронной сети носит сугубо интуитивный характер и не имеет четкой формализации и алгоритмизации ввиду большого их разнообразия, а также возрастающей сложности решаемых задач. В данной статье для решения этой проблемы предлагается использовать метод анализа иерархий, предложенный Томасом Саати [2].

Известно, что нейронная сеть включает в себя множество параметров, ключевую роль в которых играет именно архитектура. Выбор архитектуры является первым этапом создания нейронной сети.

Стоит отметить, что на данный момент существует огромный список известных архитектур [3], большая часть из которых образована путем комбинации одних с другими. В общем случае базовые архитектуры нейронных сетей представлены на рис. 1.

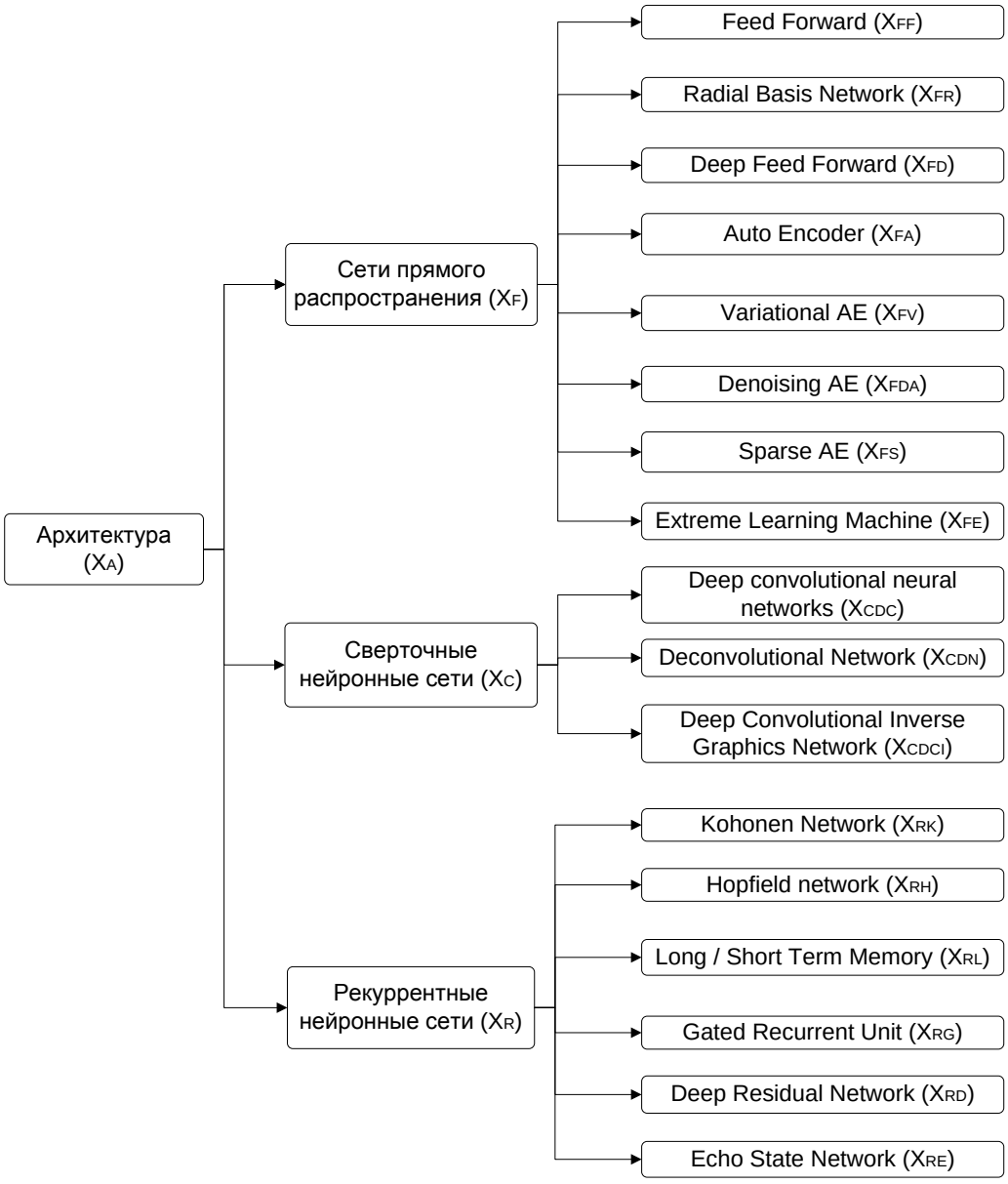


Рис. 1. Классификация архитектур нейронных сетей

Определение критериев для выбора оптимальной архитектуры

Каждая отдельная задача предъявляет собственные требования к структуре нейронной сети. Однако существующее многообразие задач ставит перед собой единственную и ключевую цель – достижение максимально возможного качества работы нейронной сети, под которым в данном случае понимается точность соотнесения поискового запроса пользователя с наиболее релевантным результатом.

Методика выбора оптимальной архитектуры нейронной сети в зависимости от решаемых задач семантического поиска

Методика выбора оптимальной архитектуры нейронной сети для решения конкретной задачи будет состоять из двух этапов.

На *первом этапе* определяется значимость архитектур.

Первый шаг – оценка архитектур первого уровня с составлением матрицы парных сравнений и получением вектора приоритетов.

Сначала составим квадратную матрицу парных сравнений третьего порядка для первого уровня архитектур:

$$A = \begin{pmatrix} 1 & a_{FC} & a_{FR} \\ a_{CF} & 1 & a_{CR} \\ a_{RF} & a_{RC} & 1 \end{pmatrix},$$

где a_{ij} – элементы матрицы, показывающие относительные приоритеты архитектуры i по отношению к архитектуре j.

Далее, путем сложения элементов каждой строки и деления каждой суммы на сумму всех элементов, вычисляется ее собственный вектор-столбец X_A:

$$X_A = \begin{pmatrix} x_F \\ x_C \\ x_R \end{pmatrix},$$

определяющий приоритет той или иной архитектуры первого уровня.

Второй шаг – оценка архитектур второго уровня. Составим 3 квадратных матрицы парных сравнений архитектур второго уровня восьмого, третьего и шестого порядка соответственно (F_8, C_3, R_6) и вычислим векторы приоритетов $X_F, X_C,\ X_R$.

На *втором этапе* происходит выбор наиболее подходящего варианта архитектуры нейронной сети путем перемножения приоритетов первого и второго уровня. Максимальное значение укажет на наиболее подходящую архитектуру нейронной сети для решения конкретной задачи семантического поиска.

Список литературы

1. Искусственный интеллект в поиске. Как Яндекс научился применять нейронные сети, чтобы искать по смыслу, а не по словам // Habr. – URL: https://habr.com/ru/company/yandex/blog/314222/ (дата обращения: 12.04.2021).

2. Саати, Т. Принятие решений: Метод анализа иерархий : учебное пособие / Т. Саати; пер. с англ. Р. Г. Вачнадзе. – М. : Радио и связь, 1993.

3. Введение в архитектуры нейронных сетей // Habr. – URL: https://m.habr.com/ru/company/oleg-bunin/blog/340184/ (дата обращения: 12.04.2021).

Миргородская В. В.[1]***,***
курсант факультета подготовки сотрудников
для подразделений экономической безопасности
и противодействия коррупции
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Дубинина Н. М.,
начальник кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО БОРЬБЕ С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ОБОРОТА ПЛАТЕЖНЫХ КАРТ

Развитие и внедрение информационных технологий в повседневную жизнь общества ускоряют процесс перехода покупателей на современные платежные технологии. Для обеспечения удобства и мобильности совершения безопасных, бесконтактных покупок ведутся разработка и совершенствование различных цифровых платежных решений. Выпуск современных платежных карт позволяет максимально удовлетворить потребности растущей клиентской базы.

В 2020 г. банковские организации выдали 19,2 расчетных и кредитных карт [5]. На каждого жителя России трудоспособного возраста в среднем приходится три платежные карты, а, следовательно, риск стать жертвой преступления достаточно велик. В 2021 г. банковская платежная карта считается наиболее уязвимым инструментом сохранности денег. Эксперты рекомендуют не хранить на ней крупные суммы денежных средств, а пользоваться услугами банков.

Органы внутренних дел осуществляют активный поиск и внедрение в свою практическую деятельность новых форм и методов противодействия преступлениям в сфере оборота платежных карт, а также минимизации размера ущерба от их совершения. Приоритетной задачей является не только выявление и раскрытие таких преступлений, но и разработка и проведение профилактических мероприятий, в том числе путем информирования населения о новых способах их совершения.

---

[1]

Ввиду значительной компьютеризации процессов банковского обслуживания и денежных расчетов в настоящее время большинство преступлений в сфере оборота платежных карт сопровождается незаконным доступом к компьютерной информации, ее копированием или модификацией. Совершение таких преступлений технически достаточно сложно, поэтому преступники объединяются в группы с чётким распределением ролей в процессе подготовки и реализации преступного замысла, обладают высокой квалификацией и глубокими знаниями технологий и организации обращения платёжных карт.

В основе способов совершения преступлений в сфере оборота платежных карт лежит обман, различные мошеннические действия или злоупотребление доверием. Ущерб от компьютерных преступлений в сфере оборота платежных карт с каждым годом растет, а раскрытие подобного рода преступлений сотрудникам органов внутренних дел сопряжено с большими затруднениями (см. рис. 1). Данного рода преступления оказывают значительное влияние на экономическую безопасность России.

Рис. 1. Трудности в раскрытии компьютерных преступлений в сфере оборота платежных карт

Исходя из данных, представленных на рис. 1, видно, что основной проблемой в раскрытии преступлений в сфере оборота платежных карт является трудоемкость доказательства вины.

Особенность проблемы раскрываемости компьютерных преступлений заключается в том, что эффективное противостояние им каждым государством в отдельности может быть затруднено. Злоумышленники, используя специальное программное обеспечение, могут определять и затем продавать номера действительных счетов кредитных карт, распространять пароли, идентификационные

номера, кредитную и другую личную информацию через компьютерные сети, что позволяет, не находясь физически на территории конкретной страны, получать незаконный доступ к кредитным офисам и компьютерным системам финансовых учреждений. Необходимо объединение усилий всего мирового сообщества в борьбе с данным видом преступлений.

В результате анализа статистики Главного информационно-аналитического центра МВД России допустимо выделить следующие тенденции развития компьютерной преступности:

– высокие темпы роста, активное вовлечение в преступные сообщества новых участников;

– повышение корыстной мотивации граждан;

– усложнение способов совершения компьютерных преступлений;

– нарастание криминального профессионализма преступников;

– увеличение доли лиц, не привлекавшихся ранее к уголовной ответственности;

– увеличение материального ущерба от компьютерных преступлений в общей доле ущерба от прочих видов преступлений;

– перерастание компьютерной преступности в класс международной преступности, что значительно подрывает не только экономическую безопасность, но и национальную [3].

По данным МВД России, в первом квартале 2021 г. в IT-сфере совершено на 33,7 % больше преступлений, чем год назад, в том числе с использованием интернета – на 51,6 % и при помощи средств мобильной связи – на 31,6 %. В аналогичном периоде прошлого года удельный вес таких деяний составлял 19,9 % общего числа зарегистрированных преступлений, а за три месяца текущего года увеличился до 27,1 %. При этом число «классических преступлений» снижается: разбоев стало меньше на 19,3 %, грабежей – на 25,2 %, краж – на 5,9 %, угонов транспортных средств – на 41,2 % [4].

Предупреждение компьютерных преступлений в сфере оборота платежных карт, становится одним из приоритетных направлений деятельности органов внутренних дел. Процент раскрываемости данных преступлений невелик, что свидетельствует о сложности раскрываемости такого рода преступлений; о недостаточном уровне взаимодействия между сотрудниками органов внутренних дел государства с международными службами, уполномоченными осуществлять борьбу с киберпреступностью; о нехватке профессиональных знаний и навыков при раскрытии высокотехнологичных преступлений.

Придерживаясь общеизвестных рекомендаций можно значительно снизить риск оказаться жертвой такого рода преступлений. Человеческий фактор здесь

играет особую роль. Зачастую жертвы преступлений сами облегчают доступ к своим личным данным, записывая пин-коды, номера счетов, пароли в легкодоступных местах, а то и на самой банковской карте, отправляют номера своих карт в СМС, не прикрывают клавиатуру банкомата или платежного терминала при наборе пин-кода, легкомысленно относятся к наличию посторонних подозрительных приспособлений на банкомате, оформляют заказы в сомнительных интернет-магазинах, оставляя полный комплект персональных данных на сайте. К тому же у граждан нашей страны не выработался навык работы с банками, отсутствует уважительное отношение к рекомендациям банковских служащих по вопросам грамотного распределения средств на различных счетах и картах, незамедлительном уведомлении об изменении своих данных в соответствующее отделение банка и пр.

Снижение роста финансовых мошенничеств с использованием методов социальной инженерии – одно из основных направлений противодействия преступному киберсообществу.

Использование электронных денег, компьютеризация и автоматизация системы по обороту денежных средств создает дополнительные возможности незаконного обогащения, так как для расчетов через интернет иногда достаточно знать только реквизиты платежной карты. Самым распространенным способом преступного посягательства является хищение денежных средств с банковских карт в интернет-магазинах.

Изучение и обобщение правовых позиций и практики правоохранительных органов позволяют сформулировать направления совершенствования противодействия компьютерным преступлениям в сфере оборота платежных карт и обеспечения экономической безопасности России:

1. Создание международных правоохранительных центров по борьбе с киберпреступностью, которые бы незамедлительно реагировали на противоправные деяния, сотрудничая с Интерполом.

2. Модернизация уголовно-правовых норм для борьбы в сфере компьютерной безопасности.

3. Создание межгосударственных следственно-оперативных групп для расследования преступлений по всему миру.

4. Формирование единой политики на международной арене в области противодействия преступности в сфере высоких технологий и создание модели технического сотрудничества.

5. Комплексное технико-программное решение задачи в сфере защиты персональных данных платежных карт.

Таким образом, развитие информационных технологий не только способствовало стремительному прогрессу общества, расширило возможности общения между людьми, подняло на новую ступень возможности экономики, науки, образования, но и стало одной из причин возникновения и развития определенных негативных процессов. Одним из них стало появление компьютерной преступности в сфере оборота платежных карт.

Противодействие преступлениям в сфере компьютерной информации, мошенническим действиям с использованием возможностей электронных платежных систем, пресечение противоправных действий в информационно-коммуникационных сетях, международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий, требует дальнейшей научной проработки указанных вопросов и совершенствования практических методик их осуществления.

Список литературы

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ (ред. 08.04.2021) // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.04.2021).

2. Шаньгин, В. Ф. Защита компьютерной информации / В. Ф. Шаньгин. – М. : ДМК Пресс, 2017.

3. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. Ч. 1 / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019.

4. Статистика и аналитика // Официальный сайт Министерства внутренних дел Российской Федерации. – URL: https://мвд.рф/Deljatelnost/statistics (дата обращения: 20.04.2021).

5. Российские банки выдали рекордное количество кредитных карт за 7 лет. // Информационный портал Бирнес.ру. – URL: https://www.business.ru/news/22677-rossiyskie-banki-vydali-rekordnoe-kolichestvo-kreditnyh-kart-za-7-let (дата обращения: 19.04.2021).

Зюзько А. Ю.[1],
сотрудник
Краснодарского высшего военного училища,
кандидат педагогических наук, доцент

Попова Ю. Н.[2],
сотрудник
Краснодарского высшего военного училища,
кандидат педагогических наук, доцент

Щербаков В. А.[3],
научный сотрудник
Краснодарского высшего военного училища

О НАПРАВЛЕНИИ СОВЕРШЕНСТВОВАНИЯ ДЕЯТЕЛЬНОСТИ ДОЛЖНОСТНЫХ ЛИЦ ПО ВВОДУ В ЭКСПЛУАТАЦИЮ ОБЪЕКТОВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ВЕДЕНИЯ РАБОТ С ИНФОРМАЦИЕЙ ОГРАНИЧЕННОГО ДОСТУПА

Одним из основных требований при осуществлении работ, обсуждении, хранении и обработке информации ограниченного доступа является обеспечение её конфиденциальности [1].

Обработка информации ограниченного доступа производится с использованием различных информационных технологий, под которыми понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [1].

Вне зависимости от избранной информационной технологии, работы с информацией ограниченного доступа проводятся в специализированных помещениях предприятий различных форм собственности, силовых структур (служебные помещения, хранилища и пр. – далее объекты). Кроме того, на объектах производится обсуждение вопросов, содержащих такую информацию, следовательно, для эффективного обеспечения конфиденциальности информации требуется реализация ряда дополнительных мер (по сравнению с обычными служеб-

[1] Зюзько А. Ю., 2021.
[2] Попова Ю. Н., 2021.
[3] Щербаков В. А., 2021.

ными помещениями структурных подразделений и должностных лиц), установленных руководящими документами в области технической защиты информации и защиты информации в автоматизированных системах [2].

Размещение, оборудование и охрана объектов должны исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в них носителей конфиденциальной информации, а система организационно-технических мероприятий реализовать защиту информации ограниченного доступа от несанкционированного доступа и утечки по техническим каналам.

Помимо технической стороны выполнения мероприятий ввода в эксплуатацию объектов есть значительные трудозатраты должностных лиц по разработке организационно-распорядительных и отчётных документов.

Одним из направлений совершенствования мероприятий по вводу в эксплуатацию объектов авторы предлагают рассматривать внедрение информационной системы – совокупность содержащейся в базах данных информации, обеспечивающих её обработку информационных технологий и технических средств, которая может быть реализована путём создания и применения специализированного программного обеспечения, которое позволит выполнять:

– заблаговременное формирование шаблонов документов в электронном виде;

– приём от пользователя данных об объекте (в заранее определённом формате) и их импорт в создаваемые документы;

– создание и сохранение документов, определённых процедурой ввода объектов в эксплуатацию, путём заполнения заранее сформированных шаблонов;

– вывод на печать полного комплекта необходимых документов.

В целях повышения оперативности и обоснованности деятельности должностных лиц по вводу объектов авторами разработана и в настоящее время проходит процедуру регистрации в ФИПС программа для ЭВМ «Информационно-справочная система поддержки деятельности должностных лиц по вводу объектов для специализированных работ» (см. рис. 1) (далее – Программа).

Раздел меню Программы «Последние модули» позволяет реализовать оперативный доступ к ранее использовавшимся модулям, созданным пользователем самостоятельно, или предоставленным ему их обладателем (см. рис. 1).

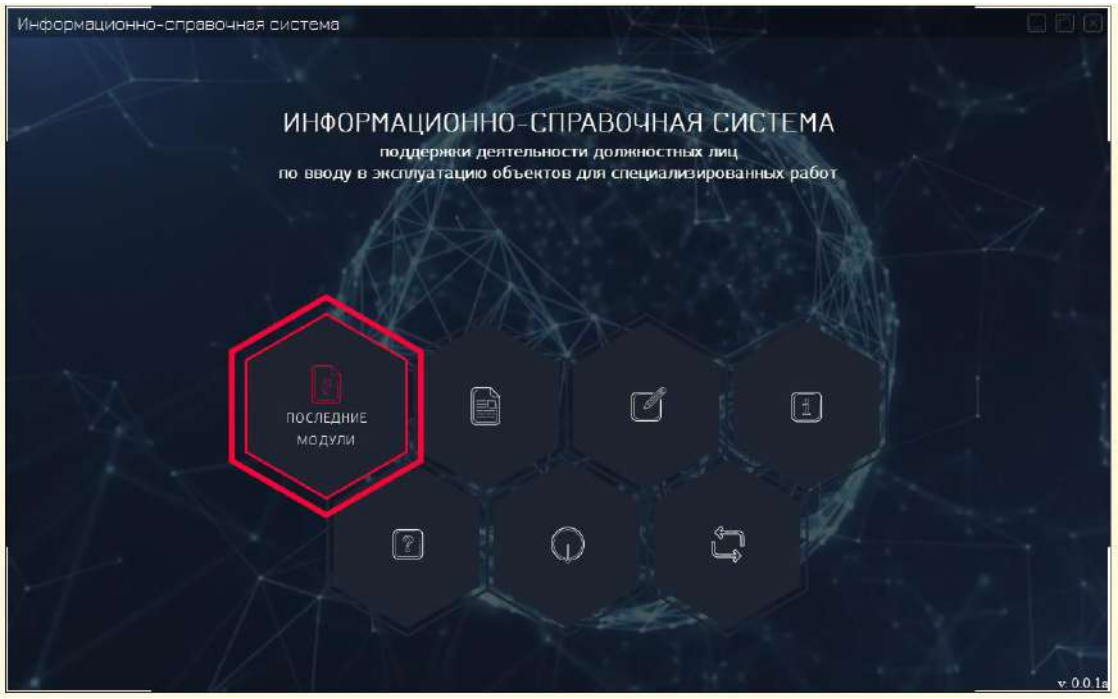


Рис. 1. Раздел меню Программы «Последние модули»

Раздел меню Программы «Открыть модуль» позволяет открыть ранее созданный или импортированный модуль, не использовавшийся пользователем ранее для формирования документов по вводу в эксплуатацию одного объекта, но необходимый для другого, либо применяется, когда модули размещены в различных директориях (см. рис. 2).

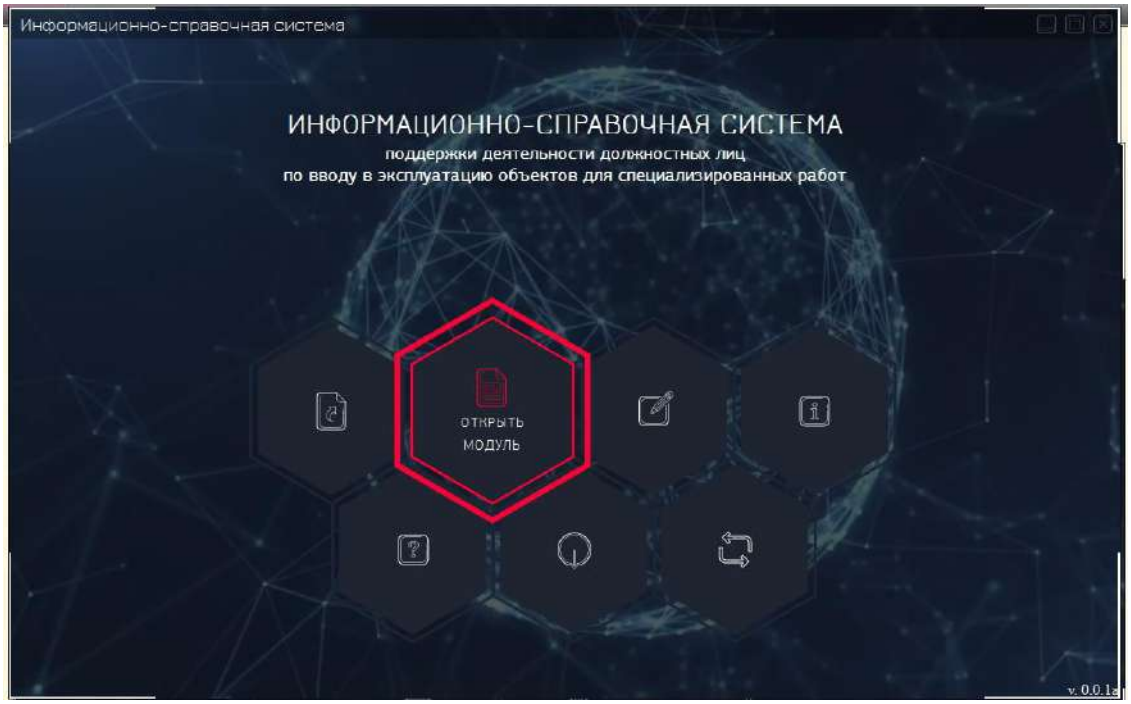


Рис. 2. Раздел меню Программы «Открыть модуль»

Раздел меню Программы «Создать модуль» позволяет реализовать самостоятельное создание пользователем модуля для формирования базы данных нормативных правовых и методических документов, а также документов по вводу в эксплуатацию объектов конкретного типа (см. рис. 3).

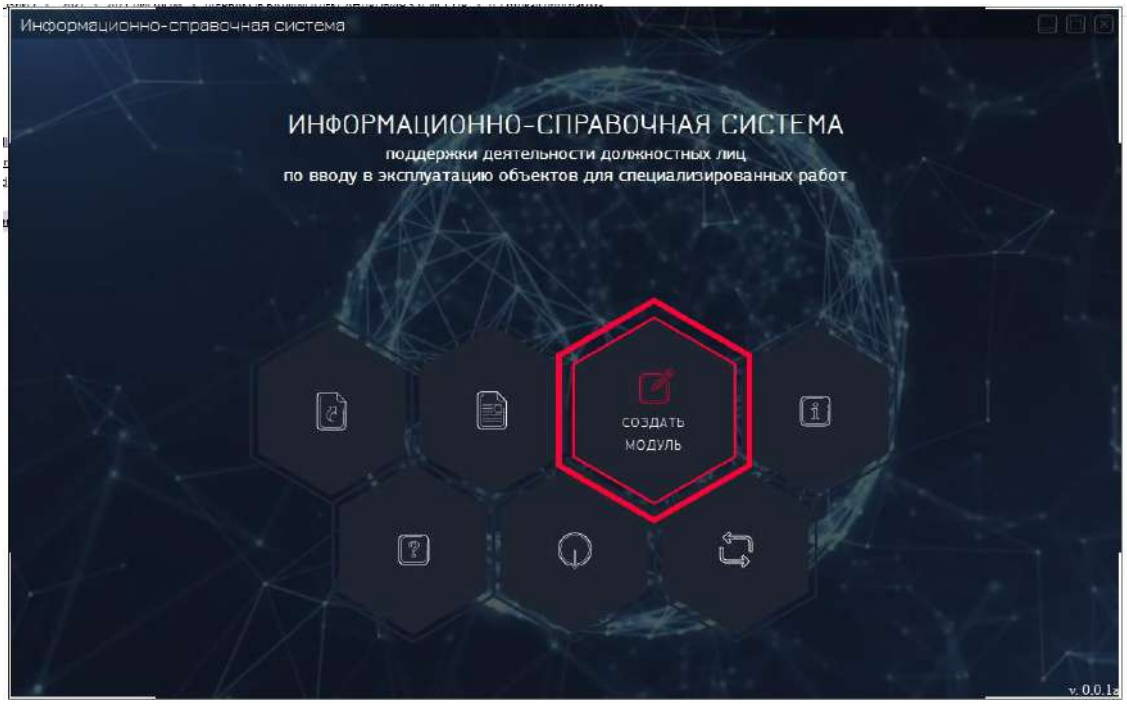


Рис. 3. Раздел меню Программы «Создать модуль»

Пользователю Программы доступны также разделы меню «Справка», «Информация о программе» и «Обновление».

К достоинству Программы относятся простота установки, автономность создаваемых или подгружаемых модулей, которые в любой момент можно отредактировать, отмасштабировать под решаемые задачи, сформировать конкретный их набор, а также предоставить установленным порядком отдельные модули или их набор другим пользователям [1].

Программа создана в языке программирования «C#», интерактивна, ориентирована на пользователя со средним уровнем владения компьютером.

При вводе реквизитов формализованного документа (Ф.И.О. лиц, подписывающих, согласовывающих и утверждающих документы, номеров помещений, инвентарных номеров технических средств, размещённых в них и т. д.), эти данные автоматически переносятся в проекты служебных документов, перечень которых заранее определяется согласно требованиям нормативных правовых и методических документов полномочных федеральных органов исполнительной власти (ФСТЭК России, ФСБ России, Минобороны России, МВД России и пр.), после чего пользователю достаточно лишь отправить их в печать и представить должностным лицам на подпись и утверждение.

Таким образом, предложенное авторами направление совершенствования деятельности должностных лиц, реализованное в виде информационно-справочной системы, создаваемой на базе представленного программного обеспечения, позволит лицам, выполняющим мероприятия ввода в эксплуатацию объектов для обсуждения, обработки информации ограниченного доступа и/или хранения её носителей, сократить время выполнения мероприятий, т. е. повысить оперативность их выполнения, а также путём объединения и реализации в одном или нескольких модулях требований значительного числа нормативных правовых актов и методических документов полномочных федеральных органов исполнительной власти, включая формы необходимых документов, повысить обоснованность мероприятий ввода в эксплуатацию объектов, предназначенных для ведения работ с информацией ограниченного доступа. Кроме того, представленное программное средство может быть полезно для должностных лиц, начинающих работать в данной сфере деятельности, т. е. представленная Программа может служить учебным материалом в ходе их самостоятельной работы, а также в ходе проверке сформированности компетенций, необходимых соответствующему специалисту [3, 4].

Список литературы

1. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 20.04.2021).

2. Бухонский, М. И. Техническая защита информации : электрон. учеб. пособие для высш. военно.-учеб. заведений / М. И. Бухонский, С. В. Землянский, В. Н. Махичев, С. В. Найдёнов. – Краснодар : КВВУ, 2016.

3. Приказ Министерства труда и социальной защиты Российской Федерации от 15.09.2016 № 522н «Об утверждении профессионального стандарта «Специалист по защите информации в автоматизированных системах» // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/71400328/ (дата обращения: 20.04.2021).

4. Приказ Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 599н «Об утверждении профессионального стандарта «Специалист по технической защите информации» // СПС «Гарант». – https://www.garant.ru/products/ipo/prime/doc/71450308/ (дата обращения: 20.04.2021).

Борзунов К. К.[1]***,***
доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

МОШЕННИЧЕСТВО В ЦИФРОВОМ МИРЕ

В этой статье будет больше вопросов, нежели ответов и предложений. Но именно вопросы, а не их отсутствие дают большую мотивацию к исследованию, познанию того, что становится крайне необходимым.

Условия, при которых «расцветает» мошенничество

Отмечаемые в последнее время социологами процессы деградации нравственности, морали, духа указывают и на появление устремления многих небрежно относиться к преданности слову, делу, долгу. Последствием этого становятся ослабление добропорядочности и законопослушности граждан в самых различных странах [1].

Условия, влияющие на мошенничество, традиционно определяются:

– социально-экономической обстановкой (объективной). Так, в частности увеличение уровней инфляции и безработицы, снижение уровней дохода населения, наличие социально-политических кризисов приводят к «расцвету» мошенничества в определенной мере;

– состоянием потенциальной жертвы (объективным и субъективным). Так, личная сложная (кризисная) ситуация – неопределенность и нестабильность, необходимость удовлетворения каких-либо потребностей – приводит к усилению уязвимости потенциальной жертвы. С другой стороны, определять повышенную уязвимость могут также личные качества потенциальной жертвы – доверчивость или хорошо известные всем «грехи»: стремление к минимальным затратам, испытывать риски, самоутверждение, честолюбие, стяжательство, тщеславие, алчность, зависть, пристрастия к удобствам жизни и даже суеверие;

– потенциями злоумышленников (субъективными). Злоумышленники используют разнообразные приемы скрытия своей истинной сути, сути сделок по товарам и услугам: прибегают к возможностям изучения потенциальной жертвы и планированию собственных злоумышленных действий (порою даже группой лиц); искусственно создают потенциальным жертвам всевозможные ограничения: принятия решения во времени, в получении дополнительной информации о

партнерах и сделках, в дополнительных проверках получаемых данных. Активно злоумышленниками использую приемы: соблазн и лесть, угождение человеческим страстям; лукавство, хитрость и бессовестность, ложь.

Обращая внимание на новые условия, возникшие в связи со всепоглощающей цифровизацией мира и отношений в нем, можно отметить резкое нарастание общей неопределенности, т. е. человечество сталкивается с проблемой ухудшения адекватности восприятия окружающей действительности [1, 2, 3]. Последствия этого – многочисленность и разнообразие рисков, с которыми сталкивается каждый человек. Однако можно констатировать отсутствие механизмов защиты как у отдельного человека, так и у социальных групп. Для выработки человечеством механизмов защиты (иммунитета) по отношению к мошенничествам в новых условиях требуется время или помощь правоохранительной системы [4].

В последнее время в условиях многочисленных ограничений, связанных с пандемией коронавирусной инфекции, когда сокращается взаимодействие людей в реальном мире, и когда оно переносится в мир виртуальный – телекоммуникаций и социальных интернет-сетей, наблюдается «расцвет» мошенничества.

Мошенничество как универсальная угроза

Естественная необходимость удовлетворения потребностей человека в каких-либо товарах и услугах, совершения каких-либо сделок сопровождается универсальной угрозой – мошенничеством [5].

Суть мошенничества в том, что даже подозревающая жертва подстерегается злоумышленником, который готов в складывающихся условиях путем обмана или злоупотребления доверием жертвы (сочетая обман действием со словесным обманом) с корыстной целью осуществить хищение чужого имущества или приобретение права на чужое имущество. Весьма часто мошенничество связано с желанием злоумышленника получить материальную выгоду.

Следует отметить, что формы мошенничества разнообразны и изощренны. Порой осуществляется фальсификации предмета сделки, иногда жертву втягивают в, казалось бы, не азартную игру. Мошенники могут применить шулерские приемы в различных играх на «интерес», отвлечь жертву с помощью «подручных». Мошенничество может быть реализовано и в виде отказа от обязательств, которые влекут убытки жертвы в пользу злоумышленника.

Злоумышленнику главное – создать для потенциальной жертвы неопределенность, отсутствие возможности проверки сведений и данных, ограниченность во времени и в критическом осмыслении происходящего [6, 7]. Последствием этого является совершение ошибок, которые приписываются исключительно жертвам.

Мошенничество подстерегает человека повсюду. А виртуальный мир для современного человека расставляет еще большее множество ловушек и, главное, новых и неизвестных ему.

Мошенничество как универсальная угроза сводится к определенной технологии, схематичное представление которой таково: Ожидание или поиск (выбор и изучение жертвы) злоумышленником – «контакт» злоумышленника с жертвой – возникновение заинтересованности жертвы в условиях неопределенности – собственно обман злоумышленником жертвы – провоцирование жертвы на совершение ошибки – злоумышленник «срывает куш» и исчезает, – жертва остается в недоумении и винит себя в ошибках, не понимая, что произошло.

Особенность современных условий в том, что потенциальные жертвы порою эту технологию знают [6, 7], но не всегда могут противопоставить этому какое-либо сопротивление в виде личных защитных действий [2, 3], оно пока не выработано, и этим пользуются злоумышленники. А правоохранительная система ожидает события…

Мошенничество как реализация преступного замысла

Преступный замысел мошенничества в том, чтобы жертва в условиях неопределенности и ограничения во времени принятия решений, совершила ошибки, не замечая их, не осознавая их, соглашаясь на неоправданный риск, а злоумышленник в итоге заполучил некоторое материальное благо, оставаясь в «глазах жертвы» невиновным в нанесении ей ущерба.

Используя представления о ключах экструзии и ключах интрузии, которые применимы в целях экструзии опорных идей и переформатирования индивидуального сознания, а также представления о ключах интерпретации и ключах актуализации, которые применимы в целях формирования заданной интерпретации и отложенной актуализации, опишем мошенничество как универсальное информационно-психологическое воздействие [4, 5, 7, 8].

Ожидание или поиск (выбор и изучение жертвы) злоумышленником, при этом он имеет уже определенные цели, создает информационную базу воздействия на потенциальную жертву.

Привлечение злоумышленником внимания потенциальной жертвы, установление контакта

На этом этапе злоумышленник максимально «накачивает» потенциальной жертве информацию, которая воспринимается ею как заслуживающая внимания [4]. «Ненавязчиво» внедряя ключи интерпретации жертве [7], злоумышленник обеспечивает возникновение определенной позиции в реакциях сознания жертвы на предложение.

Используя ключи экструзии, у жертвы накапливается именно та ресурсная информация, которая станет основой для управления жертвой в планируемой сделке [7].

Возникновение заинтересованности жертвы в условиях неопределенности

«Ненавязчиво» внедренные ранее ключи интерпретации жертве злоумышленником позволяют у жертвы сгенерировать социально-психологическую энергию для решений и поступков, а также уменьшить энтропию сознания [8].

Собственно, обман злоумышленником жертвы

Имеющаяся база воздействия, а именно накопленная ресурсная информация потенциальной жертвой, переводится в фоновую информацию [7]. При этом фоновая информация обходит защитные функции сознания и вызывает у жертвы эмоции и ожидание результатов сделки, которые согласуются с целями воздействия злоумышленника. В это временя злоумышленником «ненавязчиво» внедряются жертве ключи актуализации так же, как и ранее внедрялись ключи интерпретации. При этом происходят накопление потенциалов социально-психологической энергии жертвы и предельное сужение сознания при еще большем уменьшении его энтропии [8]. Таким образом, формируется необходимая злоумышленнику заданная жертве интерпретация.

Провоцирование жертвы на совершение ошибки

В этот период времени уже внедренными ключами актуализации вызывается разрядка, накопленных потенциалов социально-психологической энергии жертвы. Фактически жертва принимает нужное злоумышленнику решение и управляемо осуществляет решительные действия и поступки [7].

И как результат информационно-психологического воздействия на жертву злоумышленник «срывает куш», исчезает, а жертва остается в недоумении и винит себя в ошибках, не понимая, что, по сути, произошло.

Негативным последствием этого в обществе в качестве примера можно привести отказ от современных «цифровых благ»; сохранение состояния человека в «прошлом»; человек «останавливается, не делая шаг в будущее».

Проблемы противодействия мошенничеству в цифровом мире

Среди жертв мошенничества бытует мнение «о крайне низкой степени компенсации ущерба жертве со стороны злоумышленника», «о долговременных тяжбах в этих делах и бесперспективности усилий», «неэффективности имеющихся способов противодействия информационным воздействиям». Однако появляются работы по компьютерному моделированию распространения деструктивной информации в соцмедиа, описываются процессы информацион-

ного воздействия в виде потоковых диаграмм, что позволяет подойти к решению задач прогнозирования и управления, выработать информационное противодействие [3].

На уровне потенциальной жертвы возникают сложности с осмыслением сути происходящего, признания самого себя жертвой [5]. Но чаще всего причиной, по которой жертва не обращается за помощью к правоохранительной системе, является личностный компонент виновной виктимности, когда жертва возможно пусть даже и частично осознает свою способность стать жертвой из-за наличия упоминавшихся ранее «грехов», некоторого отсутствия собственной «добропорядочности». Хотя возможно причиной, по которой жертва не обращается за помощью к правоохранительной системе, может быть личностный компонент невиновной виктимности, когда жертва обращает внимание на собственные неосмотрительность, неосторожность или даже некоторое легкомыслие.

На уровне правоохранительной системы, противодействуя мошенничеству, возникают сложности с поиском доказательств виновности злоумышленников, с фиксацией доказательств событий и вины, а также по причине высокой латентности фактов мошенничества.

Когда количество событий – преступлений, которые определяются как «исключение из правила», меньше количества событий (т. е. не преступлений), которые определяются как «правило», и когда разного рода сделки осуществляются «по старинке», в частности с нотариальным заверением, правоохранительная система работает без сбоев.

Но в реальности определяющим фактором оказывается фактически предельная степень риска массовых (многомиллионных) актов покупок и продажи товаров, предоставления и получения услуг, совершения сделок, удовлетворения каких-либо потребностей человека. И это все больше и больше происходит в виртуальном пространстве интернет-коммуникаций.

При этом количество событий, требующих реакции правоохранительной системы, резко увеличивается. То есть ситуация, когда количества событий – преступлений, которые определяются как «исключение из правила», больше количества вполне законных сделок, работа правоохранительной системы перестает быть эффективной. Или быть этот переход к состоянию «коллапса» правоохранительной системы возникает ранее (к примеру, при 6/94)? Этот вопрос к исследователям. Вероятно, правоохранительная система не приспособлена к работе в этих условиях, когда правилом становится «исключение из правила».

Так ситуация складывается в настоящее время, – граждане не ощущают защиту от «расцвета мошенничества везде и во всем» со стороны правоохранительной системы.

В целом обнаруживаются две проблемы противодействия мошенничеству в цифровом мире: неэффективность противодействия мошенничеству со стороны правоохранительной системы в современном цифровом мире и отсутствие личных механизмов защиты граждан в условиях высокого риска быть подвергнутым мошенничеству в современном цифровом мире.

В этой связи очередной раз также можно ставить вопрос о необходимости расширения границ «самозащиты» граждан от мошенничества. Однако, развивая механизмы личной защиты граждан, надо уделить внимание, прежде всего, именно приемам нейтрализации действий злоумышленников и их последствий для потенциальной жертвы, по возможности активно используя информационно-психологические воздействия.

Однако появляются работы по компьютерному моделированию распространения деструктивной информации в соцмедиа, описываются процессы информационного воздействия в виде потоковых диаграмм, что позволяет подойти к решению задач прогнозирования и управления, выработать информационное противодействие [3].

Следует отметить, что остается и без ответа вопрос: почему же в обществе все больше людей склоняются к правонарушениям и преступлениям, становясь мошенниками, и не считают нужным сохранять состояние «честного труженика» в обществе? Скорее всего, это вопрос социально-психологический и криминологический.

Не всегда правоохранительные меры оказываются самыми эффективными в борьбе с преступностью. И в ситуации широкомасштабного «расцвета» мошенничества можно прибегнуть к «расширенной самозащите» граждан. Необходимо вырабатывать личные механизмы защиты для граждан в условиях высокого риска мошенничества, которые должны начинать действовать уже на этапе «возникновение заинтересованности жертвы в условиях неопределенности» и далее по нарастающей жесткости пассивного сопротивления и активного противодействия мошенникам. Основой таких защитных механизмов должны быть в перспективе информационно-психологические воздействия на злоумышленника, а приоритетными – «компенсация ущерба жертве мошенничества» и «неотвратимость наказания виновного». Это может стать прививками в условиях пандемии цифрового мошенничества.

Список литературы

1. Овчинский, А. С. Приоритетные направления в борьбе с социальной деструкцией в цифровом мире / А. С. Овчинский, К. К. Борзунов // Борьба с киберпреступностью в условиях развития цифрового общества. – 2019. – С. 127–132.

2. Овчинский, А. С. Энергоинформационные основы и приоритетные направления в борьбе с социальной деструкцией / А. С. Овчинский, К. К. Борзунов // Вестник Московского университета МВД России. – 2020. – № 1. – С. 138–144.

3. Киракосян, А. Э. Моделирование информационного противоборства в социальных медиа : монография / А. Э. Киракосян, В. А. Минаев, М. П. Сычев; под общей редакцией д-ра тех. наук, профессора В. А. Минаева. – М. : Наука, 2020.

4. Овчинский, А. С. Информационные воздействия и организованная преступность : курс лекций / А. С. Овчинский. – М. : ИНФРА-М, 2007.

5. Овчинский, А. С. Информационные воздействия с рациональной и иррациональной позиций / А. С. Овчинский, С. О. Чеботарева // Вестник Московского университета МВД России. – 2016. – № 6.

6. Овчинский, А. С. Информационное противостояние и общественная безопасность : курс лекций / А. С. Овчинский, К. К. Борзунов, С. О. Чеботарева. – М. : Московский университет МВД России имени В.Я. Кикотя, 2017.

7. Овчинский, А. С. Информационные координаты. Управление. Противоборство. Безопасность : монография / А. С. Овчинский, К. К. Борзунов, С. О. Чеботарева. – М. : Горячая линия – Телеком, 2018.

8. Овчинский, А. С. Энтропия сознания в информационно-психологических воздействиях / А. С. Овчинский // Вопросы кибербезопасности. – 2017. – № 2. – Т. 2 : Спецвыпуск. – С. 65–71.

Кудакова К. С.[1]*,*
адъюнкт адъюнктуры
Нижегородской академии МВД России

Елфимов О. М.[2]*,*
доцент кафедры экономики
и экономической безопасности
Нижегородской академии МВД России,
кандидат экономических наук, доцент

НЕОБХОДИМОСТЬ СОЗДАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ВЫЯВЛЕНИЯ НЕЗАРЕГИСТРИРОВАННЫХ ЛИЦ, УКЛОНЯЮЩИХСЯ ОТ УПЛАТЫ НАЛОГОВ, В ЦЕЛЯХ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ВЫЯВЛЕНИЯ И ПРЕСЕЧЕНИЯ ЛИЦ, УКЛОНЯЮЩИХСЯ ОТ УПЛАТЫ НАЛОГОВ, ПРИ ВЗАИМОДЕЙСТВИИ ПОДРАЗДЕЛЕНИЙ ЭБИПК МВД РОССИИ И ФНС РОССИИ

По оценкам аналитиков, на современном этапе, государство ежегодно недополучает до трети налоговых поступлений в бюджет. Налоговая преступность увеличивается с каждым годом, о чем свидетельствуют данные официальных информационных источников. Как показывает статистика, зачастую преступления в налоговой сфере направлены на уклонение от уплаты налогов, что приводит к не поступлению наиболее крупных отчислений в бюджет. Так, согласно налоговой аналитике, представленной Федеральной налоговой службой (далее – ФНС) России, государство получило в консолидированный бюджет Российской Федерации на 12,2 % меньше, чем в прошлом году за период январь–август [3].

Поступления по уровням бюджета за январь-август 2019-2020 гг.

Вид бюджета	январь-август, млрд. руб.		
	2019	2020	темп, %
Консолидированный бюджет РФ	15 037,3	**13 198,4**	87,8 ▼
Федеральный бюджет	8 293,6	**6 882,7**	83,0 ▼
Консолидированные бюджеты субъектов РФ	6 743,7	**6 315,7**	93,7 ▼

Рис. 1

Поступления по уровням бюджета за январь-август 2019-2020 гг., млрд. руб.

Рис. 2

Чаще всего такие преступления совершаются с использованием формально-легитимных организаций, или «фирмы-однодневки», которые создаются для фиктивных расходов и получения вычетов по косвенным налогам без соответствующего движения товара (работ, услуг) или с целью увеличения добавленной стоимости товара, уменьшения налоговой нагрузки на производственные подразделения.

Раскрытием и пресечением налоговых преступлений занимаются органы внутренних дел, которым для наиболее эффективной работы оказывают содействие различные ведомства и службы, в том числе и Федеральная налоговая

служба Российской Федерации. Совместная работа данных служб осуществляется по некоторым направлениям.

Взаимодействие этих служб регулируется приказом Генпрокуратуры России № 286, ФНС России ММВ-7-2/232@, МВД России, СК России от 08.06.2015 «Об утверждении Инструкции по организации контроля за фактическим возмещением ущерба, причиненного налоговыми преступлениями» через определение последовательности проводимых оперативных, следственных и процессуальных действий.

Взаимодействие между налоговыми органами и органами внутренних дел осуществляется по следующим направлениям: совместные выездные налоговые проверки (далее – ВНП) (когда сотрудники МВД России находят информацию, позволяющую предполагать о совершении налоговых правонарушений), взаимодействие между ФНС и ОВД после проведения проверки сотрудниками налоговых органов (когда ФНС проверяет деятельность организации единолично), а также работа межведомственной рабочей группы [2, с. 129–133].

Однако при совместной работе могут возникать проблемы, препятствующие эффективному взаимодействию подразделений ЭБиПК МВД России и ФНС России. К ним относятся:

– низкая квалификация сотрудников подразделений ЭБиПК МВД России;

– ограниченность полномочий ФНС;

– большая продолжительность подготовительных мероприятий к проведению налоговых проверок и время последующих действий;

– многочисленность преступлений на обслуживаемой территории.

В связи с этим возникает необходимость решения вышеуказанных проблем путем составления моделей взаимодействия подразделений ЭБиПК МВД России и ФНС России в целях повышения эффективности работы при выявлении и пресечении преступлений, совершаемых с использованием «фирм-однодневок».

Модель взаимодействия, основанного на доминировании власти, состоит в построении цепочки участников межведомственной рабочей группы, позволяющей решать вопросы территориального характера на более высоких уровнях. В рамках данной модели могут быть созданы межведомственные рабочие группы по городам, областям, субъектам, федеральным округам.

Кластерная модель – взаимодействие ФНС и ЭБиПК МВД России с использованием единой информационной системы. Данная информационная система позволяет ведомствам пользоваться в рамках своей деятельности конфиденциальной информацией о налогоплательщиках, их расчетных счетах, контрагентах в целях обеспечения экономической безопасности и контроля уплаты налогов.

Единая информационная система позволит сократить сроки на передачу запросов, так как документооборот будет реализован в электронной форме.

Корпоративная модель – образование Комитета по экономическим чрезвычайным ситуациям, в состав которого будут входить сотрудники Федеральной налоговой службы, отдела экономической безопасности и противодействия коррупции Министерства внутренних дел и Прокуратуры. В данный комитет могут входить только кадры, имеющие специальное образование. Комитет по экономическим чрезвычайным ситуациям уникален: его члены могут сразу применять полномочия ФНС, Прокуратуры и МВД. Однако создание данного комитета не совсем целесообразно в малых городах, так как количество преступлений в экономической сфере незначительно. Каждая модель взаимодействия имеет возможность реализовываться при выявлении и пресечении деятельности «фирм-однодневок» [1, с. 101–108].

Краткая характеристика описанных выше моделей повышения эффективности взаимодействия ФНС и ЭБиПК МВД России представлена в табл. 1.

Таблица 1

Модели повышения эффективности взаимодействия ФНС и ЭБиПК при выявлении и пресечении деятельности «фирм-однодневок»

Модель	Характеристика	Инструменты осуществления взаимодействия
Взаимодействие, основанное на доминировании власти	Подчинение руководителю межведомственной рабочей группы межведомственных рабочих групп по федеральным округам, субъектам, городам	Исполнение нормативных правовых актов
Кластерная модель	Объединение практической работы сотрудников ЭБиПК и ФНС России	Единая информационная система
Корпоративная модель	Объединение частей нескольких структур в Комитет по экономическим чрезвычайным ситуациям	Совместная деятельность сотрудников ЭБиПК, ФНС и прокуратуры

Однако работа сотрудников Федеральной налоговой службы и подразделений ЭБиПК МВД России в основном сконцентрирована на анализе организаций, имеющихся в базах данных, или организаций, которые выявляются в ходе проведения выездных или камеральных налоговых проверок.

В современных условиях «организации, осуществляющие предпринимательскую деятельность», в большинстве появляются в интернете. К таким организациям могут относиться не только ЮЛ, ИП, самозанятые, но также и лица, занимающиеся предпринимательством, которые, получая прибыль, не зарегистрировали свою деятельность, уклоняясь от уплаты налогов путем создания как аккаунтов в социальных сетях, так и сайтов в интернете. Примерами таких нарушителей могут служить мастера маникюра, бровей, ресниц, а также писатели курсовых, научных работ, статей, дипломов и т. д. В настоящее время можно найти незарегистрированного специалиста практически в каждой сфере.

Согласно оценкам аналитиков Федеральной налоговой службы количество организаций, сведения о которых содержатся в Едином государственном реестре юридических лиц по состоянию на 01.10.2020, составляет 3 535 553 организаций. По состоянию на 01.10.2019 количество таких фирм составляет 3 784 455.

По сравнению со статистикой за 2019 г. (тот же период) количество организаций, которые прекратили свою деятельность, увеличилось на 7,48% (2020 – 7 556 763 организаций, 2019 – 7 030 929 организаций) [4]. В связи с этим, фирмы, прекратившие свою деятельность, были в том числе реорганизованы ликвидированы, признаны банкротами, прекратили свою деятельность в связи с исключением юридического лица по решению регистрирующего органа из ЕГРЮЛ; могут быть иные основания.

Таким образом, допускается вероятность того, что руководители организаций, прекративших свою деятельность, за исключением реорганизации, решили возобновить получение прибыли путем осуществления своей деятельности в интернете без официальной регистрации своей деятельности, так как такие фирмы отследить крайне тяжело (практически невозможно отследить незарегистрированного лица, осуществляющего деятельность, через интернет).

Следовательно, возникает необходимость предпринять решения по осуществлению анализа незарегистрированных лиц, осуществляющих предпринимательскую деятельность через интернет и уклоняющихся от уплаты налогов.

Список литературы

1. Кудакова, К. С. Актуальные вопросы взаимодействия подразделений экономической безопасности и противодействия коррупции Министерства внутренних дел Российской Федерации и Федеральной налоговой службы России по вопросам «фирм-однодневок» (на материалах Нижегородской области) / К. С. Кудакова, О. М. Елфимов // Вестник Волжского университета им. В.Н. Татищева. – Тольяти : Волжский университет имени В.Н. Татищева (институт), 2020 – № 3 (46).

2. Кудакова, К. С. Особенности взаимодействия ФНС и подразделений ЭБиПК по вопросам «фирм-однодневок» / К. С. Кудакова, О. М. Елфимов // IX Всероссийский фестиваль науки : сборник докладов: в 2 т. – Нижний Новгород : Нижегородский государственный архитектурно-строительный университет, 2020.

3. Налоговая аналитика // Федеральная налоговая служба. – URL: https://analytic.nalog.ru/portal/index.ru-RU.htm (дата обращения: 28.03.2020).

4. Статистика по государственной регистрации // Федеральная налоговая служба. – URL: https://www.nalog.ru/rn77/related_activities/statistics_and_analytics/forms/8376083/ (дата обращения: 28.03.2020).

Рахмонбердиев Б. Б. угли[1]***,***
слушатель факультета
подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель
Куриленко Ю. А.,
старший преподаватель
кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОСОБЕННОСТИ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ С БАНКОВСКИМИ КАРТАМИ

Взяв на рассмотрение компьютерные мошенничества, мы можем понимать, что данный вид преступления может встречаться только в развитых странах. В 21 веке, веке развитых технологий, мы часто подвергаемся угрозе встречи с мошенниками в компьютерной сфере. Наряду с онлайн-магазинами и банковскими операциями, мошенники, пользуясь разными системами для получения личной информации, отправляют ссылки разных видов. Так, за 2020 г. число онлайн-мошенничеств увеличилось на 76 % по сравнению с первым полугодием 2019 г. [3].

Учитывая, что бесконтактная оплата NFC стала достаточно популярной и пользуется спросом в достаточно развитых странах, данный вид платежа самый уязвимый. Например, карты NFC от Сбербанка, с которых можно снять сумму до 1000 руб., а именно от 1 до 999 руб. без запроса пин-кода. Этим и пользуются мошенники.

В повседневной жизни контроль за банковскими картами и паспортом поможет уберечься от карманников. Многие карты и паспорта используют технологию RFID, и злоумышленник может воспользоваться этими предметами, даже не прикасаясь к ним физически, – они остаются у человека. Функция RFID основана на радиочастотном электромагнитном излучении. Она работает по методу бесконтактной идентификации. Данная технология используется во многих отраслях, а также в кредитных картах и паспортах для хранения личной информации,

которая может быть передана на терминал RFID. Мошеннические действия, совершаемые с помощью терминала или сканера для чтения и дублирования личной информации без ведома владельца, называют *скимминг* (от англ. skim – бегло прочитывать, скользить, едва касаться). На сегодняшний день данный вид мошенничества встречается все чаще. Исследования в области безопасности сохранения персональных данных привели к пониманию уязвимости кредитных карт и ряду возможных мошенничеств с кредитными картами, краже личных данных.

Обезопаситься от подобных ситуаций можно при помощи специальных кошельков, подкладка которых состоит из материала, предназначенного для блокирования RFID-сигналов. В таком случае карты или паспорт, имеющие подобную защиту, будут находиться в безопасности от возможного считывания сканером [4].

Развивающиеся технологии также играют на руку кибермошенникам. Так, известно о появлении нового приложения – программе *Android.Ecardgrabber*, которая работает через радиопротокол *NFC* и способна считывать платежные реквизиты банковской карты, а именно номер карты, срок ее действия, а также номер банковского счета. Для извлечения данных достаточно поднести один телефон к другому на небольшое расстояние в несколько сантиметров. Сам создатель данной программы создавал новый вид оплаты, при этом хотел показать уязвимые стороны для пользователей NFC-технологии [5].

Существует и другой вид мошенничеств с банковскими картами определенной платежной системы с помощью *NFC*. Современные смартфоны имеют функционал, при котором один из смартфонов с *NFC* функцией играет роль эмулятора платежного терминала. При поднесении банковской карты к этому эмулятору терминала считывается при проведении платежа, эмулятор запрашивает разрешение на совершение операции. Далее терминал получает разрешение от карты и одновременно при помощи второго смартфона, который использует специальную программу, совершает подмену параметров транзакции и блокирует запрос карты на введение пин-кода. Такой процесс занимает несколько секунд, и оплата покупки смартфоном без запроса пин-кода совершена [6].

Сегодня довольно сложно взломать банковскую систему с целью кражи денег с различных банковских счетов, поэтому кибермошенники всячески стараются взять информацию о счетах и банковских картах у их держателей, используя всевозможные ресурсы: телефон, интернет-сайты, онлайн и мобильный банк и др.

Самый распространенный способ вытянуть все личные данные у держателей банковских карт – это телефон. При поступающем звонке с любого незнакомого

номера кибермошенники под любым предлогом просят сообщить реквизиты карты. Чаще всего это звонки от так называемой «службы безопасности банка», когда звонящий представляется сотрудником банка, при этом называя имя и отчество жертвы, и сообщает о попытке списания с карты денежных средств. Далее он просит сообщить данные карты для того, чтобы исправить ситуацию, либо предлагает обезопасить средства на карте при помощи перевода на другой счет. Кибермошенники имеют хорошо поставленную речь, говорят четко и уверенно, а потому порой не вызывают подозрений у большинства абонентов.

Еще одна схема – «выигрыш в лотерею». На телефон абонента поступает звонок от «менеджера известной компании», который сообщает о том, что вы стали победителем и для получения денежного выигрыша нужно указать реквизиты банковской карты.

С помощью услуг мобильного банка вероятность кибермошенничества также возможна при помощи смс-команд. По номеру банка отправляется смс-сообщение с командой о переводе денег на другую карту. Такой вид мошенничества возможен в том случае, когда владелец либо потерял телефон с сим-картой, привязанной к банковской карте, и не успел заблокировать ни сим-карту, ни банковскую карту, либо когда владелец сим-карты отказался от услуг оператора, но не отключил услугу мобильного банка [7].

Киберпреступники не всегда пытаются узнать у держателя реквизиты его карты. Часто мошенники вынуждают самостоятельно перевести деньги со своей банковской карты или предоставить доступ к ней. Например, предлагают приобрести товары и услуги по очень большим скидкам именно в этот день и час, пока эти скидки действуют, не давая опомниться доверчивым гражданам. Схема по предложению некими агентствами предоставить телефон компании по устройству на работу, либо компании по предоставлению удаленной работы, где предлагается для подтверждения серьезности намерения, либо согласия перевести определенную сумму на карту агентства или компании.

Самый распространенный способ кибермошенников – «помощь родственнику», когда звонок поступает наиболее уязвимой категории граждан – пожилым людям, – им сообщают о том или ином происшествии с их родственником, для помощи которому нужно перевести на определенную карту или счет денежные средства. Злоумышленники чаще всего представляются сотрудниками правоохранительных органов или медицинскими работниками и, используя методы психологического воздействия, оказывают давление на пожилых людей, настоятельно требуя перевести деньги.

Вышеперечисленные способы мошенничеств с банковскими картами отражают далеко не полный список. Российское законодательство предусматривает наказание в соответствии со ст. 159.3 Мошенничество с использованием электронных средств платежа [1], а также ст. 159.6 Мошенничество в сфере компьютерной информации УК РФ вплоть до десяти лет лишения свободы и штрафом в размере 1 млн руб. [1]. Несмотря на это, мошенники продолжают изобретать все новые способы завладения денежными средствами доверчивых граждан.

Многие развитые страны ведут борьбу с кибермошенниками. К примеру, законодательство Республики Узбекистан также ужесточило наказание за мошеннические действия. В Уголовном кодексе Узбекистана уточнена и расширена ст. 168 «Мошенничество». В соответствии с обновленной статьей мошенничество, т. е. завладение чужим имуществом или правом на чужое имущество путем обмана или злоупотребления доверием, наказывается штрафом до шестисот базовых расчетных величин или лишением свободы до десяти лет, в зависимости от тяжести совершенного мошенничества [2].

Относительно недавно на территории Республики Узбекистан появилась система оплаты *NFC* по картам «*HUMO BANK*», это повысило число преступлений в сфере снятия денежных средств с банковских карт. На территории Республики Узбекистан действует лимит снятия денежных средств с помощью *NFC* функции карты до 50 000 сум (примерно 356 российских рублей).

Государственный правоохранительный орган МВД Республики Узбекистан также предостерегает о самых распространенных способах, которыми пользуются мошенники для обмана граждан и перевода ими денег с банковских карт.

В одном из способов активно задействуются соцсети. Абонент получает сообщение о смерти его родственника, проживающего в зарубежной стране, и том, что тот оставил большое наследство. Автор сообщения, представляясь адвокатом, просит сообщить паспортные данные, номера банковских карт и для регистрации наследства просит перечислить ему определенную сумму денег.

Другой способ – предложение организации совместного бизнеса. Некий аферист представляется военнослужащим, который за выполнение важного поручения в третьей стране получил крупную сумму денег и не может ее вывезти за границу, так как получена она нелегально. Он предлагает перевести жителю Узбекистана на счет эти денежные средства, используя их в дальнейшем для построения совместного дела.

Следующий способ, вынуждающий граждан Узбекистана переводить деньги мошенникам, – получение посылки из-за границы. Адресат получает письмо с

фотографией почтового ярлыка и квитанцию, оплатив которую можно будет получить почтовое отправление.

Распространены в Узбекистане также «лотерейные» мошенничества. Когда под предлогом выигрыша в лотерею либо участия в лотерее с ограниченным количеством призов сообщается необходимость перевода некоторой суммы денег.

Кибермошенники рассылают уведомления от имени Управления по борьбе с киберпреступностью МВД Республики Узбекистан о блокировке пользователя из-за посещения им порнографических сайтов, содержащих материалы, которые запрещены законодательством Республики Узбекистан. Для «разблокировки» мошенники предлагают перевести на пластиковый номер штраф в размере 310 000 сумов (примерно 2207 российских рублей) в государственный кошелек [9].

Такими действиями мошенники подвергают наше общество опасности. Чтобы обезопасить себя, свои личные данные, денежные средства, находящиеся в том числе на банковских картах, необходимо быть бдительными и лишний раз убедиться кто звонит или отправляет сообщения и по какой причине просит передать личные данные, данные банковской карты или осуществить перевод денег.

Список литературы

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ : ред. от 05.04.2021, с изм. от 08.04.2021 : принят государственной Думой 24.05.1996 : одобрен Советом Федерации 5.06.1996 // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/c193654ae5c3bd5b02d92ade18796cd8864ec353/ (дата обращения: 14.04.2021).

2. Уголовный кодекс Республики Узбекистан : Закон Республики Узбекистан от 22.09.1994 №2012-XII : с изм. и доп. по сост. на 30.03.2021 // Информационная система «Параграф». – URL: https://online.zakon.kz/document/?doc_id=30421110#pos=1884;-36 (дата обращения: 14.04.2021).

3. Яшкин, В. Как мошенники крадут деньги с банковских карт: новые схемы финансового мошенничества / В. Яшкин // Онлайн журнал по финансовой грамотности. – URL: https://life.akbars.ru/pf/noviye-vidi-finansovogo-moshennichestva/1 (дата обращения: 14.04.2021).

4. Финансовая грамотность // Финансовая грамотность. – URL: https://ochag-home.ru/rfid-zashhita-bankovskih-kart-svoimi-rukami/ (дата обращения: 14.04.2021).

5. CNews Conferences // Интернет-издание о высоких технологиях – CNews. – URL: https://cnews.ru/link/n189447 (дата обращения: 14.04.2021).

6. Overclockers.ru // Российский оверклокерский портал. – URL: https://overclockers.ru/blog/her/show/40961/najden-novyj-sposob-vzloma-kreditnyh-kart-visa-s-obhodom-pin-koda (дата обращения: 14.04.2021).

7. Mnogo-Kreditov.ru // Редакция Mnogo-Kreditov.ru. – URL: https://mnogo-kreditov.ru/bankovskie-karty/moshennichestvo-s-bankovskimi-kartami.html (дата обращения: 14.04.2021).

8. Новости Узбекистана // ООО «MEDIA BIZNES». – Ташкент, 2021. – URL: https://nuz.uz/proishestvie/1185139-mvd-sostavilo-top-5-populyarnyh-shem-s-pomoshhyu-kotoryh-internet-moshenniki-obmanyvayut-uzbekistanczev.html (дата обращения: 14.04.2021).

Козлова Н. С.[1]***,***
курсант Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Гончар В. В.,
заместитель начальника кафедры
информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ И ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В УСЛОВИЯХ ПАНДЕМИИ

11 марта 2020 г. Всемирной организацией здравоохранения вспышка коронавирусной инфекции была объявлена глобальной пандемией, поэтому были введены ограничительные меры, заключающиеся в ограничение контактов между людьми, в том числе посредством перехода на дистанционный режим работы, обучения. Такой образ жизни привел к логичным последствиям: преступность в общественных местах снизилась на 10 %, при этом преступность в сфере информационно-телекоммуникационных технологий заметно активизировалась. Согласно статистике ГИАЦ МВД России, за 2020 г. выявлено и зарегистрировано преступных деяний, совершенных посредством информационно-телекоммуникационных технологий, на 73,4 % больше по сравнению с 2019 [3]. На рост количества дистанционных хищений, при снижении общего количества остальной преступности, указал заместитель начальника полиции по оперативной работе по г. Москве генерал-майор полиции А. Половинка в интервью от 10.11.2020. Он указал, что, если в 2015 г. на территории Москвы дистанционные преступления составляли не более 10 %, на данный момент дистанционно каждое второе хищение [6]. Рост количества данных преступлений, причем по некоторым категориям существенный, наблюдался и ранее, однако статистические показатели указывают на структурные изменение, а именно перетекание преступности в интернет.

Рассмотрим наиболее распространенные и актуальные схемы хищений, совершённых посредством информационно-телекоммуникационных технологий периода пандемии.

Рассмотрим наиболее распространенные в последние годы способы мошенничества в интернете, а также наложенные на них схемы периода пандемии.

Наиболее распространенным способом хищения является фишинг, т. е. получение обманным путем от лица его персональных данных. Способ – основание для конкретных схем. Ярким примером фишинговой схемы времени пандемии является рассылка мнимого бюллетеня Всемирной организации здравоохранения, содержащего якобы сведения COVID-19, а фактически ссылку на поддельный сайт ВОЗ, где требовалось осуществить аутентификацию [4].

Или же фишинговая страница *We transfer* с предложением войти в корпоративный аккаунт, и при условии входа, мошенники становились обладателями данных компании, хранящихся в облаке [5]. Также популярны сообщения и звонки от якобы контролирующих государственных органов с требованиями немедленно погасить штрафы по указанному в том же сообщении номеру телефона или карты. Распространен и такой основанный на средствах голосовой связи и технологиях, синтезирующих речь способ, как вишинг. Еще одним актуальным способом дистанционного хищения является смишинг – переход по вредоносной ссылке из сообщения в *WhatsApp, Telegram, Facebook Messenger, Instagram, «ВКонтакте», Twitter, TikTok* и т. д. Таким образом, в период пандемии приходили извещения якобы от служб доставки, где за документом скрывалась вредоносная программа *Backdoor.MSIL.Crysan.gen* [5]. Особенно популярной ввиду возникшего спроса торговля мнимыми товарами, вроде лекарства от COVID-19, средствами индивидуальной защиты, пропусками на въезд и передвижение по Москве и иным городам, сдача анализа на наличие инфекции на дому и т. д. Нередко можно было столкнуться и с интернет-попрошайничеством.

На первоначальном этапе важно оперативное направление запроса в банк с целью выяснения канала движения похищенных у потерпевшего денежных средств и, если это возможно, установления счета, куда были перечислены похищенные денежные средства.

Существенный объем проводимых следственных действий в данном случае занимают действия, направленные на различные технические средства, а также на содержащуюся в них информацию.

Во время следственных действий все манипуляции с техническими средствами (включение, выключение и др.) производит исключительно специалист, как штатный или представитель частных организаций (*LETA IT-Company, Group-*

IB и др.)., поскольку изымаемое техническое средство может быть снабжено взаимосвязанным с криптодисками программным обеспечением для поточного шифрования информации, которое в случае несанкционированного вмешательства автоматически делает недоступными все содержащиеся на устройстве сведения. Изъятие возможно лишь в случаях, указанных ст. 164.1 УПК РФ.

Приоритетное место для изъятия в данных случаях занимают информативные цифровые следы – файлы с расширением log, так как они содержат исчерпывающие сведения о переходах в сети и обменах данными, что позволяет установить перечень IP-адресов, с которых (и соответственно, на которые) данным техническим устройством подавались запросы. Существенную доказательную информацию может дать знание MAC-адреса устройства (совпадающего с IMEI серийного номера), при помощи которого совершено преступное деяние. Нужно направить запрос интернет-провайдеру с задачей обнаружения IP-адресов, с которых также был зафиксирован выход в сеть устройства с данным MAC-адресом [2].

Актуальной проблемой является то, что многие коды вредоносных программ хранятся в DarkNet, базирующемся на многократном шифровании информации и сложной маршрутизации соединения [1]. Через обменные платформы DarkNet зачастую осуществляется отмывание криминальных денежных средств, посредством их обращения в криптоавалюту, которую, в свою очередь, можно конвертировать в иностранную валюту, например в доллары США. Отслеживание канала отмывание похищенных денежных средств в данном случае становится практически невозможным крайне затруднительным к тому же станет наложение ареста на криминальное имущество лица, совершившего хищение.

Транснациональный характер киберпреступности указывает на необходимость более тесного международного сотрудничества в данной области. К примеру, по делу ликвидированной в Европе киберпреступной группы, использовавшей вредоносное программное обепечение *GozNym* для кражи 89,3 млн евро, до сих пор не обнаружены пятеро из десяти ее членов, в том числе организатор, все они являются гражданами Российской Федерации [7].

Таким образом, при расследовании преступлений, совершенных посредством информационно-телекоммуникационных технологий, которые стали наиболее актуальной категорией преступности периода пандемии короновирусной инфекции, следственные органы сталкиваются со следующими отрицательно влияющими на эффективность особенностями и проблемами:

– недостаточная квалификация штатных экспертов, принимающих участие в расследовании данной категории преступлений, а также некомпетентность

самих следователей, являющихся организующим звеном всего процесса расследования;

– «молодость» регулирующей цифровые отношения нормативно-правовой базы, отсутствие правоприменительной практики (ФЗ «О цифровых финансовых активах, цифровой валюте…», как первый в нашей стране законодательный акт, регулирующий цифровые правоотношения, вступил в законную силу лишь с 01.01.2021);

– слабое развитие трансграничных каналов связи между правоохранительными органами в мировом пространстве, а также низкий уровень взаимодействия следственных органов с интернет-провайдерами, операторами сотовой связи, кредитными организациями;

– в-четвертых, слабая изученность самого киберпространства, динамичность его развития.

Список литературы

1. Бирюкова, Ю. В. Хищения, совершаемые с использованием компьютерных и телекоммуникационных технологий, способы их совершения и пути их расследования / Бирюкова Ю. В. // Научная электронная библиотека. – URL: https://www.elibrary.ru/download/ elibrary_44053392_77198922.pdf (дата обращения: 03.04.2021).

2. Малахов, А. С. Некоторые особенности раскрытия и расследования мошенничества в сети Интернет / А. С. Малахов, А. С. Дубинин // Научная электронная библиотека. – URL: https://www.elibrary.ru/download/elibrary_20413026_17746407.pdf (дата обращения: 03.04.2021).

3. Состояние преступности в России за январь–ноябрь 2020 // Официальный сайт МВД России. – URL: https://мвд.рф/reports/item/21551069/ (дата обращения: 03.04.2021).

4. Спам и фишинг в I квартале 2020 года – SECURELIST by Kaspersky // Блог Securelist. – URL: https://securelist.ru/spam-and-phishing-in-q1-2020/96806/ (дата обращения: 03.04.2021).

5. Спам и фишинг в III квартале 2020 года – SECURELIST by Kaspersky // Блог Securelist. – URL: https://securelist.ru/spam-i-fishing-v-iii-kvartale-2020-goda/99171/ (дата обращения: 03.04.2021).

6. «Интервью»: генерал-майор полиции Александр Половинка // МОСКВА 24. – URL: https://www.m24.ru/videos/obshchestvo/10112020/264996?utm_source=CopyBuf (дата обращения: 03.04.2021).

7. Cybercriminal network, which stole €89.3 million, dismantled – Europol // Официальный сайт телеканала Euronews. – URL: https://www.euronews.com/2019/05/16/cybercriminal-network-which-stole-89-3-million-dismantled-europol (дата обращения: 03.04.2021).

Мавшук И. Н.[1],
курсант факультета
подготовки специалистов в области
информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Пакляченко М. Ю.,
старший преподаватель кафедры
специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ПОДКЛЮЧЕНИЙ К СЕТИ ИНТЕРНЕТ С АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ СОТРУДНИКОВ

Обнаружение несанкционированных подключений (НСП) к сети Интернет с автоматизированных рабочих мест сотрудников (АРМ) остается актуальной проблемой, поскольку такое подключение представляет собой критическую уязвимость информационной инфраструктуры, несет угрозы самим данным, хранящимся и обрабатываемых как на рабочем месте сотрудника, так и внутри локальной сети, к которой обычно подключены АРМ.

При разработке системы защиты информации особое внимание уделяется защите локальной сети от НСП из сети Интернет, однако при рассмотрении вопроса о НСП АРМ сотрудника к сети Интернет в обход локальной внутренней сети (например, путём использования модема или беспроводной точки доступа WLAN) видно, что он регулируется исключительно организационными мерами, а мера реагирования на подобное нарушение предусмотрена в виде привлечения к дисциплинарной ответственности сотрудников, нарушающих данные требования. Несмотря на вероятность получения наказания, сотрудники организаций продолжают создавать неучтённые точки доступа к сети Интернет, а основная

причина указанных действий, явно противоречащих правилам защиты информации, это попытка обойти установленные в организации технические меры безопасности (например, минуя межсетевые экраны и системы контентной фильтрации) с целью получения доступа к определённым Интернет-ресурсам, использование которых запрещено в этих организациях.

Точки доступа к сети Интернет обычно создаются на базе модемов и беспроводных точек доступа, задаваемых на мобильных телефонах и беспроводных маршрутизаторах, способных использовать SIM-карты для выхода в сеть Интернет.

Как известно, у сетевых пакетов имеется ряд параметров, используемых маршрутизатором при передаче данных по протоколу IPv4. При разработке программного обеспечения (ПО) для анализа подключений использовался ряд ключевых параметров сетевых пакетов и рабочих машин:

– IP-адрес – это уникальный адрес, который идентифицирует устройство в интернете или локальной сети.

– MAC-адрес – это уникальный идентификатор, который назначается NIC (контроллеру сетевого интерфейса / карте). Он состоит из 48-битного или 64-битного адреса, который связан с сетевым адаптером. MAC-адрес может быть в шестнадцатеричном формате.

В основе работы программы (см. рис. 1) лежит проверка подключения сетевого интерфейса к глобальной сети путём использования реализации сетевой утилиты ping [1]:

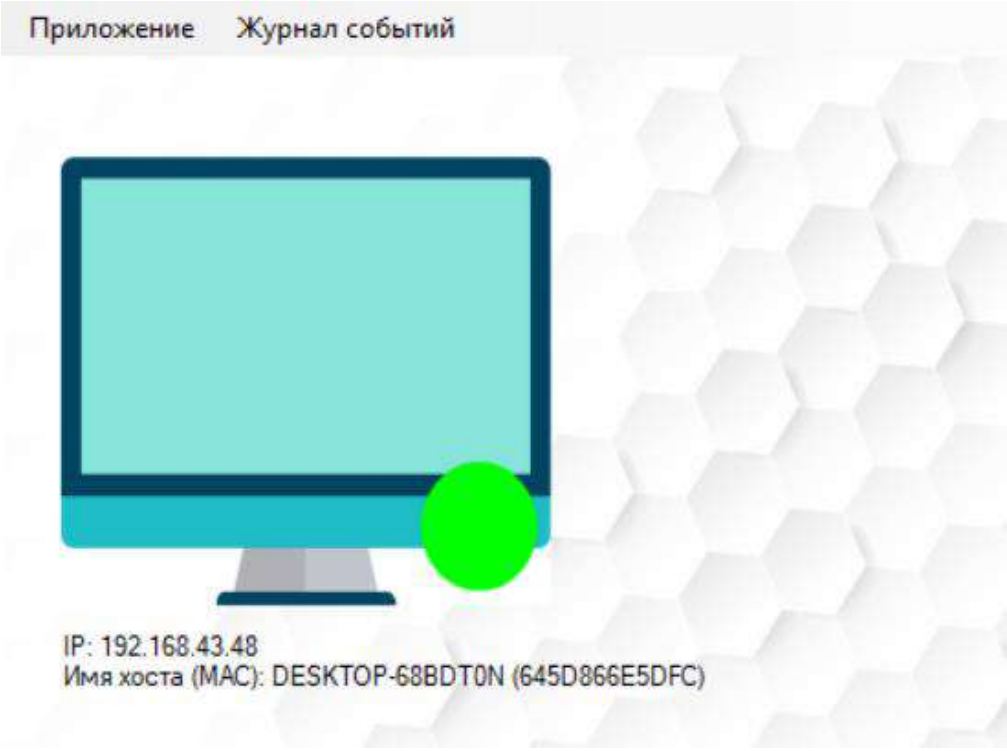


Рис. 1. Рабочий интерфейс программы

```
bool pingable = false;
 Ping pinger = null;
        try
        {
           pinger = new Ping();
           PingReply reply = pinger.Send(nameOrAddress);
           pingable = reply.Status == IPStatus.Success;
        }
        catch (PingException)
        {
        }
        finally
        {
           if (pinger != null)
           {
              pinger.Dispose();
           }
        }
        return pingable; }
```

Программа не требует дополнительных действий от пользователя и работает в автоматическом режиме, что реализовано путем применения таймера, на каждый такт которого происходит проверка текущего соединения и определение IP и MAC-адресов компьютера:

```
String host = System.Net.Dns.GetHostName();
 int i = System.Net.Dns.GetHostByName(host).AddressList.Length;
 System.Net.IPAddress ip = System.Net.Dns.GetHostByName(host).AddressList[i - 1];
 label1.Text = "IP: " + ip.ToString();
 label4.Text = "Имя хоста (MAC): " + host.ToString() + " (" + GetMacAddress(i - 1) + ")";
 if (PingHost(CheckIP) == false)
{
 timer1.Stop();
 pictureBox1.Image = im;
 string text = Environment.NewLine+"Выполнено отключение от локальной сети с последующим подключением к сети Интернет"+
```

```
 Environment.NewLine + label1.Text+Environment.NewLine+label4.Text+Environment.NewLine + DateTime.Now+ Environment.NewLine+"========================="+Environment.NewLine;
using (FileStream fstream = new FileStream(path, FileMode.Append))
{
        byte[] array = System.Text.Encoding.Default.GetBytes(text);
        fstream.Write(array, 0, array.Length);
      }
          Form2 form2 = new Form2();
          if (form2.ShowDialog(this) == DialogResult.OK)
          {
             Thread.Sleep(15000);
             restart();
              }
      }
```

При обнаружении подключения к сети Интернет в обход локальной сети в программе запускается полноэкранная форма, которая работает по принципу скрин-сейвера, блокирующего действия пользователя (см. рис. 2).

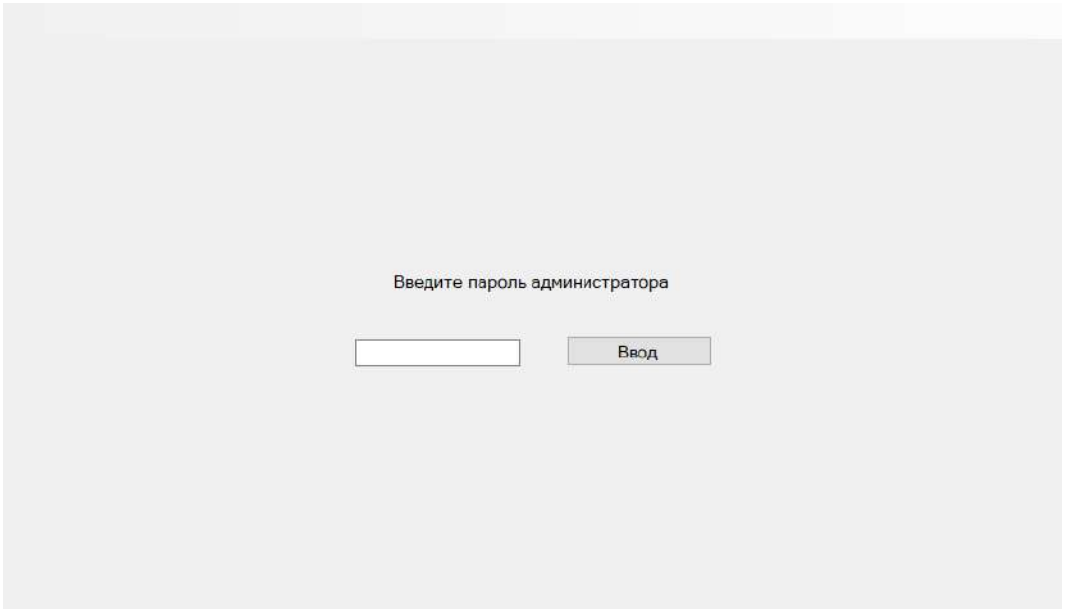


Рис. 2. Форма, блокирующая действия пользователя

Кроме того, происходит регистрация события подключения к сети Интернет с указанием типа события, IP и MAC-адресов компьютера и времени регистрации события. После ввода пароля администратора выполняется перезапуск таймера, и программа продолжает работать в обычном режиме.

С целью обеспечения постоянной работы ПО был реализован ряд функций, применяемых для предотвращения действий пользователя, направленных на

скрытие информации о работе сетевого соединения: убран заголовок с кнопками управления, реализована парольная защита очистки журнала и закрытия программы. С целью повышения удобства пользования программой была реализована возможность скрытия программы в трей.

Таким образом, разработано программное обеспечение, выполняющее обнаружение НСП к глобальной сети с АРМ пользователей. В дальнейшем планируется доработка функционала программы путем добавления функций автоматического блокирования подобного неправомерного подключения и апробация программы на действующей сети.

Список литературы

1. Сайт о программировании METANIT.COM. – URL: ttps://metanit.com (дата обращения: 06.04.2021).

Хорзова И. С.[1]***,***
курсант факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Пакляченко М. Ю.,
старший преподаватель кафедры
специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

КОНЦЕПЦИЯ СОЗДАНИЯ КИБЕРПОЛИГОНА ДЛЯ ОБУЧЕНИЯ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Актуальные проблемы в области цифровых технологий нуждаются в своевременных решениях. Большая часть государственных структур не готовы к кибератакам. На данный момент в области обеспечения информационной безопасности наблюдается нехватка квалифицированных специалистов не только с теоретическими знаниями, но и с практическим опытом работы по защите от кибератак. Поэтому для более успешной подготовки технических работников в области защиты информации создается киберполигон. На данной площадке у специалистов в области информационной безопасности и иных сотрудников организации, причастных к защите информации, появляется возможность перенести все свои теоретические знания на практику без ущерба функционирующей информационной системе, подлежащей защите [1].

Согласно постановлению Правительства Российской Федерации [2] под киберполигоном понимают инфраструктуру для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них.

Киберполигон – это «виртуальная страна», совокупность теории и практики [3]. Он одновременно может поддерживать работу более сотни виртуальных машин, а также осуществление хранения данных объемом более 10 ТБ. Проект киберполигона основан на накопленном опыте в мире, лучших практиках, интегрирует в себе достигнутые результаты научно-исследовательских лабораторий мирового уровня.

Отличие киберполигона от привычной виртуальной лаборатории в том, что он предоставляет эмуляцию бизнес-процессов и информационной инфраструктуры типовых организаций различных отраслей (кредитно-финансового сектора, промышленности, энергетики, транспорта, связи и др.). Участникам киберучений предоставляются технологии и инструменты для получения и отработки практических навыков по защите от кибератак, расследованию инцидентов, ведению реактивной работы в реальном времени.

Цель создания киберполигона – формирование устойчивого понимания принципиального и приоритетного значения информационной безопасности. При создании киберполигона преследуются две задачи [4]:

– практическая подготовка специалистов в области информационной безопасности, а также обучающихся по данному направлению. На полигоне у них появляется возможность отработки скорости, методов и качества реагирования на атаки;

– проведение тестов средств защиты, программного обеспечения и элементов информационных систем.

Основные возможности (см. рис. 1):

– доступность инфраструктуры круглый год;

– проведение тренировок на реальном оборудовании;

– развитие навыков самостоятельной подготовки к кибератаке: выстраивание процессов анализа и защиты, самостоятельное написание регламентов;

– моделирование современных видов атак, отработка их выявления и устранения.

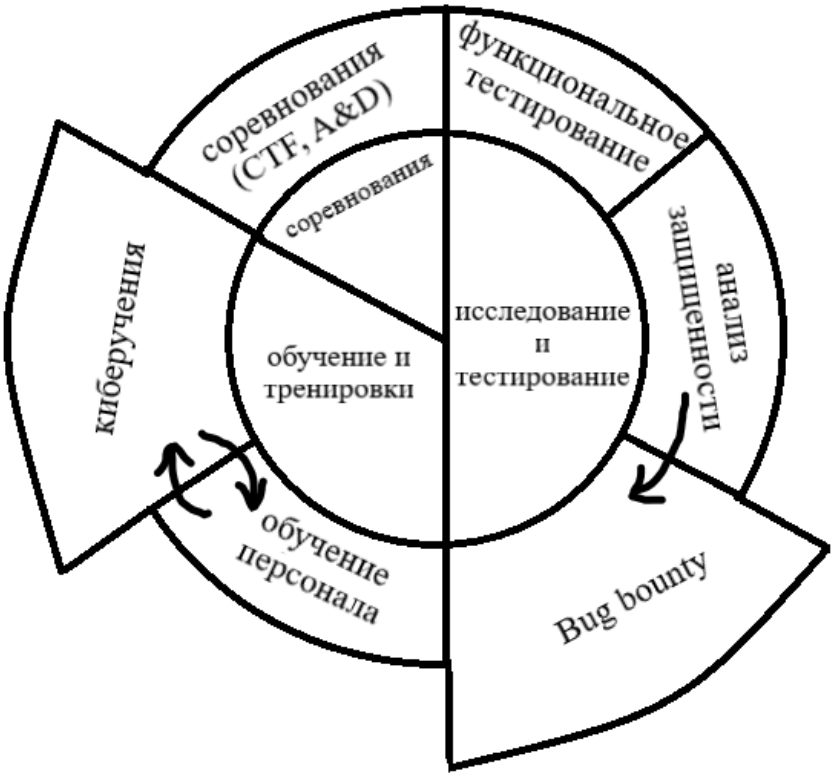


Рис. 1. Сервисная модель киберполигона

Работа на полигоне начинается с обучения, т. е. с отработки навыков оценки защищенности информационной инфраструктуры. Участникам предоставляют доступ к внутренним сервисам и рабочим станциям виртуальной модели предприятия, а также техническая документация. На этой стадии проводится оценка полноты и актуальности предоставленных документов, выявление недекларированно установленных программ, поиск всех уязвимостей. Самой главной задачей, решаемой на данном этапе, становится то, что участники знакомятся с защищаемой инфраструктурой, они полностью погружаются в учения [5].

Следующие стадии включают решение задач по мониторингу компьютерных атак и реагирование на компьютерные инциденты. Для этого происходит деление на две группы для отработки совместных действий (Red Team и Blue Team). Первая группа – группа мониторинга, участники выявляют угрозы и фиксируют их. Оценка деятельности группы осуществляется на основе количества заполненных карточек инцидентов, а также зависит от качества их заполнения. Вторая группа – команда реагирования, участники которой получают сообщения от группы мониторинга, принимают меры по устранению инцидентов. Очевидно, что для того, чтобы добиться успеха, необходимо тесное взаимодействие двух этих групп.

Как уже упоминалось ранее, киберполигон – это виртуализированная инфраструктура, которая состоит из подключаемых модулей. Защитники получают доступ к защищаемым машинам и системам мониторинга, а атакующие в свою очередь единую точку входа, собственно через нее и развивают атаку внутри сети. Сам полигон может быть развернут как в облаке, так и во внутреннюю сеть – с адаптацией под оборудование и нужды клиента. Чем крупнее и сложнее виртуальная инфраструктура, тем больше вариантов проведения тренировок (обучений, учений режима «авария», образовательных мероприятий) и тем ближе к реальности и полезнее опыт участия.

Следует выделить отличия концепции, архитектуры и функционала кибеорполигона от CTF (командных соревнований, проводимых с целью оценки способностей участников атаковать и защищать компьютерные системы) [5]:

– киберполигон ориентирован на «защитников», акцент ставится на отработку обороны от атак и их устранение;

– все действие происходит не только снаружи, но и внутри периметра, у участников имеется полный доступ к коммуникациям предприятий;

– одна из ведущих результативных задач использования киберполигона – воспитание точности, внимательности и системности у участников в применении средств защиты.

Прежде чем выбрать уровень планируемого обучения, надо оценить квалификацию участников: на основе самооценки, тестов, данных об уже пройденном обучении. Исходя из уровня участников, киберполигон может предложить вариативный набор: образовательных курсов, практических курсов, киберучений, соревнований по различным навыкам и компетенциям.

Таким образом, создание и применение кибеполигонов – одни из оптимальных решений подготовки специалистов соответствующего профиля и повышения их знаний, умений и навыков. В процессе эксплуатации киберполигона технические работники лучше понимают методы, которые используют хакерские группы, а также могут научиться им противостоять на практике. Производятся реальная демонстрация и обучение противостоянию атакам с самого начала: проникновение в периметр системы извне, продвижение по сети и повышение привилегий, получение контроля над сетью и кражи данных за контролируемый сетевой периметр, иные реализации сценариев инцидентов информационной безопасности.

По итогам учений на киберполигонах выявляются допущенные участниками Red Team и Blue Team ошибки, что является результативным средством (методом) обучения. Кроме того, участники получают новый опыт и повышают свою

квалификацию без каких-либо действительных угроз и ущерба безопасности компании. Создание полигона в большей степени снижает затраты и время на планирование и подготовку киберучений за счет готовой инфраструктуры.

Список литературы

1. Luka Safonov Киберполигон – онлайн площадка для проведения киберучений // Яндекс.Дзен. – URL: https://zen.yandex.ru/media/id/5c0d77de8f486600b085bf84/ kiberpoligon--onlain-ploscadka-dlia-provedeniia-kiberuchenii (дата обращения: 06.04.2021).

2. Постановление Правительства Российской Федераци от 12.10.2019 № 1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на введение в эксплуатацию и обеспечение функционирования киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности» // СПС «Гарант». – URL: https://base.garant.ru/72861698/ (дата обращения: 02.04.2021).

3. Олейникова, А. Хочешь мира – готовься к войне, или зачем нужен киберполигон / А. Олейникова // Security Lab: ежедн. интернет-изд. – URL: https://www.securitylab.ru/analytics/512874 (дата обращения: 02.04.2021).

4. Заполянский, В. Виртуальный город: как цифровой двойник мегаполиса помогает бизнесу снижать риски / В. Заполянский // InformationSecurity. – URL: https://www.itsec.ru/articles/virtualnyj-gorod-kak-cifrovoj-dvojnik-megapolisa-pomogaet-biznesu-snizhat-riski (дата обращения: 12.04.2021).

5. Зязин, В. Киберполигон в МИРЭА / В. Зязин // BIS Journal. – URL: https://ib-bank.ru/bisjournal/post/1172 (дата обращения: 11.04.2021).

Дош Н. А.[1]***,***
директор по рискам
Ассоциации участников Мастеркард

ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ КАК ЭЛЕМЕНТ БАЗОВЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ СОВРЕМЕННЫХ ПРЕСТУПЛЕНИЙ

За последние 10 лет платежные технологии стали самым развивающимся и одновременно самым востребованным инструментом для граждан всего Мира. Почти каждый год в разных странах запускаются новые провайдеры финансовых услуг, платежные платформы и инструменты. Доля электронных платежей с каждым годом растет и по прогнозам в ближайшем будущем может приблизиться к 90 %. В этой связи наша страна является мировым лидером платежных сервисов. Только за 8 лет (с 2010 г. по 2018 г.) доля электронных платежей в России увеличилась в 30 раз. Сегодня в России для оплаты покупок или перевода денежных средств можно использовать не только банковскую карту, но и телефон, часы, брелок. В своем отчете за 2019 г. компания «Бостон Консалтинг Групп» назвала нашу страну глобальным лидером по количеству токенизированных операций (совершенных с помощью телефонов, часов и т. д.) и самым большим Европейским рынком для использования электронных кошельков, что в том же отчете было отмечено как «Русское чудо». Практически все финансовые сервисы позволяют клиентам получать услуги удаленно, без личного присутствия, что помогает экономить время и не ограничивать себя в передвижениях по Миру.

К огромному сожалению, все эти удобства и сервисы не остались без внимания международных криминальных элементов. Досконально изучив все тонкости работы платежных инструментов, преступники начали активно ими пользоваться. Данный факт моментально стал негативно отражаться на возможностях правоохранителей всего Мира в плане эффективного противодействия криминалу. По статистике Европола около 95 % преступных денежных потоков в электронной сфере по тем или иным причинам остаются вне зоны досягаемости для правоохранителей, а как мы знаем это основной источник всех преступных сообществ. Не зря среди тех, кто в основном расследует экономические преступления, существует устоявшееся выражение «иди по пути денег», которое недвусмысленно намекает, на чем надо сконцентрировать усилия для получения поло-

жительного результата. Недавний (04/2021) опрос Европола на тему взаимодействия с финансовым сектором среди действующих сотрудников выявил ряд проблем, которые фактически, совпадают с реалиями нашей страны.

Зарубежная практика

Опрос сотрудников правоохранительных органов Европы (Апрель 2021)

1. Расследуете ли Вы преступления, связанные с финансовым сектором? 75% Да.

2. Имеются ли у Вас контакты в финансовом секторе? 75% Да.

3. Какую главную проблему Вы видите при взаимодействии с финансовым сектором?

-58% ограничения в регуляции фин. сектора, связанная с передачей данных правоохранителям;
-50% ограничения, связанные с легализацией данных, полученных из фин. сектора;
-38% недостаточно контактов в фин. секторе;
-30% недостаточно ресурсов и компетенции для качественной работы с фин. сектором;

Рис. 1. Результаты опроса сотрудников правоохранительных органов Европы

Как видно, на вопросы «Расследуете ли вы преступления, связанные с финансовым сектором?» и «Имеются ли у вас контакты в финансовом секторе?» 75 % респондентов ответили «Да». Можно сделать достаточно простой вывод – контакты в финансовом секторе имеются только у тех сотрудников, которые напрямую занимаются расследованиями финансовых преступлений. 25 % сотрудников по тем или иным причинам не имеют контактов с представителями финансовой отрасли, хотя как мы знаем, «путь денег» имеется практически в каждом преступлении.

Но самый важный вывод был сделан при анализе ответа на вопрос «Какую главную проблему вы видите при взаимодействии с финансовым сектором?», где помимо регуляторной проблематики 30 % опрошенных ответили, что для эффективного взаимодействия с финансовым сектором им недостаточно знаний и профильного опыта. Но, как показывает практика, это очень оптимистичный показатель.

Для того чтобы изменить текущую ситуацию, в большинстве стран было организовано взаимодействие с кредитно-финансовыми организациями, платежными сервисами и другими структурами платежной индустрии с целью повышения квалификации сотрудников правоохранительных органов. И уже сейчас

участники взаимодействия отмечают, что детальное погружение в механику платежных технологий дает неоспоримое преимущество специалистам и в обозримом будущем приведет к желаемому результату в плане расследования и предотвращения профильных преступлений.

Рис. 2. Принцип работы и взаимодействие с участниками рынка

Для того, чтобы детально изучать особенности платежных процессов необходимо ясно представлять базовые принципы функционирования тех или иных платежных систем, знать всех участников платежного процесса и четко понимать их функционал на каждом этапе проведения транзакции. На слайде изображена верхнеуровневая схема функционирования основных платежных систем в России. На схеме указаны участники платежа, каждый из которых выполняет исключительно свою функцию и обладает строго определенной информацией.

Для примера рассмотрим Банк-Эмитент и Банк-Эквайер. В данном случае Банк-Эмитент хранит о клиенте (кому был выдан платежный инструмент – карта) всю необходимую информацию, включая ПД, но идентифицирует его исключительно по номеру банковской карты. В свою очередь, Банк-Эквайер хранит всю необходимую информацию о торговой точке (ИНН, ОГРН и т. д.), в которой используется банковская карта, но в транзакционном сообщении передается только ее название и идентификатор POS-терминала.

В итоге, ни одна из сторон (в том числе платежные системы) не обмениваются детальной информацией о владельце банковской карты или торговом предприятии, а используют лишь буквенно-цифровые идентификаторы.

Такого рода информация позволяет оперативно оценить необходимость взаимодействия с той или иной организацией и возможности получения необходимой информации.

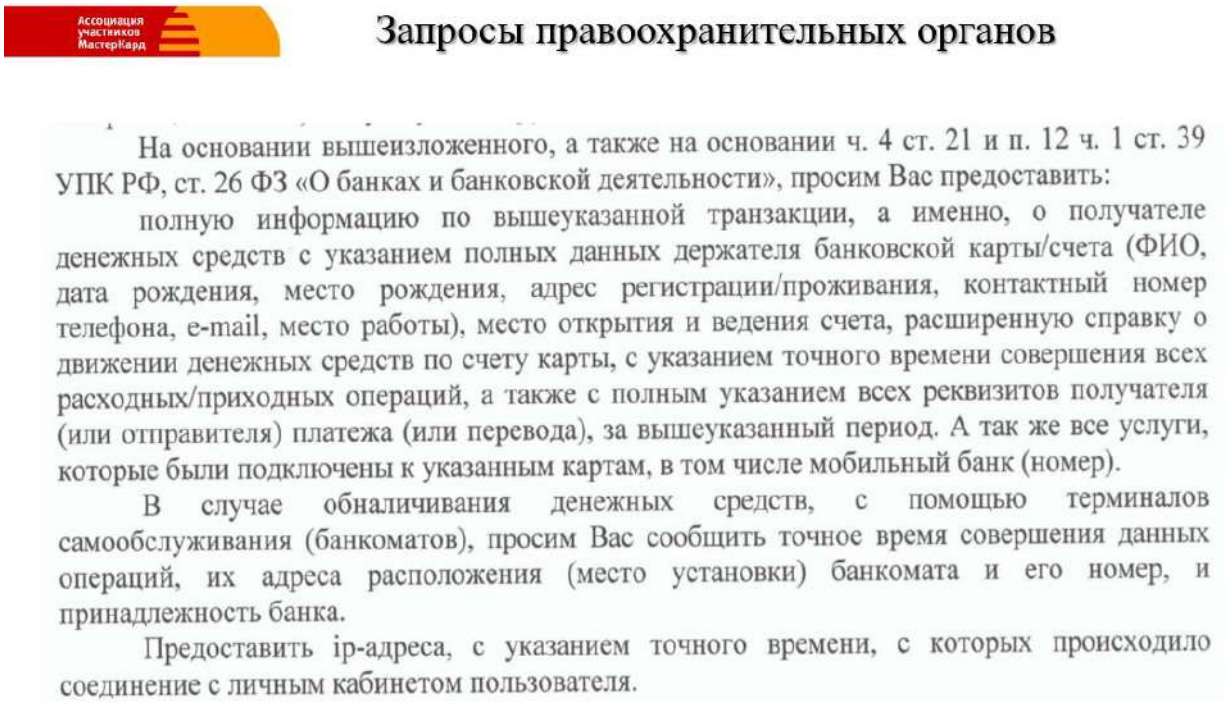


Рис. 3. Пример запроса правоохранительных органов

Незнание такого рода базисной информации приводит к снижению эффективности сотрудника и ненужной нагрузке.

На слайде представлена выдержка из запроса правоохранительных органов в адрес международной платежной системы. Это самый распространенный тип формулировки, в котором запрашивается всевозможная информация о пользователе банковской карты. К сожалению, официальный ответ на такой запрос только один – «за получением детальной информации необходимо обратиться в Банк-Эмитент», т. е. Банк, который обслуживает карту, фигурирующую в запросе.

Ассоциация участников МастерКард

Запросы правоохранительных органов

1. Платежные Системы обеспечивает техническую составляющую платежных сервисов.

2. Платежные Системы не передают и не хранят персональные данные держателей карт.

3. Платежные Системы не располагают информацией о наличии или отсутствии банковских и иных сервисов, связанных с платежными картами.

4. Платежные Системы не фиксируют, не хранят и не передают IMEI устройств, IP адреса и иные технические параметры держателей платежных карт.

5. У Платежных Систем отсутствует информация о получателе денежного перевода.

Рис. 4. Справочная информация для составления запросов

Основные тезисы, которые должны быть учтены при составлении запроса в адрес международных платежных систем на слайде.

Ассоциация участников МастерКард

*PAY

APPLE PAY

SAMSUNG PAY

Рис. 5. Платежные инструменты

Что касается иных платежных инструментов, например, таких популярных как ApplePay или SamsungPay, то здесь ситуация требует более широкого профильного взгляда, так как такие транзакции используют самые передовые технологии и их разбор может детально осуществлять только квалифицированный специалист.

Рис. 6. Платежные инструменты

С учетом того, что количество платежных сервисов стремительно растет, уже сейчас профильному специалисту необходимо обладать знаниями о тонкостях их работы и выстроить четкий диалог с компаниями интеграторами.

Следующие базовые моменты, которые требуют внимания при проведении мероприятий, связанных с токенизированными операциями:

1. На текущий момент в большинстве случаев (а в обозримом будущем на постоянной сонове) при оплате товара или услуги с помощью платежного устройства (часы, телефон и т. д.) в выписке банка-эквайера будет отображаться цифровой номер карты (Digital PAN). Цифровой номер карты – это специально сгенерированный номер, который скрывает настоящий номер карты пользователя с целью обезопасить его. Таким образом, при возможной утечке такого рода данных, а именно номеров цифровых карт, клиент будет защищен так как цифровые номера карт бесполезны с точки зрения мошеннического использования.

2. Принадлежность цифрового номера карты к банку-эмитенту распознается с помощью первых 8 символов номера (не первых 6 символов, как в случае с обычным номером карты). В последующем платежная индустрия полностью перейдет на определение принадлежности номера карты по первым 8 символам номера.

3. Для получения детальной информации об оплате, связанной с характеристиками устройства, в подавляющем большинстве случаев необходимо обращаться в организацию, чей сервис был использован при оплате (*ApplePay – Apple, SamsungPay – Samsung* и т. д.).

Рис. 7. Пример мошеннической схемы

В расследовании классических мошеннических схем, связанных с использованием сервисов для перевода денежных средств с карты на карту (т.н. p2p, c2c сервисы) необходимо понимать технологию процесса и роль каждого из его участников. В данном случае имеет место перевод с карты Банка 1 на карту Банка 3. При этом используется сервис Банка 2, и самый главный вопрос, который постоянно встречается в запросах правоохранителей связан с поиском получателя денежных средств. Преступники умышленно используют разные сервисы, что затрудняет оперативное получение информации.

Таким образом необходимо прояснить следующее:

1. Информацию о получателе денежных средств можно получить у банка-эквайера (банка-оригинатора), который обслуживает сервис по переводу денежных средств.

2. В выписке по банковской карте периодически встречаются такие названия сервисов денежных переводов как *MasterCard Money Send, Visa Money Transfer*, что говорит только о том, технология какой платежной системы была задействована и не более. Эти названия не должны вводить в заблуждение, что приводит к созданию того или иного официального запроса в сторону одной из платежных систем.

3. Для получения деталей об операциях по банковским картам рекомендуется запрашивать у банков-эмитентов информацию о банке-эквайере, который обслуживает Торгово-Сервисное Предприятие или сервис по переводу денежных средств так как банк-эквайер является полноценным носителем большинства необходимой информации с точки зрения «следования по пути денег».

Рысистов А. В.[1]*,*
студент кафедры
цифровых технологий и информационных систем
Московского авиационного института
(национальный исследовательский университет)

Максимов Н. А.[2]*,*
доцент кафедры
цифровых технологий и информационных систем
Московского авиационного института
(национальный исследовательский университет)

АВТОМАТИЧЕСКОЕ ПОЗИЦИОНИРОВАНИЕ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА С ПОМОЩЬЮ КОМПЬЮТЕРНОГО ЗРЕНИЯ

На сегодняшний день беспилотные летательные аппараты (БПЛА) являются одной из самой быстроразвивающихся и перспективных областей науки и техники. Это связано с огромным потенциалом БПЛА в решении сложных задач в различных областях жизни (картография, охрана, наблюдение и мониторинг, нефтепромышленность, сельское хозяйство).

Во всех перечисленных приложениях актуален и важным является вопрос автоматического позиционирования и автономного управления. Наряду с такими способами навигации, как системы GPS/ГЛОНАСС и инерциальные микромеханические системы, в последние годы все шире применяются системы, использующие алгоритмы компьютерного зрения. Особенно популярным подходом в данной области стали нейросетевые алгоритмы и алгоритмы, основанные на выделении, так называемых, особых точек и их дескрипторов.

Основными целями данной работы являются:

– Разработка и реализация системы автоматического позиционирования БПЛА на известной местности с использованием методов компьютерного зрения.

– Исследование эффективности алгоритмов компьютерного зрения в рамках задачи автоматического позиционирования БПЛА.

Задачи, возникающие в процессе разработки системы:

– Создание модели карты местности, составление маршрутов движения.

– Выбор и реализация алгоритмов компьютерного зрения.

– Разработка алгоритма определения положения БПЛА.

– Разработка компьютерной модели БПЛА и алгоритма его полета.

– Проведение испытаний, настройка параметров алгоритмов.

– Сравнение результатов.

– Построение маршрутов тестирования.

На первом этапе разработки системы моделирования была реализована модели местность на платформе Unity 3D, которая представляет собой приближенный к реальности горный ландшафт с водоемами. Для тестирования алгоритмов позиционирования БПЛА были выбраны три различных маршрута (см. рис. 1): вдоль лесной полосы (маршрут № 1), через горную местность (маршрут № 2) и вдоль реки (маршрут № 3).

Рис. 1. Карта местности и проложенные маршруты

Алгоритмы детектирования ключевых точек

Задача выделения и сопоставления особенностей на изображениях не новая в области компьютерного зрения. Одно из семейств алгоритмов сопоставления изображений – алгоритмы, основанные на выделении, так называемых, особых точек на изображении.

Один из наиболее важных критериев, по которому определяется эффективность алгоритмов выделения и сопоставления особых точек, – устойчивость к изменениям яркости, аффинным преобразованиям (поворот, масштабирование), проективным преобразованиям. Для сопоставления особенностей с разных изображений каждой особой точке приписывается некоторый дескриптор (описатель). Простейший дескриптор – сама окрестность точки, но такой подход будет работать, если окрестность точки предварительно нормализована по масштабу, ориентации и яркости. Для сравнения окрестностей двух точек используются подходы, основанные на коэффициенте корреляции [1]. Одними из

простейших алгоритмов выделения особых точек являются алгоритмы выделения углов на изображения [2]. Однако детекторы углов не инвариантны к изменению масштаба.

Более устойчивы алгоритмы, в которых используется так называемое scale-space представление изображения: размытие изображения при помощи свертки с функцией Гаусса с разными значениями среднеквадратического отклонения: SIFT [3], SURF [4], а также интересен алгоритм, выступающий менее точной, но более производительной альтернативой выше названным алгоритмам – алгоритм ORB [5], основанный на использовании информации об изменении яркости вокруг ключевой точки,

Во всех этих алгоритмах для каждой особой точки вычисляется ее дескриптор – вектор заданной алгоритмом размерности, который в определенной мере инвариантен к изменениям яркости, аффинным и перспективным преобразованиям.

Для сопоставления дескрипторов особых точек с двух изображений используется понятие расстояния между дескрипторами.

В качестве функций расстояния используются:

1. Косинусная мера:

$$cosine(x_i, x_j) = \frac{\overrightarrow{x_i}\overrightarrow{x_j}}{|x_i||x_j|} = \frac{\sum_{k=1}^{n} x_{ik}x_{jk}}{\sqrt{\sum_{k=1}^{n} x_{ik}^2}\sqrt{\sum_{k=1}^{n} x_{jk}^2}}$$

2. Расстояния Евклида:

$$euclid(x_i, x_j) = \sqrt{\sum_{k=1}^{n} (x_{ik} - x_{jk})}$$

3. Расстояние Хемминга:

$$hamming(x_i, x_j) = \sum_{k=1}^{n} |x_{ik} - x_{jk}|,$$

где x_i и x_j – вектора размерности n.

Таким образом, базовый алгоритм позиционирования может представлять собой простой ряд действий: сделать снимок с закрепленной камеры, найти на нем ключевые точки и сравнить их дескрипторы с заранее вычисленными дескрипторами на изображении карты местности исследуемой местности по функции расстояния, определить свое положение, рассчитав матрицу перехода точек на снимке в точки на карте.

Однако если рассмотреть этот алгоритм более детально, то становится легко понять, что он имеет серьезные недостатки:

- Низкая производительность такого алгоритма (слишком вычислительно дорого поэлементно сравнивать дескрипторы точек на снимке со всеми дескрипторами на карте), что в рамках задачи позиционирования БПЛА в реальном времени является существенным фактором.
- Исходный снимок местности и снимок, сделанный с БПЛА слишком сильно отличаются по размеру, что сильно снижает точность позиционирования.

Перцептивные хеши

Проблема производительности решается с помощью применения перцептивных хэшей (PHash) [6].

Перцептивные хэш-алгоритмы описывают класс функций для генерации сравнимых хэшей. Характеристики изображения используются для генерации индивидуального (но не уникального) отпечатка, и эти отпечатки можно сравнивать.

Идея заключается в том, чтобы совместить алгоритмы ключевых точек и алгоритм вычисления перцептивных хэшей: вычислив перцептивные хэши от дескрипторов ключевых точек, мы получаем 64 битные сравнимые между собой по функции расстояния числа. Сложность операции поэлементного сравнения двух одинаковых массивов длиной n – $O(n^2)$, когда сложность операции сравнения двух чисел – O(1) – существенный прирост в производительности. Так же оптимизируется объем хранения данных о снимках, так как отпечатки занимают меньше места на диске, чем многомерные дескрипторы, в условиях наличия большого количества снимков местностей это играет существенную роль.

Разбиение карты на участки

Идея повышения точности позиционирования заключается в разбиении исходного снимка местности на участки, так называемые тайлы, независимые друг от друга. На каждом выделенном тайле определяется заданное количество ключевых точек и их дескрипторы.

Полученные дескрипторы представляются в виде битовой матрицы, которая конвертируется в 64 битное число с помощью перцептивных хэшей. Полученные результаты сохраняются в базу данных, доступную во время полета БПЛА (например, в файл на диске).

Таким образом, поиск соответствующих дескрипторов будет производиться не на всей карте местности, а только на определенных алгоритмом позиционирования участках, что снижает вероятность ложного определения положения.

Гомогенные преобразования

В задаче позиционирования БПЛА по выделенным на снимке ключевым точкам возникает вопрос: как определить свое положение на местности, зная координаты ключевых точек на снимке и на местности. Такой переход помогают осуществить гомогенные преобразования [7].

Гомогенные преобразования – это преобразования, которые отображают точки одного изображения в точки на другом с помощью проецирующей матрицы H. Для построения данной матрицы необходима информация о местоположении четырех точек на связанных изображениях.

Таким образом, выбрав 4 наиболее близких по функции расстояния ключевые точки на снимке БПЛА и карте местности, можно построить определить матрицу, связывающую два этих изображения при любом их взаимном расположении. Результатом умножения координат центра снимка на данную матрицу будут координаты БПЛА на местности.

Алгоритм позиционирования

Этап решения задачи позиционирования состоит в выполнении следующих действий:

0. Пусть задана максимальная скорость полета БПЛА v_{max} , размер снимка БПЛА (n, m), время между двумя последовательными снимками t, количество выделяемых на изображении ключевых точек k, а также известны координаты центров q выделенных тайлов (p_i, h_j) местности и множество ключевых точек соответствующих им $\left\{x_l^{tile_p}, y_l^{tile_h}\right\}, i = (\overline{1,q}),\ j = (\overline{1,q}),\ l = (\overline{1,k})$

1. На снимке с камеры, закрепленной на БПЛА, помощью алгоритма выделить ключевые точки $\{x_l^*, y_l^*\}$ и вычислить их дескрипторы $d_l, l = (\overline{1,k})$.

2. Каждый дескриптор представить в виде битовых матриц M_l и вычислить от них перцептивные хэши $PHash(M_l), l = (\overline{1,k})$.

3. Построить окружность с центром в предыдущей точке БПЛА и радиусом равным максимальному расстоянию, которое может пройти БПЛА между двумя снимками $R = v_{max}t$. Определить с какими из тайлов местности пересекается данная окружность и выбрать из этих тайлов 4 наилучшие по функции расстояния точки.

4. На основе четырех найденных точек построить матрицу гомографии H и рассчитать текущую позицию на карте местности.

В качестве алгоритма определения ключевых точек можно использовать любой из вышеназванных, в рамках данной работы проводились эксперименты с алгоритмами ORB и SIFT.

Алгоритм движения БПЛА

Теперь, когда определена последовательность шагов для автоматического позиционирования, для проведения исследования необходимо задать алгоритм движения БПЛА. Данный алгоритм представляет собой следующую последовательность шагов:

0. Инициализация параметров движения БПЛА:

a. Маршрута движения.

b. Максимальной скорости.

c. Начальной высоты полета.

d. Предельного угла курса.

e. Размер снимка.

f. Интервал времени между двумя снимками.

g. Точность достижения точек маршрута.

Далее начинается итеративная процедура, окончанием которой является достижение финальной точки маршрута:

1. С заданным интервалом времени делается снимок местности.

2. Определяется текущее положение на карте по представленному алгоритму позиционирования. В случае недостаточного количества найденных ключевых точек, необходимых для построения матрицы H переходим к пункту 3.

3. БПЛА начинает вращаться вокруг вертикальной оси в горизонтальной плоскости, чтобы зацепить новые ключевые точки и определить свое местоположение.

Если положение определено, то переходим к пункту 4.

Если при полном повороте точки так и не были найдены, происходит движение в направлении первоначального вектора скорости и переход к пункту 1.

Происходит проверка на достижение точки маршрута: вычисляется расстояние Евклида между точкой назначения и точкой маршрута.

4. И если это расстояние меньше заранее заданной точности, то вычисляется вектор скорости к следующей точке, происходит переход на пункт 1. В противном случае продолжается движение по направлению текущего вектора скорости, переходим к пункту 1.

На рис. 2 представлен пример полета БПЛА по маршруту №1 с использованием алгоритма ORB:

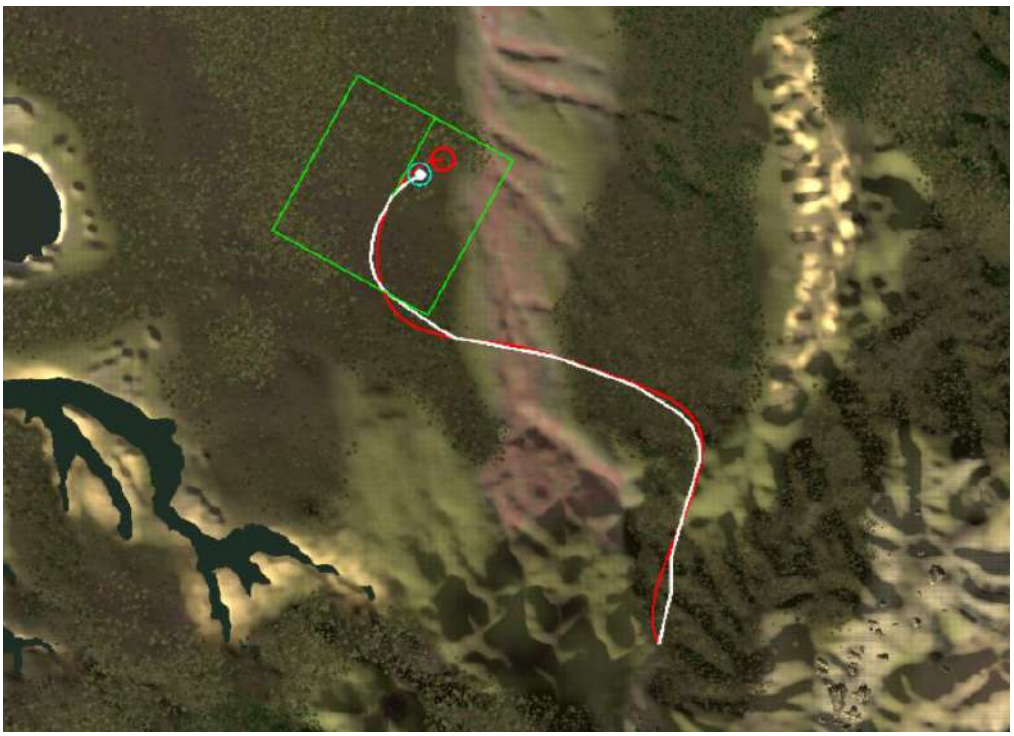


Рис. 2. Движение БПЛА по маршруту № 1

Сравнение результатов алгоритмов ORB и SIFT

В качестве критериев сравнения алгоритмов компьютерного зрения ORB и SIFT выступают следующие показатели:

- Среднее время позиционирования:

$$\bar{t} = \frac{1}{n}\sum_{i=1}^{n} \Delta t_i$$

где Δt_i – интервал времени между моментом прихода iого снимка на вход алгоритма и получением координаты БПЛА на карте.

Средняя ошибка позиционирования:

$$\bar{e} = \frac{1}{n}\sum_{i=1}^{n} \sqrt{(x_i^* - x_i)^2 + (y^* - y_i)^2}$$

где (x_i, y_i) – истинная координата БПЛА в момент времени t_i, а (x_i, y_i) – детектированная координата БПЛА в момент времени t_i.

В табл. 1 представлены результаты работы алгоритма ORB на трех различных маршрутах движения БПЛА. В каждом маршруте равномерно взято n точек, в которых БПЛА делает снимок.

Таблица 1

Номер маршрута	Размер изображения, пиксель	Среднее время позиционирования, с	Средняя ошибка, м
1	512x512	0.81	2,55
	300x300	0.39	6,75
2	512x512	1,06	5,70
	300x300	0.42	10,20
3	512x512	1,04	5,10
	300x300	0.37	7,65

В табл. 2 представлены результаты работы алгоритма SIFT на тех же маршрутах:

Таблица 2

Номер маршрута	Размер изображения, пиксель	Среднее время позиционирования, с	Средняя ошибка, м
1	512x512	1,61	2,25
	300x300	0,49	7,95
2	512x512	1,89	3,90
	300x300	0.51	6,15
3	512x512	1,55	4,65
	300x300	0.54	6,15

Результаты экспериментов показали, что наилучшую точность в позиционировании показывает алгоритм SIFT, однако он почти в 2 раза уступает алгоритму ORB в скорости, что в условиях задачи позиционирования в реальном времени может отрицательно сказаться на работе всей системы.

Так же отчетливо прослеживается прямо пропорциональной зависимости между разрешением снимка и точностью позиционирования.

Наилучшие результаты алгоритмы показывают на лесной местности, что можно объяснить хорошей различимостью лесного покрова.

В результате данной работы реализована программа моделирования полета БПЛА с автоматическим позиционированием на известной местности.

Благодаря внедрению в систему перцептивных хэшей достигнута высокая скорость сравнения дескрипторов ключевых точек.

Разработанный алгоритм позиционирования является устойчивым к изменениям угла курса БПЛА и высоте съемки.

Результаты экспериментов показали, что алгоритм детектирования ключевых точек ORB является более эффективным в условиях данной задачи, нежели алгоритм SIFT, так как его соотношение скорость/точность является наилучшим из предложенных.

В дальнейших исследованиях планируется использование алгоритма позиционирования в 3D симуляторе для автоматического управления роботами. При успешном прохождении испытаний в симуляторе этот алгоритм ляжет в основу системы автоматического наблюдения и мониторинга за местностью.

Планируется проведение экспериментов в различных условиях видимости с использованием карты высот местности.

Список литературы

1. Harris, C. A combined corner and edge detector / C. Harris, M. Stephens // Proceedings of the 4th Alvey Vision Conference. – 1988. – P. 147–151. DOI: 10.5244/c.2.23.

2. Introduction to SIFT (Scale-Invariant Feature Transform) // Кроссплатформенная библиотека. – URL: https://docs.opencv.org/master/da/df5/tutorial_py_sift_intro.html (дата обращения: 26.03.2021).

3. Introduction to SURF (Speeded-Up Robust Features) // Кроссплатформенная библиотека. – URL: https://docs.opencv.org/master/df/dd2/tutorial_py_surf_intro.html (дата обращения: 26.03.2021).

4. ORB (Oriented FAST and Rotated BRIEF) // Кроссплатформенная библиотека. – URL: https://docs.opencv.org/3.4/d1/d89/tutorial_py_orb.html (дата обращения: 26.03.2021).

5. Как работает перцептивный хэш // Сайт тематических блогов Хабр. – URL: https://habr.com/ru/post/120562/ (дата обращения: 28.03.2021).

6. Проективное преобразование // Википедия. – URL: https://ru.wikipedia.org/wiki/Проективное_преобразование (дата обращения: 12.03.2021).

Самолаева Е. Ю.[1]*,*
доцент кафедры
предварительного расследования
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИЧЕСКИХ СРЕДСТВ И ПСИХОТРОПНЫХ ВЕЩЕСТВ

Стремительное развитие науки и техники обусловило развитие новых способов совершения преступлений Использование информационно-телекоммуникационных технологий для целей сбыта и распространения наркотических средств в последние годы приобрело глобальные масштабы. Так, в январе–декабре 2020 г. более 90 % преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, совершены данным способом [5]. При этом статистические данные, характеризующие состояние преступности рассматриваемого вида, существенно не изменились (–0,2 % относительно АППГ). Это свидетельствует о существенном изменении за последние годы механизма совершения преступления и характеристики личности преступника.

Этот способ распространения наркотиков направлен на повышение доступности их приобретения, а современный сбытчик и покупатель сейчас – это активные пользователи сетью Интернет, современными средствами коммуникации и интернет-площадками. К сожалению, часто в данную преступную деятельность вовлекается молодое поколение: подростки и молодежь. Данная категория нередко сама подключается к деятельности по сбыту и распространению наркотиков, рассчитывая на быстрый и достаточно высокий доход, или уже находясь в зависимом от употребления запрещенных к обороту веществ состоянии.

Борьба с распространением в сети Интернет наркоконтента ведется не один год. Так, установлена повышенная уголовная ответственность за незаконный сбыт с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) [4]. Роскомнадзор России организовал создание нейронной сети с целью осуществ-

ления мониторинга запрещенной информации в сети Интернет, которая позволяет максимально оперативно выявить и блокировать наркоконтент. Подготовлена серия законов, направленная на противодействие пропаганде наркотических средств и психотропных веществ.

Так, федеральным законодательством предусмотрена обязанность владельцев социальных сетей осуществлять их мониторинг в целях выявления информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодежащих растений. Внесены соответствующие изменения и в нормы административного законодательства (например, введена ст. 13.41 КоАП РФ; и др.). Данные изменения направлены на повышение эффективности противодействия наркоконтенту и подобной информации в сети.

Противодействие незаконному обороту наркотических средств и психотропных веществ должно осуществляться с использованием всего арсенала научно-технических средств, которые включают и современные информационные технологии. Без их использования невозможно оказать адекватное и весомое воздействие на преступность в рассматриваемой сфере[1].

Однако несмотря на то, что новые способы совершения преступлений в сфере незаконного оборота наркотиков достаточно прочно вошли в современную преступную практику, силы, ей противодействующие, также активно наращивают свой потенциал информационно-технического характера.

Осуществление оперативно-разыскной и следственной деятельности в современных условиях невозможно без использования научно-технических средств и информационных технологий. В первую очередь это сказывается на раскрываемости преступлений[2]. Наибольшее количество технических средств применяется при разработке и раскрытии преступлений в сфере незаконного оборота нарко-

---

[1] Принятой 23 ноября 2020 г. Стратегией государственной антинаркотической политики Российской Федерации на период до 2030 г. проанализирована наркоситуация в стране за последние десять лет, определены угрозы национальной безопасности в данной сфере. Наркотизация населения признается одной из глобальных угроз безопасности нашей страны // См.: Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года» // Собрание законодательства Российской Федерации. 2020. № 48, ст. 7710.

[2] Так, за январь–декабрь 2020 г. в России уровень раскрываемости преступлений, совершаемых с использованием информационных технологий составил всего 45,5 %, а раскрываемость незаконного сбыта наркотиков, совершаемых данным способом, – 71.1 % // Официальный сайт МВД России. URL : https://мвд.рф/reports/item/22678184/ (дата обращения: 17.04.2021).

тиков, совершаемых организованными преступными группами, осуществляющими сбыт запрещенных к обороту веществ через интернет и электронные системы платежей.

Использование информационных технологий[1] в раскрытии и расследовании преступлений многостороннее и разнонаправленое. К ним относятся базы данных и информационно-поисковые системы, содержащие информацию о лицах, предметах, событиях, имеющих отношение к совершенному и подготавливаемому преступлению; системы электронного документооборота, использование которой позволяет сократить сроки передачи и рассмотрения поступающей информации, снижает материальные затраты за пересылку, хранение, копирование документов (например, ИСОД МВД России); электронные архивы уголовных дел и иных документов, позволяющие систематизировать материалы, предотвращать утрату информации по уголовным делам; технологии видеоконференцсвязи, с помощью которых можно получать показания дистанционно; системы видеонаблюдения и видео-фиксации, установленные в торговых центрах, учреждениях и организациях, на дорогах, во дворах жилых домов и других общественных местах, не раз способствовали раскрытию преступлений и доказали на практике свою эффективность; и др. [1, с. 227]

В перспективе планируется поставить на «вооружение» и применять для целей раскрытия и расследования преступлений самые последние достижения науки и техники. Так, в настоящее время ведется разработка ИИ-систем (искусственный интеллект) в целях их использования для поиска лиц, совершивших преступление. Предполагается, что данные технологии будут автоматически анализировать информацию о месте и обстоятельствах преступления, личности преступника, определять его по фотороботу, биоматериалу с места преступления.

Планируется создание дата-центра МВД России (Федеральный центр обработки данных МВД России), в котором будет храниться сведения из баз данных Министерства[2].

Таким образом, государство активно внедряет современные информационные технологии в деятельность правоохранительных органов.

---

[1] Согласно законодательному определению, информационные технологии – это «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» (п. 2 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 165.

[2] На этот проект в марте 2021 г. Правительством Российской Федерации выделило соответствующие средства. Запуск объекта в эксплуатацию запланирован на 2024 г. (см.: https://www.tadviser.ru/index.php/Проект:Дата-центр_МВД_России).

В ходе расследования преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ, применимы все вышеперечисленные средства, приемы и методы информационно-технического характера.

Выделим также некоторые специальные технологии, которые используются в расследовании рассматриваемой категории преступлений. К ним относятся, например, технические устройства доступа к электронным мобильным устройствам (планшетным компьютерам, телефонам) и стационарным ПК – специальные приборы, способные считывать информацию с мобильных устройств и восстанавливать удаленные пользователем файлы (например, мобильные комплексы по сбору и анализу цифровых данных «*UFED*»[1] (израильского производителя *Celebrite*), «Мобильный криминалист»[2] (российского производителя «Оксиджен *Софтер*», аппаратно-программный комплекс «Сегмент-С»,)[3]; автоматизированные информационно-поисковые системы (например, АИС «незаконный оборот наркотиков» (АИС «НОН»), содержащая информацию о нераскрытых преступлениях, сбытчиках, обстоятельствах приобретения наркотических средств (в том числе совершенных с использованием интернета и иных информационно-телекоммуникационных технологий), или ИПС «Дистанционный сбыт наркотических средств» (созданная в Мурманской области и Удмуртской Республике) [2]; и др.[4]

В целях раскрытия и расследования преступлений, связанных с незаконным оборотом наркотиков, нередко используются открытые источники информации (сайты интернет-регистраторов, социальные сети, медиахранилища, поисковые ресурсы интернета, он-лайн базы данных и др.) Для изучения данных источников широко привлекаются специалисты в сфере компьютерной информации и информационных технологий (IT-специалистов): программисты, системные администраторы, инженеры компьютерного оборудования и др.

Как было отмечено ранее, использование специальных познаний в сфере IT-технологий представляет неотъемлемую часть деятельности по раскрытию и расследованию преступлений, связанных с незаконным оборотом наркотиков. В то же время успех работы следователей и сотрудников оперативных подразделений

---

[1] Программа позволяет получать доступ к устройствам на базе ОС Android, IOS и скачивать с них информацию, в том числе переписку мессенджера Telegram.

[2] Программа позволяет загружать и анализировать биллинги, получаемые от операторов сотовой связи, извлекать файлы, данные об устройстве, учетные записи и пароли.

[3] Указанные технологии применяют специалисты экспертно-криминалистических подразделений МВД России, СК России, специальные подразделения ФСБ России.

[4] МВД выделило почти 80 млн руб. на средства взлома смартфонов // MBK-news (10.11.2020, 16:03). URL: https://mbk-news.appspot.com/news/vzlom/ (дата обращения: 17.04.2021).

зависит также и от иных факторов: насколько эффективно будет построено взаимодействие со специалистами; своевременно ли назначены судебные экспертизы (компьютерно-технические – по изъятым у обвиняемых телефонам, компьютерам, планшетам; дактилоскопические – по следам папиллярных узоров рук, обнаруженных на упаковках наркотических средств; физико-химические – по изъятым веществам; фоноскопические – по предоставленным оперативными подразделениями записям телефонных переговоров); и др.

На практике мы нередко сталкиваемся с ситуациями, когда следователи по нескольку месяцев ожидают проведения назначенной компьютерно-технической экспертизы. В результате качественное исследование изъятых технических устройств (из-за невозможности продления сроков) в некоторых случаях приходится заменять проведением осмотров (в лучшем случае с участием специалиста). Самостоятельный осмотр мобильного устройства иногда заканчивается на этапе ввода пароля, который следователь обычно не знает. В некоторых случаях осмотр вообще не приводит к получению доказательственно значимой информации. Из данного примера следует, что проведение судебных экспертиз заменить невозможно без ущерба для уголовного дела. При этом число специалистов, в частности, в области информационных и компьютерных технологий, необходимо увеличивать, чтобы их число отвечало современным требованиям практики [3, с. 245].

При этом сотрудники оперативных подразделений и следователи не должны отгораживаться или самоустраняться от происходящих процессов получения новой информации по преступлениям, в которых преступники применяли высокотехнологичные средства совершения преступления. Современные реалии требуют от представителей органов, осуществляющих раскрытие и расследование преступлений, активного вовлечения во все происходящие процессы. Следователи и оперативные сотрудники должны владеть информацией о работе с программным обеспечением, интернет-ресурсами, иметь представление как организовано размещение данных в интернете, уметь пользоваться поисковыми интернет-сервисами, уметь находить в нем информацию, реагировать на обнаруженный противоправный контент (например, направить в Роскомнадзор соответствующее обращение по выявленному факту), знать и соблюдать меры информационной безопасности и даже владеть методами социальной инженерии. Для этого необходима соответствующая подготовка сотрудников, сталкивающихся в своей деятельности с преступлениями, совершаемыми указанными способами (в частности, с использованием информационно-телекоммуникационных сетей).

Подводя итог всего вышеизложенного, отметим следующее. Современное стремительное развитие цифровых технологий кардинально изменило современное общество. Эпоха интернета трансформировала информационное пространство, расширила ее границы до порой непостижимых границ. В настоящее время в информационном поле находится большая часть человечества, информационные ресурсы проникли во все сферы жизни общества и так происходит во всем мире.

Изменились не только способы совершения преступлений, но и средства борьбы с ними. В свете современных реалий основным методом противодействия незаконному обороту наркотических средств и психотропных веществ, становится активное внедрение новых современных информационных технологий, их использование в целях своевременного раскрытия и всестороннего расследования преступлений. Своевременное, грамотное и полноценное использование современных научно-технических достижений в сфере информационных технологий при соответствующей подготовке лиц, участвующих в раскрытии и расследовании преступлений, позволит достичь желаемого результата и повысить их раскрываемость.

В то же время практика показывает, что успешное расследование преступлений, связанных с незаконным оборотом наркотиков (впрочем, как и любого преступления), зависит от степени взаимодействия следователей, оперативных сотрудников и специалистов экспертно-криминалистических подразделений. При грамотно организованном взаимодействии достигается максимальная эффективность противодействия незаконному обороту наркотиков. В ином случае не поможет даже самое современное техническое обеспечение.

Список литературы

1. Романова, Г. В. Технологии электронного расследования уголовного дела: особенности современного законодательства зарубежных стран / Г. В. Романова, В. И. Романов // Проблемы современного законодательства России и зарубежных стран. – Иркутск, 2020. – С. 227–233.

2. Особенности борьбы с наркопреступностью в сфере информационно-телекоммуникационных технологий // Официальный сайт Объединенной редакции МВД России. – URL: http://pda.ormvd.ru/pubs/102/drug-control/ (дата обращения: 19.04.2021).

3. Самолаева, Е. Ю. Организационно-тактические особенности расследования преступлений, совершенных с использованием компьютерных технологий / Е. Ю. Самолаева // Актуальные проблемы обеспечения кибербезопасности. – 2018. – С. 245– 248.

4. Федеральный закон от 01.03.2012 № 18-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (ред. от 03.07.2016) // Российская газета. – 2012. – № 48.

5. Состояние преступности в России (за январь–декабрь 2020 года) // Официальный сайт МВД России. – URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 19.04.2021).

Ивличева Н. А.[1]***,***
профессор кафедры
экономической безопасности Рязанского филиала
Московского университета МВД России имени В.Я. Кикотя,
кандидат физико-математических наук, доцент

Морсакова Ю. В.[2]***,***
доцент кафедры
экономической безопасности Рязанского филиала
Московского университета МВД России имени В.Я. Кикотя,
кандидат физико-математических наук

КОСВЕННЫЕ ПРИЗНАКИ ОСУЩЕСТВЛЕНИЯ XSS-АТАК НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Понятие межсайтового скриптинга (или XSS-атак) появилось в рамках концепции Web 2.0, в которой пользователи сети Интернет получили возможности участвовать в создании и распространении контента на различных площадках сети Интернет. В рамках этой концепции появились такие виды ресурсов, как форумы, социальные сети, имиждборды и т. д. Ключевой особенностью этих ресурсов является возможность пользователей создавать материалы, оставлять отзывы и взаимодействовать с аудиторией площадок посредством сообщений.

Появление таких ресурсов вызвало всплеск интереса к сети Интернет, поскольку в отличие от классической концепции, в соответствии с которой размещение информации было возможно только путем создания собственного сайта, концепция Web 2.0 для организации сетевого общения избавляет пользователя от необходимости изучения веб-дизайна, заключения договора хостинга и администрирования собственного ресурса [1].

Бурное развитие новых технологий сетевого общения привело к тому, что практически сразу же появились проблемы информационной безопасности, предусмотреть появление которых до начала реализации концепции было практически невозможно. Эти проблемы были связаны преимущественно с внедрением кода в созданные или создаваемые веб-страницы [3].

Организовывая сетевое общение, создатели сайтов исходили из того, что пользователи их ресурсов будут вести себя добросовестно. К тому же степень

угроз из-за недобросовестных действий при эксплуатации ресурсов сетевого общения была существенно недооценена. Разработчики исходили из соображений о том, что даже в случае злого умысла со стороны пользователей ресурсов нанести сколько-нибудь серьезный ущерб ресурсу и его пользователям злоумышленники не смогут. Средства разработчиков также содержали уязвимости, способствующие совершению атак на информационные ресурсы.

Общей чертой атак на внедрение кода является интерпретация запроса пользователя как команды для выполнения. В зависимости от атакуемого инструмента, характер атак и их разновидности могут отличаться.

Так, к современным видам атак на внедрение кода относят [2]: инъекции; межсайтовый скриптинг; внедрение XML-сущностей.

Из этих разновидностей атак особое место занимает межсайтовый скриптинг, что связано с особенностью его функционирования и организации атак.

Несмотря на то, что OWASP в настоящее время считает межсайтовый скриптинг наименее опасной атакой типа внедрения кода, тем не менее последствия для бизнеса из-за XSS-атак могут быть намного более разрушительными. Оценка OWASP базируется преимущественно на технических последствиях для системы, оценить экономический ущерб в общем случае не представляется возможным. Однако при детальном сравнении межсайтового скриптинга с инъекциями и внедрением XML-сущностей можно отметить следующее.

1. Межсайтовый скриптинг применим в отношении значительно большего количества ресурсов, нежели инъекции. Это связано с тем, что серьезные ресурсы традиционно при создании и эксплуатации баз данных уделяют особое внимание противодействию инъекциям. Последствия инъекций разрушительны именно для создателей сайта, их недоработки при осуществлении таких атак очевидны. Межсайтовый скриптинг для создателей сайтов не очевиден. Поскольку код не выполняется на сервере, заметить такую атаку со стороны сервера достаточно проблематично. В 2007 г. специалисты OWASP отмечали, что межсайтовому скриптингу подвержены все информационные системы.

2. Межсайтовый скриптинг значительно проще в реализации, чем внедрение XML-сущностей, поскольку при внедрении сущностей злоумышленнику никогда не известны возможности конкретного парсера. Для успешной атаки требуется значительный объем подготовительной работы, и затраченные усилия не будут окуплены результатом. К тому же возможности, открываемые успешным внедрением XML-сущностей, достаточно узкоспециализированны, в то время как межсайтовый скриптинг привлекает злоумышленников для совершения бытовых, фоновых нарушений [4].

Таким образом, даже несмотря на то, что степень опасности XSS-атак неуклонно снижается год от года, вопросы противодействия межсайтовому скриптингу остаются актуальными.

Идея межсайтового скриптинга состоит в выполнении на компьютере пользователя скрипта с постороннего сайта. При любом типе атаки вредоносный скрипт размещается за пределами атакуемого сервера, поэтому проверка содержимого сервера бессмысленна, а пользователь ресурса, размещенного на сервере, зачастую находится в неведении о том, что фактически в его браузере выполняется код с другого сайта.

Для реализации классического межсайтового скриптинга требуется подготовка специальных ссылок, в URL которых входят параметры методов GET или POST, активирующие выполнение скрипта на постороннем ресурсе. Традиционно метод GET считается более уязвимым, однако, манипуляции со скриптами возможны и при передаче параметров методом POST [5].

Успешность атак межсайтового скриптинга, как и других атак внедрением кода, обусловлена отсутствием проверки данных, вводимых пользователем. Хранение непроверенных данных порождает очень опасную уязвимость, которую называют активной XSS-атакой и с которой будут взаимодействовать все пользователи сайта. В случае если непроверенные данные передаются обработчику, речь идет о пассивной атаке, степень опасности которой оценивается, как правило, ниже, но последствия ее применения могут быть не менее тяжелыми.

Несмотря на то, что механизмы межсайтового скриптинга достаточно давно изучены, атаки такого типа до сих пор актуальны. Это обусловлено тем, что уязвимости обработчиков в популярных средах PHP, JavaScript, ASP.NET могут быть обнаружены автоматически, сами среды хорошо проработаны и изучены, а также не содержат встроенных средств защиты.

Предпринимаемые разработчиком меры считают достаточными, однако заподозрить успешные XSS-атаки можно по некоторым косвенным признакам, связанным с возможностями, предоставляемыми межсайтовым скриптингом.

Перед анализом последствий и признаков, в случае межсайтового скриптинга атакуемый сайт выступает в роли так называемого «водопоя», т. е. часто посещаемого места, в котором злоумышленником разбрасываются приманки в виде специально подготовленных ссылок. Очевидно, что такие действия будут иметь смысл только в том случае, если место «водопоя» достаточно посещаемо, и анализировать на уязвимость сайты с низким уровнем популярности не имеет смысла.

Последствия применения злоумышленниками межсайтового скриптинга полностью определяются возможностями скриптовых языков, например *JavaScript*. К таким последствиям могут быть отнесены следующие [6].

1. Кража данных авторизации.

Скриптовый язык позволяет перехватить данные сессии для дальнейшего использования злоумышленником, причем в любом виде: в виде куки или в виде идентификатора сессии. Заподозрить со стороны сервера проведение межсайтового скриптинга можно, если на сервере проводится запись логов, в которые записывается идентификатор устройства пользователя или его IP-адрес.

Наличие автоматического скрипта на сервере, который бы аннулировал сессию пользователя при несовпадении любых сетевых параметров, позволяет прекратить атаку практически в самом начале, однако, несет очевидные неудобства для легальных пользователей сайта.

В данном случае ложное срабатывание возможно при использовании различных VPN-сервисов, в том числе встроенных в браузеры. Если браузер настроен на использование VPN в целях создания оптимального по скорости соединения, то в процессе одной сессии пользователя его IP-адрес моет меняться постоянно. При сбросе сессии сайта пользователь будет вынужден заново проходить авторизацию, что может вызвать раздражение, а в случае массовых атак привести к оттоку аудитории сайта.

Тем не менее логирование событий обязательно. В случае массовых срабатываний необходимо проанализировать данные сессии пользователя в целях оптимизации работы защиты и уменьшения доли ложных срабатываний.

2. Выполнение запросов к сайтам от имени пользователя.

Как правило, целью выполнения таких запросов является проведение атак на отказ в обслуживании. При этом атакуемый на отказ в обслуживании сайт взаимодействует исключительно с компьютером конечного пользователя, поэтому «сайт-водопой» с вредоносной ссылкой межсайтового скриптинга остается в тени.

Выявить такую атаку со стороны сервера крайне проблематично, поскольку признаки атаки на сервере отсутствуют. Вредоносный скрипт размещен на сайте злоумышленников, запросы делает компьютер пользователя.

Однако со стороны пользователя сайта признаки атаки будут видны. К таким признакам относятся замедление работы страницы, открытие новых вкладок и окон браузера. При этом опытный пользователь в состоянии проследить взаимосвязь между обращением к «сайту-водопою» и появлением подозрительных действий.

Службе поддержки следует крайне внимательно относиться к появлению в сети Интернет отзывов о таких инцидентах.

3. Перенаправление пользователей на сайты злоумышленников.

Как и предыдущее действие, такие последствия остаются для «сайта-водопоя» незамеченными, однако, как и в предыдущем случае, действия злоумышленников достаточно очевидны для пользователей.

Целью действия злоумышленников является получение данных авторизации пользователей, достаточно часто такие сайты легко распознаются пользователями.

Чтобы облегчить обнаружение и реагирование на атаки такого рода, необходимо добавлять на сайт возможности взаимодействия между пользователями. В частности, наличие возможности пожаловаться на комментарий пользователя, позволит администраторам сайта не только выявить попытку атаки, но и удалить вредоносный контент и заблокировать недобросовестного пользователя.

4. Получение доступа к хранилищу браузера.

К сожалению, качественно отследить такую атаку проблематично, поскольку целью злоумышленников могут быть идентификационные данные пользователя не только на атакуемом сайте, но и на посторонних сайтах.

Сами пользователи при этом далеко не сразу заметят результат атаки и впоследствии заподозрить именно межсайтовый скриптинг на конкретном сайте по конкретной ссылке будет достаточно проблематично.

5. Выполнение распределенных вычислений.

Без обратной связи с пользователями проведение такой атаки со стороны сервера не заметно. Пользователь может обратить внимание на замедление работы браузера в целом. Поскольку такое замедление наступает не сразу, то при отсутствии у пользователя средств антивирусной защиты атака останется незамеченной для пользователя.

Однако если компьютер пользователя защищен, то открытие ссылки будет заблокировано. Ряд антивирусных средств при этом автоматически посылает отчет, поэтому многократные срабатывания могут привести к тому, что «сайт-водопой» будет заблокирован браузером.

Поэтому надо регулярно проверять работоспособность сайта и реагировать на сообщения пользователей о срабатывании средств антивирусной защиты.

6. Эмулирование активности пользователя на сайте.

Целью такого эмулирования является накрутка показателей посещаемости, поэтому резкое изменение статистики должно вызвать у владельцев сайта подо-

зрения. Реагировать на это происшествие необходимо, поскольку в случае выявления такой накрутки партнерами владельцам сайта может быть нанесен существенный экономический и репутационный ущерб.

Анализ целей межсайтового скриптинга показывает, что выявление попыток атак по последствиям далеко не всегда возможно, однако, в случае вовлечения в систему обратной связи пользователей сайта позволяет достаточно своевременно обнаружить многие типы атак. В условиях отсутствия эффективных рекомендаций по повышению безопасности на этапе разработки сайта, такое взаимодействие целесообразно.

Список литературы

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

2. Ивличев, П. С. Обеспечение информационной безопасности в условиях современной криминальной среды : учебное пособие / П. С. Ивличев, Н. А. Ивличева. – Рязань : Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2018.

3. Ивличев, П. С. Анализ актуальных механизмов неправомерного доступа к компьютерной информации : учебно-практическое пособие / П. С. Ивличев, Н. А. Ивличева, М. Н. Трофимов. – Рязань : Рязанский филиал Московского университета МВД России имени В.Я. Кикотя, 2019.

4. Низамутдинов, М. Тактика защиты и нападения на web-приложения / М. Низамутдинов. – СПб. : БХВ-Петербург, 2005.

5. Полное пособие по межсайтовому скриптингу // Ahmed Elhady Mohamed. – URL: https://www.securitylab.ru/analytics/432835.php (дата обращения: 18.04.2021).

6. Савин, И. В. Межсайтовый скриптинг как актуальная угроза для современных веб-систем / И. В. Савин // Наука, техника и образование. – 2017. – № 9 (39). – С. 40–43.

Яковлева К. Ю.[1]*,*
слушатель Института подготовки сотрудников
для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Андреев А. В.,
старший преподаватель
кафедры уголовного процесса
Московского университета МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ ХРАНЕНИЯ НОСИТЕЛЕЙ ЭЛЕКТРОННОЙ ФОРМЫ ВЕЩЕСТВЕННОГО ДОКАЗАТЕЛЬСТВА

Вопрос организации процесса хранения в уголовном судопроизводстве всегда был актуален. Процессуалисты утверждают, что, если не исполнить порядок хранения доказательств, то они могут утратить свою ценность и в соответствии с Уголовно-процессуальным кодексом Российской Федерации [1] (далее – УПК России) приобретут статус недопустимых доказательств по уголовному делу.

Обратимся к ст. 82 УПК России «Хранение вещественных доказательств». Хранение вещественных доказательств подразумевает не только хранение, но и утилизацию, реализацию, учёт и передачу вещественных доказательств [2]. Данные процессы далеко не синонимы. Можно понять, что хранение включает все остальные действия. В таком случае существует неизвестность о способе хранения вещественных доказательств. Хранение вещественных доказательств – обеспечение сохранения их свойств и признаков.

Активно используется электронная форма передачи информации. Носители электронной информации представляют собой отдельную группу вещественных доказательств.

Цифровая информация записывается и хранится на электронном носителе, который применяется для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники [3]. Проанализируем определение «электронного носителя», сформулированное в ученых кругах по

отношению к процессу хранения. По мнению Ю. В. Гаврилина, электронный носитель – устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах [4].

Пункт 5 ч. 2 ст. 82 УПК России определяет места хранения электронных носителей информации: подпунктом «а» закреплено хранение в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации; подпунктом «б» – возвращаются их законному владельцу после осмотра и производства других необходимых следственных действий, если это возможно без ущерба для доказывания.

Белкин А. Р. в научных трудах выдвигает формулировки норм необходимых закреплению в уголовно-процессуальном законодательстве. Одна из его разработок – предложение в части хранения источников вещественных доказательств. Учёный предлагает установить такое место хранения, как финансовое подразделение органа, принявшего решение об изъятии имущества. Данное предложение обеспечит гарантированную сохранность и подотчётность имущества [5, с. 175].

Арбитражный апелляционный суд г. Москвы рассмотрел арбитражное дело, связанное с уголовным делом, в котором впервые в судебной практике квалифицировал криптовалюту в качестве имущества [6, 7]. Должны быть выработаны правила хранения, утилизации и реализации. В данное время отсутствует правовое поле обращения криптовалюты, а преступления совершаются, где собственнику данного имущества причинен в большинстве случаев крупный и особо крупный ущерб. Для решения вопроса с изъятием больших объёмов данных потребуется большой объём мест хранения.

Необходимо УПК России дополнить нормой, позволяющей создать виртуальный-кошелёк МВД России, «облачное» хранилище МВД России. Возможно, областью разработки будут интернет-пространство, специализированная сеть МВД России – единая система информационно-аналитического обеспечения деятельности МВД России (ИЦЕ ИСОД) [8].

В целях дальнейшей оптимизации электронного документооборота [9] и соблюдения требований надо: исключить факты подписания руководителями документов на бумажных носителях с последующим помещением в СЭД ИСОД МВД России и направления в подразделения распечатанных документов из СЭД ИСОД МВД России обычной почтой.

В силу того, что развитие информационно-телекоммуникационных технологий привело к созданию в МВД России ИЦЕ ИСОД, необходимо добавить в нее новую функцию по хранению электронной формы вещественного доказательства. Такое умозаключение сложилось из того, что указанная система знает облачную инфраструктуру, Сервис электронного документооборота (СЭД) – работа с электронной подписью [10], наличие электронных образов [11], Сервис электронной почты (СЭП) – почтовый ящик ведомственной структуры [12], а также имеется сторона безопасности – сервис управления доступом (СУДИС) [13].

В следственной практике ОМВД России по району Косино-Ухтомский города Москвы отправления запросов в коммерческие организации и получение ответов от них посредством почтовой связи [14] есть трудности. Отсутствие правильности применения ведомственных и межведомственных нормативных правовых актов, обеспечивающих меры по сокращению документооборота, в ходе предварительного расследования приводит к потере доказательств.

Проанализируем процесс отправки запроса. Следователь составляет запрос руководителю АО «Альфа Банк». По средствам использования СЭД ИСОД МВД России сохраняет документ как электронный образ, подписывает своей электронной подписью и направляет в отдел делопроизводства и режима (канцелярию) для присвоения исходящего номера и даты. Канцелярия, поставив соответствующие данные, отправляет «Почтой России» данный запрос. Такой процесс документооборота подразумевает быструю отправку запроса. Коммерческая организация отвечает на данный запрос, ссылаясь на п. 1 ст. 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [15]: представленный запрос Банк не может рассматривать как оформленный надлежащим образом; запрос, направленный посредством почтовой связи должен содержать собственноручную подпись уполномоченного лица.

Сложность в том, что толкование ведомственного документа и федерального закона на низком уровне у правоохранительных органов. Следователь (дознаватель) должен ставить собственноручную подпись для того, чтобы ускорить процесс предварительного расследования и соблюсти принцип разумного срока. Данный практический пример не говорит о том, что неправильное применение информационных технологий в предварительном расследовании требует отказаться от нововведений. Повышение квалификации сотрудников правоохранительных органов, устранение пробелов в УПК России – основные направления развития и внедрения новых технологий в МВД России.

Ведомственный акт, регламентирующий организацию работы ИСОД, наделен функцией – хранение документации ИСОД в электронном виде [16]. Следователи (дознаватели) работают в этой системе и знают ее специфику. Необходимо внести изменение в постановление Правительства Российской Федерации от 8 мая 2015 г. № 449 «Об условиях хранения, учета и передачи вещественных доказательств по уголовным делам», которым утверждены «Правила хранения учета и передачи вещественных доказательств по уголовным делам» (далее – Правила) [17]. Пункт 2 изложить в следующей редакции: утвердить прилагаемые Правила хранения, учета и передачи вещественных доказательств и электронной формы вещественных доказательств по уголовным делам.

В Правилах в пункте 1 добавить к вещественным доказательствам электронную форму вещественных доказательств.

В пункт 2 добавить: электронную форму вещественных доказательств в виде электронных (цифровых) данных переместить на хранение в «облачное» хранилище ИСОД МВД России. Электронную форму вещественных доказательств в виде крипто-активов переместить на хранение в «крипто-кошелек» МВД России, ключ к которому имеет ответственное лицо или лицо, его замещающее, за хранение электронной формы вещественного доказательства.

Представитель тылового обеспечения ОМВД России будет иметь ключ (пароль) от данных мест хранения и выдаваться в ходе предварительного расследования следователю или дознавателю. В процессе создания постановления о признании и приобщении электронной формы вещественного доказательства следователь указывает в нем, что хранение электронной формы вещественного доказательства осуществляется в «облачном» хранилище ИСОД ОМВД России по району города Москвы.

В силу того, что в проведении следственных действий, связанных с электронной формой вещественных доказательств, должно быть обязательное участие IT-специалиста, создание резервной копии не обязательный признак. Резервное копирование обеспечивает создание копии электронных данных с целью обеспечить сохранность доказательств. Если, по мнению IT-специалиста, есть угроза потери электронной формы вещественного доказательства, то необходимо создать его резервную копию. Данное действие следователь обязательно должен отобразить в протоколе того следственного действия, в ходе которого проводился осмотр, а также указать основание совершения резервной копии.

Доступ к соответствующим данным виртуального пространства будет иметь следователь (дознаватель), в производстве которого находится уголовное дело, а

также руководитель следственного органа. Допустимость доказательств обеспечена тем, что гарантия от произвольной модификации информации лицами, имеющими к ней доступ и обеспечения защиты конфиденциальной информации, обеспечится построением мест хранения в виртуальном пространстве на базе технологии «Блокчейн»[1]. В настоящее время «Сбербанк России» и «Альфа банк» разрабатывают систему электронного документа оборота на базе технологии «Блокчейн». Функционирование систем криптовалют основано на технологии блокчейн (англ. *blockchain* – цепочка блоков). Она заключается в том, что списки операций с криптовалютой объединяются в блоки, а блоки – в цепочки по определенным правилам, гарантирующим невозможность отменить перевод криптовалюты между участниками и дважды потратить криптовалюту.

Данное право следует закрепить в дополнение к пдп. «а» п. 5 ч. 2 ст. 82 УПК России, а именно: вещественное доказательство в виде электронной формы хранится на созданных правоохранительными органами интернет-пространствах, в условиях, исключающих возможность ознакомления посторонних лиц с содержащихся на них информацией и обеспечивающих их сохранность и сохранность указанной информации.

Таким образом, рассмотрены организация и порядок хранения доказательств в отношении носителей электронной формы вещественных доказательств. Предложены следующие поправки в законодательство России.

Электронную форму вещественных доказательств в виде крипто-активов переместить на хранение в «крипто-кошелек» МВД России, ключ к которому имеет ответственное лицо или лицо, его замещающее, за хранение электронной формы вещественного доказательства.

Данная идея позволит решить трудность в ходе фиксации электронных данных с соблюдением всех требований закона и определение мест хранения. Места хранения, закреплённые п. 5 ч. 2 ст. 82 УПК России, для электронных носителей информации могут быть применены для электронной формы вещественных доказательств. Необходимо пункт 5 обозначить как электронные носители информации и электронная форма вещественных доказательств.

---

[1] Под технологией «блокчейн» (англ. blockchain или block chain) понимается – выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию.

Список литературы

1. Уголовно-процессуальным кодексом Российской Федерации : Федеральный закон от 24.12.2001 № 174-ФЗ (ред. от 19 октября 2020 года № 328-ФЗ) // Собрание законодательства Российской Федерации. – 2001. – № 52, ст. 4921; 2020. – № 42, ст. 6515.

2. Постановление Правительства Российской Федерации от 08.05.2015 № 449-ФЗ // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 16.04.2021).

3. Межгосударственный стандарт ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения». Электронный ресурс // Электронный фонд актуальных правовых и нормативно-технических документов. – URL: http: // does.cntd.ru/ document/420205524 (дата обращения: 16.04.2021).

4. Гаврилин, Ю. В. Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2017. – № 4.

5. Белкин, А. Р. УПК РФ: отменить нельзя поправить? В 2 т. Т. 1. Общая часть / А. Р. Белкин. – 2-е изд., испр. и доп. – М. : Юрайт, 2020.

6. Приговор Десятого арбитражного апелляционного суда г. Москвы от 15.05.2018 по делу № А40-124668/2017 // Судебные и нормативные акты. – URL: http://sudact.ru/regular/doc/ (дата обращения: 10.02.2021).

7. Гражданский кодекс Российской Федерации. Часть первая : Федеральный закон от 30.11.1994 № 51-ФЗ // Официальный интернет-портал правовой информации. – URL http://www.pravo.gov.ru (дата обращения: 16.04.2021).

8. Приказ МВД России от 23.11.2016 № 755 «Вопросы эксплуатации центра разработки, поддержки, внедрения и администрирования сервисов единой системы информационно-аналитического обеспечения деятельности МВД России» // Специализированная территориально распределенная автоматизированная система (СТРАС) МВД России «Юрист».

9. Распоряжение МВД России от 09.11.2015 № 1/9112 «О мерах по переходу на электронный документооборот» // Специализированная территориально распределенная автоматизированная система (СТРАС) МВД России «Юрист».

10. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства Российской Федерации. – 2011. – № 15, ст. 2036.

11. Приказ ГУ МВД России от 18.11.2016 № 465 «О мерах по использованию СЭД ИСОД МВД России в системе ГУ МВД России по г. Москве» // Специализированная территориально распределенная автоматизированная система (СТРАС) МВД России «Юрист».

12. Распоряжение МВД России от 31.12.2019 № 1/15321 «О некоторых вопросах использования ведомственного сервиса электронной почты в системе МВД России» // Специализированная территориально распределенная автоматизированная система (СТРАС) МВД России «Юрист».

13. Приказ МВД РФ от 20.06.2012 № 615 «Об утверждении инструкции по делопроизводству в органах внутренних дел» (в ред. приказов МВД России от 28 мая 2013 года № 296, от 28 декабря 2016 года № 915) // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 16.04.2021).

14. Федеральный закон от 17.07.1999 № 176-ФЗ «О почтовой связи» // Собрание законодательства Российской Федерации. – 1999. – № 29, ст. 3697.

15. Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства Российской Федерации. – 2011. – № 15, ст. 2036.

16. Приказ МВД России от 23.11.2016 № 755 «Вопросы эксплуатации центра разработки, поддержки, внедрения и администрирования сервисов единой системы информационно-аналитического обеспечения деятельности МВД России» // Специализированная территориально распределенная автоматизированная система (СТРАС) МВД России «Юрист».

17. Постановление Российской Федерации от 08.05.2015 № 449 «Об условиях хранения, учета и передачи вещественных доказательств по уголовным делам» // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 16.04.2021).

Измайлов А. Э.[1]*,*
курсант факультета
подготовки сотрудников для подразделений
экономической безопасности
и противодействия коррупции
Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:
Калашникова А. А.,
преподаватель кафедры
информатики и математики
Московского университета МВД России имени В.Я. Кикотя

ИНТЕРНЕТ-ЗАВИСИМОСТЬ КАК ПРОБЛЕМА ОБЩЕСТВА

В настоящее время более 4,5 млрд людей пользуются интернетом, а аудитория социальных сетей перевалила за отметку в 3,8 млрд [2]. Более половины, т. е. около 60 % населения всего мира уже онлайн, и есть все основания полагать, что уже к середине года половина всех людей на планете будут пользоваться соцсетями.

Разберем, что же такое интернет?

Это телекоммуникационная сеть, которая стала всемирной и стала основой для Всемирной паутины (WORLD WIDE WEB). Согласно отчету о состоянии цифровой сферы Digital 2020, который каждый год готовят *We Are Social* и Hootsuite, цифровые технологии, мобильные устройства и социальные сети стали неотъемлемой частью повседневной жизни людей во всем мире.

Понятие цифровых технологий достигло новых высот, и все больше людей во всем мире тратят огромное время в интернете, решая там все больше задач:

- Количество интернет-пользователей в мире до 4,54 млрд, это на 7 % больше прошлогоднего значения (+298 миллионов новых пользователей в сравнении с данными на январь 2019 г.).
- В январе 2020 г. в мире насчитывалось 3,80 млрд пользователей социальных сетей, аудитория соцмедиа выросла на 9 % по сравнению с 2019 г. (это 321 млрд новых пользователей за год).
- Сегодня более 5,19 млрд человек пользуются мобильными телефонами – прирост на 124 млн (2,4 %) за последний год. Данные представлены на рис. 1.

---

[1] © Измайлов А. Э., 2021.

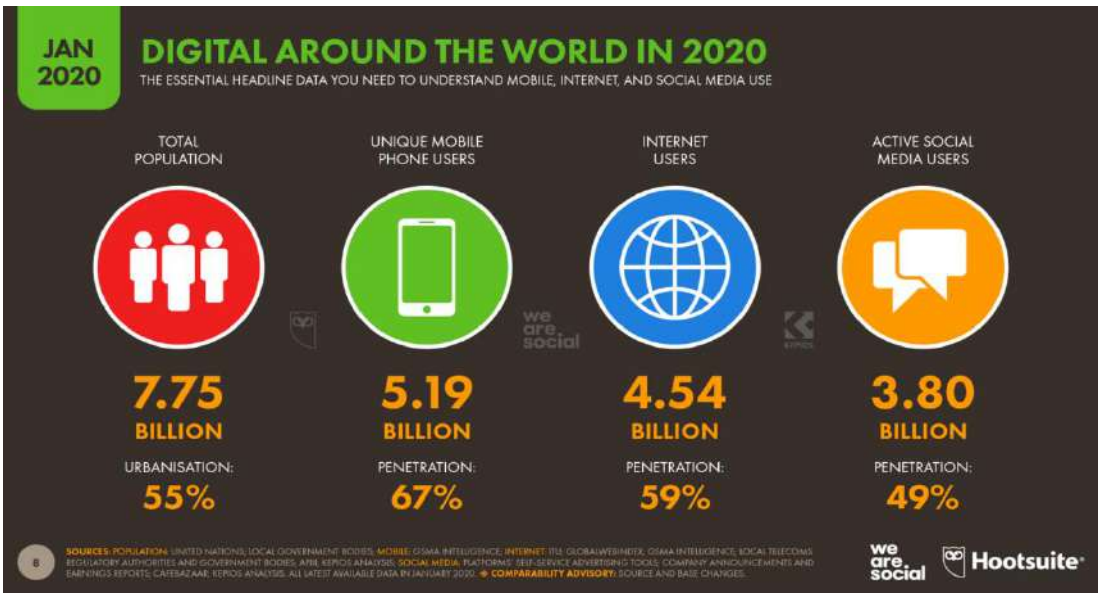


Рис. 1. Статистика использования сети Интернет

Проблема интернет-зависимости очень актуальна, поскольку, во-первых, постоянным увеличением числа пользователей интернета (около 60 % в настоящее время); во-вторых, тем, что чрезмерное пристрастие к интернету разрушающе действует на общество, вызывает отрицательное воздействие на психику и сознание людей и общество в целом; в-третьих, отсутствием расширенных опытов, исследований в этой области в силу относительной новизны понятия интернет-зависимости, который до сегодняшнего момента в русскоязычной литературе практически не рассматривался.

У каждого человека присутствует некая зависимость, начиная от употребления алкоголя, сигарет, употребления большого количества пищи или покупка материальных ценностей. В силу развития молодого поколения и информационных технологий выделяют новый вид зависимости, как интернет-зависимость – психологическое расстройство, которое побуждает людей тратить время за компьютером или смартфоном, что влияет на их здоровье, внешний вид, работу, финансы или взаимоотношение с людьми. Важно понимать, что существует как минимум пять конкретных типов интернет-зависимости:

- Навязчивая финансовая потребность. Потребность касается интерактивных действий в интернете, которые могут быть чрезвычайно вредными, например азартные игры, торговля акциями, онлайн-аукционы (например, E-bay) и принудительные покупки.
- Киберсексуальная зависимость – интернет-сайты для взрослых, сексуальные чаты фантазии.

- Кибер (онлайн) отношения – формируются в чатах или на разных сайтах социальных сетей, но могут происходить везде, где вы можете общаться с людьми в интернете.
- Навязчивый веб-серфинг. Интернет предоставляет пользователям множество данных и знаний. Для некоторых возможность найти информацию так легко превратилась в неконтролируемое стремление собирать и систематизировать данные.
- Компьютерная или игровая зависимость – действия, выполняемые как на компьютере, так и в автономном режиме.

Большинство людей могут быть подвержены интернет-зависимости. Просмотр в интернете роликов, статей или бесполезных видеоматериалов вызывает привыкание у людей, если у них есть проблемы, например беспокойство. Люди с депрессивными жалобами или психологическим расстройством могут легко стать зависимыми от интернета. Социальная изоляция, одиночество и депрессия откладываются в сознании, и это увеличивает серьезность ситуации. Интернет-зависимость может легко возникнуть у людей, у которых есть проблемы: наркотики, алкоголь, азартные игры и сексуальность.

Основные причины интернет-зависимости:

– недопонимание со стоны друзей и близких в реальной жизни;

– повышенная ранимость;

– трудности относительно адаптации в новом обществе;

– неумение строить отношения.

Озабоченность общества, интерес к познаванию и изучению интернет-использования объясняются тем, что становится все сложнее и труднее находить параллель между интернетным и реальным миром. Интернет обладает огромным потенциалом, чтобы повлиять на эмоциональную составляющую людей и изменять уровень восприятия и уровень тревоги. Одна из наиболее приемлемых диагностических оценок расстройства интернет-зависимости была предложена в статье *KW Beard's* 2005 г. в *CyberPsychology and Behavior*. В ней предлагается пять диагностических критериев при выявлении расстройства интернет-зависимости у населения. В Китае и Гонконге проводят специальные лечения интернет-зависимости.

Наиболее распространенные психологические методы лечения расстройства интернет-зависимости:

– индивидуальная, групповая или семейная терапия;

– модификация поведения;

– диалектическая поведенческая терапия (ДБТ);

– когнитивно-поведенческая терапия (КПТ);

– конная терапия (ипотерапия);

– арт-терапия;

– оздоровительная терапия;

– реальная терапия.

Так как понятие и расстройство интернет-зависимости достаточно новый феномен, то для решения и эффективности лечения данной проблемы существует недостаточно методов, чтобы дать полный отчет действиям человека и выработать определенное лечение для каждого из них. Некоторые специалисты выступают за воздержание от интернета.

Интернет – отличное средство массовой информации. Он помогает быстро искать различные данные, которые требуются человеку за короткий промежуток времени. С его помощью него люди способны общаться, а также через различные мессенджеры или посредством электронной связи. Огромный плюс заключается в общении на расстоянии и проведении различных веб-семинаров или конференций. Но не стоит забывать о реальном мире, все же лучше выйти на улицу и подышать свежим воздухом, пообщаться с реальными людьми в реальном времени.

Интернет-зависимость – глобальная проблема, и самый лучший способ одолеть эту зависимость – научиться ценить реальную жизнь, заняться спортом, здоровьем, найти подходящее для себя дело. Повсюду происходят удивительные вещи, и пока мы находимся в виртуальном мире, и наша жизнь протекает в игре, мы не сможем познать всю жизнь, которую нам дали для нашего развития и будущего.

Список литературы

1. Арестова, О. Н. Мотивация пользователей Интернета. Гуманитарные исследования в Интернете / О. Н. Арестова, Л. Н. Бабанин, А. Е. Войскуновский; под ред. А. Е. Войскунского. М. : Можайск-Терра, 2019.

2. Глобальная статистика интернета на 2020 год // Web. Canape. Создание и продвижение сайтов. – URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (дата обращения: 20.04.2021).

3. Виды интернет-зависимости // Безопасный интернет – проект городского методического центра. – URL: http://security.mosmetod.ru/internet-zavisimosti/77-vidy-internet-zavisimosti (дата обращения: 20.04.2021).

4. Войскунский А.Е. Актуальные проблемы зависимости от интернета от 2018 года // Интернет-проект CYBERPSY. – URL: https://cyberpsy.ru/articles/vojskunskij-internet-addiction/ (дата обращения: 20.04.2021).

Поликарпов Е. С.[1],
начальник кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

РОЛЬ И МЕСТО ПОЛИЦИИ В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ, ОТЕЧЕСТВЕННЫЕ И ЗАРУБЕЖНЫЕ ПРИМЕРЫ

Особое внимание сегодня уделено кибербезопасности. Перед правоохранительным органом ставятся задачи обеспечения кибербезопасности. Рассмотрим нормативные правовые акты в области информатизации и кибербезопасности, определяется роль и место полиции, приводятся примеры зарубежных стран.

На разных периодах развития органов государственной власти ведомственными исследователями и учеными помещаются на передний план мировые научно-технические тренды. Долгое время приоритетом в развитии органов внутренних дел была широкая информатизация. В 2005 г. было положено начало информационного развития ведомства, созданием ЕИТКС.

Приказом от 20.05.008 № 435 «Об утверждении новой редакции Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел» определены этапы и период развития ЕИТКС. Своевременно принятое решение дало существенную оптимизацию работы ведомства, но очень скоро стало не универсальным.

В 2012 г. Министерство утвердило концепцию создания единой системы информационно-аналитического обеспечения деятельности ИСОД МВД России. Новая система стала продолжением развития ЕИТКС с учетом современного развития информатизации и гибкости к интеграции. Создание ИСОД МВД России в основном связано с объединением разрозненной информационной инфраструктуры министерства внутренних дел.

Сегодня ИСОД МВД России сложная и мультисервисная система, имеющая внутренние сегменты с подключением через межсетевое экранирование к сети Интернет. Практически у каждого сотрудника имеются идентификаторы для доступа к системе.

Социальная сфера не отставала в информационном развитии. Фундаментом для информатизации общества стал Интернет. Общедоступная сеть на столько распространена и переплетена с информационной структурой государства, что изолироваться от нее контрпродуктивно для ведомства. Отдельными политиками безопасности можно ограничить рабочее место сотрудника органов внутренних дел от интернета, но ряду служб и подразделений это сделать невозможно по специфике работы. Это делает информационную структуру министерства уязвимой для компьютерных атак, осуществляемых спецслужбами иностранных государств, профессиональными и дилетантскими хакерскими группировками так называемого внешнего нарушителя.

Кроме того, возникает проблема внутреннего нарушителя. Сотрудники, имеющие низкую компьютерную грамотность или умышленно игнорирующие требования по безопасности информации, создают большую угрозу ведомственной информационной структуры. Все это ставит на первый план кибербезопасность.

Согласно ГОСТ Р 56205-2014 кибербезопасность – это действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов [7].

Для понимания роли и места правоохранительного ведомства в обеспечении кибербезопасности классифицируем ее на три направления: личная; корпоративная (ведомственная); государственная.

Каждый, использующий современные информационные технологии создает на основе сети Интернет свое цифровое пространство – экосистему. Часто создание личной цифровой экосистемы обусловлено использованием технических и программных средств одно производителя, например пользователи *Apple* могут открывать ссылки в браузерах одновременно на всех устройствах общей системы, использовать единую систему электронных платежей, синхронизацию файлов и многое другое.

Современные облачные сервисы позволяют объединить устройства разных производителей в одну цифровую экосистему, где пользователи хранят в облаке копии документов, фотографии, пароли и т. д. Это удобствно, но может стать киберугрозой. Роль сотрудников органов внутренних дел в данном случае, заключается в расследовании уже случившегося факта нарушения личной кибербезопасности. Таким образом нарушение личной кибербезопасности в конечном итоге оборачивается преступлением в сфере компьютерной информации. Для того чтобы провести эффективную работу, необходимо участие следователей и оперативных с областью знаний по основам кибербезопасности.

Цифровая экосистема формируется, как для отдельной личности, так и для отдельной корпорации. Одна из основных причин – переход к цифровым услугам и ориентация на современного пользователя, кроме того, в условиях пандемии большинству организаций пришлось организовать многофункциональные удаленные рабочие места. Обеспечение корпоративной кибербезопасности, как и личной, обеспечивается собственными силами владельцев цифровой экосистемы. Базовый набор средств – это межсетевые экраны, системы предотвращения компьютерных атак, системы обнаружения вторжений, антивирусы и пр. В случае если указанные средства не сработали или были атакованы, то в большинстве случаев все также сходится к расследованию преступления.

В государственном масштабе кибербезопасность один из составных элементов обеспечения информационной безопасности. Основополагающим документом является доктрина информационной безопасности. В структуре основных информационных угроз доктрины можно обозначить направления органов внутренних дел. Трансграничный оборот информации и информационно-психологическое воздействие имеет прямое отношение к деятельности ведомства, типовой пример – пресечение размещению экстремистских и террористических материалов в интернете. Компьютерная преступность – компетенция всех правоохранительных ведомств, но относится к личной и корпоративной кибербезопасности.

Нарушение кибербезопасности осуществляется путем реализации компьютерных атак. Для понимания будем опираться на следующее определение. Компьютерная атака – целенаправленное воздействие программных и/или программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и/или прекращения их функционирования и/или создания угрозы безопасности обрабатываемой такими объектами информации [4]. Компьютерные атаки на объекты критической информационной инфраструктуры на данный момент единственная из угроз увязанная с государственной кибербезопасностью. В действующем правовом поле деятельность органов внутренних дел по обеспечению кибербезопасности в масштабах страны ничем не определена. Информационная структура органов внутренних дел к объектам критической информационной инфраструктуры не относится.

По своей уголовно-правовой и административной направленности, а также в соответствии с Федеральным законом «О полиции» от 07.02.2011 № 3-ФЗ направление кибербезопасности не функциональная обязанность полиции, и рассматривать ее можно только с позиции собственной безопасности [3]. Реализации таких функций, ведомственного центра обнаружения, предупреждения и

ликвидации последствий компьютерных атак осуществляет департамент информационных технологий, связи и защиты информации МВД России [6]. Обеспечение же кибербезопасности государства в соответствии с Указом Президента Российской Федерации от 15.01.2013 № 31с возложено на Федеральную службу безопасности России [1]. Расследование таких преступлений также осуществляется следователями органов федеральной службы безопасности [2].

Замыкание государственной кибербезопасности страны на одно ведомство вряд ли принесет максимальный уровень защищенности. По примеру зарубежных стран необходимо на уровне государства создать свою систему взглядов в виде стратегии, где будут распределены полномочия всех органов государственной власти.

Стратегия кибербезопасности Японии от 2018 г. предусматривает создание Стратегического штаба, который действует совместно с стратегическим IT-штабом, советом национальной безопасности и национальным центром готовности к инцидентам и стратегии кибербезопасности. Национальное полицейское агентство является членом стратегического штаба кибербезопасности. Все члены проводят совместные учения по реагированию на инциденты, определяют роли соответствующих структур, таких как полиция и силы самообороны, проводят анализ новых угроз, которые появляются вместе с новыми услугами, в том числе социальными сетями и групповой почтой [8].

Стратегия кибербезопасности Великобритании на 2016–2021 гг. определяет широкий круг мер. Министерство внутренних дел сотрудничает с ведущими телекоммуникационными компаниями для того, чтобы предоставить операторам критически важных элементов национальной инфраструктуры услуги по улучшению кибербезопасности. Среди важных мер, призванных обеспечить достижение этой важнейшей цели, – создание национального подразделения по вопросам киберпреступности при национальном агентстве по борьбе с преступностью.

Великобритания регулярно принимает участие в международных киберучениях, в частности – организуемых Евросоюзом (ЕС), НАТО, Европейским оборонным агентством (ЕОА) и Министерством внутренней безопасности США (учения «Кибер-шторм») с целью понимания характера взаимной зависимости сторон, а также упрочения возможностей реагирования всеми странами-участницами.

Кроме того, Национальное криминальное агентство (NCA) создало новое киберподразделение, которое объединило усилия отдела по киберпреступности при Агентстве по борьбе с организованной преступностью (SOCA) и Централь-

ного отдела по борьбе с киберпреступностью столичной полиции. Это подразделение осуществляет работу для четырех областей криминального агентства NCA (охрана границ, борьба с организованной преступностью, экономическими преступлениями и эксплуатацией детского труда и их онлайн-защиты) посредством предоставления экспертной поддержки и разведданных, а также общих советов. Киберподразделение служит национальным органом по борьбе с наиболее серьезными киберпреступлениями и является частью группы реагирования на инциденты национального масштаба [9].

В декабре 2020 г. Европейская комиссия и Верховный представитель Союза по иностранным делам и политике безопасности представили новую Стратегию кибербезопасности Европейского Союза, которая направлена на защиту глобального и открытого интернета путем использования и усиления всех инструментов и ресурсов для обеспечения безопасности и защиты европейских ценностей и основных прав каждого человека. В Стратегии определена совместная работа по предотвращению, сдерживанию и реагированию на киберугрозы с помощью своевременного и слаженного гражданского, полицейского и судебного реагирования [10].

В Стратегии работа по кибербезопасности строится на внедрении инструментов регулирования, мобилизации и сотрудничества. Система кибербезопасности – это объединение институтов, органов и агентств, а также властей государств-членов. Эти объединения включают: органы управления; правоохранительные и судебные органы; органы кибер-дипломатии; органы киберзащиты.

В ходе рассмотрения зарубежного примера можно с уверенностью отметить важнейшую роль правоохранительных органов в комплексной работе по обеспечению кибербезопасности государства. Кибербезопасность имеет устойчивую связь с ростом киберпреступности.

Для повышения уровня кибербезопасности в России можно выделить ряд основных направлений, а также перенять положительные решения зарубежных стран. Во-первых, в России необходимо создать стратегию кибербезопасности которая повысит эффективность реагирования путем разделения ответственности органов государственной власти. Во-вторых, создать единую информационную площадку для оперативного обмена информацией между участниками, обеспечивающими кибербезопасность, а также проведения межведомственных учений.

Эффективная борьба с киберпреступностью ложится в канву единой системы кибербезопасности. Поэтому очень важно способствовать сотрудничеству и обмену между структурами кибербезопасности и правоохранительными органами.

Важно создать специализированные подразделения полиции. Созданные подразделения должны быть полностью оснащены для проведения расследований компьютерных преступлений и иметь соответствующие квалификации.

Список литературы

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 20.04.2021).

2. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон от 18.12.2001 № 174-ФЗ // СПС «Гарант». – URL: https://base.garant.ru/12125178/ (дата обращения: 20.04.2021).

3. Федеральным закон от 07.02.2011 № 3-ФЗ «О полиции» // СПС «Гарант. – URL: https://base.garant.ru/12182530/ (дата обращения: 20.04.2021).

4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «Гарант». – URL: https://base.garant.ru/71730198/ (дата обращения: 20.04.2021).

5. Указ Президента Российской Федерации от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/70199068/ (дата обращения: 20.04.2021).

6. Приказ МВД России от 16.06.2011 № 681 «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации» // СПС «Гарант». – URL: https://base.garant.ru/71282618/ (дата обращения: 20.04.2021).

7. ГОСТ Р 56205-2014 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1–1. Терминология, концептуальные положения и модели» // Электронный фонд правовых нормативных документов. – URL: https://docs.cntd.ru/document/1200114169 (дата обращения: 20.04.2021).

8. Commitment to a Free, Fair and Secure Cyberspace // Официальный сайт японского Национального центра готовности к инцидентам и стратегии кибербезопасности. – URL: https://www.nisc.go.jp/eng/ (дата обращения: 20.04.2021).

9. Киберготовность соединенного королевства: краткий обзор, Ведущий исследователь: Мелисса Хатауэй Крис Демчак, Джейсон Кербен, Дженнифер МакАрдл, Франческа Спидальери Октябрь 2016 // Портал о цифровой экономике и

ИКТ-политике. – URL: https://digital.report/kibergotovnost-soedinennogo-korolevstva-2-0/ (дата обращения: 20.04.2021).

10. The EU's Cybersecurity Strategy for the Digital Decade // Официальный сайт Евросоюза. – URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (дата обращения: 20.04.2021).

Белых-Силаев Д. В.[1]*,*
старший научный сотрудник 3 отдела НИЦ № 2
ФГКУ «ВНИИ МВД России»

Коровин Я. С.[2]*,*
генеральный директор
НИИ МВУС им. академика А.В. Каляева,
кандидат технических наук

Каляев И. А.[3]*,*
член Попечительского совета
ФГКУ «ВНИИ МВД России»
академик РАН, доктор технических наук

НЕКОТОРЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Президент Российской Федерации В. В. Путин отметил, что скорость технологических изменений в мире многократно возрастает, в связи с чем необходимо создать собственные технологии и стандарты по тем направлениям, которые определяют будущее. Речь идет прежде всего об искусственном интеллекте [6].

Искусственный интеллект (англ. *artificial intelligenc*) – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека.

По степени соответствия результатам интеллектуальной деятельности человека принято выделять «сильный» (*strong*) и «слабый» (*weak*) искусственный интеллект.

«Сильный» искусственный интеллект (*strong artificial intelligence*) призван наиболее полно воспроизводить когниции человека, т. е. его психические познавательные процессы (в том числе память, мышление, речь), более того, в перспективе искусственный интеллект может стать цифровым эквивалентом всех

элементов структуры психики человека – психических процессов, свойств, состояний и образований.

«Слабый» искусственный интеллект (*weak artificial intelligence*), наиболее распространен в наши дни, не стремится воспроизвести человека во всем спектре присущих ему возможностей, но решает частные прикладные задачи, при этом решая эти частные задачи, искусственный интеллект способен выполнять их значительно лучше естественного интеллекта человека, превосходя его в таких когнитивных процессах, как, например, память и мышление.

В России возможностям искусственного интеллекта в правоохранительной сфере посвящены работы Кожокаря В. В., Маслова А. А., Бабушкина А. А., Овчинского В. С. [1, с. 162–178; 2, с. 82; 3, с. 34; 4, с. 16].

Могут быть обозначены следующие *основные направления применения искусственного интеллекта* в правоохранительной деятельности: сбор, хранение и обработка информации; аналитическое и прогнозное моделирование; проведение цифровых расследований; обеспечение коммуникаций и взаимодействия.

Среди технологий, которые уже вошли в повседневную жизнь сотрудников полиции за рубежом и в России, можно отметить следующие системы искусственного интеллекта, адаптированные для целей правоохранительной деятельности:

1) программы идентификации лиц, находящихся в розыске (например, программа *Next Generation Identification (NGI) system*, разработанная ФБР США, а также проект компьютерного зрения *Janus*, разработанный в США в рамках проекта *Intelligence Advanced Research Projects Activity* [7]);

2) системы искусственного интеллекта, нацеленные на распознавание подозрительных или украденных транспортных средств, а также системы автоматического обнаружения ДТП (например, программа *Automated Accident Detection at Intersections* [5], разработанная и апробированная в Польше [5, с. 87]);

3) биометрические методы, позволяющие проводить идентификацию граждан, распознавать преступников и обнаруживать подозрительное, девиантное (отклоняющееся) поведение граждан (например, программы, как *VibraImage* (Россия), анализирующая перемещение точек тела в пространстве; *HireVue* (США), анализирующая движения рук и тела; бесконтактные мониторинговые устройства, разработанные во Франции (*iBorderCtrl*) [8] и в России – в НИИ МВУС им. академика А.В. Каляева [9]);

4) программы, позволяющие определять психоэмоциональное состояние человека по мимике, жестам, пантомимике, пара- и экстралингвистике, ча-

стоте сердечных сокращений, что позволяет использовать их для бесконтактной психофизиологической детекции лжи (например, программы – *Affectiva* (США), анализирующая лицевые экспрессии; *BeyondVerbal* (Израиль), анализирующая тональность речи; *AutoEmotive* (США), анализирующая частоту пульса и лицевые экспрессии; программный комплекс *VeriPol* (Испания) [10], бесконтактные полиграфные устройства, разработанные в НИИ МВУС им. академика А.В. Каляева);

5) системы искусственного интеллекта, предназначенные для выявления, пресечения и расследования мошенничества, финансовых правонарушений в киберпространстве; алгоритмы, позволяющие проводить цифровые расследования [11];

6) применение искусственного интеллекта для совершенствования осмотра места происшествия, например система *ShotSpotter* (США) позволяет определить место выстрела по звуку, а система *Cadre Research Labs* (США) позволяет по аудиозаписи выстрела установить тип и калибр оружия, которым было совершено преступление [12]);

7) применение искусственного интеллекта в судебной экспертизе (например, отдел судебной биологии Главного медицинского эксперта Нью-Йорка (США) эффективно использует интеллектуальный анализ данных для целей судебно-медицинской экспертизы и ДНК-анализа [13]);

8) системы искусственного интеллекта, разработанные для управления беспилотными летательными устройствами, позволяющими осуществлять мониторинг уличной преступности, предупреждать, пресекать и расследовать массовые беспорядки, акты вандализма, а также пресекать несанкционированное проникновение на охраняемые объекты (система искусственного интеллекта, осуществляющая управление беспилотными летательными устройствами, разработанная в НИИ МВУС им. академика А.В. Каляева).

Внедрение искусственного интеллекта в правоохранительную деятельность вызывает необходимость сформулировать *принципы* (основные, руководящие начала) его применения, среди которых за рубежом принято выделять следующие: законность (*justice*); безопасность (*security*); прозрачность (*transparency*); предсказуемость (*explainable*); управляемость (*manageable*); контролируемость (*controlled*). Поскольку содержание этих принципов в разных странах может быть различным, то требуется целенаправленная работа заинтересованных органов и организаций по унификации содержания принципов применения искусственного интеллекта, в том числе в правоохранительной сфере.

Необходимо также сформулировать *условия* эффективного применения искусственного интеллекта в правоохранительной деятельности, к которым относятся: изучение и анализ передового зарубежного опыта применения искусственного интеллекта; адаптация и внедрение передового зарубежного опыта в отечественную правоохранительную практику; формирование у сотрудников органов внутренних дел установки, отношения (*attitude*) к искусственному интеллекту как к технологии, способной повысить эффективность их оперативно-служебной деятельности; повышение квалификации сотрудников органов внутренних дел до уровня, достаточного для применения технологий искусственного интеллекта в повседневной оперативно-служебной деятельности.

К концу 2020 г. более 35 стран, включая Россию, приняли национальные стратегии развития искусственного интеллекта, а общий объем затрат на искусственный интеллект в мире в 2020 г. оценивался в 50 млрд долл. США.

Полагаем, что изучение зарубежного опыта применения искусственного интеллекта в правоохранительной деятельности, его своевременная адаптация для нужд органов внутренних дел Российской Федерации позволит существенно повысить эффективность правоохранительной деятельности.

Список литературы

1. Кожокарь, В. В. Основы оперативно-розыскного обеспечения коллективной безопасности государств-участников ОДКБ : монография / В. В. Кожокарь, А. А. Маслов, А. А. Бабушкин. – М. : ВНИИ МВД России, 2020.

2. Овчинский, В. С. Использование искусственного интеллекта в оперативно-аналитической деятельности ФБР по борьбе с преступностью / В. С. Овчинский // Актуальные проблемы теории оперативно-розыскной деятельности. – М. : ИНФРА-М, 2017.

3. Овчинский, В. С. Криминология цифрового мира / В. С. Овчинский. – М., ИНФРА-М, 2018.

4. Овчинский, В. С. Судья с искусственным интеллектом / В. С. Овчинский // Газета «Завтра». – 2019. – 13 февр.

5. Oskarbski J., Zawisza M., Zarski K. Automatic incident detection at intersections with use of telematics // Transportation Research Peocedia. – 2016. – Т. 14.

6. Послание Президента Российской Федерации Федеральному Собранию от 15.01.2020 «Послание Президента Федеральному Собранию» // СПС «Консультант Плюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_342959/ (дата обращения: 29.03.2021).

7. Официальный сайт исследовательского агентства США. – https://www.iarpa.gov/index.php/research-programs/janus (дата обращения: 31.03.2021).

8. Информационное письмо Представителя МВД России во Франции от 16.03.2021 № 30 // официально опубликовано не было.

9. Официальный сайт ООО «НИИ МВУС». – URL: https://niimvus.org.ru/ (дата обращения: 31.03.2021).

10. Информационное письмо Представителя МВД России в Испании от 16.03.2021 № 82 // официально опубликовано не было.

11. Официальный сайт «InfoWorld». – URL: https://www.infoworld.com/article/2907877/how-paypal-reduces-fraud-with-machine-learning.html (дата обращения: 31.03.2021).

12. Официальный сайт «National Institute of Justice». – URL: https://nij.ojp.gov/funding/awards/2016-dn-bx-0183 (дата обращения: 31.03.2021).

13. Официальный сайт «National Institute of Justice». – URL: https://nij.ojp.gov/libraty/publications/hybrid-machine-learning-approach-dna-mixture-interpretation (дата обращения: 31.03.2021).

Дядык Е. С.[1]*,*
курсант Института-факультета
судебной экспертизы
Московского университета МВД России имени В.Я. Кикотя

Финогенова А. Д.[2]*,*
курсант Института-факультета
судебной экспертизы
Московского университета МВД России имени В.Я. Кикотя

Александров Ю. Н.[3]*,*
заместитель начальника
кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ТАБЛИЧНЫХ ПРОЦЕССОРОВ ДЛЯ АВТОМАТИЗАЦИИ СИСТЕМ УЧЕТА СЛУЖЕБНОЙ ДЕЯТЕЛЬНОСТИ

При выполнении служебных обязанностей сотрудник органов внутренних дел обязан производить учет своей деятельности, составлять разнообразные отчеты. Объектами такого типа учетов могут быть очень разными по своей структуре и при этом в связи с изменениями нормативной базы могут меняться с течением времени. Учитывая доступность программного обеспечения, гибкость и возможность самостоятельной модернизации пользователями, для автоматизации этой рутинной операции могут быть использованы электронные таблицы, в частности электронные таблицы *Microsoft Excel*. Возможности этого табличного процессора позволяют организовать учет разнообразных видов деятельности [5, 6].

Рассмотрим в качестве примера программу посещаемости огневой и физической подготовки постоянным составом Московского университета МВД России имени В.Я. Кикотя, созданную авторами данной статьи по заказу отдела профессиональной служебной и физической подготовки управления по работе с личным составом университета.

Профессиональная служебная и физическая подготовка в МВД России регламентируется ведомственными нормативными правовыми актами: приказ Министерства внутренних дел Российской Федерации от 05.05.2018 № 275 «Об утверждении Порядка организации подготовки кадров для замещения должностей в органах внутренних дел Российской Федерации» [3]; приказ Министерства внутренних дел Российской Федерации от 01.07.2017 № 450 «Об утверждении Наставления по организации физической подготовки в органах внутренних дел Российской Федерации» [1]; приказ Министерства внутренних дел Российской Федерации от 23.11.2017 № 880 «Об утверждении Наставления по организации огневой подготовки в органах внутренних дел Российской Федерации» [2], а также приказом Московского университета МВД России имени В.Я. Кикотя от 15.07.2020 № 768 «Об организации занятий по профессиональной служебной и физической подготовке в Московском университете МВД России имени В.Я. Кикотя» [4].

Необходимость проведения данных занятий обусловлена тем, что постоянный состав университета может быть привлечён в качестве приданных сил по охране правопорядка в общественных местах, при чрезвычайных ситуациях и чрезвычайных обстоятельствах.

Занятия по служебной и физической подготовке проводятся в подразделениях университета регулярно согласно расписанию. Формирование данного расписания достаточно трудоёмкий процесс, который имеет ряд закономерностей, поэтому может быть упорядочен и автоматизирован.

Кроме того, на занятиях по служебной и физической подготовке ведётся учёт посещаемости, который требует автоматизации сбора, хранения и обработки. Эти данные позволяют формировать отчетную документацию.

Программа учета посещаемости огневой и физической подготовки постоянным составом Московского университета МВД России имени В.Я. Кикотя используется отделом профессиональной служебной и физической подготовки управления по работе с личным составом Университета. Рассматриваемая программа сформирована на базе книги *Microsoft Excel* версии 2010 с макросами.

Можно выделить четыре этапа работы с рассматриваемой программой:

- ✓ подготовительный,
- ✓ заполнение расписания,
- ✓ внесение данных о количестве человек, посещающих занятия по подразделениям,
- ✓ получение отчетных данных.

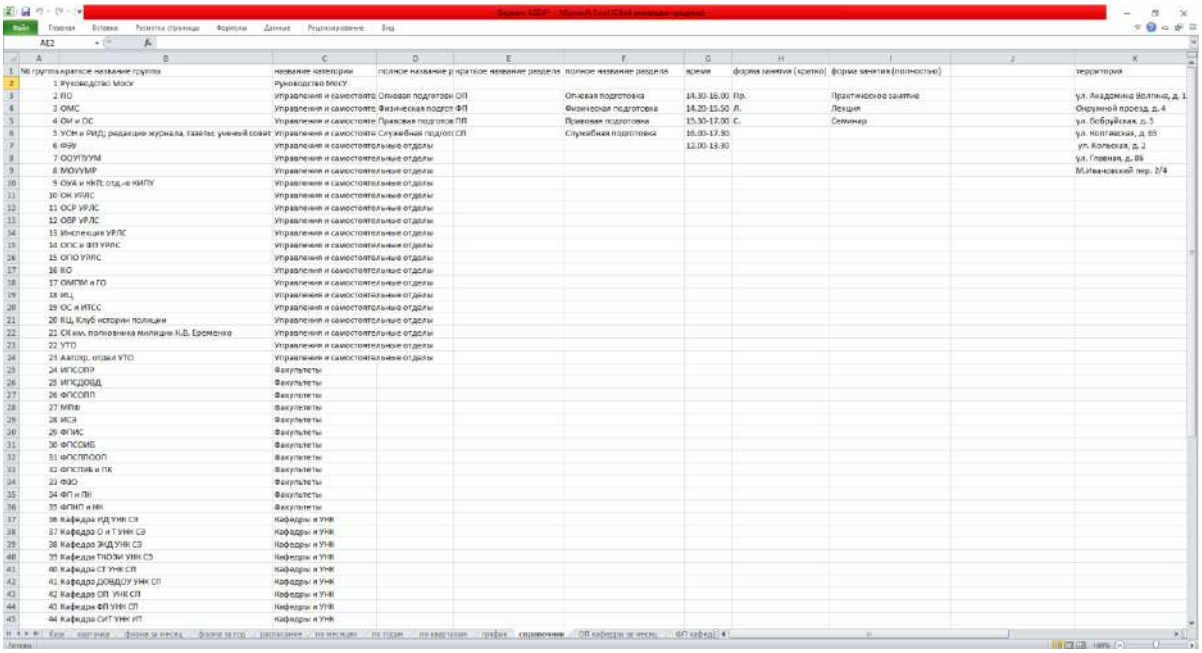


Рис. 1. Лист «СПРАВОЧНИК»

На первом этапе необходимо заполнить так называемые справочники – таблицы, содержащие списки возможных значений отдельных полей – список подразделений, их категорий, видов подготовки, времени занятий, залов их проведения и т. д. С их помощью организуются упрощенный ввод данных, защита от неправильно введенных данных, опечаток, а также на их основе будут формироваться расписание и учётные формы. Перед первым использованием и во время использования возможно редактирование справочников при изменении нормативных документов или при проведении организационно-штатных мероприятий. Описанные справочники вынесены в отдельный лист, называемый «СПРАВОЧНИК».

Второй этап – формирование листа расписания занятий по физической и огневой подготовке, заполнение табличной информации в листе «РАСПИСАНИЕ». Поскольку расписание огневой и физической подготовки имеет явную периодичность (недельную/двухнедельную), то при заполнении данной табличной формы удобно пользоваться копированием и протягиванием ячеек на соседние с использованием арифметической прогрессии. После того как расписание введено на определенный период, оно может дублироваться сходными блоками для заполнения на различные периоды любой продолжительности.

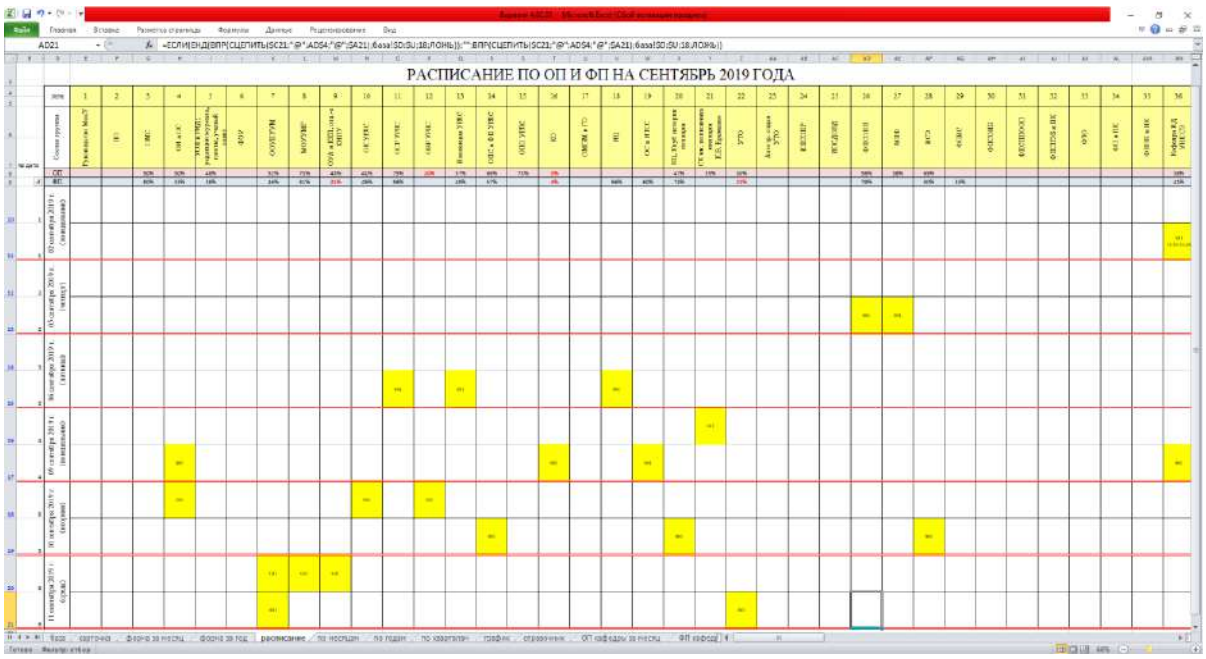
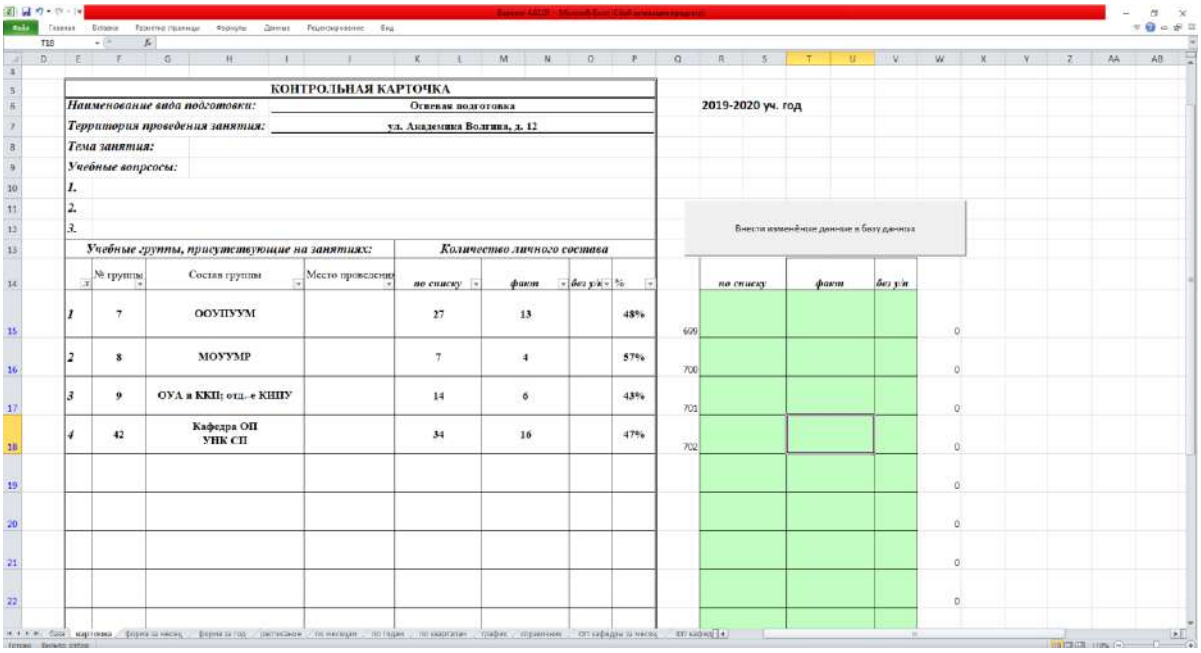


Рис. 2. Лист «РАСПИСАНИЕ»

Когда имеются все необходимые базовые сведения, возможен переход к работе в рамках третьего этапа – ежедневное внесение информации о посещаемости занятий. В связи с тем, что данный этап работы самый рутинный и практически ежедневный, то он должен быть наиболее автоматизирован и доступен персоналу с невысокой квалификацией и при этом исключал возможность ошибочного ввода информации и разрушения всей базы данных.

Для удобства использования был создан отдельный лист в «КАРТОЧКА» книге *Microsoft Excel*. Вначале на этом листе вводят данные (дата, вид подготовки и место дислокации). После того как на основании параметров фильтра будут отобраны группы, удовлетворяющие критериям поиска, возможно внесение количества людей в группе, посетивших занятие и отсутствующих без уважительной причины. Так как данная «карточка» связана с расписанием с помощью макроса, она позволяет внести данные сразу в имеющуюся базу, при этом редактировать табличные документы и искать в многочисленных строчках нужное занятие необходимость отпадает.

Таким образом, данная форма представления информации позволяет видеть и вносить информацию в наглядном виде, что значительно упрощает рутинную работу.



КОНТРОЛЬНАЯ КАРТОЧКА

Наименование вида подготовки: Огневая подготовка

Территория проведения занятия: ул. Академика Волгина, д. 12

Тема занятия:

Учебные вопросы:

1.
2.
3.

2019-2020 уч. год

Внести изменённые данные в базу данных

	Учебные группы, присутствующие на занятиях:			*Количество личного состава*			
	№ группы	Состав группы	Место проведения	*по списку*	*факт*	*без уч.*	%
1	7	ООУПУУМ		27	13		48%
2	8	МОУУМР		7	4		57%
3	9	ОУА и ККП; отд.-е КИПУ		14	6		43%
4	42	Кафедра ОП УНК СП		34	16		47%

	по списку	*факт*	*без уч.*	
699				0
700				0
701				0
702				0

Рис. 3. Лист «КАРТОЧКА»

Последний этап работы с базой данных – это получение отчетных форм и диаграмм, иллюстрирующих уровень посещаемости занятий по физической и огневой подготовке постоянным составом университета. В программе имеются соответствующие формы отчета за год, за месяц, за квартал. Кроме того, существует возможность сравнивать посещаемость занятий по видам занятий для отдельных подразделений или групп подразделений, например управления и самостоятельные отделы, факультеты, кафедры.

Работа над совершенствованием программы не прекращается. С момента внедрения в работу программы непрерывно осуществляются ее сопровождение, совершенствование отчетных форм, обучение вновь назначенных для работы с ней сотрудников, исправление найденных недостатков. На данный момент ведется работа по оформлению сопутствующей документации и акта внедрения программы учета посещаемости огневой и физической подготовки постоянным составом Московского университета МВД России имени В. Я. Кикотя.

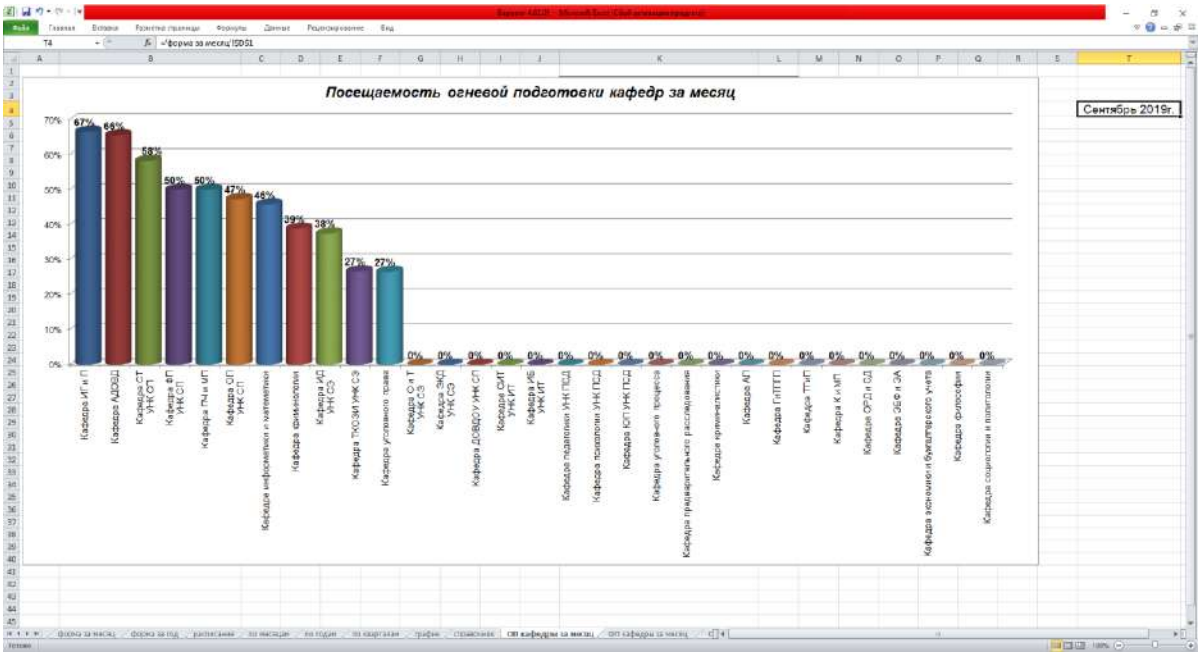


Рис. 4. Отчетная форма по огневой подготовке за выбранный период

Таким образом, данная программа уже показывает свою эффективность, позволяет вести учет посещаемости занятий по физической и огневой подготовке, получать статистику посещаемости, и формировать готовые отчетные документы. Кроме того, справочные листы и база динамичны, есть возможность добавления некоторых параметров учета, таких как иные виды подготовки, интересующие отчетные периоды, альтернативные принципы деления групп на категории и т. д., что делает возможным её использование другими подразделениями.

Программа учета посещаемости огневой и физической подготовки постоянным составом Московского университета МВД России имени В. Я. Кикотя уже используется в деятельности отдела профессиональной, служебной и физической подготовки управления по работе с личным составом Московского Университета МВД России имени В.Я. Кикотя, а также остается достаточно гибкой для внесения возможных изменений.

Список литературы

1. Приказ МВД России от 01.07.2017 № 450 «Об утверждении Наставления по организации физической подготовки в органах внутренних дел Российской Федерации» // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/71647620/ (дата обращения: 20.04.2021).

2. Приказ МВД России от 23.11.2017 № 880 «Об утверждении Наставления по организации огневой подготовки в органах внутренних дел Российской Федерации» // СПС «Гарант». – URL: https://base.garant.ru/71888290/ (дата обращения: 20.04.2021).

3. Приказ МВД России от 05.05.2018 № 275 «Об утверждении Порядка организации подготовки кадров для замещения должностей в органах внутренних дел Российской Федерации» // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/71877330/ (дата обращения: 20.04.2021).

4. Приказ МВД России от 15.07.2020 № 768 «Об организации занятий по профессиональной служебной и физической подготовке в Московском университете МВД России имени В.Я. Кикотя» // Официально опубликован не был.

5. Гарнаев, А. Ю. Microsoft Excel 2010: разработка приложений / А. Ю. Гарнаев, Л. В. Рудикова. – СПб. : БХВ-Петербург, 2011.

6. Задохина, Н. В. Обработка электронных документов в ОВД с помощью приложения MS Excel 2010 : учебно-методическое пособие / Н. В. Задохина, Н. М. Дубинина, Е. А. Слесарева, А. А. Страхов. – М. : Московский университет МВД России имени В.Я. Кикотя, 2018.

Комлева Т. В.[1]*,*
курсант факультета подготовки
сотрудников для подразделений
экономической безопасности
и противодействия коррупции
Московского университета МВД России имени В.Я. Кикотя

Дубинина Н. М.[2]*,*
начальник кафедры
информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

Бубнов В. В.[3]*,*
доцент кафедры И-15
Московского авиационного института
(национального исследовательского университета) (МАИ),
кандидат экономических наук, доцент

КРИПТОВАЛЮТА КАК НОВШЕСТВО СОВРЕМЕННОЙ ЭКОНОМИКИ: ОСОБЕННОСТИ И РИСКИ ФУНКЦИОНИРОВАНИЯ

Деньги являются «кровью» экономики, обеспечивая скорость и удобство расчетов между экономическими агентами. Развитие денежного обращения прошло длительную историю. В настоящее время денежная масса представлена различными агрегатами, в которых отражены исторические формы денег (от наличных до кредитных, а также ценных бумаг, выполняющих функции денег).

В XIX–XXI вв. идет развитие мировой валютной системы. В XIX в. сложилась система золотого стандарта. В 70-е годы прошлого века золото было демонетизировано, валютные курсы стали определяться на рынке, любая национальная валюта получила возможность использоваться в качестве платежного средства в мировой торговле (девиза), появились новые платежные средства – специ-

альные права заимствования (SDR). В XXI в. в попытке ускорить обращение денег и уйти от контроля государственных органов власти сложились новые платежные системы, в том числе система криптовалют (см. рис. 1).

Рис. 1. Развитие товарно-денежных отношений (предпосылки к «возникновению» цифровых активов)

В традиционном представлении, сложившемся в последние столетия, эмиссия денег (национальной валюты) в государстве производится центральным банком или органами, его заменяющими. Контроль над денежной массой и ее обращением – важнейшая задача государства, которая реализуется в разработке и осуществлении денежной политики, как элемента социально-экономической политики государства.

Обращение денег жестко регулируется государством; под его контролем находится и финансовая система. Ряд экономических агентов выступает против такого жесткого контроля. Как альтернатива была разработана децентрализованная платежная система, которая пока слабо регулируется государственными органами власти. Элементом этой платежной системы являются криптовалюты. Статус этих валют пока окончательно не сложился. Задумывались они как механизм бесконтрольного со стороны государства перевода средств между экономическими агентами с помощью криптографических записей с открытым ключом. Создатели многих криптовалют не известны широкой общественности, как

следствие не известны конечные бенефициары системы обращения криптовалют. Изучение функционирования рынка криптовалют, его влияние на национальную безопасность государства – одна из задач современной науки.

Появление криптовалют стало следствием развития информационных технологий, формирующих современную социально-экономическую действительность, что нашло отражение и в правовом поле государств. В настоящее время экономисты и законодатели разных стран определяют место криптовалюты в экономической системе, отвечая на вопрос о целесообразности использования или запрета работы данной платежной системы [7].

Особенность функционирования механизма криптовалют заключается в полной анонимности адресата и адресанта денежных средств, что является угрозой национальной безопасности государства, создавая условия для оборота средств теневой экономики. Таким образом, риск обращения криптовалют связан с формированием условий для совершения противоправных действий.

Неопределенность эмиссии криптовалют говорит о повышении инфляционных рисков национальной экономики, особенно если разрешить покупку товаров и услуг через платежные средства, эмиссия которых никак не контролируется государством.

В системе электронных переводов есть опасность многоразового расходования одних и тех же средств. В современной электронной системе денежных расчетов банки и операторы электронных платежных систем страхуют от такой опасности, жестко контролируя состояние счетов экономических агентов.

Особенность платежной системы криптовалют – отсутствие внешнего контроля. Контроль анонимен и осуществляется с помощью информационных технологий. Анонимность контроля, невозможность отследить получателя, случайные потери ключей приводят к рискам незаконной утраты средств, размещенных в платежной системе криптовалют. В современных условиях правоохранительные, налоговые и иные государственные органы и учреждения не могут отследить и/или отменить совершенный платеж, даже если будет доказана его незаконность, возникают трудности получения доказательной базы о совершении противоправных действий при обороте денежных средств (криптовалют).

Существуют различные криптовалюты, объем которых неизвестен. Риск их функционирования – создание финансовой пирамиды. Они оттягивают на себя свободные национальные денежные средства (валюты), ограничивая средства, поступающие на инвестиционный рынок. Таким образом, криптовалюты сами становятся финансовым инструментом, надежность которого никем не гарантирована и не имеет должного законодательного регулирования. Криптовалюты

после первого эмиссионного размещения, когда необозначенные владельцы криптографических записей получают традиционные валютные средства (национальные деньги), могут быть перепроданы как ценные бумаги, хотя таковыми не являются. Держателю криптографической записи такая продажа может принести как прибыль, так и убыток.

В мировом сообществе можно отследить несколько точек зрения о развитии криптовалют:

– положительная: криптовалюта – это естественное развитие финансовой системы, в которой применяются современные цифровые технологии, позволяющие увеличить скорость обращения денег, используются возможности альтернативного вложения денежных средств;

– негативная: криптовалюты – увеличивают риски национальной безопасности, создают условия для роста безнаказанности лиц, нарушающих законы;

– нейтральная: не учитывают в своей деятельности наличие криптовалют [4];

– взвешенная: появление криптовалют – сложившаяся реальность, в которой государство должно поставить криптовалюты и платежный рынок, связанный с ними, под жесткий контроль (в случае крайней необходимости при наличии доказанных угроз национальной безопасности максимально ограничить функционирование рынка криптовалют).

Для преодоления рисков криптовалютного рынка и использования его потенциала для развития народного хозяйства Российской Федерации были предприняты шаги по государственному регулированию оборота цифровых валют. С 2021 г. вступили в силу большинство норм Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». В соответствии с этим законом в Российской Федерации под цифровой валютой понимается совокупность электронных данных, которые одновременно являются инвестициями и средствами платежа, при этом не являются денежной единицей. Подчеркивается отсутствие обязательств перед обладателем указанных электронных данных. Регулируется оборот цифровой валюты. Особо подчеркивается запрет распространять сведения о предложении и приеме цифровой валюты как способе оплаты товаров, работ и услуг.

Появление криптовалюты (цифровой валюты) – новшеством в экономике, в котором отражены инновации в информационных технологиях, применяемыми в денежной и финансовой системах. Криптовалюты создают систему упрощенных анонимных расчетов, что, с одной стороны, создает условия для быстрого решения хозяйственных вопросов, а с другой, учитывая анонимность операций,

непредсказуемость поведения эмиссионного центра, создают угрозы национальной безопасности и обеспечению правопорядка в стране. Сокращение рисков лежит в продуманном правовом регулировании обращения криптовалют, создании правовых условий для борьбы с анонимностью рынка.

Список литературы

1. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 16.04.2021).

2. Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 16.04.2021).

3. Закон о цифровых активах вступил в силу. Что изменилось? // Официальный сайт группы компаний RBC. – URL: https://www.rbc.ru/crypto/news/5fedaf549a794784d89eb416 (дата обращения: 18.04.2021).

4. Национальная криптовалюта Rucoin. Есть ли у нее перспективы? // Криптовалюты, майнинг и блокчейн простыми словами. – URL: https://cryptomagic.ru/kriptovaluty/rossijskaya-rucoin.html (дата обращения: 18.04.2021).

5. Новости мира криптовалюты и майнинга // Майнинг криптовалюты. – URL: https://mining-cryptocurrency.ru/ (дата обращения: 18.04.2021).

6. Девять лучших криптовалют на рынке. На каких альткоинах можно заработать // Официальный сайт группы компаний RBC. – URL: https://www.rbc.ru/crypto/news/5fbf546a9a7947891e643924 (дата обращения: 18.04.2021).

7. KPMG: Обзор законодательного регулирования криптовалюты в отдельных государствах // Официальный медиапортал KPMG. – URL: https://assets.kpmg/content/dam/kpmg/ru/pdf/2017/11/ru-ru-cryptocurrency-legislative-regulation-worldwide-november-2017-upd.pdf (дата обращения: 18.04.2021).

8. Что такое криптовалюта и как она работает? Отличительные черты, принцип обращения, плюсы и минусы // Майнинг криптовалюты. – URL: https://mining-cryptocurrency.ru/chto-takoe-kriptovalyuta/ (дата обращения: 18.04.2021).

Тетенева А. Г.[1]*,*
старший научный сотрудник
научно-исследовательской лаборатории
научно-исследовательского центра
Краснодарского высшего военного училища,
кандидат технических наук

Мезенцев А. С.[2]*,*
Врио начальника отдела – начальник
научно-исследовательской лаборатории
научно-исследовательского центра
Краснодарского высшего военного училища

СОВРЕМЕННЫЕ СТРАТЕГИИ КИБЕРАТАК

Развитие сетевых технологий способствует росту числа кибератак. Буквально за несколько десятилетий персональные электронные вычислительные машины (ПЭВМ) полностью изменили жизнь каждого человека на планете, а интернет, первоначально разрабатываемый как военная информационная сеть, создал новую реальность. Сегодня без ПЭВМ не сможет работать ни государственное учреждение, ни огромная корпорация, ни аэропорт, ни генеральный штаб вооруженных сил. И все они имеют выход в глобальную информационную сеть. Поэтому грамотно спланированная и проведенная кибератака может принести вред не меньший, чем оружие массового поражения.

Ежедневно против государственных и корпоративных сетей совершаются тысячи кибератак. К сожалению, многие из этих атак успешны, и об этом сообщается в средствах массовой информации. Для организаций, ставших жертвами таких атак, финансовый и репутационный ущерб может быть катастрофическим.

Так в конце 2017 г. стало известно о проведении некоторой хакерской группировкой в отношении международной корпораций с штаб-квартирой в Азии кибероперации, получившей название *Cobalt Kitty*. Руководство корпорации пригласило специалистов по информационной безопасности для того, чтобы разобраться в ситуации с подозрением о компрометации своей сети. По оценкам исследователей, на момент начала их работы и в течение в 2016–2017 гг. хакеры

находились внутри сети корпорации. Первичное проникновение было осуществлено путем тщательно подготовленного целевого фишинга, направленного на высшее и среднее руководство компании. Для доставки полезной нагрузки использовались поддельные инсталятор *Flash* и документы *Word*. В результате дальнейшего проникновения хакеры взломали контроллер домена, файловые серверы, серверы web-приложений и базы данных. При этом успешно обошли все штатные средства защиты [1, с. 44].

В феврале–марте 2019 г. хакерская группировка *Ocean Lotus*, основными направления деятельности которой кража корпоративной информации и кибершпионаж, провела серию атак на подразделения *Toyota* и *Lexus* в Австралии, Японии и Вьетнаме, похитив корпоративную информацию, с том числе персональные данные, более чем трех миллионов клиентов автопроизводителя [2, с. 4].

Резонансная атака произошла в 2020 г. Компания *FireEye* сообщила о вскрытии кибероперации *Sunburst*, в ходе которой неустановленная хакерская группировка скомпрометировала американского разработчика программного обеспечения *SolarWinds* и распространила троян в его *NMS Orion*, который затем попал к тысячам клиентов, включая государственные учреждения, крупные корпорации и силовые ведомства [3, с. 39].

Анализ показывает, что основными акторами современных кибератак являются:

– киберпреступники. Действуя самостоятельно или в составе организованной преступной группы, они совершают акты кражи данных, растраты, мошенничества и/или вымогательства с целью получения финансовой выгоды;

– государственные (прогосударственные) группы. Спонсируемые или связанные с государством, эти организации обладают практически неограниченными ресурсами для проведения очень сложных и устойчивых атак, имеют хорошую техническую подготовку и широкую направленность, а также хорошо финансируются. Они часто преследуют стратегические цели: подрыв экономики, выведение из строя критически важной инфраструктуры, включая электросети, водоснабжение, транспортные системы, системы реагирования на чрезвычайные ситуации, а также медицинские и промышленные системы;

– хактивисты. Мотивированные политическими или социальными причинам группы хакеров или отдельные хакеры, обычно выполняющие атаки типа «отказ в обслуживании» (DoS) против целевых организаций либо занимающиеся кибершпионажем;

– кибертеррористы. Террористические организации, использующие интернет для вербовки и обучения сторонников, а также для распространения страха и паники в целях продвижения своих идеологий. В отличие от других участников, кибертеррористы в основном не избирательны в своих атаках. Их цели – нанесение физического вреда и дестабилизация общественной жизни.

Современная стратегия кибератак эволюционировала от прямой атаки на сетевые ресурсы и активы до кропотливого многоступенчатого процесса, сочетающего применение эксплойтов, вредоносного программного обеспечения, скрытность и уклонение в скоординированной сетевой атаке.

Жизненный цикл кибератаки (рис. 1) иллюстрирует последовательность событий, через которые проходит преступник, чтобы проникнуть в сеть и извлечь ценные данные (данные, составляющие коммерческую тайну, персональные данные сотрудников и т. д.) [4, с. 169].

Рис. 1. Жизненный цикл кибератаки

1. Разведка. Злоумышленники детально планируют кибератаки, исследуют, идентифицируют и устанавливают цели, часто извлекая общедоступную информацию из профилей целевых сотрудников в социальных сетях или корпоративных веб-сайтов, которые могут быть полезны для социальной инженерии и фишинговых схем.

Злоумышленники используют различные инструменты для поиска сетевых уязвимостей, сервисов и приложений, а именно:

– сетевые анализаторы (также известные как анализаторы пакетов, анализаторы протоколов), применяемые для мониторинга и захвата необработанного сетевого трафика (пакетов);

– сканеры сетевых уязвимостей, обычно включающие набор инструментов, взломщики паролей, сканеры портов и сканеры уязвимостей и используются для проверки сети на наличие уязвимостей (включая ошибки конфигурации);

– взломщики паролей;

– сканеры портов, применяемые для поиска открытых портов на конечной точке;

– сканеры уязвимостей веб-приложений, используемые для проверки веб-приложений на наличие таких уязвимостей, как межсайтовый скриптинг, SQL-инъекции и обход каталогов;

– сканеры уязвимостей Wi-Fi, применяемые для сканирования беспроводных сетей на наличие уязвимостей (включая открытые и неправильно настроенные точки доступа), для захвата трафика беспроводной сети и взлома беспроводных паролей.

Так, в феврале 2021 г. на различных теневых форумах появились объявления о продаже базы данных 16 000 клиентов инвестиционной компании *Freedom Finance*, работающей на рынках России и Казахстана. Владельцы компании сделали заявление, в котором говорилось, что они стали жертвой хакеров. Однако в ходе проверки выяснилось, что у компании, управляющей полу миллиардом долларов, нет ни программных решений, ни технических устройств для предотвращения утечек данных и конфиденциальной информации из информационной системы, не проводятся тренинги сотрудников по вопросам информационной безопасности и по всей видимости, нет и самого подразделения информационной безопасности. Это дает основание полагать, что данная ситуация скажется соответствующим образом на репутации *Freedom Finance* [5].

Нарушение жизненного цикла кибератаки на этой стадии начинается с обучения пользователей безопасным способам обработки информации, которые фокусируются на таких темах, как методы противодействия социальной инженерии (например, фишингу), безопасность социальных сетей (например, вопросы безопасности и конфиденциальности), а также выполнения требований политики безопасности (например, требований к паролям, организации удаленного доступа и физической безопасности). Еще одна контрмера – непрерывный мониторинг и инспекция потоков сетевого трафика для обнаружения и предотвращения несанкционированного сканирования портов и уязвимостей, сканирования узлов (зачистки хостов) и других подозрительных действий. Эффективные процессы управления изменениями и конфигурацией помогают обеспечить правильную настройку и обслуживание вновь развернутых приложений и конечных точек (например, отключение ненужных портов и служб).

2. Выбор средств. На данной стадии злоумышленник определяет, какие методы использовать для компрометации целевой конечной точки. Он может встраивать код в такие, казалось бы, безобидные файлы, как PDF-файл или документ Microsoft Office Word, сообщения электронной почты.

По информации американских СМИ, в марте 2021 г. была совершена атака на объект критической инфраструктуры, в процессе которой хакер попытался напрямую нанести ущерб здоровью и жизни людей. Злоумышленник получил доступ к системе управления водоочистительного объекта города Олдсмар, подобрав пароль к *TeamViewer*, который стоял на машине, управляющей системой водоочистки, и повысил концентрацию едкого натра, поступающего в воду более чем в 100 раз. Оператор, следивший за системой водоочистки, зрительно обнаружил удаленную активность на рабочем столе взломанного компьютера и предотвратил вмешательство [6].

Нарушение жизненного цикла кибератаки на этой стадии сложная задача, поскольку выбор средств обычно происходит в сети атакующего. Однако анализ артефактов (как вредоносных программ, так и средств кибероружия) может предоставить важную информацию об угрозах, чтобы обеспечить эффективную защиту при попытке доставки.

3. Доставка. Злоумышленник пытается доставить свою боевую полезную нагрузку на целевую конечную точку, например, по электронной почте, в системе обмена мгновенными сообщениями (IM), путем прямой загрузки (веб-браузер конечного пользователя перенаправляется на веб-страницу, которая автоматически загружает вредоносное программное обеспечение на конечную точку в фоновом режиме) или зараженному файловому ресурсу.

В качестве примера можно упомянуть экзотический вид атак, отличающийся оригинальным способом доставки. Группа исследователей из израильского Университета Бен-Гуриона сообщила о новой атаке на физически изолированные (air-gapped) сети через сигналы Wi-Fi, не требующей наличия Wi-Fi-модуля в атакованной системе. Атака получила название *AIR-FI*. Основной способ атак на физически изолированные сети – использование вредоносов, распространяющихся и проводящих последующую эксфильтрацию данных через USB-носитель. В новой атаке USB-носитель используется исключительно на первичном этапе для доставки вредоноса на целевую машину. Следующий шаг хакеров – заражение находящегося поблизости от атакованного компьютера подключенного к интернету устройства с Wi-Fi-модулем на борту, например маршрутизатора. После вредонос собирает интересующую информацию, кодирует ее и использует шину DDR SDRAM для генерации электромагнитных излучений в диапазоне Wi-Fi 2,4 ГГц. Исследователи обнаружили, что таким образом на расстоянии до нескольких метров возможно организовать канал связи на скорости от 1 до 100 бит/с. Скорость невысокая, но достаточная для передачи сжатого текста [7].

Нарушение жизненного цикла кибератаки на этой стадии требует прозрачности всего сетевого трафика (включая удаленные и мобильные устройства), чтобы эффективно блокировать вредоносные или опасные веб-сайты, приложения и IP-адреса, а также предотвращать известные и неизвестные вредоносные программы и эксплойты.

4. Эксплуатация. После того как боевая полезная нагрузка доставлена в конечную точку назначения, она должна быть активирована. Конечный пользователь может непреднамеренно запустить эксплойт, например, щелкнув вредоносную ссылку или открыв зараженное вложение в электронном письме, или злоумышленник может удаленно запустить эксплойт против известной уязвимости в целевой сети.

На рис. 2 показана представленная словацкой компанией ESET статистика атак на открытые сервера Microsoft Exchange с целью эксплуатации уязвимостей из набора ProxyLogon. Из диаграммы видно, что на 5 марта 2021 г. пришелся пик – 6,5 тыс. попыток.

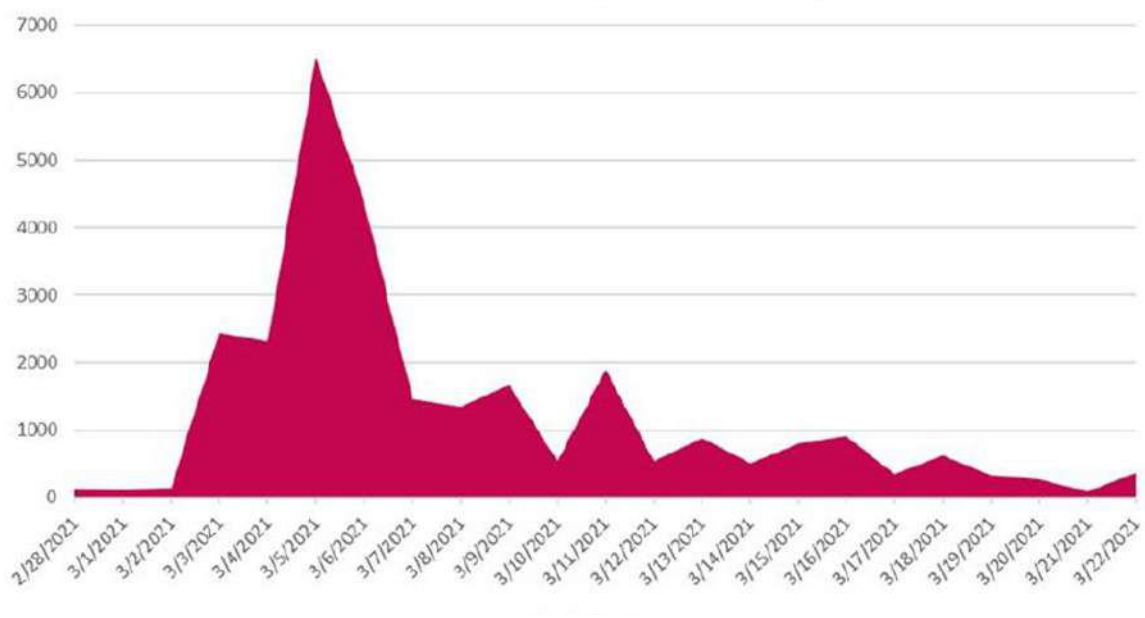


Рис. 2. Попытки атак серверов Microsoft Exchange с целью эксплуатации уязвимостей из набора ProxyLogon

Нарушение жизненного цикла кибератаки на этой стадии, как и на стадии разведки, начинается с обучения безопасности конечных пользователей, которое фокусируется на таких темах, как противодействие вредоносным программам и безопасность электронной почты. Другие важные меры безопасности включают управление уязвимостями и исправлениями; обнаружение и предотвращение вредоносных программ; анализ угроз (включая известные и неизвестные); блокирование рискованных, несанкционированных или ненужных

приложений и служб; управление правами доступа к файлам или каталогам, а также привилегиями администратора; а также ведение журнала и мониторинг сетевой активности.

5. Установка. Целью злоумышленника на данном этапе является повышение привилегий на скомпрометированной конечной точке. Например, наладив удаленный доступ к оболочке и установив руткиты или другие вредоносные программы, злоумышленник имеет контроль над конечной точкой и может выполнять команды в привилегированном режиме из интерфейса командной строки (CLI). Затем злоумышленник перемещается по сети цели, выполняя код атаки, выявляя другие возможные цели и компрометируя дополнительные конечные точки для обеспечения устойчивости управления.

Исследователи из команды *Netlab* китайской компании *Qihoo 360* обнаружили новый ботнет *ZHtrap*, содержащий функцию развертывания ханипотов. Их цель – сбор IP-адресов, принадлежащих конкурирующим ботнетам. Таким образом, *ZHtrap* может перехватывать конкурирующие боты для расширения своего охвата. Кроме модуля для проведения *DDoS* бот устанавливает на зараженное устройство веб-шелл с функциями сканирования, а также возможностью установки полезной нагрузки, что может быть использовано хакерами для компрометации сети, в которой стоит зараженный девайс [8].

Ключевыми аспектами к нарушению жизненного цикла кибератак на этой стадии являются ограничение перемещения злоумышленников в сети, использование сегментации сети и модели нулевого доверия, которая отслеживает и проверяет весь трафик между зонами или сегментами, а также детальный контроль приложений, разрешенных в сети.

6. Управление и контроль. Злоумышленник устанавливает зашифрованные каналы связи со своими серверами управления и контроля (C2) через интернет, чтобы динамично менять цели и методы атаки по мере выявления дополнительных потенциальных целей в сети жертвы или уклоняться от любых контрмер безопасности, которые организация может попытаться развернуть в случае обнаружения артефактов атаки. Обратная связь необходима для атаки, поскольку она позволяет атакующему удаленно управлять ею. Поэтому для успешной атаки трафик C2 должен быть устойчивым и скрытым. При этом основными инструментами и методами сокрытия являются:

– шифрование с помощью SSL, SSH (Secure Shell) или другого специального или проприетарного шифрования;

– обход через прокси, инструменты удаленного доступа или туннелирование. В некоторых случаях использование сотовых сетей позволяет полностью обойти целевую сеть для атаки трафика C2;

– проброс портов с помощью сетевых анонимайзеров или скачкообразное перемещение портов для обхода;

– динамический DNS для прокси-сервера через несколько зараженных конечных точек или несколько постоянно меняющихся серверов C2 для перенаправления трафика и затруднения определения истинного пункта назначения или источника атаки;

– DNS-туннелирование используется для связи C2, а также для проникновения данных (например, отправка вредоносного кода, команд или двоичных файлов жертве) и эксфильтрации данных.

По утверждению американских СМИ, выявлен вредонос для *Linux* под названием *Drovorub* – многокомпонентная система, включающая руткит модуля ядра, предназначенный для скрытия вредоносной деятельности. Основное предназначения *Drovorub* – поиск и эксфильтрация информации [9].

Нарушение жизненного цикла кибератаки на этой стадии требует проверки всего сетевого трафика (включая зашифрованные сообщения), блокировки исходящих сообщений C2 с анти-C2 сигнатурами (наряду с загрузкой файлов и шаблонов данных), блокировки всех исходящих сообщений на известные вредоносные URL-адреса и IP-адреса, блокировки новых методов атаки, использующих методы уклонения от портов, предотвращения использования анонимайзеров и прокси-серверов в сети, мониторинга DNS на наличие вредоносных доменов и противодействия или отравлению DNS, а также перенаправления вредоносных исходящих сообщений на ханипоты для идентификации или блокировки скомпрометированных конечных точек и анализа атакующего трафика.

7. Действия по достижению цели. Злоумышленники часто преследуют несколько различных целей атаки: кража данных, разрушение или модификация критических систем, сетей и данных, а также отказ в обслуживании. Этот этап жизненного цикла кибератаки используется злоумышленником для продвижения ранних этапов жизненного цикла кибератаки в отношении другой цели. Злоумышленник направляет атаку против первоначальной сети жертвы на другую сеть жертвы, таким образом делая первоначальную жертву невольным сообщником.

Компания *Gartner*, одна из ведущих консалтинговых компаний в области информационных технологий, провела исследования и пришла к выводу о том, что к 2024 г. 75 % CEO будут нести личную ответственность за киберинциденты,

произошедшие с подведомственными им системам киберфизической безопасности (CPS). *Gartner* определяет CPS как компьютерные системы, которые оказывают непосредственное влияние на физический мир (включая людей). В настоящее время подобные системы встречаются преимущественно в критической информационной инфраструктуре и медицинских учреждениях, однако, по мнению консультантов, в ближайшие годы они получат широкое распространение благодаря внедрению «умных» городов и зданий, автомобильных автопилотов и других систем управления транспортом, удаленной медицине и пр. А при таких условиях инциденты могут привести к физическому ущербу для людей, разрушению имущества или экологическим катастрофам. Финансовые последствия атак на CPS, по оценкам экспертов компании, к 2023 г. составят более 50 млрд долл. С учетом такого развития событий национальные правительства и международные органы будут вынуждены резко ужесточить ответственность должностных лиц за происходящие с их CPS инциденты.

Таким образом, не в каждой атаке присутствуют все семь этапов. И, напротив, в некоторых случаях какие-либо этапы могут повторяться несколько раз. Однако блокировка всего лишь одного шага разрывает последовательность событий, через которые проходит злоумышленник, и может эффективно защитить сеть, а также личные и корпоративные данные организации.

Список литературы

1. Галушкин, А. А. К вопросу о кибертерроризме и киберпреступности / А. А. Галушкин // Вестник РУНД. Серия: Юридические науки. – 2014. – № 2.

2. Чесноков, Н. А. Правовые основы информационной безопасности в современных условиях / Н. А. Чесноков // Правовая инициатива. – 2013. – № 4. – С. 4.

3. Антипов, К. Киберконфликт в китайско-американских отношениях и поиски диалога / К. Антипов // Проблемы Дальнего Востока. – 2013. – № 6. – С. 39–54.

4. Ибрагимова, Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности / Г. Ибрагимова // Индекс безопасности. – 2013. – № 1 (104). – С. 169–184.

5. Электронный архив научных статей. – URL: http://www.covertchannels.comhttps://arxiv.org/abs/20 (дата обращения: 23.03.2021).

6. Reuters.com. – URL: https://www.reuters.com/article/us-usa-cyber-florida/hackers-broke-into-florida-towns-water-treatment-plant-attempted-to-poison-supply-sheriff-says-idUSKBN2A82FV(дата обращения: 09.02.2021).

7. Официальный сайт компании Gartner. – URL: https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75-of-ceos-will-be-personally-liabl (дата обращения: 03.03.2021).

8. Официальный сайт компании CrowdStrike. – URL: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/ (дата обращения: 22.03.2021).

9. Официальный сайт компании Bloomberg. – URL: https://www.bloomberg.com/news/articles/2019-12-05/u-s-sanctions-evil-corpblamed-for-100-million-cyber-theft. (дата обращения: 26.03.2021).

Цимбал В. Н.[1]*,*
доцент кафедры специальных информационных
технологий учебно-научного комплекса
информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРОБЛЕМЫ РЕАЛИЗАЦИИ В СОВРЕМЕННЫХ ГЕОПОЛИТИЧЕСКИХ УСЛОВИЯХ

Международная информационная безопасность в современных геополитических условиях представляется достаточно актуальной для обсуждения и принятия актуальных решений. Развитие информационных технологий, трансграничный обмен информацией, слабое ее регулирование приводят к реализации угроз в информационной сфере на уровне отдельного государства и на межгосударственном уровне.

Угрозами международной информационной безопасности, согласно резолюции Генеральной Ассамблеи ООН 1999 г. (предложены Россией) являются: военно-политические (т. е. использование информационных технологий государствами для достижения военных либо политических целей), террористические (то есть совершение террористических актов для устрашения широких слоев населения, в политических целях) и преступные (киберпреступления и т. д.).

Международная информационная безопасность выдвинулась на передовые рубежи глобальной безопасности. Информационное пространство превратилось в настоящее «поле боя», на котором развертываются масштабные и непрерывные информационно-кибернетические атаки с участием преступных групп (финансируемых как отдельными государствами, так и действующих самостоятельно), а также индивидуальных преступников. Тематика противодействию информационно-телекоммуникационным технологиям в преступных целях, которая по масштабу и всеохватности давно превратилась в глобальную угрозу, от которой страдают как развивающиеся, так и развитые страны, предстает все более проблемной для международного сообщества [1, с. 87].

12 апреля текущего года Президент Российской Федерации подписал Указ № 213 «Об утверждении Основ государственной политики Российской Федера-

ции в области международной информационной безопасности», согласно которому под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности [2].

Согласно данному указу основные угрозы международной информационной безопасности – это информационно-коммуникационные технологии, которые используются для достижения различных целей: подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности; экстремистских и террористических; преступных (в сфере компьютерной информации, мошенничестве, совершения компьютерных атак); использование различными странами технологического доминирования в глобальном информационном пространстве и т. д.

Иным документом, затрагивающим аспекты рассматриваемой деятельности в нашей стране, является Доктрина информационной безопасности Российской Федерации, согласно которой в п. «д» ч. 8 одним из национальных интересов России в информационной сфере являются: «…содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве». А в п. 19 данного подзаконного акта отмечается, что «отсутствуют международно-правовые нормы, регулирующие межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий» [3].

По словам руководителя Сбербанка, наша страна из-за кибернападений теряет в год более 600 млрд долл. По данным Совета Безопасности России 4,5 вредоносных в информационном пространстве акций, происходящих в мире, приходится на нашу страну. Президент России на коллегии ФСБ озвучил цифру в 70 млн нападений в год на государственные информационные ресурсы.

На международной арене Российская Федерация обращает внимание других государств на проблемы, возникающие в информационной сфере, в частности начиная с конца XX в., а именно с 1998 г., когда инициативно подняла данный

вопрос на целенаправленное обсуждение в рамках ООН; в том же году предложила США подписать заявление на уровне президентов в «Совместном заявлении об общих вызовах безопасности на рубеже XXI века»; в 1999 г. предложен документ «Принципы, касающиеся международной информационной безопасности», который впервые предложил некоторое количество терминов: информационное пространство, информационная война, международная информационная безопасность, международная информационная преступность, терроризм и иное; в 2002 г. Россия и США приняли резолюцию «Создание глобальной киберкультуры»; в 2011 г. Россия представила проект «Конвенции об обеспечении международной информационной безопасности». В проекте конвенции речь шла о предотвращении военных конфликтов в киберпространстве, борьбе с кибертерроризмом и кибермошенничеством. К ней присоединились Китай и Индия. Негативную реакцию конвенция вызвала у США, Великобритании и некоторых стран Европейского Союза. Впоследствии многие из положений рассматриваемого проекта вошли в документы, принятые на уровне ОДКБ, СНГ и ШОС. Также серьезные предложения были и в 2015, 2017, 2018, 2019 гг.

На уровне ООН данным направлением также занимаются ее специализированные подразделения: Региональное содружество в области связи; Всемирная организация по интеллектуальной собственности; ООН по вопросам образования, науки и культуры (ЮНЭСКО); Международный союз электросвязи. Иные международные организации уделяют серьезное внимание вопросам международной информационной безопасности, а именно ШОС, БРИКС, ЕС, G7, G20, ОДКБ, СНГ. На постоянной основе, например, наша страна проводит двусторонние встречи с Белоруссией, Бразилией, Кубой, КНР, Индией и рядом арабских стран.

Граждане подавляющего большинства стран ощущают воздействие глобальной информационной революции в виде манипуляции общественным мнением. Транснациональное воздействие на граждан, на социальные группы становится одним из драйверов глобальной турбулентности, в рамках которой развиваются такие мощные процессы, как социальная поляризация стран и регионов, возрастание социально-психологической конфликтности, демографического взрыва и миграционных волн [1, с. 88].

Отметим некоторые цифры, касающиеся существующих угроз безопасности информации: в 2017 г. из-за сетевого червя WannaCry было заблокировано более 5 млн компьютеров (пострадали при этом и компьютеры МВД России, примерно 200 тыс.); траты США на восстановление от утечек данных более

1,5 млрд долл.; в 2019 г. зафиксировано 395 случаев утечки данных из российских компаний и государственных органов, а это 15,7 % числа утечек по всему миру; более 170 млн раз срабатывало приложение «Лаборатории Касперского» по данным на октябрь 2020 г., на уникальные вредоносные URL было отражено более 660 млн атак.

Эффективное противодействие актуальным угрозам в информационном пространстве и на уровне отдельного государства невозможно выполнять в одиночку. Только совместная, скоординированная деятельность государств позволит качественно противостоять имеющимся и появляющимся угрозам в современных реалиях.

Выделим акценты современной международной информационной безопасности:

– совместная деятельность государств (взаимовыгодное партнерство, обмен информацией, разработка технологий, межгосударственные договоренности);

– развитие информационных технологий;

– урегулирование инцидентов информационной безопасности;

– колоссальные затраты (на поддержание в актуальном состоянии системы информационной безопасности и восстановление после возможных воздействий).

Министерство внутренних дел Российской Федерации в данной области осуществляет следующую деятельность:

– борьба с преступностью (криминальные угрозы и терроризм);

– подготовка кадров в области информационной безопасности (Московский университет МВД России имени В. Я. Кикотя, Санкт-Петербургский университет МВД России, Краснодарский университет МВД России, Воронежский институт МВД России);

– сотрудничество с зарубежными правоохранительными организациями;

– различная деятельность подразделений МВД России (в пределах своей компетенции), к примеру, Департамент информационных технологий, связи и защиты информации; Договорно-правовой департамент МВД России; Департамент государственной службы и кадров; НЦБ Интерпола и др.

Как показывает анализ, интерес международного сообщества к проблемам международной информационной безопасности стал более активным и внимательным, примерно с конца XX в. – начала XXI в., это связано с беспрецедентным ростом и засильем разнообразных информационных технологий (подвижной радиотелефонной связи, компьютерных устройств, информационных сетей,

технологий ускоряющих обмен информацией и др.), их доступности для населения даже вне самых обеспеченных стран, активизации случаев использования информационно-телекоммуникационных технологий в преступной деятельности трансграничного и трансконтинентального характера, разведывательными и иными службами государств в собственных интересах и не всегда мирных, и иные причины.

Список литературы

1. Шерстюк, В. П. Рецензия на книгу «Международная информационная безопасность: теория и практика» / В. П. Шерстюк // Вопросы кибербезопасности. – 2020. – № 1 (35). – С. 87–88.

2. Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (дата обращения: 20.04.2021).

3. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Гарант». – URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 20.04.2021).

Полянская Е. П.[1]*,*
преподаватель кафедры уголовного процесса
Московского областного филиала
Московского университета МВД России имени В.Я. Кикотя

Куриленко Ю. А.[2]*,*
старший преподаватель кафедры
информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

ПРОБЛЕМНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И СЛУЖБ НЕГОСУДАРСТВЕННЫХ ОРГАНИЗАЦИЙ, ВОЗНИКАЮЩИЕ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Взаимодействие является достаточно сложным и многофункциональным процессом в правоохранительной системе, особенно когда речь о специфических направлениях, таких как выявление, раскрытие и расследование преступлений, совершенных с использованием информационных технологий и телекоммуникационных систем.

Существует много определений взаимодействия в криминалистике и в уголовном процессе, но все они сводятся к тому, что это взаимная помощь и содействие органов дознания и органов предварительного следствия, оказываемые в процессе расследования преступлений. Часто во время производства по уголовному делу организованное взаимодействие между следователем и сотрудниками органов дознания является гарантом успешного решения задач уголовного судопроизводства [1, с. 116]. Однако форма может быть процессуальной, носящей правовой характер, регламентирующей совместную согласованную деятельность, а может быть не процессуальной, сводящейся к взаимному обмену информацией, совместному анализу и оценке, т. е. информационному взаимодействию.

Взаимодействие касается и служб негосударственных организаций и финансово-кредитных учреждений (интернет-провайдеров, служб безопасности, секторов по противодействию мошенничеству, операторов сотовой связи и др.) и

главное, его целью является быстрое раскрытие преступлений. Без слаженной работы всех заинтересованных служб и подразделений невозможны эффективное раскрытие и расследование рассматриваемой категории преступлений. Деятельность участников раскрытия и расследования преступления организована следователем, выполняющим роль руководителя и несущего безусловно полную ответственность, и состоит в решении тех задач, которые поставил следователь.

В настоящее время любой вид взаимодействия невозможно представить без информационной составляющей. Эффективность данного взаимодействия напрямую зависит от информации. Так, в сфере законности и правопорядка эффективность информационно-справочного обеспечения правоохранительных органов может быть достигнута при полном и достоверном его содержании, а также при своевременном использовании [2, с. 2].

Сам термин «информация» происходит от латинского «informatio», что означает «осведомление», «разъяснение» и предполагает осуществление диалога в различной форме между «отправителем» и «получателем» информации [3, с. 97].

Без информационного обеспечения сотрудников, осуществляющих расследование, и эффективного взаимодействия формирование доказательственной базы и направление уголовного дела в суд становятся невозможными.

Приведем несколько примеров. В ходе проведенного анкетирования сотрудников предварительного следствия и дознания было установлено, что большая часть сотрудников не знает, что можно получить не только детализацию соединений абонентского номера, но и детализацию соединений IMEI, что намного эффективнее для доказывания, а также сэкономит время. В зависимости от следственной ситуации, если не используется виртуальный номер, а обычная симкарта, преступник моментально избавляется от нее. Но с такой частотой не меняются сами устройства, поэтому, запрашивая детализацию соединений по абонентскому номеру, попросту теряется время.

Кроме того, часты случаи, когда сотрудники направляют запросы в финансово-кредитные учреждения о предоставлении сведений об IP-адресах и иной подобной информации, если держатель карты заходил в приложение, а в ответ получают письмо с нулевым результатом, поскольку многие учреждения не располагают подобной информацией, либо не хранят ее. Также случалось, что в ходе осмотра места происшествия при хищении денежных средств банкомата путём его повреждения, не дождавшись специалиста сервисного центра, обслуживающего устройство, либо сотрудника службы банковской организации следователь неаккуратно изымал видеокассету с записью из устройства, допустив значительные ее повреждения, хотя без помощи вышеперечисленных лиц и специального

обеспечения использовать ее он всё равно бы не смог. Подобное происходит из-за отсутствия необходимой информации у сотрудников, осуществляющих раскрытие и расследование уголовных дел.

До настоящего времени фактически не завершен процесс формирования договорной правовой базы информационного взаимодействия в электронном виде органов внутренних дел с органами государственной власти, кредитными организациями, интернет-провайдерами, операторами связи и интернет-сервисов, в том числе социальных сетей. Особенно актуальным остается вопрос об обеспечении доступа правоохранительных органов к идентификационным сведениям о лицах, совершивших платежные операции посредством банковских и иных платежных систем [4].

До сих пор не разрешена проблема не только неисполнения запросов правоохранительных органов негосударственными организациями, но и согласования перечня сведений, представляющих интерес для получения в рамках межведомственного взаимодействия. Кроме того, отсутствует информационное взаимодействие с правоохранительными органами иностранных государств [4].

Для недопущения подобных проблем и достижения эффективных результатов должна быть качественно сформирована договорная база между ведомствами и негосударственными организациями.

Благодаря правильно организованному взаимодействию повышается качество расследования, сокращаются сроки раскрытия преступлений и в полном объеме формируется доказательственная база, что способствует скорейшему направлению уголовных дел в суд.

Список литературы

1. Арестова, Е. Н. Предварительное следствие : учебник / [Е. Н. Арестова и др.]; ред. М. В. Мешков. – 2-е изд., перераб. и доп. – М. : Юнити, 2015.

2. Полещук, О. В. Некоторые аспекты информационно-справочного обеспечения процесса раскрытия и расследования преступлений / О. В. Полещук, М. И. Прохорова // Российский следователь. – М. : Юрист, 2010. – № 9. – С. 2–4.

3. Ивушкина, Е. Б. Генезис информации, информатика и информационное взаимодействие в эпоху научно-технической революции : монография / [Е. Б. Ивушкина и др.]. – Шахты : ЮРГУЭС, 2008.

4. Приказ МВД России от 25.11.2019 № 878 «Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км» // СПС «КонсультантПлюс». – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=519451&dst=100001#7Rv7HlSIDkSm5jlF1 (дата обращения: 15.04.2021).