



ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ УНИВЕРСИТЕТ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ В.Я. КИКОТЯ»

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

**Сборник научных трудов Всероссийской конференции
(23 апреля 2020 г.)**

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

Научное электронное издание

Москва
2020

© Московский университет МВД России
имени В.Я. Кикотя, 2020
ISBN 978-5-9694-0908-8

ББК 66.4
А43

Рецензенты:

профессор кафедры информационной безопасности
Краснодарского университета МВД России
доктор технических наук, профессор **А. В. Еськов**;
начальник Центра информационных технологий,
связи и защиты информации ГУ МВД России по г. Москве **А. Ф. Прокопчук**

Составитель *И. С. Мельцева*

А43 **Актуальные проблемы кибербезопасности в сети Интернет :**
сборник научных трудов Всероссийской конференции. – М. : Москов-
ский университет МВД России имени В.Я. Кикотя, 2020. – 180 с. –
1 электронный оптический диск (CD-R). – Системные требования:
CUP 1,5 ГГц ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места
на жестком диске.
ISBN 978-5-9694-0908-8

В сборнике публикуются статьи авторов – участников Всероссийской кон-
ференции «Актуальные проблемы кибербезопасности в сети Интернет», про-
шедшей в Московском университете МВД России имени В.Я. Кикотя 23 апреля
2020 г.

В сборник вошли статьи курсантов, молодых ученых и преподавателей, спе-
циализирующихся в сфере обеспечения кибербезопасности Российской Феде-
рации. В них отражены проблемные вопросы контроля и правового регулиро-
вания безопасности государства, анализа угроз обеспечения кибербезопасности
страны, а также противодействия преступности в сфере информационных тех-
нологий.

Представляет интерес для научных и практических работников, участвую-
щих в борьбе с преступностью.

Научное электронное издание

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

Номер государственной регистрации
обязательного федерального экземпляра электронного издания – 0000000000

© Московский университет
МВД России имени В.Я. Кикотя, 2020

Издание подготовлено
с помощью программного обеспечения Microsoft Word

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

Подписано к изданию: 21.09.2020
Объем издания: 2407 Кб
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-0908-8



Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12
<http://www.mosu.mvd.ru>; e-mail: support_mosu@mvd.ru

СОДЕРЖАНИЕ

Абдрахманова Л. Р., Иванов В. Ю.

Получение информации из облачных хранилищ в криминалистических целях.. 8

Алиманов П. Е., Сизоненко А. Б.

Алгоритм распределения функций между сотрудниками
для эффективного решения критичных задач кибербезопасности 14

Аласкяров Н. Б., Гаврилина А. А.

О вопросах физического самовоспитания и самосовершенствования,
как одного из условий здорового образа жизни..... 18

Гончар В. В.

Актуальные проблемы раскрытия и расследования киберпреступлений 20

Григорьев Д. А., Егоренко Е. Ю.

О некоторых вопросах применения искусственного интеллекта
в противодействии преступности 23

Григорьев О. Д., Усков А. С.

Новые способы совершения компьютерных преступлений 29

Гусев Д. В.

Отдельные проблемные вопросы расследования киберпреступлений..... 34

Гуськова А. Б., Калимуллин Н. Р.

Актуальные вопросы правового регулирования робототехники
и искусственного интеллекта 38

Данилова Ю. В., Гончар В. В.

Некоторые проблемы борьбы с киберпреступностью 44

Дутикова А. А., Галиев Д. В.

Информация, извлеченная с NAS хранилищ, как цифровое доказательство
при расследовании и раскрытии киберпреступлений 49

Евлашкина А. В., Кардашевская М. В.

Криминалистическая характеристика отдельных видов
мошенничества в сфере компьютерной информации 52

Ефременко М. А.

Развитие силы и выносливости курсантами и слушателями
образовательных организаций МВД России в условиях самоизоляции 56

Иванов И. В., Иванов В. А., Егоров М. В.

Снижение вычислительной сложности декодирования сигналов
с турбокодированием в каналах связи с памятью..... 59

Иванов И. В., Иванов В. А., Шаповалов С. Л.

Исследование механизмов подавления вирусных эпидемий
в компьютерных сетях 62

<i>Кардашевская М. В.</i>	
Обстановка совершения преступлений с использованием электронной платежной системы	66
<i>Клочкова Е. Н.</i>	
Проблемы защиты информации при организации дистанционной работы.....	69
<i>Коньшев В. Ю., Максимов Н. А.</i>	
Построение защищенной опорной сети связи на базе беспилотных летательных аппаратов.....	71
<i>Коньшева В. Ю.</i>	
Анализ структурных свойств нелинейных динамических систем.....	74
<i>Кальницкая В. М., Еськов А. В.</i>	
Обзор реализации разграничения доступа операционной системы LINUX.....	77
<i>Кравцов О. Г.</i>	
Паттерны отклоняющегося поведения не криминального характера в интернете.....	80
<i>Кругликова С. А., Ульянова И. В.</i>	
Профилактика киберзависимости несовершеннолетних средствами подвижных и интеллектуальных игр.....	86
<i>Лустин В. И.</i>	
Взаимосвязь цифровой экономики и киберпреступности	89
<i>Майорова О. В.</i>	
О некоторых аспектах преступлений против несовершеннолетних, совершаемых в сети Интернет	92
<i>Мандрикова В. В., Иванов В. Ю.</i>	
Проведение исследования при выявлении следов работы эксплойтов	96
<i>Марков Е. И., Гончар В. В.</i>	
Некоторые способы совершения преступлений в информационной сфере и пути их предупреждения	99
<i>Михайленко Н. В.</i>	
Отдельные проблемы цифровизации органов внутренних дел Российской Федерации	102
<i>Щелкина Е. А., Никулова Е. А.</i>	
К анализу поведенческих проявлений курсантов образовательных организаций МВД России в киберпространстве	106
<i>Платонов Д. А.</i>	
Основные методы обучения двигательным умениям и навыкам курсантов и слушателей образовательных организаций системы МВД России.....	109
<i>Попов А. В., Анисимов С. Л.</i>	
Перспективы применения нейросетевых технологий в деятельности органов внутренних дел.....	111

Рудакова Н. К., Клочкова Е. Н.

Распространение в сети Интернет контента суицидального характера
как угроза безопасности общества 114

Савенкова Д. Д.

Новые тренды киберугроз: как не стать жертвой 118

Саморока В. А.

Принципы осуществления уголовно-процессуальной деятельности
с применением технологий искусственного интеллекта 123

Синицын Ю. Ю.

Применение адаптивного алгоритма канального кодирования данных
с беспилотных летательных аппаратов с использованием
свойств сверточных кодов..... 129

Склеимин Ю. Б., Чеботарева В. А.

Применение дискретного косинусного преобразования
для фильтрации изображений. Реализация метода
во встраиваемых системах..... 133

Таланова Н. В., Ульянова И. В.

Индивидуальная беседа с курсантами как метод
профилактики киберзависимости 136

Тутынин И. Б.

Влияние сети интернет на уголовно-процессуальное
принуждение имущественного характера 138

Ульянова И. В.

Актуализация в образовательном процессе проблемы формирования
киберкультуры у курсантов..... 142

Ушаков М. А.

Способы оптимизации учебного процесса по физической подготовке
слушателей и курсантов образовательных организаций МВД России 146

Орехов П. В.

Математическая модель взвешенной оценки возможности
утечки информации по виброакустическому каналу 149

Пакляченко М. Ю., Милютин Р. В.

К вопросу обеспечения безопасности платежных терминалов..... 153

Курбатова М. С., Поликарпов Е. С.

Обзор зарубежных методик аудита безопасности информационных систем... 157

Франковская К. Д., Куренков И. А.

Противодействие вовлечению несовершеннолетних в совершение
преступлений и административных правонарушений
путем использования сети Интернет..... 161

Харисова З. И., Файзулова Р. Р., Дюсьмекеева Д. С.

Современные угрозы информационной безопасности
в условиях глобализации информационного пространства..... 163

Химичева О. В., Андреев А. В.

Необходимость противодействия киберпреступлениям как фактор,
определяющий эволюцию уголовного судопроизводства 166

Черногоров Г. В., Галиев Д. В.

Уязвимости USB интерфейса 171

Шарова К. М., Поликарпов Е. С.

Статистика киберпреступности зарубежных стран 174

Яковлева К. Ю., Андреев А. В.

Предотвращение использования социальной инженерии
киберпреступниками в социальных сетях 178

*Абдрахманова Лидия Ринатовна¹,
слушатель Московского университета
МВД России имени В.Я. Кикотя;*

*Иванов Вячеслав Юрьевич²,
начальник кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя*

ПОЛУЧЕНИЕ ИНФОРМАЦИИ ИЗ ОБЛАЧНЫХ ХРАНИЛИЩ В КРИМИНАЛИСТИЧЕСКИХ ЦЕЛЯХ

Современное состояние уголовно-процессуального законодательства, общества позволяет с уверенностью утверждать, что выявление и расследование преступлений, в сфере компьютерной информации и телекоммуникационных технологий предполагает процессуальные, т. е. предусмотренные уголовно-процессуальным законодательством и, что не мало важно, не процессуальные, т. е. не предусмотренные УПК РФ формы.

Анализ применения экспертных систем, программно-аппаратных комплексов, биометрии, формирует некий феномен, связанный с тем, что большие объемы информации, имеющей доказательственное значение, обрабатываются и хранятся за пределами компьютера пользователя, а возможно и за пределами государства, например, на облачном сервере.

При этом технически существует возможность получения такой информации для формирования определенных выводов, помогающих принять процессуальное решение, однако техническая сторона деятельности, применяемые алгоритмы, остаются вне поля зрения следователя.

В связи с тем, что производство некоторых видов экспертиз (в частности, компьютерных) очень затратно по времени и средствам, следователи достаточно часто производят осмотр компьютеров (веб-страниц, носителей, видеозаписей) с привлечением специалиста.

Однако не совсем понятно, почему в правоприменительной практике и научной литературе сложилось обыкновение считать любое следственное действие с объектами информационно-коммуникативного характера именно осмотром, а не обыском.

Еще один аргумент в пользу позиции о том, что осмотр с участием специалиста в данном случае не совсем корректный выход, это то, что в силу присущей «электронному доказательству» неочевидности содержания, файлы, исследование которых необходимо произвести, находятся за пределами свободного доступа.

¹ © Абдрахманова Л. Р., 2020.

² © Иванов В. Ю., 2020.

Для их открытия и изучения необходимо осуществить определенные целенаправленные поисковые действия в виртуальной среде, что возможно только при проведении обыска.

Законодательное определение понятия «электронного доказательства» отсутствует в УПК РФ, и данный термин пока используется только в научной литературе.

Сбор таких доказательств, является наиболее сложным. Сотрудники правоохранительных органов часто сталкиваются с процедурными проблемами, например получение своевременного доступа к данным на зашифрованных устройствах или в облаке.

Из вышеуказанного следует, что при осмотре максимум, что может позволить себе следователь, это отразить в протоколе осмотра внешние признаки осматриваемого объекта, например, модель объекта осмотра, серийный номер, операционная система и др.

Все остальные действия, просмотр облачного хранилища, истории браузера посредством введения логина и пароля владельца устройства следует относить к поисковым действиям, следовательно, это будет уже не осмотр, а обыск в целях поиска информации внутри данного объекта.

При получении информации из закрытых источников интернета оформление ее протоколом осмотра не логично и неправильно с процессуальной точки зрения. В таких условиях целесообразнее проведение обыска.

Важнейшую роль при расследовании уголовного дела играет своевременное и правильное изъятие электронных носителей информации. Это изъятие осуществляется при производстве таких следственных действий как осмотр, обыск и выемка. Первостепенное значение в правовом регулировании изъятия информации из облачных хранилищ имеет Конституция Российской Федерации, в которой установлены основы деятельности исполнительных органов, к которым относятся правоохранительные органы, а также гарантируется защита прав и свобод человека [10].

Ключевое значение в правовом регулировании изъятия информации из облачных хранилищ имеют положения Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) и в первую очередь, это нормы, касающиеся проведения следственных действий [1].

Так, в главе 24 УПК РФ указаны нормы, касающиеся порядка осмотра, в частности это регулируется ст. 176 и ст. 177 УПК РФ [1].

В декабре 2018 г. в УПК РФ была введена статья, регламентирующая особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий – в частности ст. 164.1 УПК РФ [1].

Необходимость изъятия электронных носителей, а также непосредственно изъятия информации из облачных хранилищ, не только в рамках обыска и выемки, но и других следственных действий, привела к необходимости введения новой статьи – ст. 164.1 УПК РФ, которая регламентирует изъятие [1].

Доктрина информационной безопасности Российской Федерации представляет собой систему взглядов на обеспечение государственной защищенности России в информационной сфере.

В Доктрине под информационной сферой понимаются информация, объекты информатизации, информационные системы, веб-сайты в информационно-телекоммуникационной сети «Интернет» (далее – интернет), сетей связи, информационных технологий, субъектов, связанных с формированием и обработкой информации, развитием и внедрением вышеупомянутых технологий, обеспечением информационной защищенности, а также совокупность устройств регулирования соответствующих социальных отношений.

Особенности правового статуса информации регулируют:

Федеральный закон от 27.07.2006 №1 49-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон «О полиции» от 07.02.2011 № 3-ФЗ (ст. 11 «Использование достижений науки и техники, современных технологий и информационных систем»);

приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (совместно с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации»);

ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме»;

Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»;

приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».

Производимые судебные экспертизы, осмотр места происшествия, обыск и выемку выполняют (в большинстве случаев) сотрудники экспертно-криминалистических центров Министерства внутренних дел Российской Федерации. Таким образом, специалисты и эксперты должны:

- соблюдать и уважать права и свободы человека и гражданина (ст. 5 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции»);

- соблюдать законность (ст. 6 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции»);

- не нарушать права и обязанности полиции (гл. 3 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции»).

На первоначальных этапах развития информационных систем использовались технологии, работающие с локальными хранилищами данных. Это было обусловлено тем, что степень компьютеризации была достаточно низкой, в прикладных программах еще не было необходимого количества технологических задач. На этом этапе было принято использование вычислительной техники несколькими специалистами. Базы данных располагались на этой же рабочей станции.

Основные недостатки работы с информацией на одной рабочей станции:

- вероятность потери данных вследствие сбоя техники;
- сложность в администрировании;
- нерациональное использование рабочего времени специалистов.

Следующий этап развития информационных технологий был связан с распространением сетевых задач и работой с данными, расположенными на серверах в локальных сетях организаций. Применение решений, связанных с использованием локальных вычислительных сетей имеет преимущества:

- возможность совместной обработки данных;
- возможность резервирования информации;
- вся информация, находящаяся в системе, не выходит за пределы организации;
- возможность управления рабочими местами пользователей при помощи средств администрирования;
- возможность управления политикой безопасности.

Решения, основанные на использовании ресурсов локальных вычислительных сетей, не для всех организаций являются оптимальными, из-за следующих причин:

- для малых организаций приобретение серверов и прикладного программного обеспечения нецелесообразно из-за малого количества персонала организации;
- нецелесообразно использование дорогостоящих прикладных решений, работа с которыми предполагается лишь в единичных случаях;
- организации с малой численностью сотрудников, разбирающихся в области информационных технологий.

Таким образом, с увеличением доступности интернета, развитием корпоративных систем в организациях среднего и крупного бизнеса, государственных структурах все большую область применения получают технологии, связанные с использованием ресурсов удаленных серверов – облачные технологии.

Облачное хранилище – это модель облачных вычислений, которая хранит данные в интернете через поставщика облачных вычислений, который управляет хранением данных как услугой. Он поставляется по требованию со своевременной емкостью и затратами, и устраняет необходимость покупки и управления собственной инфраструктурой хранения данных. Это дает гибкость, глобальный масштаб и долговечность с доступом к данным «всегда и везде».

Преимущества облачных хранилищ:

1. Долговечность. Загруженные в облако данные, хранятся на отдельных серверах, предоставляемые определенной организацией, которые могут находиться за пределами страны пользователя.

2. Доступность. Все данные должны быть доступны через интернет. Таким образом, можно получить доступ к своим данным с любого устройства, у которого имеется выход к глобальной сети.

3. Низкая вероятность потери данных. На все данные, загружаемые в облачное хранилище, создается резервная копия, что резко уменьшает вероятность потери данных в результате сбоя техники.

4. Передача файлов больших размеров. Не все файлы можно отправить через электронную почту и определенный накопитель информации может не оказаться под рукой. Облачное хранилище позволяет загружать файлы больших размеров и, если необходимо, обеспечить общий доступ к ним.

Недостатки облачных хранилищ:

Безопасность. Ко всем загруженным файлам имеет доступ сам сервис и его сотрудники. Если произойдет хакерская атака на сервис и случится взлом серверов, то частная информация может попасть в открытый доступ.

Изъятие информации из облачных хранилищ, проводимое в рамках следственных действий, предполагает получение доступа к ресурсам, расположенным в облачных хранилищах.

Основные проблемы в данном случае:

- расположение файловых ресурсов у иностранного поставщика облачных сервисов;
- наличие проблем в определении статуса хранимой информации при разрешении доступа к ней.

В настоящее время в МВД России имеются специальные программно-аппаратные решения, позволяющие проводить исследование облачных технологий, посредством которых обеспечиваются возможности проведения расследований при наличии необходимости доступа к облачным хранилищам. Посредством указанного комплекса специалисты, проводящие расследование, могут получать учетные данные пользователей облачных хранилищ посредством исследовательских методов, применяемых в процессе производства судебных компьютерных экспертиз.

Для обеспечения надежности получения данных из облачных хранилищ необходимо наличие специальных знаний, поскольку нужно применять методы по получению доступа к данным, хранящимся на удаленных серверах, что осложняет процессы исследования важной информации. Информация, полученная из облачных хранилищ, может обеспечить быстрое раскрытие инцидентов по горячим следам, подтверждение или опровержение предварительных версий следствия.

Наиболее сложная задача – получение доступа к информации, хранимой на облачных хранилищах, так как для выполнения данной задачи необходимо проходить аутентификацию посредством введения логина и пароля с подтверждением доступа к облачным сервисам.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 24.04.2020).
2. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции».
6. Приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».
7. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».
8. ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме».
9. Приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».
10. Иванова, А. В. 3D-моделирование места преступления / А. В. Иванова, А. О. Путилов // Борьба с киберпреступностью в условиях развития цифрового общества : сб. науч. статей Междунар. конференции. – 2019. – С. 191–192.

*Алиманов Павел Евгеньевич¹,
соискатель Краснодарского высшего военного училища;*

*Сизоненко Александр Борисович²,
начальник кафедры Краснодарского высшего военного
училища, доктор технических наук, доцент*

АЛГОРИТМ РАСПРЕДЕЛЕНИЯ ФУНКЦИЙ МЕЖДУ СОТРУДНИКАМИ ДЛЯ ЭФФЕКТИВНОГО РЕШЕНИЯ КРИТИЧНЫХ ЗАДАЧ КИБЕРБЕЗОПАСНОСТИ

Функционирование любой крупной организации связано с использованием, обработкой, хранением большого объема информации. Безопасность информационных процессов напрямую влияет на эффективность ее работы. Еще в большей степени это утверждение касается объектов критической информационной инфраструктуры, нарушение функционирования которых может привести к существенным негативным последствиям для граждан, общества и государства. Для критической информационной инфраструктуры Российской Федерации обеспечение ее устойчивого и бесперебойного функционирования одно из национальных интересов в информационной сфере. Такие системы можно рассматривать как сложные кибернетические системы, а процессы обеспечения безопасности в них – как обеспечение кибербезопасности.

Наряду с техническими и организационными мерами обеспечения информационной безопасности не меньшее значение придается и кадровым мерам. [1] Ранее рассматривался подход, позволяющий формализовано описать возможности сотрудников структурного подразделения защиты информации по решению задач, возложенных на эти подразделения [2, 3], и методика подбора сотрудников в такие подразделения на основе метода анализа иерархий Т. Саати [6]. При этом оценивались такие качества соискателя, как специальность и уровень образования, личные качества, опыт работы, результаты испытаний. Это позволило выработать механизм отбора на определенные должности сотрудников, способных с наибольшим качеством выполнять возложенные на них повседневные обязанности.

В процессе повседневной деятельности могут возникнуть нештатные ситуации (инциденты) в сфере информационной безопасности, обладающие неприемлемым уровнем риска для организации. Перечень таких ситуаций известен заранее, и у руководителя службы защиты информации имеется возможность спланировать мероприятия по противодействию инцидентам и минимизации последствий. Для предотвращения (минимизации) последствий инцидентов информационной безопасности создаются группы реагирования на инциденты информационной безопасности, состоящие из наиболее доверенных и обученных сотрудников организации. [4] Данная группа обрабатывает инциденты ин-

¹ © Алиманов П. Е., 2020.

² © Сизоненко А. Б., 2020.

формационной безопасности во время их жизненного цикла и иногда может дополняться внешними экспертами, например, из общепризнанной группы реагирования на компьютерные инциденты или компьютерной группы быстрого реагирования. [4] Таким образом, необходимо разработать алгоритм, позволяющий перераспределять сотрудников подразделений информационной безопасности для предотвращения инцидентов, обладающих повышенным уровнем критичности.

Обозначим задачу по противодействию угрозы как множество функций: $F = (f_1, f_2, \dots, f_n)$, $|F| = n$, где n – количество функций защиты информации. множество сотрудников подразделения защиты информации. Множество сотрудников, обладающими компетенциями по устранению угрозы обозначим: $P = (p_1, p_2, \dots, p_m)$, $|P| = m$, где m – количество сотрудников.

Применяя подход, изложенный в [6], составим для каждой функции вектор-столбец приоритетности привлечения к ее выполнению того или иного сотрудника A_i , $i = (1 \dots n)$, $|A_i| = m$ и составим из них матрицу: $A = (A_1, A_2, \dots, A_n)$, при этом примем, что $a_{ij} \in (1 \dots 100)$. Каждый сотрудник обладает определенными ресурсами по решению устранения последствий воздействия угроз. Обозначим их через вектор ресурсов $R = (r_1, r_2, \dots, r_m)$. Для удобства вычислений примем $r_j \in (1 \dots 100)$. Для выполнения задачи защиты информации по противодействию угрозе необходимо, чтобы для каждой функции был выделен определенный ресурс. Другими словами, каждая функция обладает определенной трудоемкостью $T = (t_1, t_2, \dots, t_n)$. Тогда задача определения сотрудников, способных решить критичную задачу с максимальным качеством сводится к классической транспортной задаче [5]:

1. Суммарное количество ресурсов j -того сотрудника, распределяемое между функциями защиты информации должно быть равно r_j . Это даст m уравнений:

$$\left. \begin{aligned} x_{11} + x_{12} + \dots + x_{1n} &= r_1 \\ x_{21} + x_{22} + \dots + x_{2n} &= r_2 \\ \vdots \\ x_{m1} + x_{m2} + \dots + x_{mn} &= r_m \end{aligned} \right\}$$

2. Суммарные трудозатраты на выполнения каждой i -той функции должны быть равны t_i :

$$\left. \begin{aligned} x_{11} + x_{21} + \dots + x_{m1} &= t_1 \\ x_{12} + x_{22} + \dots + x_{m2} &= t_2 \\ \vdots \\ x_{1n} + x_{2n} + \dots + x_{mn} &= t_n \end{aligned} \right\}$$

3. При этом суммарное значение коэффициентов a_{ij} , определяющих качество выполнения задач в критических ситуациях, должно быть максимальное, а следовательно:

$$\sum_{i=1}^n \sum_{j=1}^m a_{ij} x_{ij} \rightarrow \max$$

Рассмотрим пример: пусть имеются три функции, которые определены в качестве первоочередных при вирусной атаке на критически важные ресурсы организации: f_1 – локализация зараженных ресурсов; f_2 – проверка всех имеющихся ресурсов с использованием средств антивирусной защиты; f_3 – оценка величины возможного ущерба от инцидента, связанного с вирусной атакой. В распоряжении начальника службы безопасности имеется пять сотрудников, для которых ранее разработана матрица качества выполнения указанных функций, векторы ресурсов трудоемкости:

$$A = \begin{pmatrix} 40 & 10 & 30 \\ 10 & 30 & 20 \\ 10 & 50 & 20 \\ 20 & 5 & 30 \\ 20 & 5 & 0 \end{pmatrix}; R = \begin{pmatrix} 90 \\ 100 \\ 100 \\ 80 \\ 50 \end{pmatrix}; T = (150 \quad 70 \quad 200).$$

Решение транспортной задачи дало следующие результаты:

$$\begin{pmatrix} 90 & 0 & 0 \\ 10 & 0 & 90 \\ & 70 & 30 \\ 0 & 0 & 80 \\ 50 & 0 & 0 \end{pmatrix},$$

которые можно трактовать следующим образом: сотрудники p_1 и p_5 занимаются выполнением только первой функции; сотрудник p_4 выполняет только третью функцию вместе с сотрудником p_2 ; вторая функция выполняется только сотрудником p_3 ; после выполнения своих основных назначенных функций сотрудник p_2 присоединяется к выполнению первой функции, а сотрудник p_3 – к третьей.

Таким образом, решение задачи определения состава сотрудников для наиболее эффективного предотвращения или минимизации последствий инцидентов информационной безопасности сведено к решению транспортной задачи. Разработанный алгоритм может использоваться в системах поддержки принятия решений, принимаемых руководителями подразделений защиты информации. Развитием предложенного алгоритма является определение необходимости привлечения сторонних экспертов для реагирования на инциденты информационной безопасности.

Список литературы

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Доктрина информационной безопасности Российской Федерации» // СПС «Консультант-Плюс». – URL: <http://www.consultant.ru>.

2. Алиманов, П. Е. Формализация процесса определения оптимальной организационно-штатной структуры подразделений защиты информации / П. Е. Алиманов, А. Б. Сизоненко // Научные труды КубГТУ. – 2019. – № 7. – С. 73–79. – URL: [http:// ntk.kubstu.ru/tocs](http://ntk.kubstu.ru/tocs).
3. Алиманов П. Е. Модель организационно-штатного обеспечения подразделений защиты информации / П. Е. Алиманов, А. Б. Сизоненко // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 33–38. – URL: <https://vi.mvd.pf/Nauka/nauchnij-zhurnal-vestnik>.
4. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности: ГОСТ Р ИСО/МЭК ТО 18044-2007 // СПС «КонсультантПлюс».
5. Вентцель, Е. С. Исследование операций / Е. С. Вентцель. – М. : Советское радио, 1972.
6. Алиманов, П. Е. Методика подбора сотрудников в структурные подразделения защиты информации на основе метода анализа иерархий / П. Е. Алиманов, А. Б. Сизоненко // Охрана, безопасность, связь. – 2019. – Вып. 5 (Ч. 2). – С. 7–13.

Аласкяров Низами Байрам оглы¹,
*старший преподаватель кафедры физической подготовки,
 учебно-научного комплекса специальной подготовки,
 Московского университета МВД России
 имени В.Я. Кикотя;*

Гаврилина Анастасия Андреевна²,
*слушатель Института психологии
 служебной деятельности ОВД,
 Московского университета МВД России
 имени В.Я. Кикотя*

О ВОПРОСАХ ФИЗИЧЕСКОГО САМОВОСПИТАНИЯ И САМОСОВЕРШЕНСТВОВАНИЯ, КАК ОДНОГО ИЗ УСЛОВИЙ ЗДОРОВОГО ОБРАЗА ЖИЗНИ

Физическое самовоспитание и самосовершенствование сочетают методы и приемы, направленные на создание гармоничного и слаженного человека. Физическое самовоспитание – это процесс целенаправленной, сознательной, планомерной работы над собой, ориентированный на формирование физической культуры личности, включающей совокупность приемов и видов деятельности, которые определяют и регулируют эмоционально окрашенную, эффективную позицию личности по отношению к своему здоровью, физическому совершенствованию и воспитанию. Физическое самовоспитание и самосовершенствование способствуют тому, что полученные навыки, знания и умения практического характера начинают расширяться. Однако результаты будут носить кратковременный характер, если у человека не возникнет последующего желания к постоянному физическому развитию личности.

Внутренняя сила базируется на двух важнейших ее составных компонентах – силе воли и самодисциплине. Абсолютно каждый человек может овладеть ими, а также развить их, потому что это те внутренние качества, которые не являются ограниченными. Но чтобы иметь возможность преуспеть в этом направлении, нужно вести систематическую непрерывную работу над собой.

Самовоспитание требует от человека воли. Она формируется и закрепляется в деятельности человека, состоящей в преодолении трудностей, стоящих на пути к цели. Воля может быть связана и с другими видами самообразования – нравственным, интеллектуальным, трудовым, эстетическим и др. Нередко занятия собственным телом человека заставляет понимание того, что он не соответствует социальным требованиям общества или же профессиональным требованиям.

Физическое самосовершенствование – это спортивное здоровое тело, красота, сила и выносливость. Физически развитым людям гораздо проще достичь

¹ © Аласкяров Н. Б., 2020.

² © Гаврилина А. А., 2020.

успеха в любой области. Физическое развитие или самосовершенствование предполагает следующие мероприятия:

- общее укрепление организма. Предполагается выполнение упражнений по совершенствованию движений, выносливости, повышению иммунитета;
- подготовка молодых людей к военной службе и будущей работе;
- воспитание уважения к различным видам физической активности и спорту;
- раскрытие и развитие спортивных талантов.

Физическое самосовершенствование и самовоспитание заключается в трех основных этапах, которые сейчас и будут рассмотрены.

На первом этапе человек занимается личностным самопознанием, выделяет положительные физические и психические качества, а также отрицательные, которые ему необходимо преодолеть. Именно требовательность к себе приводит к самопознанию и саморазвитию человека. В процессе используются такие методы, как самооценка, самоанализ и самонаблюдение.

На втором этапе определяется цель, подбирается программа самовоспитания и составляется личный план, который у каждого индивидуален. Цель также у каждого своеобразна. Она может быть, как обобщенной и долгосрочной (например, достичь физической культуры личности), так и четкой, и краткосрочной. Но в любом случае общая программа должна учитывать конкретные условия жизни, особенности самой личности, а также ее потребности.

Примерная программа самовоспитания может включать следующие задачи физического самосовершенствования:

- переход на здоровый образ жизни и в результате улучшение здоровья;
- изучение познавательной информации о физической культуре и практические занятия физкультурно-спортивной деятельностью;
- формирование нравственно-волевых качеств личности;
- повышение уровня физической подготовки и развития.

Третий этап связан непосредственно с применением полученных знаний и навыков на практике и их оттачиванием. Личностью используются такие методы, как: самоприказ, самовнушение, самокритика, самоодобрение, самоупражнение, самоотчет, самоконтроль. Методы самовоздействия, направленные на совершенствование личности, именуют методами самоуправления.

Список литературы

1. Волкова, Л. М. Здоровье студента и создание потребности в физическом самосовершенствовании / Л. М. Волкова, В. Ю. Волков, Д. Н. Давиденко // Здоровье – основа человеческого потенциала: проблемы и пути их решения. – 2009. – № 1.
2. Воронов, Н. А. Физическое самовоспитание как необходимое условие формирования здорового образа жизни – курсантов / Н. А. Воронов // Эпоха науки. – 2019. – № 19.
3. Плещев, А. М. Главные составляющие здорового образа жизни / А. М. Плещев // Вестник Шадринского государственного педагогического университета. – 2018. – № 3 (39).

Гончар Владимир Владимирович¹,

*заместитель начальника кафедры информационной
безопасности учебно-информационного комплекса
информационных технологий*

*Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Четвертая промышленная революция, сопровождающаяся цифровой трансформацией различных сфер общественной жизни, создает значительные преимущества для потребителей различных услуг, увеличивает качество, скорость, доступность получения гражданами различных электронных сервисов, совершенствуются различные сферы общественной жизни и бизнес-модели функционирования организаций. Новые технологии и дополнительные возможности создают дополнительные риски, увеличивается вероятность эксплуатации интернета для совершения противоправных действий.

В настоящее время отмечается высокая латентность таких противоправных действий, во многом обусловленная возможностью преступников оставаться анонимными, избегать непосредственного контакта с потерпевшими, широкой аудиторией пользователей информационных ресурсов, простотой доступа к этим ресурсам, а также организованным и трансграничным характером подобных деяний.

По данным АО «Лаборатория Касперского» только в одном квартале 2019 г. их защитные решения обнаружили более 48 млн вредоносных почтовых вложений, что формально подпадает под квалификацию ст. 273 УК РФ, с помощью системы Антифишинг предотвращено 137,4 млн попыток перехода пользователя на фишинговые интернет-страницы, ведущие, как правило, к хищениям денежных средств.

В последнее время увеличилось количество преступлений рассматриваемой категории и появилось много новых вариативных методов, способов и средств их совершения. Исходя из этого и в соответствии с решением Коллегии Министерства внутренних дел Российской Федерации № 3км «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий» в органах внутренних дел были созданы специализированные подразделения по раскрытию и расследовании IT-преступлений.

В 2019 г. отмечается значительный рост количества преступлений рассматриваемой категории, уголовные дела о которых находились в производстве правоохранительных органов Российской Федерации – 339.3 тыс., что на 64 % превышает показатель аналогичного периода прошлого года (206.8 тыс.).

¹ © Гончар В. В., 2020.

Непосредственно в отчетном периоде зарегистрировано 294,4 тыс. преступлений (+ 68,5 % к АППГ, 174,7 тыс.).

В общем числе зарегистрированных преступлений, удельный вес IT преступлений увеличился с 8,8 % в 2018 г. до 14,5 % в 2019 г. Большую их часть, а именно 289,8 тыс. (98,4 %), выявили сотрудники органов внутренних дел. Почти половина из них (48,5 %) относится к категориям тяжких и особо тяжких: 142,7 тыс. (+149,0 %); половина (53,3 %) совершается с использованием сети «Интернет»: 157,0 тыс. (+45,4 %), более трети (39,5 %) – с использованием средств мобильной связи: 116,2 тыс. (+89,5 %).

Раскрываемость IT-преступлений по-прежнему невысока и по итогам 2019 г. составила 22,2 %.

К основным трудностям в расследовании и раскрытии указанной категории преступлений относится невозможность определения IP-адресов подозреваемых, в связи с использованием прокси-серверов, а также принадлежность абонентских номеров, используемых при совершении преступлений, в связи с регистрацией на подставных лиц. Следует отметить, что имеют место случаи, когда следователь, получив судебное решение о получении информации о соединениях абонентов и абонентских устройств, направляет постановление оператору связи, которые не исполняют его. При дополнительной проверке устанавливается, что данная компания имеет небольшую емкость абонентских номеров (как правило использующие IT-технологии), по юридическому адресу отсутствует, сервер находится в неизвестном месте.

К не менее актуальной проблеме в расследовании и раскрытии мошенничеств к указанной категории относится факт регистрации телефонных номеров, с которых производились звонки потерпевшим, на территории других регионов. Это значительно затрудняет производство следственных и оперативных мероприятий по «горячим следам», в том числе получение информации об абоненте, осуществляющем звонок, а также его местонахождении в период совершения преступления. Большое количество запросов в сотовые компании и поручений в другие регионы по настоящее время остаются без ответов.

Денежные средства, направляемые посредством банковских переводов либо через платежные терминалы, мошенник получает через иное лицо, введенное последним в заблуждение относительно своих преступных намерений, за пределами области. Особенность этого вида преступлений создаст сложность в его раскрытии, а также обуславливает длительность расследования уголовных дел.

Необходимость получения в суде соответствующих решений не позволяет органам внутренних дел оперативно получать сведения о пользователях банковских карт, а получаемые с большим запозданием сведения становятся неактуальными ввиду смены злоумышленниками устройства мобильной связи, сим-карт.

Кроме того, в ходе изучения соответствующих уголовных дел было установлено, что потерпевшие, обратившиеся с заявлением в полицию о совершении в отношении них противоправных действий, скрывают часть информации, не желая казаться в глазах родственников или сотрудников полиции доверчивыми и не имеющими познаний в области современных финансовых технологий. в процессе предварительного следствия удастся выяснить, что «неожиданное» списание де-

нежных средств с банковского счета потерпевшего является всего лишь ежемесячной платой за оказание каких-либо на сайтах, подписчиком которых был потерпевший. Не разобравшись с особенностями оплаты, пострадавшие вводят данные своей банковской карты, рассчитывая на однократное списание. Однако из-за невнимательности упускают тот факт, что услуга подключается на длительное время с периодическим списанием денежных средств.

Несмотря на отсутствие события преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ, при описании денежных средств с согласия заявителя расследование таких «тяжких преступлений» активно продолжается путем переписки между следователями и сотрудниками органа дознания, которые по объяснимым причинам не могут установить лицо, совершившее преступление.

Кроме того, изучение уголовных дел показало, что в ряде случаев хищения денежных средств формально подпадающее под признаки уголовно-наказуемого деяния могли быть урегулированы гражданско-правовыми способами на стадии проведения доследственной проверки (в случаях признания банками сомнительных транзакций; отмены покупки в интернет-магазине и добровольном возврате денежных средств на счет кредитной карты заявителя).

Проверки организации работы по раскрытию преступлений указанной категории показали, что одной из причин, по которой данные преступления остаются нераскрытыми, является ненадлежащее взаимодействие заинтересованных служб в их раскрытии, а также не своевременное проведение следственных действий, что приводит к затягиванию сроков расследования.

Как правило, работа в дежурные сутки сводится к допросу потерпевшего, работа сотрудников оперативных служб к подготовке рапортов о принадлежности абонентских номеров.

Вместе с тем в ходе изучения приостановленных уголовных дел, возбужденных по фактам мошеннических действий, совершенных посредством интернет-технологий и телефонных коммуникаций, установлено, что при наличии детализации абонентских номеров и расчетных счетов, на которые перечислялись похищенные денежные средства, следственные и оперативно-разыскные мероприятия не проводились, что свидетельствует о том, что в основном работа по приостановленным уголовным делам ведется по остаточному принципу.

Имеют место быть случаи несвоевременного выхода следователей с ходатайствами в суд о получении детализации телефонных переговоров подозреваемого, а также принадлежности абонентских номеров.

Указанные факты в ряде случаев имеют объективные причины, обусловленные судебной практикой, предоставления информации об абонентских соединениях в период с момента совершения преступлений, до обращения в суд, в связи с чем следователи намеренно выходят в суд спустя месяц, с целью увеличения срока контроля телефонных переговоров и периода возможной активации абонентских номеров.

Список литературы

1. Информационно-аналитические материалы Следственного Департамента МВД России.
2. <https://мвд.рф/Deljatelnost/statistics> - статистика МВД России.

Григорьев Дмитрий Александрович¹,
*заведующий лабораторией «Криминалистика и специальная техника»
 кафедры государственно-правовых
 и уголовно-правовых дисциплин РЭУ имени Г.В. Плеханова,
 кандидат юридических наук;*

Егоренко Евгений Юрьевич²,
*старший разработчик компьютерных программ
 АНО «Анитех»*

О НЕКОТОРЫХ ВОПРОСАХ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ

Автоматизация, цифровизация и использование алгоритмов машинного обучения и глубокого машинного обучения на сегодняшний день – неотъемлемая часть повседневной жизни граждан. Ныне имеется множество сервисов, в которых используются указанные выше технологии, и задействованы в разных областях и для разных целей, и, к сожалению, в том числе и преступных.

Цель данной статьи – рассказать о технологиях, которые используются для автоматизации работы с большими данными, и выдвинуть идеи, итоговым результатом которых станет профилактика, прогнозирование правонарушений и частичная автоматизация процессов расследования преступлений.

Что такое искусственный интеллект и машинное обучение и чем они отличаются от человеческого интеллекта?

Многие считают, что искусственный интеллект подобен человеческому разуму. Это одновременно верно, и заблуждение.

Искусственный интеллект – это свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека [1]. Термин обычно применяется к системам, которые имеют способности: рассуждение, обобщение и обучение на предыдущем опыте.

Еще в 2011 г. консалтинговая компания McKinsey & Co сообщала, что «большие данные станут ключевой основой конкуренции, которая послужит основой для новых волн роста производительности, инноваций и потребительского излишка – при условии наличия правильной политики и инструментов» [2].

Машинное обучение – это система методик анализа данных, позволяющих аналитической системе постоянно обучаться в ходе решения множества сходных задач. Машинное обучение базируется на идее о том, что аналитические системы могут обучиться выявлять закономерности и принимать решения с минимальным участием человека.

¹ © Григорьев Д. А., 2020.

² © Егоренко Е. Ю., 2020.

Таким образом, любой продукт машинного обучения – есть некий алгоритм, который обобщая заранее определенный набор признаков позволяет на их основе сделать определенный прогноз.

Поясним наглядно как это работает сразу с рабочим предложением, но слегка упрощенным для понимания.

Предположим, перед нами стоит задача профилактики правонарушений с гражданами, освободившимися из мест лишения свободы, и, мы имеем всего два признака – номер статьи, за нарушение которой он был ранее отправлен в места лишения свободы и, например, национальность. (Разумеется, для полноценного варианта рабочей модели нужно больше различных признаков, например возраст, пол, образование, профессия, дети, семейное положение факт условно-досрочного освобождения, дисциплинарных нарушений, и даже хронические заболевания и др.). Но для простоты объяснения обойдемся только двумя признаками. И совокупим этот набор признаков с фактом рецидива после освобождения из мест лишения свободы. За это отвечает красный цвет точки на графике – значит, был рецидив, а зеленый – не было.

Представим, что имеется небольшая база данных с около 100 примерами, собранными за год работы правоохранительных органов; нанесем это все на координатную плоскость, после чего раскрасим соответствующим (красным) цветом рецидивистов и более не нарушавших закон граждан – зеленым.

Цель машинного обучения, нейронных сетей поиск такой функции, проводя которую через набор всех признаков можно отделить их друг от друга максимально достоверно. Есть масса метрик, определяющих точность моделей машинного обучения, и используя различные параметры и настройки можно достичь требуемые значения точности результатов.

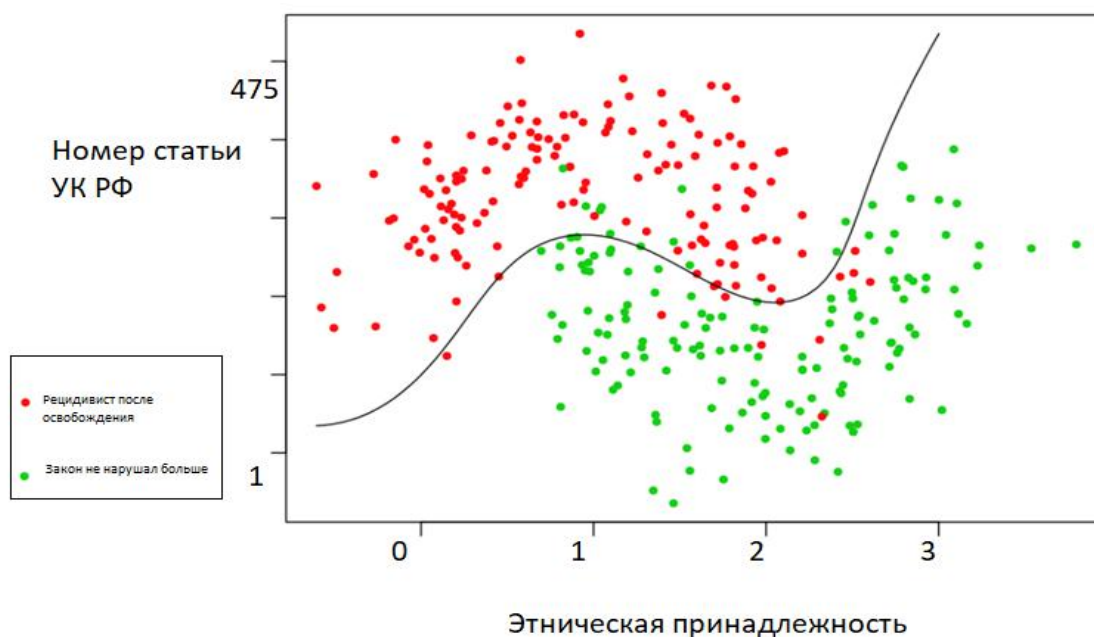


Рис. 1. Этническая принадлежность

После нахождения нужной функции – ее можно использовать уже на абсолютно новых данных, что актуально в силу непрерывности процесса совершения преступлений и последующих после них наказаний.

Стоит согласиться с мнением Д. В. Бахтеева, что искусственный интеллект способен выявить скрытые, неочевидные связи и закономерности, исключив информационный шум, дезинформацию [3].

Разобравшись, что такое машинное обучение, перейдем к разбору случаев, имевших резонанс и негативные последствия, а именно к тому, как можно было бы их предотвратить.

Сделаем это на примере нахождения источника вброса фейковых новостей.

Интенсивность обмена информацией, ее генерация и скорость распространения в последнее время растут, и человеческого ресурса не всегда достаточно чтобы оперативно реагировать на их распространение, выявлять первичные источники распространения ложной информации.

Для решения указанных выше проблем и выведения работы правоохранительных органов на более высокий качественный уровень целесообразно наладить взаимодействие с негосударственными организациями, которые успешно реализуют свои возможности по обеспечению информационной безопасности.

В частности, технологии компании «АНИТЕХ» позволяют осуществлять непрерывный сбор и фильтрацию в режиме онлайн всех размещаемых онлайн публикаций СМИ, с количеством аудитории, при влиянии на которую ситуация может приобрести неконтролируемый характер. Сбор данных осуществляется по различным статьям набора данных, например время создания, заголовки и текст статьи. Для достижения максимального результата есть возможность гибкой настройки правил даже при малой базе данных.

Тексты публикаций можно представить по определенным правилам в виде цифр и тогда они станут применимы для задач машинного обучения. Один из способов использования таких данных кластеризация данных, т. е. заранее собранный массив текстов по определенным математическим правилам можно сгруппировать по их темам. В данном случае это делается путем нахождения определенных закономерностей имеющих слов, словосочетаний, их семантике в каждом тексте новости в сравнении со всеми остальными.

Получившиеся наборы сгруппированных текстов можно разными способами дополнительно анализировать на их «тональность» или на наличие экстремизма по заранее обученным моделям и уже по временным меткам и ссылкам ресурса выявлять «аномальные» новости и в случае подтверждения факта вброса фейковой новости – решать вопрос о привлечении издания к ответственности, согласно законодательству Российской Федерации.

Алгоритмы машинного обучения действительно идеально подходят для работы с текстами, если использовать заранее размеченные данные, как мы это сделали в примере с рецидивами преступлений.

Рассмотрим применение искусственного интеллекта для противодействия преступлений на примере мошеннических действий с банковскими картами.

Личный опыт одного из авторов данной статьи по построению аналогичных моделей при применении в коммерческой сфере для обеспечения безопасности

составляет не один год. Самой интересной задачей противодействия анализируемому деянию был большой проект, который выявлял и давал возможность предотвратить попытки операторами центра обработки телефонных обращений одного крупного банка совершить факт мошенничества с использованием данных карты клиента.

Предприимчивые операторы пытались узнать у клиента его номер карты, секретный код для дальнейшего несанкционированного снятия личных денежных средств или фиксации этих данных для дальнейшей продажи мошенникам. Преобразование речи в режиме разговора в текст и его дальнейшая обработка подобными моделями в случае, когда клиент называл что-то похожее на номер карты, либо когда оператор спрашивал эти данные, позволяли незамедлительно передать эти данные уполномоченному лицу и оперативно принимать решение о привлечении к дисциплинарной ответственности, и в дальнейшем, передачи материалов проверки, проведенной службой безопасности банка в орган предварительного расследования для принятия процессуального решения в соответствии с УПК РФ.

Данный опыт можно переложить и на деятельность по профилактике экстремизма. Известно немало случаев блокировки по решению суда контента, являющегося экстремистским. Это отличный материал для построения точно таких же моделей, своевременно и оперативно анализирующих информационное пространство на предмет таких публикаций. Такие размеченные данные могут дать возможность обучить модель с высокими показателями точности и сделать ее достаточно гибкой для применения на новых, ранее не изученных моделью данных.

При анализе материалов групп в социальных сетях, различных публикаций на сайтах, комментариев к видеоматериалам можно оперативно выявить нарушающие закон объекты и их авторов с использованием небольшого количества людей для постоянной верификации результатов работы моделей.

Для профилактики и расследования преступлений, совершенных с помощью новых технологий можно использовать и алгоритмы машинного обучения.

Если речь идет о профилактике, то один из способов предотвращать несанкционированный доступ, совершенный с помощью вирусов (троянов, иных вредоносных программ) является анализ последовательности действий программ или действий пользователя и параметров данных, для чего активно используют антивирусы.

Основной метод работы антивируса заключается в поиске вредоносного кода, т. е. текста. Но киберпреступники стараются быть на шаг впереди и проверяют каждую вредоносную программу в базе антивирусов, пытаются сделать код более уникальным и запутанным. Но у всех этих программ, как правило, определенная последовательность действий, которую можно точно установить.

Предположим, на почту пришло письмо с вредоносной программой, замаскированной под документ Microsoft Office, при открытии которого происходит загрузка какого-то файла с неизвестного ресурса, т. е. конкретный запрос к нему, затем запись на диск или в память и исполнение этого файла.

С высокой вероятностью антивирус это мог бы допустить, особенно если код вредоносной программы качественно обфусцирован («запутан») но если был бы развернут Security Operation Center (Центр оперативного управления), анализирующий поступающие данные с компьютеров пользователей и обрабатывающий их в реальном времени алгоритмами машинного обучения и оперативно выявляющий подобные инциденты и допускающий легитимные действия пользователей – смог бы стать эффективным средством профилактики киберпреступлений.

В случае создания подобного алгоритма его можно использовать для более оперативного и точного выявления уже совершенных инцидентов, так как ручной анализ большого количества данных из файлов регистраций действий пользователя или программ (логов) займет большое количество времени и ресурсов, а применение обученной модели позволит быстрее установить время и конкретный способ получения несанкционированного доступа, что позволит быстрее выйти на след злоумышленника.

Об успешном применении искусственного интеллекта говорит опыт США, где «ФБР для противодействия компьютерной преступности совместно с компанией ForAllSecure и университетом штата Пенсильвания разработала систему Mayhem, которая действует с 2017 г. Цель данной системы распознавание индивидуального почерка хакеров и хакерских группировок, обнаружение атак, активное тестирование и преследование хакеров вплоть до установления их локации. Опытным путем на конференции по кибербезопасности Blac Hat в 2016 г. в состязании между хакерами и Mayhem, последняя успешно опознала четырех хакеров из пяти» [4].

С помощью искусственного интеллекта можно осуществлять и прогнозирование некомпьютерных преступлений.

Степень криминогенной обстановки конкретного района на конкретный момент времени точно так же можно описать различными зависящими друг от друга цифрами.

Социально-демографические показатели:

- доля мигрантов;
- доля иногородних граждан;
- возрастное и гендерное соотношение;
- распределение уровня образования;
- распределение доходов граждан;
- занятость граждан.

Экономические показатели района:

- средний уровень доходов;
- денежные потоки, проходящие через контрольно-кассовые машины;
- уровень инфраструктуры;
- количество социально-значимых объектов.

И многое другое можно объединить в модель, которая будет прогнозировать степень криминогенности района, улицы, субъекта Российской Федерации или любого образования на текущий момент времени.

Это позволит ротировать своевременно личный состав правоохранительных органов, оптимизировать их деятельность.

Таким образом, несмотря на то, что для каждой цели нужно строить свою модель, алгоритмы машинного обучения имеют существенные преимущества: быстрота принятия решения, гибкость настройки, умение обобщать новые данные, прогнозирование или распределение данных. Применение искусственного интеллекта поможет осуществить рывок в противодействии преступности с использованием компьютерных технологий, так и иной преступности, повысить эффективность всей правоохранительной системы, это один из основных запросов законопослушных граждан Российской Федерации.

Список литературы

1. Аверкин, А. Н. Толковый словарь по искусственному интеллекту / А. Н. Аверкин, М. Г. Гаазе-Рапопорт, Д. А. Пospelов. – М. : Радио и связь, 1992.
2. Big data: The next frontier for innovation, competition, and productivity - <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation/>.
3. Бахтеев, Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования / Д. В. Бахтеев // Российское право. Образование, практика, наука. – 2018. – № 2. – С. 43–48.
4. Овчинский, В. С. Технологии будущего против криминала / В. С. Овчинский. – М. : Кн. мир, 2017. – 240 с.

Григорьев Олег Дмитриевич¹,
исполнительный директор АНО «Анитех»;

Усков Александр Сергеевич²,
*старший разработчик компьютерных программ
АНО «Анитех»*

НОВЫЕ СПОСОБЫ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

В современном высокотехнологичном мире многие важнейшие и жизненно необходимые процессы зависят от работы ряда служб и сервисов, одна из которых – всемирная сеть, одно из важнейших достижений современного человечества. Определенная инфраструктура, связанная со всемирной сетью, обеспечивает корректную работу основных служб и систем в современном обществе. Поэтому сбой в их работе, будь это хакерская атака, техническая неполадка или другие обстоятельства, приводящие к остановке или повреждению этой инфраструктуры, будут иметь серьезные последствия для работы служб, сервисов, например обеспечивающих безопасность авиаперевозок.

Киберпреступность – это совокупность преступлений, когда компьютер как объект преступления используется в качестве орудия для совершения преступления. Киберпреступник может использовать устройство для доступа к личной информации пользователя, конфиденциальной деловой информации, правительственной информации или дистанционного отключения устройства.

В связи с широким внедрением информационно-коммуникационных технологий значительно выросло и количество преступлений, совершаемых с применением компьютерных технологий. Об этом свидетельствуют данные Генеральной прокуратуры Российской Федерации: «За 9 месяцев 2018 года в Российской Федерации зарегистрировано 121 тыс. 247 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Таким образом, если в 2017 году их регистрировалось в среднем 7,5 тыс. в месяц, то в 2018 г. уже более 13 тыс. в месяц. В общем числе преступлений их доля выросла с 4,4 % до 8,1 %, при этом расследовано только 31,8 тыс. таких преступлений. С 2013 года киберпреступность, выросла в 10 раз (в 2013 году аналогичных преступлений было 11 тыс., в 2014 году – 44 тыс., в 2016 году – 66 тыс.). Так же средняя сумма убытков в одной компании, согласно данным составляет 299 940 рублей. В целом по стране потери от кибератак оцениваются в 115 967 руб. За весь 2017 год – 90 тыс. 587» [1].

«В январе – декабре 2019 года зарегистрировано более 294 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий или, что почти на 70 % больше, чем за аналогичный период про-

¹ © Григорьев О. Д., 2020.

² © Усков А. С., 2020.

шлого года. Половина таких преступлений совершается с использованием сети «Интернет», а более трети – средств мобильной связи. Свыше 98 % таких преступлений выявляется органами внутренних дел». [2]

В данной статье мы попытаемся проанализировать новые способы совершения киберпреступлений, появившиеся в последнее время. К ним мы относим следующее:

Ботнеты – это сети от скомпрометированных компьютеров, которые внешне контролируются удаленными хакерами. Затем удаленные хакеры рассылают спам или атакуют другие компьютеры через эти ботнеты. Последние также могут использоваться как вредоносные программы и выполнять вредоносные задачи.

Потенциально нежелательные программы (ПНП). PUPS или потенциально нежелательные программы менее опасны, но представляют собой тип вредоносного программного обеспечения (далее – ПО). Они удаляют необходимое программное обеспечение в вашей системе, включая поисковые системы и предварительно загруженные приложения. Они могут включать в себя шпионское или рекламное ПО, поэтому рекомендуется установить антивирусное программное обеспечение, чтобы избежать подобную вредоносную загрузку.

Запрещенный/незаконный контент. Этот вид преступления включает в себя действия, состоящее в распространении ненадлежащего контента, при котором последний может считаться крайне огорчительным и оскорбительным. Оскорбительный контент может включать и сексуальную активность между взрослыми, видео с интенсивным насилием и видео с криминальной активностью. Незаконное содержание включает материалы, пропагандирующие акты терроризма, и материалы по эксплуатации детей. Этот тип контента существует как в обычном интернете, так и в темной сети, анонимной сети.

Наборы эксплойтов. Наборы эксплойтов используются для выявления уязвимости (ошибки в коде программного обеспечения), чтобы получить контроль над компьютером пользователя. Это готовые инструменты, которые преступники могут покупать в интернете и использовать против любого, у кого есть компьютер. Наборы эксплойтов регулярно обновляются, как и обычное программное обеспечение, и доступны на хакерских форумах.

Пользовательские данные – новая нефть. С текущим развитием технологий и постоянно появляющимися новыми сервисами, и службами главной ценностью, выходящей на первый план, становятся пользовательские данные. Сегодня пользователь – основной источник важных данных, можно сказать что сейчас пользовательские данные – это новая нефть. Ценность представляют практически все данные о пользователе, его активность в соцсетях и круг общения, лайки, часто посещаемые сайты, запросы в интернете, покупки и т. д.

На такие данные найдутся покупатели и продавцы, например сервисы рекламы – Advertising. Google adsense, yandex, clickbooth их главная задача сделать максимальную конверсию из этих данных. Или сервисы аналитики – Yandex metrika, google analytics. Их интересует сбор информации, что заинтересовало, сколько времени провели на сайте, откуда узнали. Социальные сети –

VK, OK, FB, Twitter хотят о вас знать буквально все – ФИО, увлечения, ваших друзей, ваши фото, делают свои сервисы оплаты.

Отдельно стоят посредники – Data brokers, Doubleclick, Datalogix, Epsilon, BlueKai. Они собирают информацию о пользователях и затем продают ее другим посредникам или компаниям, т. е. продают цифровой портрет пользователя. Обладание подобным портретом дает возможность манипуляции данными, удобными для владельца «портретов». В телефоне, одном из носителей информации, сформированы почти все данные о человеке, его повседневные маршруты, способы оплаты, контактные лица, места в которых часто бывает, документы, фото – все это представляет повышенный интерес и объект охоты на подобные данные.

Кейс cambridge analytica. В июле 2019 г. Федеральная торговая комиссия США оштрафовала Facebook на \$5 млрд. из-за утечки данных 87 млн пользователей. Все это произошло из-за одной компании, которая занималась сбором и анализом пользовательских профилей. Источником утечки считается компания Cambridge Analytica, имевшая отношение к созданию политической рекламы кампании Дональда Трампа, направленную на пользователей соцсети.

Основная идея Cambridge Analytica сбор данных пользователей для моделирования поведения пользователей на ту или иную политическую рекламу. Как итог – выдача релевантной рекламы на определенное событие. Сбор информации позволил выявить у пользователя следующие аспекты жизнедеятельности: убеждения, особенности характера, интересы, политические взгляды и т. д. Больше всего информации давали «лайки», по таким отпечаткам удавалось выстроить модель поведения человека. По мнению центра психометрии Майкл Козински: «Анализа 68 лайков в Facebook уже достаточно, чтобы установить цвет кожи испытуемого (с 95 % вероятностью), его гомосексуальность (88 % вероятности) и приверженность Демократической или Республиканской партии» [3].

Психометрия и новые технологии. Психометрия или психография – эта дисциплина психологии, пытающаяся измерить человеческую личность. В своей работе Козински использовал метод OCEAN, так называемый «метод океана». На основании этой модели, в которую входит пять показателей: открытость, нейротизм, сознательность, экстраверсия и доброжелательность, можно понимать, как будет вести себя человек и что он из себя представляет. Создав такой «отпечаток» можно эффективно «предсказывать» предпочтения человека, его поведение, а также влиять определенным образом, например, показывая рекламу или новости определенной тематики, как это было в случае с Cambridge Analytica.

Развитие всемирной сети и всеобщей информатизации сделало более эффективным сбор подобных данных, появилась возможность анализировать пользователей в соцсетях и прослеживать связи между пользователями, создавать приложения с огромными пользовательскими данными, распространение защищенных баз данных на черном рынке также дает злоумышленникам информацию для анализа и последующих атак на пользователей. Например, Maltego – одна из программ, позволяющая строить графы и связи пользователей с раз-

личными аккаунтами в соцсетях. Основная задача – выявление отношений и связей между различными группами людей, компаний, организаций, документами, интернет-структурами.

Создание «датасета». С приходом технологии Big Data данные параметры стали объединяться в «датасеты» – набор данных структурированный и обработанный для дальнейшего процесса обучения программы. Для его создания и формирования используются многочисленные данные, например, база мобильных номеров с пользовательским Ф. И. О, база проживающих людей в определенном районе, списки владельцев огнестрельного оружия и т. д.

Благодаря технологии больших данных можно предсказывать те или иные события, например реакции людей на определенное событие.

В ближайшие годы киберпреступники, вероятно, начнут атаковать устройства интернета вещей (Internet of Things (IoT)), появятся программы с машинным обучением и искусственным интеллектом. Помимо этого существенным может оказаться рост в кибератаках на мобильные устройства, которые обладают широким спектром информации как о владельце, так и о его платежной информации.

Для успешного противостояния современным вызовам киберпреступности следует укреплять государственно-частное партнерство (далее – ГЧП) при расследовании преступлений данной направленности. Ни для кого не секрет, что экспертные подразделения правоохранительных органов испытывают определенный кадровый голод и зачастую не имеют в наличии новейшие технические средства для производства судебно-компьютерных экспертиз, что нельзя сказать о специализированных негосударственных экспертных учреждениях.

Такие примеры уже существуют как в Европе, так и в США, где государственные структуры (например, Агенство национальной безопасности) сотрудничают с частными компаниями для расследования преступлений, как это было во время расследования недоказанного вмешательства Российских хакеров в выборы в США в 2016 г. В 2019 г. «Норникель» также озабочился о данной проблеме, высказав мнение, что в связи с быстрым развитием цифровой экономики необходима «консолидация усилий государства и бизнеса в вопросах информационной безопасности на национальном, и на международном уровнях [4].

Стоит согласиться с мнением А. Л. Осипенко о необходимости разработки федеральной программы для развития частного сектора обеспечения кибербезопасности, в которой был бы учтен как российский, так и международный опыт организации ГЧП в этой сфере [5].

Такие государственно-частные партнерства целесообразны для следующих направлений:

1. Мониторинг киберпространства.
2. Сбор цифровых доказательств.
3. Проведение компьютерно-цифровых экспертиз.
4. Разработка и внедрение программного обеспечения для выявления и предотвращения киберугроз.
5. Анализ больших данных.
6. Разработка и совершенствование законодательства.
7. Подготовка и повышение квалификации специалистов.

Для более успешного противодействия новым проявлениям киберпреступности, в рамках ГЧП следует объединить ключевых игроков рынка систем кибербезопасности в ассоциации, это позволит консолидировать усилия негосударственных организаций и правоохранительных органов на важнейших направлениях совместной деятельности.

Список литературы

1. Генпрокуратура сообщила почти о двукратном росте числа киберпреступлений в Российской Федерации в 2018 году // URL: <https://tass.ru/proisshestiya/5733551> (дата обращения: 08.04.2020).
2. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2019 года // URL <https://мвд.рф/reports/item/19412450/> (дата обращения: 08.04.2020).
3. Ирхин, Ю. В. Стратегии и особенности выборов 45-го президента США: новые возможности и технологии / Ю. В. Ирхин // Социально-гуманитарные знания. – 2017. – № 2. – С. 18–33.
4. Норникель предложил сформировать «триаду практического взаимодействия» в сфере информационной безопасности // URL: <http://www.norilsk-zv.ru/news/2019-10-24/43396> (дата обращения: 08.04.2020).
5. Осипенко, А. Л. Государственно-частное партнерство в сфере противодействия киберпреступности / А. Л. Осипенко // Вестник Воронежского института МВД России. – 2016. – № 4. – С. 37–44.

Гусев Дмитрий Владимирович¹,
*старший следователь по особо важным делам I отдела
(контроля расследования преступлений
в сфере экономики и совершенных
с использованием информационно-телекоммуникационных технологий)
контрольно-методического управления
Следственного департамента МВД России*

ОТДЕЛЬНЫЕ ПРОБЛЕМНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Происходящая в настоящее время очередная промышленная революция, сопровождающаяся цифровой трансформацией различных сфер общественной жизни, создает значительные преимущества для потребителей различных услуг, увеличивает качество, скорость, доступность получения гражданами различных электронных сервисов, совершенствуются различные сферы общественной жизни и бизнес-модели функционирования организаций. Новые технологии и дополнительные возможности создают дополнительные риски, увеличивается вероятность эксплуатации интернета для совершения противоправных действий.

Сегодня можно отметить высокую латентность таких противоправных действий, во многом обусловленную возможностью преступников оставаться анонимными, избегать непосредственного контакта с потерпевшими, широкой аудиторией пользователей информационных ресурсов, простотой доступа к этим ресурсам, а также организованным и трансграничным характером подобных деяний.

АО «Лаборатория Касперского» информирует, что только в одном квартале 2019 г. их защитные решения обнаружили более 48 млн вредоносных почтовых вложений, что формально подпадает под квалификацию ст. 273 УК РФ, с помощью системы Антифишинг предотвращено 137,4 млн попыток перехода пользователя на фишинговые интернет-страницы, ведущие, как правило, к хищениям денежных средств.

1 ноября 2019 г. состоялась коллегия Министерства внутренних дел Российской Федерации № 3км «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий», посвященная решению проблем неуклонного роста количества преступлений рассматриваемой категории и появлением новых вариативных методов, способов и средств их совершения.

Одним из основных ее результатов стало принятие решения о создании в органах внутренних дел специализированных подразделений по раскрытию и расследованию преступлений, совершенных с использованием информационно-телекоммуникационных технологий, которые также можно назвать киберпреступлениями.

¹ © Гусев Д. В., 2020.

В 2019 г. отмечается значительный рост количества преступлений рассматриваемой категории, уголовные дела о которых находились в производстве правоохранительных органов Российской Федерации – 339,3 тыс., что на 64 % превышает показатель аналогичного периода прошлого года (206,8 тыс.).

Непосредственно в отчетном периоде зарегистрировано 294,4 тыс. преступлений (+ 68,5 % к АППГ, 174,7 тыс.).

В общем числе зарегистрированных преступлений, удельный вес рассматриваемых преступлений увеличился с 8,8 % в 2018 г. до 14,5 % в 2019 г. Большую их часть, а именно 289,8 тыс. (98,4 %), выявили сотрудники органов внутренних дел. Почти половина из них (48,5 %) относится к категориям тяжких и особо тяжких: 142,7 тыс. (+149,0 %); половина (53,3 %) совершается с использованием интернета: 157,0 тыс. (+45,4 %), более трети (39,5 %) – с использованием средств мобильной связи: 116,2 тыс. (+89,5 %).

Раскрываемость данного вида преступлений по-прежнему невысока и по итогам 2019 г. составила 22,2 %.

В результате анализа судебно-следственной практики по уголовным делам рассматриваемой категории установлено, что на территории Российской Федерации в последнее время обрели массовый характер «дистанционные преступления», где в качестве главного «орудия» совершения преступления выступают средства мобильной связи и информационно-коммуникационная сеть «Интернет», причиной «популярности» у криминалитета такого способа хищения чужого имущества у граждан денежных средств является широкая распространенность и относительная доступность для большинства населения услуг мобильной связи, интернета.

Так, совершение данных преступлений стало возможным в связи с доверчивостью граждан из-за их недостаточной грамотности в сфере пользования ресурсами интернета, в том числе мобильными устройствами и программами. Результаты анализа показали, что бесконтактным преступлениям подвергаются граждане в возрасте 20–50 лет, что связано с использованием последними сайтами по продаже товаров в интернете или бесплатных объявлений «Авито», «Юла», а также общением в социальных сетях и т. д.

Сложности установления лиц, причастных к совершению рассматриваемой категории преступлений связаны с тем, что зачастую звонки потерпевшим происходят с мобильных телефонов, зарегистрированных на подставных или несуществующих лиц, а банки информацию о движении денежных средств предоставляют с большим опозданием. Платежные системы, в свою очередь, информацию о движении денежных средств предоставляют не в полном объеме, и часто в схеме обналичивания денежных средств задействуются несколько платежных систем и различные электронные кошельки, что делает весьма затруднительным и долговременным установление держателей счетов, получивших денежные средства. К тому же нельзя забывать об анонимности, т. е. предоставляемые возможности находятся в интернете и совершение различных действий полностью не идентифицировано либо использованы чужие данные.

Эти проблемные обстоятельства создают трудности в раскрытии данного вида преступлений и требуют разрешения.

Особо остро в настоящее время стоит вопрос правильной квалификации преступлений, связанных с телефонными мошенничествами и отграничения их от квалифицированной кражи.

Ранее возникавшие проблемы правоприменения норм уголовного и уголовно-процессуального законов по данному направлению деятельности разъяснены постановлением Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». В частности, разрешен вопрос о необходимости дополнительной квалификации по ст. 272–273 или 274.1 УК РФ мошенничества в сфере компьютерной информации, совершенного посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных программ. Разъяснено также, что если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные, то оно считается оконченным с момента их изъятия с банковского счета владельца.

Однако Федеральный закон от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» в ст. 158 УК РФ внесены изменения, а именно, ч. 3 ст. 158 УК РФ дополнена пунктом «г» следующего содержания: «с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ)». Статья 159.3 УК РФ предусматривает уголовную ответственность за мошенничество, совершенное с использованием электронных средств платежа.

Несмотря на разъяснения, изложенные в постановлении Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48, в данных нормах не учитывается конкретный способ хищения денежных средств с банковских счетов, что в свою очередь вызывает различия в их трактовке со стороны следствия, органов прокуратуры и суда.

Таким образом, при квалификации действий лица, связанных с хищением денежных средств потерпевшего с банковского счета последнего, внимательно изучаются фактические обстоятельства деяния, разграничивая действия квалифицируемые, как тайное хищение чужого имущества от совершенных посредством обмана или злоупотребление доверием.

Понимая остроту данного вопроса Следственный департамент МВД России, совместно с заинтересованными подразделениями МВД России во взаимодействии с Генеральной прокуратурой Российской Федерации, до конца текущего года разработает методические рекомендации «Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей».

Кроме того, в текущем году ожидается издание постановления Пленума Верховного суда Российской Федерации по внесению изменений в постановления пленумов Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое» и от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором планируется разъяснение имеющихся спорных моментов.

При возникновении вопросов определения места производства доследственных проверок и предварительного следования в целях защиты конституционных прав граждан, потерпевших от преступлений, и повышения оперативности их раскрытия, полноты возмещения причиненного им вреда, соблюдения разумного срока уголовного судопроизводства следственным подразделениям необходимо руководствоваться приказом МВД России от 03.04.2018 № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений». Данным приказом предписано проведение полной проверки и принятие решения о возбуждении уголовного дела по признакам преступлений, предусмотренных ст. 158, 159–159.3, 159.5, 159.6 УК РФ, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети «Интернет», в том органе внутренних дел Российской Федерации, в который поступило заявление о противоправном деянии.

Дальнейшая передача уголовного дела в соответствии со ст. 152 УПК РФ возможна только при условии выполнения всех возможных процессуальных действий по месту возбуждения уголовного дела и получения достаточных доказательств о совершении преступления на территории обслуживания другого территориального органа МВД России.

Мониторинг правоприменительной практики противодействия преступлениям в сфере информационных технологий, в целях повышения эффективности их раскрытия и расследования будет продолжен, данный вопрос находится на постоянном контроле руководства Следственного департамента МВД России.

Список литературы

1. Информационно-аналитические материалы Следственного департамента МВД России.
2. <https://мвд.рф/Deljatelnost/statistics> – статистика МВД России.

Гуськова Анна Борисовна¹,

*курсант факультета подготовки сотрудников полиции
Уфимского юридического института МВД России;*

Калимуллин Наиль Расфарович²,

*преподаватель кафедры управления в органах
внутренних дел Уфимского юридического института
МВД России*

АКТУАЛЬНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ РОБОТОТЕХНИКИ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В современном мире, все больше интегрируемого с цифровым пространством, вопросы применения искусственного интеллекта (далее – ИИ) и сфера разработки интеллектуальных технологий крайне важны и актуальны. Его развитие открывает множество новых возможностей в различных сферах жизнедеятельности человека. Искусственный интеллект способен осуществлять некоторые когнитивные функции, ранее считавшимся исключительно прерогативой людей, причем он делает это в существенно быстрее и качественнее. В ИИ отсутствует человеческий фактор, а значит, что при работе ИИ будет допускать меньше ошибок и погрешностей, которые может допустить человек из-за психофизиологического состояния. У ИИ, несомненно, имеется много положительных черт, что провоцирует его активное развитие и продвижение.

Технологии ИИ активно развиваются сегодня, в том числе из-за развития технологий машинного обучения (в первую очередь нейронных сетей), инфраструктур облачных вычислений, роевого интеллекта и т. д. и охватывают многие сферы жизни, в том числе критически важные, связанные с обороной страны, инфраструктурой городов, энергетикой и т. д. При этом общемировой остается проблема неразработанности нормативного правового и технического регулирования основ, условий и особенностей разработки, запуска в работу, функционирования, интеграции в другие области и контроля применения системы искусственного интеллекта. Лишь некоторые страны начинают заполнять нормативной правовой базой отдельные участки данного поля. К сожалению, Россия не находится в числе лидеров стран по применению ИИ и развитости правовой системы, регулирующих данную сферу, несмотря на актуальность и масштабность вопроса. Ситуация с регулированием на законодательном уровне усложняется тем, что до сих пор не ясно, что же представляет собой ИИ, как быстро и в какой степени могут эволюционировать данные системы в будущем и каким правовым статусом следует наделить ИИ и результаты его деятельности. Особенно стоит выделить вопрос о разграничении ответственности за действия интеллектуальных систем, т. е. нужно разобраться, кто ответит за результат деятельности ИИ: разработчик, владелец или сам ИИ (и как это реализовать)?

¹ © Гуськова А. Б., 2020.

² © Камуллин Н. Р., 2020.

Термин «искусственный интеллект» (artificial intelligence, или AI) сформулирован еще в 1956 г. Д. Маккарти. Он определял его как свойство роботов, компьютерных программ и систем выполнять интеллектуальные и творческие функции человека, самостоятельно находить и принимать решения.

Сегодня понятие «искусственный интеллект» одновременно изученная и дискуссионная научная категория и по-разному определяется учеными различных специальностей.

Наиболее интересны точки зрения специалистов в IT-сфере и правоведов. Так, по мнению Г. С. Осипова, ИИ предмет компьютерных наук, а создаваемые на ее основе технологии являются информационными технологиями, позволяющими совершать разумные рассуждения и действия с помощью вычислительных систем и иных искусственных устройств [1].

Существуют другие точки зрения на ИИ как на полностью или частично автономную самоорганизующуюся компьютерно- аппаратно- программную виртуальную или киберфизическую систему, наделенную способностями и возможностями мыслить, обучаться, принимать решения.

Технологии искусственного интеллекта активно развиваются сегодня и охватывают все большие сферы жизнедеятельности человека, становясь неотъемлемой частью повседневности. Еще 10 лет назад роботы могли выполнять относительно узконаправленные функции «помощников» в тяжелом физическом труде либо сборе и анализе больших объемов информации. К середине второго десятилетия XXI века уровень развития ИИ повысился и расширилась сфера его применения. Искусственная нейронная сеть моделирует работу нервной системы человека, ее способность к самообучению, а также способность действовать на основании предыдущего опыта, допуская все меньше ошибок. Сегодня нейронные сети могут выполнять широкий круг задач: распознавать лица, синхронизировать голоса, обучать людей и машины и т. д. Дальнейшее развитие технологий с ИИ может привести к повсеместному внедрению роботов в повседневную жизнь. На производстве уже используются роботы-погрузчики, в домашнем хозяйстве – роботы-пылесосы, на улицах разных стран начинают появляться беспилотные автомобили. По словам профессора РГУ нефти и газа им. И.М. Губкина А. Карцхия, человек оказался вовлеченным в период технологических революционных преобразований, происходящих одновременно: развитие интеллектуальных баз данных (Big Data), бурный рост облачных вычислений (cloud computing) и всеохватывающее распространение мобильности. Это сопровождается информацией, которая не могла бы быть обработана человеком, что стимулирует развитие ИИ [2]. Новейшие технологии нашли широкое применение в медицине, промышленности, образовании, агроиндустрии, дорожном движении и быту.

Правоохранительная деятельность активно внедряет результаты разработок в области ИИ. Имеется немало примеров различных программных решений с использованием ИИ, направленных на противодействие преступности и ее профилактику: анализ больших данных (Big Data), прогнозирование преступности, освобождение правоохранителей от рутинной деятельности (например, Межведомственная экспериментальная программа «Искусственный интеллект

в расследовании и оперативно-разыскной деятельности при совершении уголовных преступлений» (США, 2013–2016 гг.), обработка суперкомпьютером больших данных потокового видео с камер видеонаблюдения, распознавание изображения (например, фрагментов татуировок), контекстное распознавание ситуации (например, взрослый ведет упирающегося ребенка или драка на улице и т. д.), моделирование профилей преступников, системы поддержки принятия решений для различных служб [3] и т. д. Возрастающее количество реализуемых программ в правоохранительной деятельности подчеркивает перспективу и эффективность технологии.

Экспертное и научное сообщество предсказывают, что со стремительным развитием технологий ИИ и расширением сферы их применения, перед человечеством возникает новая проблема – правового регулирования, неразрывно связанная с этическими аспектами поведения. Робот является объектом права, ответственность за действия которого несет его владелец. Вопрос о необходимости формирования нормативно-правовой базы стоит на переднем плане во многих странах: в США, в странах Европейского союза, в Японии, в Китае и т. д. Глава компаний Tesla и SpaceX И. Маск называет ИИ основной угрозой для человечества, способной заменить людей на информационные алгоритмы, и настаивает на регулировании его развития. Для этих целей в 2015 г. под его руководством создана некоммерческая организация OpenAI [4].

В настоящее время комплексного регулирования ИИ не осуществляется ни в одной стране мира. В то же время ведутся поиски по обнаружению безопасных путей внедрения новых технологий в современную жизнь, важную роль в котором призвано играть именно правовое регулирование.

Если технический прогресс позволит создать так называемый «сильный», или универсальный, ИИ, то человечество столкнется с беспрецедентными юридическими проблемами. Современные правовые системы, существующие на основах антропоцентризма, заложенного в эпоху Возрождения, не позволяют человечеству сегодня решать возникающие в связи с развитием технологий проблемы.

Принципы регулирования при создании программ (в том числе и роботов), по мнению Р. Ибрагимова и Е. Сурагина, должны быть направлены на достижение двух глобальных целей [5]:

- 1) обеспечить защиту человека, его прав и основных свобод, а также защиту общества, государства и человечества;

- 2) способствовать развитию технического прогресса в области новейших информационных технологий и робототехники в той мере, в которой это не противоречит достижению первой цели».

В 2017 г. Европарламент принял резолюцию для Еврокомиссии, предложив признать специальный правовой статус электронной личности (electronic personhood) для сложных роботов, способных принимать самостоятельные решения. По мнению ряда парламентариев, это позволит возложить на роботов ответственность за причиненный вред, в первую очередь это касается беспилотных автомобилей. Предполагается также создание фонда по выплатам компенсаций пострадавшим в авариях с беспилотниками.

В России начата разработка законопроекта о робототехнике. Рассмотрением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р утверждена (ныне отменена распоряжением Правительства Российской Федерации от 12.02.2019 № 195-р «О признании утратившим силу распоряжения Правительства РФ от 28.07.2017 № 1632-р»). Программа «Цифровая экономика Российской Федерации», предполагала разработку правового регулирования для роботов, обладающих автономностью в своих решениях: дронов, беспилотных автомобилей, медицинских роботов и т. д. Это вызвано объективно необходимой потребностью. Сегодня, например, ведется создание беспилотного автомобиля для компании «КамАЗ».

Первая концепция российского закона о робототехнике была сформулирована основателем инвестиционного фонда «Grishin Robotics», председателем совета директоров «Mail.Ru Group» Д. Гришиным в 2016 г. Данная концепция предполагает создание реестра роботов и формулировании в законе разграничение ответственности их создателей и владельцев, что прояснит риски их инвесторов и создателей, а также потребителей. Концепция предусматривает внесение изменений в Гражданский кодекс РФ, в первой части которого должна появиться глава, регулирующая статус «роботов-агентов», т. е. роботов, зарегистрированных в специальном государственном реестре и предназначенных для участия в гражданском обороте. Данная регистрация добровольная. Если робот не зарегистрирован, за его действия будет отвечать владелец [6].

Концепция Д. Гришина подверглась критике со стороны известных российских юристов, именно председатель упраздненного в 2014 г. Высшего Арбитражного Суда Российской Федерации А. А. Иванов и сотрудник Института законодательства и сравнительного правоведения при Правительстве Российской Федерации С. Сеницын. Они указали на непроработанность концепции. Создание новой главы в ГК РФ влечет за собой признание роботов-агентов субъектами гражданского права, что предполагает наличие у них сознания и воли, необходимых для участия в гражданском обороте. Исходя из имеющегося уровня развития робототехники признание робота самостоятельным субъектом права, который без содействия людей способен участвовать в гражданском обороте, будет фикцией. К тому же, концепция рассматривает машины одновременно как объект и как субъект, что приводит к появлению двойственного статуса, а соответственно, и к появлению множества теоретических проблем (например, если у робота-агента есть имущество, то какое право на это имущество он имеет: право собственности или ограниченное поддерживает проекты по внедрению дронов вещное право?). По мнению А. А. Иванова, проблему правового регулирования отношений с участием роботов проще решить без признания их субъектами гражданского права. Достаточно признать их имуществом особого рода, подробно урегулировав правовой режим этого имущества [7].

Более того, в научном мире до сих пор нет общепринятых терминов «робот» и «искусственный интеллект», а то определение, которое дается в концепции, расплывчато и нечетко и при условии фиксации в законе не позволит достичь заявленных целей правового урегулирования.

На сложность формулирования определения робота как юридической конструкции обращают внимание авторы статьи «О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности». По мнению авторов статьи, создание законодательной базы осложняется тем, что фундаментальные понятия «личность» и «правосубъектность» исторически связаны с людьми, с физическими лицами.

Все это создает трудности при создании закона о робототехнике. Почему же важно заниматься формированием законодательной базы уже сейчас? Почему нельзя отложить ее создание на неопределенное будущее?

Дело в том, что многие технологии уже проникли в нашу жизнь, и отсутствие законодательных актов, регулирующих данную сферу, создает трудности во взаимодействии роботов и человека. Наглядным примером и одним из факторов, указывающих на необходимость урегулирования данной сферы, является создание нейропротезов- медицинских имплантов, вживляемых в нервную систему человека с целью возвращения двигательных или чувственных функций. Предположим, человек с нейропротезом держит ребенка и роняет его. Кто будет ответственен за причинение вреда: данный человек, производитель или же ученые-разработчики? Кроме того, связь с имплантом могла быть нарушена злоумышленниками через интернет.

Пока что законотворческие инициативы и в России, и в зарубежных странах не имеют четкой методологической основы. Принятая в 2017 г. Резолюция европейского парламента правил гражданского права в области робототехники больше напоминает «сборник предложений» по регламентации без формулирования основных принципов выбора правовых средств по защите. Концепция Д. Гришина тоже является довольно противоречивой, хотя и настаивает о необходимости комплексного урегулирования всей сферы ИИ, в отличие от европейских парламентариев.

Тем не менее необходимость разработки в России закона о робототехнике представляется неоспоримой с учетом развития уровня ИИ в передовых странах, что меняет структуру общества в мире в целом.

Важным этапом явилось принятие Национальной стратегии развития искусственного интеллекта на период до 2030 года Указом Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» [7]. Принятая стратегия может стать основой для выстраивания нормативно-правовой базы, разработки индикаторов эффективности и целевых показателей.

Поскольку проблематика ИИ сравнительно новая, можно выделить лишь общепризнанные проблемы, обсуждаемые в юридических доктринах.

1. Проблема отсутствия понятийного аппарата. При изучении какой-либо темы, нужно иметь четкое понимание терминов. Единого понимания термина «искусственный интеллект» нет и в различных сферах он понимается по-своему, причем каждое определение существенно отличается от других. То же можно сказать о терминах «робот», «робототехника», «кибернетика» и др.

2. Проблема реалистичного понимания уровня развития общественных отношений и информационной техники. Во многих странах проблема регулирования кибернетических систем не воспринимается в должной мере по причине

того, что у человечества отсутствует реальное понимание текущего развития как общественных отношений, так и самого искусственного интеллекта.

3. Проблема ответственности. Это самая большая и актуальная проблема среди юристов. Вопрос в том, кто должен отвечать за действия робота, особенно обладающего автономией, – сам робот, его создатель или владелец.

4. Проблема экзистенциальных рисков ИИ и проблем его урегулирования. Под данной проблемой подразумевается наличие угрозы разумной жизни на Земле или же нанесение необратимого вреда человечеству. Этот вопрос в большей степени находит обсуждение среди философов и журналистов, нежели юристов.

5. Проблема правосубъектности роботов-агентов.

Это лишь часть проблем, возникающих при прогрессивном росте информационных технологий, на самом деле их много больше. Полный перечень проблем, которые будут возникать с развитием искусственного интеллекта, требуя урегулирования, предусмотреть невозможно.

Принимая закон о регулировании ИИ и робототехнике, законодатель должен максимально учитывать все возможные проблемы, которые могут возникнуть при обеспечении безопасности использования роботов в потенциально сильно изменившейся окружающей человека среде.

Список литературы

1. Осипов, Г. Искусственный интеллект: Состояние исследований и взгляд в будущее / Г. Осипов // URL:<http://www.raai.org/about/persons/osipov/pages/ai/ai.html>.

2. Карцхия, А. Искусственный интеллект: «ларец Пандоры» или новая надежда? / А. Карцхия // Авторское право и смежные права. – 2017. – № 4 – С. 24.

3. Антонов, В. В. Метод формирования интегрированной системы поддержки принятия решений для руководителей подразделений и кадровых служб в органах внутренних дел / В. В. Антонов, Н. Р. Калимуллин // Сборник VII Всероссийской научной конференции «Информационные технологии интеллектуальной поддержки принятия решений (ITIDS'2019)». – 2019. – С. 180–183.

4. Higgins T. Elon Musk Lays Out Worst-Case Scenario for AI Threat // The Wall Street Journal. 2017. July 15.

5. Ибрагимов, Р. Право машин. Как привлечь робота к ответственности / Р. Ибрагимов, Е. Сурагина // Корпоративный юрист. – 2017. – № 11. – С. 10–17.

6. Филипова, И. А. Правовое регулирование искусственного интеллекта: регулирование в России, иностранные исследования и практика / И. А. Филипова // Государство и право. – 2018. – № 9. – С. 79–88.

7. Иванов, А. А. Мечтают ли андроиды об электроовцах? / А. А. Иванов // Закон.ru. URL: http://zakon.ru/blog/2017/2/15/mechtayut_li_androidy_ob_elektroovsah (дата обращения: 19.03.2020).

8. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собр. законодательства Рос. Федерации. – 2019. – № 41. – Ст. 5700.

Данилова Юлия Викторовна¹,

курсант института подготовки сотрудников

для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя;

Гончар Владимир Владимирович²,

заместитель начальника кафедры информационной

безопасности учебно-научного комплекса

информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

НЕКОТОРЫЕ ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

В настоящее время становится актуальной проблема совершения преступлений в сфере компьютерной информации. Еще в начале XXI в. источником угроз и опасностей становится глобальная киберпреступность. Данные, опубликованные международной службой по обеспечению безопасности в области киберугроз, говорят, что каждую секунду в мире подвергаются кибератаке 12 человек, а ежегодно в мире совершается около 556 млн преступлений в данной сфере. Ущерб от такого рода преступлений может быть очень велик. Для реализации своих преступных действий киберпреступники используют различные ресурсы, от вредоносных компьютерных программ, приложений, банковских технологий до троянских программ-шпионов, которые воруют деньги из электронных кошельков пользователей, например, со счетов пользователя в WebMoney, PayPal, Qiwi или Яндекс.Деньги. Так проявляется глобальная природа киберпреступности – ее транснациональный характер. Подготовка и реализация к совершению преступления осуществляются в одной стране, а ущерб причиняется другой. Платежные средства, которые существуют только в электронном виде, в основном используются в интернете.

Изучим вопросы, возникающие у сотрудников органов внутренних дел по уголовным делам данной категории и проанализируем основные проблемы, влияющие на результативность расследования киберпреступлений, а также рассмотрим способы ее решений.

Киберпреступление – это преступная деятельность, дестабилизация обстановки в обществе с целью нанесения морального, политического, экономического, культурного и других видов ущерба гражданину, организации или государства с помощью любого технического средства с доступом в интернет. Киберпреступления отличаются друг от друга в зависимости от целей совершения, а также по объектам, способам и средствам их реализации. Данные преступления чаще всего совершаются ради экономических целей (получение незакон-

¹ © Данилова Ю. В., 2020.

² © Гончар В. В., 2020.

ным путем денежных средств). Это понятие по смыслу шире, чем «компьютерная преступность», и более точно отражает весь спектр противоправных действий. Киберпреступления совершаются не только с помощью компьютеров, но и с использованием информационных технологий и глобальных сетей.

Кибербезопасность – это реализация различных мер по защите систем, программ и приложений от цифровых кибератак. Зачастую такие атаки направлены на получение доступа к закрытой (конфиденциальной) информации, ее уничтожение или вымогательство денежных средств у граждан и организаций, а также нарушение нормальной работы предприятий. Реализация специальных мер по обеспечению кибербезопасности очень проблемный вопрос. С каждым днем преступники становятся все более находчивыми и изобретательными, а компьютерных устройств существует огромное количество [1].

Высокие темпы развития современных информационных, финансовых, банковских и кредитных технологий дают возможность преступникам с помощью новых платежных механизмов получать доход при самых минимальных затратах и рисках быть привлеченными к уголовной ответственности [2].

Ужесточена санкция ст. 159.3 УК РФ, которая предполагает ответственность за мошенничество с использованием электронных платежных средств. Приведенные составы преступления отличаются способом и методом совершения преступления. Пункт «г» ч. 3 ст. 158 УК РФ предусматривает ответственность за тайное хищение денежных средств с банковского счета или электронных денежных средств. Например, лицо тайно похитило банковскую карту с пин-кодом, далее использовало устройство самообслуживания и с его помощью произвело снятие денег с банковского счета потерпевшего.

В соответствии с разъяснениями постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» в случае, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты, путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты, преступление квалифицируется, как мошенничество [3].

Главной целью сотрудников органов внутренних дел по уголовным делам о кражах электронных денежных средств, краж с банковских счетов и других видов киберпреступлений с помощью использования вредоносных компьютерных программ является установление всех данных о совершенном преступлении, сбор необходимой информации и доказательств виновности конкретных лиц.

Если проанализировать судебно-следственную практику, то можно заметить, что расследование киберпреступлений представляет особую сложность. Их особенность в многоэпизодности противоправной деятельности, разном характере периода совершения преступлений, частом затруднении в вопросах сотрудничества свидетелей и задержанных. Стоит отметить нежелание людей обращаться в правоохранительные органы за помощью, так как существуют различные методы совершения подобного рода преступлений. Например, злоумышленники могут за короткий промежуток времени обработать большое ко-

личество банковских карт, снимая при этом небольшие суммы денежных средств. В результате у следователей возникают трудности в работе с большим объемом процессуальных действий и оперативно-розыскных мероприятий.

Противодействие расследованию киберпреступлений, которые совершаются с помощью цифровых, банковских и иных технологий, понимается как совокупность различных неправомерных действий/бездействий участников уголовного процесса в отношении фактических данных, имеющих криминалистическую значимость. Эти деяния совершаются с помощью взаимодополняющих друг друга действий кредитных организаций и Банка России. Они обеспечены всеми необходимыми ресурсами. Эти ресурсы, в свою очередь, направлены на систематическую и комплексную реализацию банковских операций для того, чтобы воспрепятствовать предварительному расследованию [4].

Проводя анализ и оценку информации по данной теме, можно обнаружить определенную статистику в исследовании В. В. Лысенко. Для изучения преступлений, которые совершаются с использованием банковских, кредитных и иных технологий была запрошена оперативная информация с 83 органов предварительного расследования в системе ОВД за 2018–2019 гг. Было опрошено 420 сотрудников и 120 уголовных дел рассматриваемой категории. Полученные данные были проанализированы и обобщены. Был сделан вывод о том, что киберпреступления, в том числе кражи электронных денежных средств на практике квалифицируются по ст. 159–159.6, 172, 176, 183, 195–197, 272, 273 Уголовного кодекса Российской Федерации. Наиболее часто данные преступления совершаются при помощи кассовых и расчетных операций, а инструментом банковской деятельности выступают расчетные и кредитные банковские карты.

Статья 159.6 УК РФ появилась не так давно. Федеральным законом от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» УК РФ был дополнен данной статьей. В соответствии с новой нормой за хищения денежных средств и иного имущества посредством ввода, удаления, блокирования компьютерной информации и иного вмешательства в функционирование средств хранения, предусмотрена уголовная ответственность, которая должна защитить отношения собственности, имущественные интересы, охрану компьютерной информации и безопасность информационно-телекоммуникационных сетей.

На основании данных официальной статистики можно сделать вывод о том, что, несмотря на появление данной статьи УК РФ, ее редко применяют правоохранительные органы. При расследовании уголовных дел данной категории выявляются ошибки и недочеты, в результате чего они не доходят до судебного разбирательства.

Данные следственной практики показывают, что такие преступления, как хищения денежных средств с банковского счета, квалифицируются по п. «г» ч. 3 ст. 158 «Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств», ст. 159 «Мошенничество», ст. 159.3 «Мошенничество с использованием платежных карт» и по ст. 183 «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

Деятельность сотрудников правоохранительных органов по указанным выше делам часто не эффективна из-за нехватки у сотрудников необходимых зна-

ний и умений о вредоносных компьютерных программах и имеющихся научно-технических достижений в этой области. Для обеспечения защиты от противоправных действий в интернет-пространстве необходимо руководствоваться мнением граждан по данному вопросу, выяснить, понимают ли они угрозы возможных кибератак, какой информацией они обладают, и какие меры по сохранению своих личных персональных данных они используют.

Проведенные в области киберпреступлений социологические исследования указывают на то, что не все российские граждане способны защитить себя в интернет-пространстве. В 2013 г. было проведено исследование на психологическом факультете МГУ им. М.В. Ломоносова. Оппонентами стали около полутра тысяч подростков, студентов и их родителей, которые проживают в различных уголках нашей страны. Исследователи обнаружили у них недостаток знаний, умений и грамотности при использовании интернета. Подростки и их родители обладают высокой вероятностью столкновения с киберпреступниками из-за распространения информации о себе при общении с неизвестными людьми [5]. Таким образом, молодежь часто недооценивает негативные последствия, к которым может привести их чересчур активная деятельность в сети (скачивание программ, фильмов, музыки, общение в социальных сетях). Ученые считают, что информировать о киберпреступности и правилах пользования ресурсами необходимо не только сотрудников органов внутренних дел, но и обычных граждан, которые являются потенциальными жертвами [6].

Е. С. Шевченко провел опрос среди следователей (респондентами стали 185 следователей и 25 дознавателей.). После обобщения данных был сделан вывод о том, что 95 % имеют юридическое образование и лишь 5 % опрошенных получили дополнительную специальную подготовку (образование по специальности «информатика и вычислительная техника»). 60 % сотрудников оценивают уровень владения персональным компьютером, как «среднестатистический пользователь», 40 % – «продвинутый». Около 80 % опрошенных следователей получают необходимые знания в области компьютерных технологий самостоятельно, т. е., занимаясь самообразованием, 20 % – с помощью курсов повышения квалификации для сотрудников правоохранительных органов и 5 % – платные коммерческие курсы или специальное образование. Таким образом, из вышеприведенной статистики можно сделать вывод о слабой подготовке сотрудников ОВД в области компьютерных и информационных технологий.

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;
- работать на предупреждение киберпреступлений, так как они очень 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. Имеются основания полагать, что данный вид преступности стремительными темпами перерастает в международный. Об этом свидетельствуют 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. https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html.
2. Информационное письмо Банка России от 11.03.2016 № ИН-017-45/12 Памятка «Об электронных денежных средствах».
3. <https://procrf.ru/region/1-generalnaya-prokuratura-rf.html>.
4. Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 02.08.2019) «О национальной платежной системе» (с изм. и доп., вступ. в силу с 15.09.2019).
5. Карпова, Д. Н. Киберпреступность: глобальная проблема и ее решение / Д. Н. Карпова. – М., 2014.
6. Мешков, М. В. Досудебное соглашение о сотрудничестве: проблемы и перспективы / М. В. Мешков, В. В. Гончар // Закон и право. – М., 2011.

*Дутикова Анастасия Александровна¹,
слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя;*

*Галиев Денис Вадимович²,
преподаватель кафедры специальных информационных
технологий учебно-научного комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя*

ИНФОРМАЦИЯ, ИЗВЛЕЧЕННАЯ С NAS ХРАНИЛИЩ, КАК ЦИФРОВОЕ ДОКАЗАТЕЛЬСТВО ПРИ РАССЛЕДОВАНИИ И РАСКРЫТИИ КИБЕРПРЕСТУПЛЕНИЙ

В рамках расследования киберпреступлений немаловажную роль играют не только данные, обнаруженные непосредственно на средствах совершения преступления, но и их архивные копии. Так, например, архивные копии могут помочь восстановить картину событий или же получить совершенно новые доказательства, сокрытые преступником. В связи с этим возникают задачи исследования файловых хранилищ NAS.

Актуальность данной темы продиктована практикой предварительного расследования, поскольку в судебные лаборатории поступают такие цифровые носители информации, и обязательным условием экспертного исследования является извлечение удаленной информации для дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний. В рамках следственных действий у специалистов возникает проблема с поиском NAS хранилищ, ведь на данный момент имеются хранилища и в мобильном исполнении, и никто даже не задумывается о таком варианте непосредственно при осмотре места происшествия или обыске. Поэтому важно исследовать мобильные NAS хранилища.

Одним из типов хранения данных является сетевое хранилище NAS. Проведенный анализ позволил сделать вывод, что NAS – это устройство, которое имеет свой собственный процессор, оперативную память, хранилище и подключение к сети, также немаловажно, что данные устройства имеют собственную операционную систему.

Настройка NAS проста, что делает его отличным выбором для домашних сетей. А мобильные варианты сетевых хранилищ целесообразно относить не только к информационным технологиям, используемым во благо общества и государства, но и к средствам сокрытия цифровых доказательств в расследуемом преступлении, ведь зачастую их размещение нетривиально и не позволяет правоохранителям в полной мере зафиксировать следовую картину.

¹ © Дутикова А. А., 2020.

² © Галиев Д. В., 2020.

Непосредственно сам процесс получения информации с NAS хранилищ имеет свои особенности. В рамках выполнения исследования был проведен эксперимент. Смоделировано NAS устройство средствами виртуализации. За основу взят один из самых популярных дистрибутивов для реализации NAS хранилища – Nas4Free. Доступ к хранилищу осуществляется через веб-интерфейс.

В виртуальной машине был создан виртуальный диск, отформатирован в файловую систему UFS, настроены необходимые службы и сетевые настройки и несколько общих папок, в них перенесены файлы разных форматов. Виртуально были изъят диски и смонтирован образ.

Выявление в памяти данных устройств криминалистически значимой информации подтверждает необходимость освоения компьютерным экспертом методик, необходимых для целенаправленного поиска, фиксации, изъятия указанных объектов, а также извлечения информации, имеющей значение для уголовного дела. Многие зависят и от возможностей программных и программно-аппаратных комплексов, находящихся в экспертно-криминалистических подразделениях, которые позволяют в минимальные сроки извлечь важную информацию из памяти устройств. Эксперт проводит исследования объективно, на строго научной и практической основе, в пределах соответствующей специальности, всесторонне и в полном объеме [1].

Для полноты исследования эксперту необходимо рассматривать информацию среди удаленных данных. Можно предположить, что были сбои и ошибки, при которых данные могут быть удалены, либо подозреваемый просто стер следы на месте преступления. К счастью, существует программное обеспечение, позволяющее восстановить информацию с подобных устройств, например UFS Explorer. Но прежде чем восстановить информацию, необходимо указать начало раздела (63 по умолчанию) и размер раздела.

Чтобы найти размер раздела, надо его рассчитать по формуле:

(Число блоков * размер блока) + 1 сектор = общее число секторов в разделе.

Размер блока в разделе расположен по смещению 24 от начала сектора и имеющих длину 4 байта. Это значение равно 02 00 00 00 или 2 в формате с порядком следования байтов начиная с младшего. Размер блока по умолчанию – 1024 байта (2 сектора). Значение 2 указывает, что размер блока равен 4096 байт. Таким образом, размер блока в разделе равен 8 секторам.

Затем следует найти размер блока (в секторах). Эти данные длиной 4 байта находятся по смещению 4 относительно начала сектора и хранятся в формате с порядком следования байтов от младшего к старшему. Данные шестнадцатеричные значения переводим в десятичное в порядке от младшему к старшему. Получается число блоков (кластеров) в разделе.

Переводим 5E21016 в десятичную систему:

$5E21016 = 5 \cdot 164 + 14 \cdot 163 + 2 \cdot 162 + 1 \cdot 161 + 0 \cdot 1 = 38555210$.

Теперь подставляем найденные данные в формулу:

$(385\,552 * 8) + 1 = 3\,084\,417$ секторов в разделе.

Вносим полученные необходимые данные во всплывающее окно и нажимаем применить. Затем устанавливаем режим восстановления с технологией In-

tellRAW, которая анализирует список индексных узлов файловой системы. Через некоторое время выводится список восстановленных файлов.

Таким образом, из NAS серверов эксперт может извлечь множество данных, которые могут служить цифровым доказательством. В свою очередь, цифровое доказательство – это информация, которая хранится, обрабатывается и передается в электронной форме, устанавливающая наличие или отсутствие обстоятельств, изобличающего доказательства в процессе предварительного расследования или судебного производства.

Список литературы

1. Федеральный закон Российской Федерации от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».
2. Булыжкин, А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения / А. В. Булыжкин, В. Ф. Васюков // Российский следователь. – 2016. – № 6. – С. 3–8.
3. Гаврилин, Ю. В. Электронные носители информации в уголовном судопроизводстве / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2017. – № 4 (44). – С. 45–50.

Евлашкина Александра Владимировна¹,
*слушатель института подготовки
сотрудников для органов предварительного расследования
Московского университета МВД России имени В. Я. Кикотя;*

Кардашевская Марина Владимировна²,
*профессор кафедры криминалистики
Московского университета МВД России имени В.Я. Кикотя,
доктор юридических наук, профессор*

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ОТДЕЛЬНЫХ ВИДОВ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

С большим развитием компьютерных технологий и ростом популярности безналичной формы расчета, банковских пластиковых карт растет и количество мошеннических операций с использованием банковских карт. Развиваются не только положительные стороны нашей жизнедеятельности, но и преступность не стоит на месте. Все типы мошенников приобретают больше знаний и умений, навыков в банковской и компьютерной сфере, изобретают различные способы хищения, поэтому нужно быть бдительнее чем когда-либо, научиться распознавать и предотвращать такие преступные посягательства.

Рассмотрим способы совершения мошенничества в сфере компьютерной информации и личность, совершающая преступления такого рода.

В действующий Уголовный кодекс Российской Федерации Федеральным законом от 29.11.2012 № 207-ФЗ была введена ст. 159.6, как отдельный состав, предусматривающий ответственность за мошенничество в сфере компьютерной информации. В связи с глобальным ростом мошенничества в сфере компьютерной информации, а именно с банковских карт, увеличиваются опасность и распространенность преступлений, которые посягают на нормальную деятельность компьютерных автоматизированных систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные с имущественным ущербом для граждан.

Мошенничество отличается большим количеством способов совершения данного преступления. Поэтому и мошенничество в сфере компьютерной информации не стало исключением. Главное отличие данного вида мошенничества в том, что при мошенничестве, связанном с компьютерной информацией всегда исключается непосредственный контакт злоумышленника и потерпевшего, информационные технологии дают ряд дополнительных возможностей для преступника, это и позволило выделить данную категорию преступлений в отдельный состав (ст. 159.6 УК РФ).

¹ © Евлашкина А. В., 2020.

² © Кардашевская М. В., 2020.

Существует множество различных классификаций совершения данного вида мошенничества. Наиболее подробное исследование при решении данного вопроса провел В. В. Коломинов, который предложил такую квалификацию:

- противозаконное приобретение регистрационных сведений, которые позволяют обрести доступ к собственности;
- организация сайтов с размещением на них ложных сведений о вероятности приобретения сверхкрупных прибылей для введения в заблуждение потенциальных жертв;
- похищение денежных средств путем взламывания электронных кошельков;
- рассылка писем-оферт об инвестировании бизнеса путем пополнения счетов денежными средствами;
- рассылка спам-писем, которые содержат вредоносные программы, на электронную почту жертв;
- приобретение денег через виртуальные интернет-магазины;
- создание благотворительных акций через интернет;
- похищение путем применения вредоносного программного обеспечения или сайтов – двойников номеров пластиковых карт пострадавших [1].

Данный перечень не исчерпывающий, так как в современное время компьютерные технологии имеют все большее развитие и, соответственно, будут развиваться и способы совершения таких категорий мошенничества.

В настоящее время существует множество видов мошенничества с применением банковских карт. Наиболее распространенные способы:

Скимминг – похищение реквизитов пластиковых карт с помощью устройства «скиммер». Такое устройство снимает с магнитной полосы карты все данные, а миниатюрная камера, которая располагается на панели для введения пин-кода, или прозрачная пленка позволяет преступнику получить код доступа к данной банковской карте.

Фишинг – создание поддельного сайта банка, после чего мошенник делает рассылку писем или СМС-сообщений клиентам данного банка, прося их перейти на поддельный сайт, на котором он впоследствии, просит клиента указать все данные его карты.

Вишинг – аналог фишинга, но средством для махинаций становится телефон. Так, жертва принимает звонок от «служащего» службы безопасности банка, который заявляет о попытке противозаконного списания денежных средств со счета. Мошенник просит перезвонить по указанному им номеру сотового телефона, что и производит потерпевший. Указанный номер подставной, позвонив по нему, у пострадавшего запрашивают данные его карты или предлагают послать SMS-сообщение со сведениями о карте. [2]

Траппинг – установление на банкоматы особого устройства, удерживающего банковскую карту, вследствие чего она заклинивается. Пока потерпевшее лицо обращается за помощью к сотрудникам банка или едет в отделение банка, злоумышленник убирает устройство из банкомата, спокойно забирает карту и распоряжается денежными средствами на ней по своему усмотрению.

Использование поддельных банкоматов – приобретение фальшивого банкомата. Отличие состоит в том, что «подделка» существенно легче, поскольку внутри нее ничего нет, а также преступники меняют программный интерфейс,

удаляя лишние, с их точки зрения, функции, например, отпуск наличных. Держатель карты вставляет карту в «подделку», вводит ПИН-код. Но при попытке совершить операцию, происходит ошибка «При совершении операции произошла ошибка, дождитесь выдачи карты». Потерпевший получает карту обратно и идет к другому банкомату. Но данные карты, введенные держателем и скопированные преступником с магнитной ленты банковской карты, сохранились на механизме «подделки» [2].

Одним из главных признаков способа совершения данного вида мошенничества является его значительный размер, что подтверждается судебной практикой.

Следующий элемент криминалистической характеристики – *личность преступника*, которая занимает центральное место в курсе криминалистики. К ярко выраженной типичной черте нынешней криминальности относится повышение количества таких видов правонарушений, имеющих интенсивное корыстолюбивое устремление, а также носящих сильно проявленный умственный характер.

Проведем сравнительные черты личности преступника – мошенника и мошенника в сфере компьютерной информации. Итак, изучение личности мошенников дает нам понятие об их узкой специализированной направленности, высоком профессионализме, широком кругозоре и об их правовых знаниях. От личности преступника зависят такие факторы, как: сам объект преступления, место его совершения, способ совершения, его мотивы, причины и условия совершения преступления, его сокрытие, различные следственные ситуации и дальнейшие следственные действия сотрудников и т. д.

Личность преступника важнейший элемент криминалистической характеристики преступления, значимые аспекты которых социально-демографические и нравственно-психологические аспекты личности преступника.

Личность мошенника – неотъемлемое направление деятельности следователя, так как характеристика типичной личности мошенника дает хорошую возможность сузить круг подозреваемых лиц, среди которых может находиться конкретный преступник.

Так в чем же отличие преступников, орудующих в компьютерной сфере? Группы лиц, совершающих преступления в компьютерной сфере:

– Хакеры (англ. Hack) – это профессиональные взломщики защит компьютерных программ, а также создатели различных компьютерных вирусов, главное отличие которых их высокий профессионализм в сочетании с компьютерным фанатизмом.

Хакеры делятся на конкретные специализации, на языке компьютерных преступников они называются:

1) *крякеры* (англ. Crack) – IT-специалист, который взламывает системы защиты (защит программного обеспечения), занимается созданием или доработкой «кряков», взламывающих программное обеспечение и другое. Кряки – это специальные программы, позволяющие осуществить взлом любого программного обеспечения;

2) фризеры (англ. Phreaker) – люди, которые занимаются фрикенгом. Это так называемые люди, которые используют в своих неправомерных действиях телефон с целью оказания психологического воздействия на потерпевшего;

3) кардеры (англ. Carder) – люди, которые оплачивают свои расходы с помощью чужих кредитных и банковских карт;

4) сетевые хакеры – очень квалифицированный IT-специалист, человек, который понимает все тонкости работы различных программ ЭВМ и электронных сетей.

Психически больные лица, страдающие компьютерными фобиями (профессиональными информационными заболеваниями) и уничтожают или повреждают компьютерную технику даже без наличия преступного умысла с частичной или полной потерей контроля своих действий.

Криминальные профессионалы – различные преступные группировки, преследующие, к примеру, политические цели, а также лица, занимающиеся промышленным шпионажем и группировки, которые стремятся к большой наживе. Такие преступления обычно носят серийный и многоэпизодный характер, совершаются неоднократно и обязательно с применением мер по сокрытию преступления, иногда, характерным только для конкретной группировки.

Итак, данному типу личности присущи высокий уровень интеллектуального развития, сильный профессионализм и фанатичность, нестандартность мышления, изобретательность, развитая и богатая фантазия, а также особенная скрытность.

В настоящее время существует необходимость создания и разработки систем рекомендаций по расследованию мошенничества и, особенно, мошенничества в сфере компьютерной информации, совершение которого характеризуется ярко выраженными личностными свойствами мошенников. Такие рекомендации смогли бы грамотно дополнять уже существующие алгоритмы расследования отдельных видов преступлений.

Список литературы

1. Коломинов, В. В. О способе совершения мошенничества в сфере компьютерной информации / В. В. Коломинов // Человек: преступление и наказание. – 2015. – № 3. – С. 145–149.
2. Танасейчук, Я. В. Мошенничество с использованием пластиковых карт / Я. В. Танасейчук // Право: современные тенденции : материалы V Междунар. науч. конф. (г. Краснодар, февраль 2018 г.). – Краснодар : Новация, 2018. – С. 60.
3. Третьяк, М. Проблемы понимания способа компьютерного мошенничества в судебной практике / М. Третьяк // Уголовное право. – 2015. – № 5. – С. 109–110.

Ефременко Максим Андреевич¹,
старший преподаватель кафедры
физической подготовки учебно-научного комплекса
специальной подготовки
Московского университета МВД России имени В.Я. Кикотя,
кандидат педагогических наук

РАЗВИТИЕ СИЛЫ И ВЫНОСЛИВОСТИ КУРСАНТАМИ И СЛУШАТЕЛЯМИ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ В УСЛОВИЯХ САМОИЗОЛЯЦИИ

Современная непростая эпидемиологическая ситуация в мире, в том числе и в Российской Федерации, неизбежно привела к ограничительным мерам во многих областях жизни каждого человека. Коснулось это и деятельности МВД России. Для недопущения распространения коронавирусной инфекции (COVID-19) учебные заведения МВД России перешли на дистанционный режим обучения. Таким образом, данные меры помогли решить проблему необходимости ездить в общественном транспорте и непосредственно заниматься в учебных аудиториях (поскольку вирус передается воздушно-капельным путем) в целях защиты здоровья постоянного и переменного состава университетов, а также членов их семей.

Физическая подготовка – неотъемлемая часть профессиональной подготовки курсантов и слушателей образовательных организаций МВД России. Данный вид подготовки к профессиональной деятельности определяется их соответствующей физической развитостью, оптимальным функциональным состоянием организма, психологической подготовленностью и требуемым уровнем развития двигательной подготовленности [1]. Все это способствует эффективному выполнению служебно-боевых задач, которые возлагаются на сотрудников практических подразделений. К сожалению, в вышеупомянутых условиях стала практически невозможной специальная физическая подготовка под руководством преподавателей и тренеров. Выход из данной ситуации самостоятельная подготовка курсантов и слушателей как часть общей подготовки, ее основная цель – овладение изучаемых навыков и умений, без участия преподавателя, но на основе его рекомендаций, в определенное поставленное время.

Самостоятельная подготовка курсантов и слушателей признана решить следующие поставленные задачи:

- 1) изучение нормативной правовой базы, учебных пособий, рекомендаций для глубокого усвоения теоретических основ физической подготовки;
- 2) исследование собственной имеющейся литературы, использование информационных технологий, например интернета, с целью развития умения самостоятельно нахождения материала и использования его;
- 3) развитие целеустремленности и силы воли, воспитание инициативности и находчивости для непосредственного изучения имеющихся материалов и применения его.

¹ © Ефременко М. А., 2020.

На самостоятельных занятиях слушатели формируют и совершенствуют навыки боевых приемов борьбы, самостоятельные занятия возможны при условии владения слушателями навыками приемов страховки и самостраховки. Другое обязательное условие проведения безопасного самостоятельного занятия специальная разминка [2].

В условиях самоизоляции курсанты и слушатели вынуждены ограничиться местом проживания при выполнении физических упражнений. Развитие силы в таком случае можно выполнять и без использования какого-либо специального оборудования. Домашние упражнения с использованием различных безопасных, простых и легко выполняемых упражнений хорошо подходят для того, чтобы избежать заражения и поддержать уровень физической подготовки. Такие формы упражнений включают упражнения на укрепление мышц, упражнения на равновесие и контроль, упражнения на растяжку или их комбинацию. Примеры домашних упражнений включают в себя хождение по дому и в магазин по мере необходимости, подъем и перенос продуктов, чередование выпрямлений в ногах, подъем по лестнице, приседания и отжимания [3].

Самостоятельная индивидуальная подготовка требует определенной силы воли у курсантов и слушателей. Помимо разработанной индивидуальной программы, возможно проведение групповых тренировок с использованием информационных технологий, «ZOOM», «Whatsapp», где преподаватель в назначенное время вместе с курсантами учебного взвода выполняет комплекс упражнений в режиме видеоконференции. К сожалению, регулярному проведению таких видов занятий препятствуют возможные неудобства в материально-техническом и психологическом аспектах, и у учащихся, и у преподавателей (отсутствие технического оборудования и нужного спортивного инвентаря, жилищные условия, семейные проблемы).

Наиболее эффективной себя показала дистанционно-индивидуальная работа. Она заключается, во-первых, в подробном описании комплекса упражнений, в котором есть конкретное количество выполнений и подходов, а также описана техника выполнения. Данный комплекс разрабатывается непосредственно преподавателем. Во-вторых, при получении данных материалов курсанту нужно не только внимательно их изучить и выполнить, но и зафиксировать это выполнение на видео с целью непосредственной оценки и контроля со стороны преподавателя.

Физическая активность и методы расслабления, помогают сохранять спокойствие и защищать здоровье. Таким образом, в период пандемии организация дистанционного обучения требует от преподавателей разработки новых форм и методов работы с курсантами и слушателями образовательных организаций МВД России.

Список литература

1. Алдошин, А. В. Физическая подготовка как неотъемлемая составная часть профессиональной подготовки курсантов и слушателей образовательных организаций МВД России / А. В. Алдошин, С. А. Моськин // Актуальные проблемы физической культуры и спорта курсантов, слушателей и студентов. – 2016.

2. Зайцева, Н. В. Пути реализации дисциплины «физическая культура» в период самоизоляции студентов вуза / Н. В. Зайцева, Ю. В. Кульчицкая // Развитие науки, национальной инновационной системы и технологии : сб. науч. трудов по материалам Междунар. науч.-практ. конференции. 13 мая 2020 г. – С. 126–133.

3. Кунаева, К. А. Мотивация к занятиям физической культурой и спортом у курсантов образовательных организаций МВД России / К. А. Кунаева // Совершенствование физической, огневой и тактико-специальной подготовки сотрудников правоохранительных органов. Физическая подготовка и спорт : сб. статей. – Орел, 2015. – С. 210–212.

4. Муслимов, Р. А. Организация самостоятельной физической подготовки слушателей образовательных организаций МВД России / Р. А. Муслимов // Концепт. – 2014. – С. 21–25.

5. Хоружев, А. Г. Программы самостоятельных занятий физической культурой в соответствии с группой физической и функциональной подготовки / А. Г. Хоружев // Известия высших учебных заведений. Уральский регион. – 2015. – № 2. – С. 110–114.

Иванов Иван Владимирович¹,
генеральный директор компании «Психодинамика»,
доктор технических наук;

Иванов Владимир Алексеевич²,
начальник отдела Управления делами Президента Российской Федерации,
доктор военных наук, профессор,
член-корреспондент Академии криптографии Российской Федерации;

Егоров Максим Викторович³,
аспирант

СНИЖЕНИЕ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ ДЕКОДИРОВАНИЯ СИГНАЛОВ С ТУРБОКОДИРОВАНИЕМ В КАНАЛАХ СВЯЗИ С ПАМЯТЬЮ

Одним из наиболее эффективных методов обеспечения достоверности передачи сообщений в каналах связи с памятью является применение методов помехоустойчивого кодирования, базирующихся на турбокодировании [1]. Декодирование турбокодов (ТК) представляет собой итеративную процедуру, каждая итерация основана на обмене информацией о достоверности символов двух «простых» помехоустойчивых кодов, формирующих ТК, что позволяет постепенно снизить уровень априорной неопределенности относительно статистических свойств потока ошибок и исправлять большее (относительно классических кодов) количество ошибок в смысле их отношения к избыточности кодов.

Основная проблема использования ТК на практике – высокая вычислительная сложность процесса их декодирования, обусловленная необходимостью выполнения нескольких (иногда более десятка) итераций, включающих процедуры декодирования и процедуры оценивания надежностей символов кода. Современный уровень развития аппаратных средств цифровой обработки сигналов недостаточен для реализации процессов декодирования ТК настолько, чтобы обеспечить получение на их основе потенциально возможного эффекта при приемлемых на практике затратах на их практическую реализацию.

Одним из перспективных направлений решения вышеуказанной проблемы является подход, основанный на использовании новых методов оценивания статистических свойств потока ошибок в каналах связи с ТК, позволяющий получать пригодные (несмещенные, состоятельные и эффективные) [2] оценки параметров марковского случайного процесса (значений элементов матриц переходных вероятностей) на основе обработки выборок ограниченного объема с пропусками данных.

¹ © Иванов И. В., 2020.

² © Иванов В. А., 2020.

³ © Егоров М. В., 2020.

В [3] предложен метод оценивания статистических характеристик источника ошибок по выборке ограниченного объема с пропусками, основанный на анализе свойств двоичной цепи Маркова (ЦМ), основанный на том, что распределение финальных вероятностей двумерной двоичной случайной величины (ДСВ), задаваемой односвязной ЦМ, полностью определяется распределением финальных вероятностей одномерной ДСВ и значением любого из элементов матрицы переходных вероятностей. При этом границы области значений переходных вероятностей двоичной ЦМ, определяются выражением

$$p(0/0)_{\min} = \begin{cases} 0 & \text{при } p(0) < 0,5 \\ \frac{p(0) - p(1)}{p(0)} & \text{при } p(0) \geq 0,5 \end{cases} \quad (1)$$

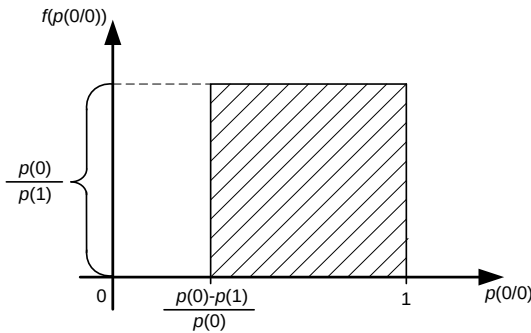


Рис. 1. Плотность распределения переходной вероятности $p(0/0)$ для односвязной цепи Маркова при $p(0) \geq 0,5$

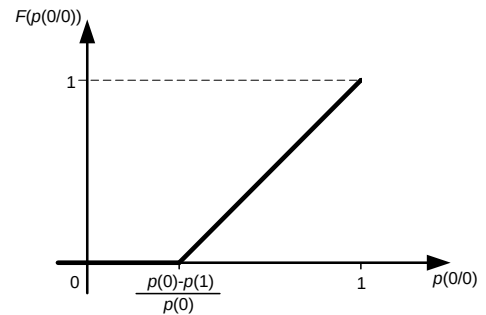


Рис. 2. Функция распределения переходной вероятности $p(0/0)$ для одношаговой цепи Маркова при $p(0) \geq 0,5$

Полагая плотность распределения переходной вероятности равномерной на интервале с границами, равными границам области значений, получены плотности и функции распределения переходной вероятности, представленные на рис. 1 и 2, и соответствующие им выражения:

$$p(0) \geq 0,5: f(p(0/0)) = \begin{cases} \frac{p(0)}{p(1)} & \text{при } \frac{p(0) - p(1)}{p(0)} \leq p(0/0) \leq 1 \\ 0 & \text{при } p(0/0) < \frac{p(0) - p(1)}{p(0)} \end{cases} \quad (2)$$

$$p(0) > 0,5: F(p(0/0)) = \begin{cases} 0 & \text{при } p(0/0) < \frac{p(0) - p(1)}{p(0)} \\ 1 - \frac{p(0)}{1 - p(0)} (1 - p(0/0)) & \text{при } \frac{p(0) - p(1)}{p(0)} \leq p(0/0) \leq 1 \end{cases} \quad (3)$$

Так как математическое ожидание равномерно распределенной случайной величины является ее пригодной оценкой, выражение для оценки переходной вероятности $p(0/0)$ имеет вид:

$$\hat{p}(0/0) = 1 - \frac{p(1)}{2p(0)} \text{ при } p(0) \geq 0,5 \quad (4)$$

Выражения для оценок переходных вероятностей $p(0/1)$, $p(1/0)$ и $p(1/1)$ имеют вид:

$$\hat{p}(1/0) = 1 - \bar{p}(0/0) = 1 - \frac{p(0/0)_{\min} + 1}{2} = \frac{1}{2} - \frac{p(0/0)_{\min}}{2}, \quad (5)$$

$$\hat{p}(0/1) = \frac{p(10)}{p(1)} = \frac{p(1/0)\bar{p}(0)}{1 - \bar{p}(0)} = \frac{(1 - \hat{p}(0/0))\bar{p}(0)}{1 - \bar{p}(0)} = \frac{\left(1 - \frac{p(0/0)_{\min} + 1}{2}\right)\bar{p}(0)}{1 - \bar{p}(0)}, \quad (6)$$

$$\hat{p}(1/1) = 1 - p(0/1) = 1 - \frac{\left(1 - \frac{p(0/0)_{\min} + 1}{2}\right)\bar{p}(0)}{1 - \bar{p}(0)}. \quad (7)$$

Использование указанного метода на первом (предварительном) этапе декодирования турбокодов, согласно результатам проведенного вычислительного эксперимента, позволяет значительно (в среднем в 2,3 раза при отношении сигнал/шум 5 дБ) снизить количество требуемых для сходимости результатов декодирования количество итераций.

Список литературы

1. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса. – М. : Техносфера, 2005.
2. Юсупов, В. М. Статистические методы обработки результатов наблюдений / [В. М. Юсупов и др.]. – Министерство обороны СССР, 1984.
3. Конышев, М. Ю. Идентификация модели двоичного марковского процесса по выборке ограниченного объема / [М. Ю. Конышев и др.] // Радиолокация, навигация, связь : сб. докладов 18-й Международной конференции (RLNC). Т. 1. – Воронеж : Изд. ВГУ, 2012. – С. 22–33.

Иванов Иван Владимирович¹,
генеральный директор компании «Психодинамика»,
доктор технических наук;

Иванов Владимир Алексеевич²,
начальник отдела Управления делами Президента Российской Федерации,
доктор военных наук, профессор,
член-корреспондент Академии криптографии Российской Федерации;

Шаповалов Сергей Леонидович³,
доцент кафедры защиты информации от НСД
Краснодарского высшего военного училища
им. С.М. Штеменко, кандидат военных наук, доцент

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ПОДАВЛЕНИЯ ВИРУСНЫХ ЭПИДЕМИЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

Анализ источников [1,2] показал, что современные компьютерные вирусы классифицируются по способу распространения, особенностям алгоритма работы, деструктивным возможностям и другим признакам. С точки зрения потенциальной возможности возникновения и развития ЭКВ наиболее опасно заражение особым классом вируса – сетевым червем [1,2], который способен не только заражать файлы операционной системы, но и распространяться от узла к узлу по всей компьютерной сети.

По методу активации все черви можно разделить на две большие группы: неавтономные и автономные. При распространении червей первой группы требуется активное участие пользователя, например открытие писем электронной почты или активация приложений. При этом используется ряд методов социального инжиниринга (обман, заманивание, рекламные трюки, поздравление с праздником и др.), побуждающих пользователя к активации вируса. Вторая группа червей распространяется независимо от пользователя, используя для этого уязвимости операционных систем, служб, протоколов, или бреши в системе безопасности компьютерной сети. Вирусы данной группы наиболее опасны и зачастую вызывают глобальные эпидемии.

Исторически первая эпидемия компьютерного вируса зафиксирована в 1988 г. и вызвана «червем Морриса». Распространение указанного вируса привело к массовому заражению компьютеров пользователей и причинило немалый материальный ущерб. Однако усиленное изучение проблемы распространения сетевых вирусов и эпидемий компьютерных вирусов началось после появления вирусов Code Red, Nimda, Klez, Slammer и др. (начиная с 2001 г.).

¹ © Иванов И. В., 2020.

² © Иванов В. А., 2020.

³ © Шаповалов С. Л., 2020.

С тех пор основные исследования в области подавления эпидемий компьютерных вирусов были сфокусированы на следующих направлениях:

- моделирование процесса распространения сетевых вирусов, с позиций получения инструмента определения эффективных средств защиты (SI, SIR, PSIDR);
- исследование техник сканирования IP-адресов узлов компьютерной сети, используемых сетевыми вирусами;
- исследование механизмов распространения сетевых вирусов и определение показателей развития эпидемии;
- исследование превентивных механизмов защиты от эпидемий компьютерных вирусов.

Первоначальный анализ моделей развития ЭКВ показал, что основным направлением в данной области является использование аппарата эпидемиологии, заимствованного из биологии и медицины [3], поэтому основные исследования были направлены на анализ классических моделей эпидемий. Свойство автономности сетевых червей позволяет моделировать их распространение посредством динамических моделей, как детерминированных, так и стохастических. Однако большинство моделей все-таки детерминированные, поскольку влияние случайных факторов в компьютерных сетях большого размера незначительно.

Самые распространенные модели: SI, SIR, PSIDR. Они основаны на том, что узлы сети находятся в различных состояниях: S – уязвимом, I – зараженном, R – невосприимчивом, D – обнаруженном (соответственно названиям моделей). Их суть заключается в аналитическом представлении зависимости количества узлов находящихся в данных состояниях в виде дифференциальных уравнений и систем ДУ. Например, аналитическая форма модели SI имеет вид, представленный в (1):

$$\frac{di}{dt} = \beta \cdot (1-i) \cdot i, \quad (1)$$

где i – доля зараженных узлов в момент времени t , β – частота заражения.

На рис. 1 показан график зависимости (1), полученный по результатам моделирования сетевого вируса Code Red при следующих исходных данных: $i_0=10$, $N=36000$, $\beta=358$ мин⁻¹.

Эпидемия в принятой модели полностью определяется двумя параметрами: скоростью размножения червя (β) и начальной зараженностью рассматриваемой сети (i_0).

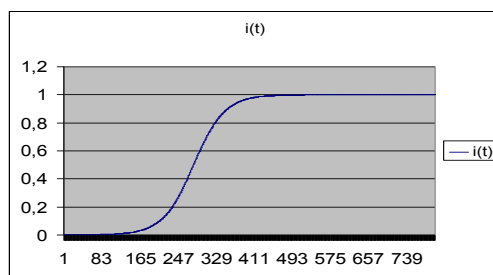


Рис. 2. Характеристика заражения модели 3

Недостаток данных моделей в том, что они оперируют с фактами заражения и по ним можно только отслеживать динамику роста численности зараженных узлов, при этом нет возможности непосредственно обнаруживать сетевой вирус или влиять на ход развития эпидемии. Кроме этого простые эпидемические модели не учитывают размер и топологию компьютерной сети, по которой вирус распространяется, а также различные техники сканирования, используемые для поиска целей поражения.

Установлено [5], что техника сканирования является одним из факторов, влияющих на скорость распространения вируса в сети, а, следовательно, и на динамику эпидемии. В источниках литературы [5 6] выделяют 5 типов техник сканирования: последовательное, по хит-листам, перестановки, топологическое, по приоритетам. Наиболее опасной техникой сканирования является техника сканирования по хит-листам, при которой заранее составляется список целевых хостов, подвергаемых атаке сетевым вирусом.

В настоящее время для обнаружения сетевых вирусов используют два основных метода:

- сигнатурный;
- обнаружение аномалий.

Достоинство сигнатурного метода в высокой вероятности обнаружения вирусов. Однако используется он, в основном, для обнаружения известных вирусов, сигнатуры которых имеются в базе данных. Для распознавания неизвестных сетевых вирусов более подходит применение метода обнаружения аномалий, основанный на выявлении различий (аномалий) в процессе функционирования узла сети или в сетевом трафике. В качестве эталонного значения для сравнения используется совокупность признаков сетевого трафика (например, число пакетов сканирования) или функционирования узла сети в нормальном (незараженном) состоянии. Недостаток этого метода – высокая вероятность ложного срабатывания. Кроме этого некоторые сетевые вирусы способны обучать систему обнаружения, в результате чего аномальное состояние рассматривается, как нормальное.

Обнаружение сетевых вирусов является одним из механизмов защиты компьютерной сети от эпидемий. Механизмы защиты можно делить на три больших класса [6]:

- предупреждение (уменьшение количества уязвимых хостов, например, отключение хостов);

- лечение (распределение и установка патчей в компьютерной);
- сдерживание (установка и конфигурирование файрволов на хостах или сегментах сети, фильтрация содержимого на сетевом уровне, автоматизированное создание и распространение черных списков адресов).

В работе [7] предложен метод динамического карантина, обладающий возможностью управления скоростью распространения эпидемии на основе блокирования портов. При этом компьютерная сеть предполагается однородной (каждый узел обладает одинаковой частотой заражения), а скорость распространения постоянной. Однако в ряде случаев отключение портов не всегда приводит к сдерживанию распространения вирусов в компьютерной сети, а задача защиты от эпидемии приоритетна. Например, необходимо любой ценой сохранить работоспособность части сети: отдельных узлов или сегментов.

Таким образом, предлагается разработать систему автоматического подавления эпидемий компьютерных вирусов на основе комбинирования механизмов сдерживания и предупреждения. Реализовать данную систему предполагается на основе динамического управления блокированием портов и отключением элементов компьютерной сети (узлов, сегментов) с использованием динамической пакетной фильтрации (DPF).

Список литературы

1. <http://www.viruslist.com>.
2. <http://www.kaspersky.ru>.
3. Ризниченко, Г. Ю. Математические модели биологических продукционных процессов / Г. Ю. Ризниченко, А. Б. Рубин. – М. : Изд. МГУ, 1993.
4. Matthew M. Williamson, Jasmin Léveillé, «Epidemic Spreading in Technological Networks», Information Infrastructure Laboratory HP Laboratories Bristol HPL-2003-39, February 27th , 2003.
5. Tom Vogt, «Simulating and optimising worm propagation algorithms», 29th September 2003.
6. Justin Lewis Balthrop, «RIOT: A Responsive System for Mitigating Computer Network Epidemics and Attacks», B.S., Computer Science, University of New Mexico, 2001.
7. Cliff Changchun Zou, Weibo Gong, Don Towsley, Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense, Univ. Massachusetts Amherst, MA.

*Кардашевская Марина Владимировна¹,
профессор кафедры криминалистики
Московского университета МВД России
имени В. Я. Кикотя, доктор юридических наук, профессор*

ОБСТАНОВКА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПЛАТЕЖНОЙ СИСТЕМЫ

Развитие технического прогресса привело к появлению новых технологий, которые активно используются преступниками в своих целях. Для разработки эффективных мер противодействия преступным действиям в интернете следует вначале сформировать адекватную, отвечающую современным требованиям криминалистическую характеристику данных преступлений. Криминалистическая характеристика каждого вида правонарушений представляет собой систему криминалистически значимой информации о различных элементах преступления. Она результат проведения криминалистического исследования конкретного вида или группы преступлений. Входя в содержание методики расследования преступлений в качестве ее первого элемента, она существенно влияет и фактически определяет содержание других разделов методики. Поэтому правильное понимание структуры данной характеристики и содержание ее элементов оказывают большое влияние на эффективность рекомендаций, разработанных в методике.

Одним из элементов криминалистической характеристики преступлений является обстановка их совершения, т. е. пространственно-временные условия, влияющие на выбор преступником способа действий, оставляющего свои следы в этом пространстве. Таким образом, обстановка совершения преступления закономерно связана с личностью преступника, прежде всего, с наличием у него определенных, в том числе преступных навыков; со способом преступления (подготовкой, непосредственным совершением и его сокрытием) и оставляемыми при этом следами. Поэтому уяснение сути обстановки совершения преступления позволяет выдвигать обоснованные версии о закономерно связанных с ней других элементах криминалистической характеристики.

Рассмотрим обстановку совершения преступлений на примере хищений с использованием электронной платежной системы.

Прежде всего, определим, что такое электронная платежная система. Ряд ученых [2], которые занимались изучением электронных платежных систем, утверждают, что данные системы – это компонентный элемент банковской среды. Однако разница между классическими банковскими расчетными системами и электронными платежными системами заключается в том, что между банком и клиентом существует третье лицо – провайдер. Хотя электронные платежные системы и представляют составную долю банковской системы, но в тоже вре-

¹ © Кардашевская М. В., 2020.

мя – это самостоятельная система, которую образуют юридические лица, осуществляющие расчетные операции.

Основные принципы правового регулирования электронных платежей раскрыты в Федеральном законе «О национальной платежной системе». В ст. 3 данного ФЗ сформулированы основные понятия, к которым относятся, в рамках данной статьи, «электронное денежное средство» (п. 18), «электронное средство платежа» (п. 19) и «операторы по переводу денежных средств» (п. 1). [1]

В настоящее время Центробанком постоянно ведется контроль операторов электронных денежных средств, список их постоянно изменяется. Так, по состоянию на 28.02.2020 в этот перечень входит 85 юридических организаций [4].

По мнению Н. В. Олиндера, электронные платежные средства и системы преступник применяет как средство совершения корыстного преступления (хищения), а умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации [3]. Однако, если электронная платежная система – это юридическое лицо, то система никак не может быть средством совершения преступления, а электронная платежная система является обстановкой совершения преступления.

Как уже говорилось ранее, обстановка совершения преступления – это пространственно-временные условия. При совершении хищений с использованием электронных платежных систем время их совершения не имеет криминалистического значения, поскольку практически никак не влияет на выбор преступных действий. В интернете нет времени года, суток, электронная платежная система работает всегда (за исключением случаев технического сбоя системы). Место, откуда преступник входит в систему, также не влияет на его действия, поскольку в современных условиях в электронную платежную систему можно войти в любой точке мира с любого электронного устройства, подключенного к интернету. Однако сама по себе электронная платежная система – это виртуальное пространство определенного юридического лица, которое осуществляет определенные действия для сохранения этого пространства от действия посторонних лиц, не являющихся клиентами системы. Вот именно эти условия охраны данного пространства и оказывают существенное, фактически определяющее воздействие на выбор преступником способа действий.

Криминалисты, характеризуя обстановку совершения хищения (время, место), часто упускают из виду еще один существенный элемент обстановки – условия хранения имущества. Электронная платежная система, как юридическое лицо, на основании заключенного договора с пользователем этой системы обязуется выполнять только те операции с его денежными средствами, которые санкционировал пользователь, т. е. электронная платежная система – это место хранения имущества пользователя, обладающее специфическими условиями его хранения. Именно поэтому электронная платежная система в криминалистической характеристике хищений должна рассматриваться как обстановка совершения преступления. При таком подходе к криминалистической сути данной системы можно найти ее взаимосвязь с другими элементами криминалистической характеристики.

Для ее формирования следует использовать следующую информацию:

- последовательность действий пользователя при регистрации в системе;
- последовательность осуществления расчетных и обменных операций;
- последовательность операций по внесению и получению денежных средств;
- специфика доступа к электронной платежной системе через интернет;
- аппаратные и программные средства, используемые при функционировании определенной электронной платежной системы;
- используемые средства защиты сведений.

Все эти сведения определяют способ действий преступника по хищению электронных платежных средств и оставляемые при этом следы. Выявленные в ходе формирования криминалистической характеристики закономерности будут лежать в основе выдвигаемых следственных версий и путей их проверки.

Список литературы

1. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе»(ред. от 27.12.2019).
2. Тедеев, А. А. Электронные банковские услуги / А. А. Тедеев. – М., 2005;
3. Успенский, И. В. Интернет-маркетинг : учебник / И. В. Успенский. – СПб. : СПГУЭиФ, 2003.
4. Олиндер, Н. В. Криминалистическая характеристика электронных платежных средств и систем / Н. В. Олиндер // Lex russica. – 2015. – № 10. – С. 128–138.
5. Перечень операторов электронных денежных средств / Банк России (дата обращения: 11.04.2020).

Клочкова Екатерина Николаевна¹,
*доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя*

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОРГАНИЗАЦИИ ДИСТАНЦИОННОЙ РАБОТЫ

В условиях распространения пандемии COVID-19 многие организации столкнулись с ситуацией, когда возникла необходимость срочного перевода сотрудников на дистанционную работу, миллионы людей в нашей стране одновременно перешли «на работу из дома». Если часть коммерческих организаций уже имела некоторый опыт организации удаленной работы сотрудников, то большинство государственных структур с этим столкнулись впервые и вынуждены спешно прорабатывать механизмы ее реализации.

Внедрение и использование дистанционной работы имеют свои преимущества и недостатки. С точки зрения работника, переход на удаленную работу позволил сэкономить на времени и стоимости проезда до работы, а также при правильной организации труда в домашних условиях, повысить производительность труда, за счет возможности сосредоточиться на поставленной задаче, можно не отвлекаться на посторонние вопросы. Если с сотрудниками все достаточно просто, то для работодателя сразу же возникает проблема обеспечения информационной безопасности при организации такого режима труда своих служащих.

Угроза безопасности, связанная с утечкой информации через сотрудников, работающих дистанционно, достаточно велика. Это связано прежде всего с тем, что специалисты по информационной безопасности не имеют возможности для организации защиты использовать все свои технические средства и политики безопасности, которые в обычных условиях обеспечивают надежную защиту информации, обрабатываемую с использованием средств вычислительной техники, в организации.

В этом случае к угрозам, которые применимы к локальным сетям и давно известны, добавляются новые, так как специалисты по защите информации не могут в должной мере контролировать удаленную систему. Возникает ситуация, когда в вопросах обеспечения безопасности устройств (персональных компьютеров, ноутбуков, планшетов и т. д.) приходится полагаться на рядовых сотрудников, которым не хватает квалификации, знаний или опыта для организации их защиты. Нередко сотрудники могут по незнанию посещать опасные web-ресурсы или не соблюдать правил безопасности при работе с почтой, или не устанавливать всех необходимых обновлений ОС и других приложений.

Помимо этого, огромное разнообразие технических средств, используемых для удаленного подключения, приводит к отсутствию централизованного управления, а как следствие к тому, что защита мобильных устройств и персональных компь-

¹ © Клочкова Е. Н., 2020.

ютеров, подключенных дистанционно, изначально значительно слабее, чем защита стационарных компьютеров на рабочих местах в организации.

Говоря об обеспечении информационной безопасности при организации удаленной работы, нельзя забывать, что в большинстве случаев связи и доступ к данным осуществляются через общедоступный интернет. Резкое увеличение количества организаций, перешедших на дистанционную работу, может спровоцировать рост числа хакерских атак в целях хищения не только данных, но и денежных средств, если речь идет о кредитных организациях.

Еще одна проблема, с которой столкнулись многие организации, связана с резким ростом нагрузки на серверы, а как следствие нехватка их мощностей, но это технический аспект организации дистанционной работы.

В целях обеспечения надежной защиты информации при организации дистанционной работы необходимо проведение следующих мероприятий:

1. Инструктаж с сотрудниками, осуществляющими выполнение своих должностных обязанностей в дистанционном режиме, на предмет соблюдения ими правил безопасного удаленного взаимодействия, а также недопущения возможности доступа к техническим средствам посторонних лиц.

2. Составление перечня информационных ресурсов, к которым будет предоставлен удаленный доступ.

3. Установление необходимых прав пользователям для осуществления дистанционной работы. По возможности рекомендуется пользователей обеспечить служебными портативными техническими средствами, в которых встроены средства защиты информации. Сотрудникам, работающим на своих технических средствах, рекомендуется назначать минимальные необходимые права доступа.

4. Обеспечение идентификации технических устройств, работающих в удаленном режиме, по их физическим адресам.

5. Обязательное применение на компьютерах и мобильных устройствах, работающих в дистанционном режиме, программных средств антивирусной защиты.

6. Фиксирования всех действий сотрудников при осуществлении удаленной работы с информационными материалами организации.

7. Блокирование сеанса удаленного доступа работника при длительном неактивном использовании информации.

Использование предложенных мероприятий позволит повысить надежность защиты информации, попадающей в группу риска, при организации удаленного режима труда сотрудников организаций.

Список литературы

1. Письмо ФСТЭК России от 20.03.2020 г. № 240/84/389 Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при удаленной работе должностных лиц субъектов КИИ // Официальный сайт ФСТЭК России: <http://fstec.ru>.

2. <https://www.rbc.ru/finances/18/03/2020/5e70b8a79a79470d20100a41>.

3. <https://searchinform.ru/blog/2015/12/08/udalennaya-rabota-vzglyad-s-pozitsii-rabotodatelaya>.

Коньшев Василий Юрьевич¹,
студент кафедры информационных технологий
Московского авиационного института;

Максимов Николай Анатольевич²,
доцент кафедры информационных технологий
Московского авиационного института,
кандидат технических наук

ПОСТРОЕНИЕ ЗАЩИЩЕННОЙ ОПОРНОЙ СЕТИ СВЯЗИ НА БАЗЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

В последнее время стремительно происходит развитие беспилотных технологий, появляются новые варианты их использования. Один из таких вариантов – обеспечение сотовой связи в условиях отсутствующей или разрушенной инфраструктуры. Это может быть актуально, например, при ликвидации последствий аварии необходимо особенно оперативно разворачивать системы связи [1].

Беспилотные летательные аппараты (БЛА) способны обеспечивать покрытие благодаря технологии сотовой связи на территории площадью сотни квадратных километров. Они позволяют работать как непосредственно с абонентами, так и обеспечивать канал для наземных станций связи, которые в свою очередь обеспечивают раздачу интернета через сети фиксированного доступа или Wi-Fi.

БЛА используются в виде ретрансляторов базовых станций, расположенных не на земле, а в воздухе. Использование БЛА превосходит базовые станции оперативностью восстановления опорной сети, за счет дополнительных летательных аппаратов, возможностью большего покрытия территорий, быстротой и более низкой стоимостью разворачивания сети.

Реализовать опорную сеть можно при помощи Mesh сетей, – это довольно крупные, отдельные, и активно развивающиеся технологии динамических сетей. Наиболее общее определение Mesh сети: «Mesh – сетевая топология, в которой устройства объединяются многочисленными соединениями. Сеть представляется в виде узлов, которые предоставляют возможность связи с сетью и для других узлов этой же сети выполняют функции маршрутизаторов и ретрансляторов. Это позволяет создать самоустанавливающейся и самовосстанавливающейся сети» [2].

Достоинства Mesh сети:

- не зависят от поставщика интернет-услуг;
- современные протоколы для Mesh сетей позволяют осуществить шифрование всех передаваемых данных;
- динамическая, автоконфигурируемая маршрутизация.

Недостатки Mesh сети:

- практически отсутствует доступ к расширенным функциям;

¹ © Коньшев В. Ю., 2020.

² © Максимов Н. А., 2020.

- эффективная работа достигается, когда в сети много участников;
- негарантированная ширина канала;
- негарантированное качество связи [2].

В нынешнее время самые популярные протоколы для организации Wi-Fi Mesh сетей это: CJDNS, B.A.T.M.A.N., DTN, Netsukuku, OSPF. Перечисленные протоколы поддерживают функции автоматической настройки маршрутизации; осуществляют распределенную маршрутизацию. Наилучшим для организации Mesh сетей является протокол CJDNS. Он характеризуется низким потреблением ресурсов и обладает возможностью шифрования трафика внутри сети.

Сейчас, как никогда, важна защита сети от взломов, так как опорная сеть связи на базе БЛА может быть построена как в мирное время, так и в военное, именно поэтому важна конфиденциальность и безопасность передаваемой информации. Есть два варианта борьбы со взломами:

1. Располагать точку доступа так, чтобы она снабжала только нужное покрытие территориально, и это покрытие не выходило за контролируемую территорию. Для этого нужно настраивать мощность передачи сигнала или применять специальную аппаратуру для контроля распространения сигнала.

2. Применять современные алгоритмы шифрования.

Однако CJDNS устаревший протокол, последние новости о сети датируются 2017 г., именно поэтому активно разрабатывается набор новых протоколов. Сейчас происходит разработка полноценного движка Mesh сети, которая бы отвечала всем необходимым требованиям.

Для создания работоспособной и надежной Mesh сети нужно:

1. Ячеистая топология – предполагает, что топология компьютерной сети построена на основе использования так называемых «ячеек», в качестве ячеек здесь выступают рабочие станции, соединенные между собой. При этом каждая из рабочих станций может выполнять роль коммутатора для всех остальных.

2. Наличие алгоритмов управления трафиком (выбор пути) – для оптимальной передачи трафика.

3. Возможность перестроения топологии сети в любой момент с сохранением связности – чтобы в момент покидания сети или перемещения в другое место, сеть незамедлительно продолжит работу.

4. Автонастройка – предполагает, что сеть можно использовать без установки дополнительного программного обеспечения.

5. Безопасность в соответствии с технологиями IEEE 802.11 и IEEE 802.11i. [3].

Оригинальный стандарт 802.11 использует для обеспечения безопасности беспроводных сетей стандарт «конфиденциальности, эквивалентной проводной» (Wired Equivalent Privacy). Беспроводные сети, использующие стандарт WEP, требуют задания начальных настроек статического WEP-ключа, который используется для аутентификации и шифрования передаваемых данных. Любая компроментация ключа требует незамедлительной смены ключей на всех подключенных устройствах.

Аутентификация, основанная на применении WEP-ключей, предполагает, что используемые беспроводные станции передают запрос соответствующей точке доступа, в ответ на который они получают незашифрованное сообщение.

С помощью своего WEP-ключа клиент шифрует свое сообщение и передает его обратно точке доступа. Точка доступа, используя собственный WEP-ключ, расшифровывает полученное сообщение. Если WEP-ключ клиент истинный, то полученное после расшифровки сообщение является оригинальным, и можно говорить об успешной аутентификации, о чем соответствующее уведомление отправляется клиенту.

Когда успешно завершаются аутентификация и ассоциация, беспроводное устройство получает доступ к WEP-ключу для шифрования трафика, который передается между устройством и точкой доступа.

Стандарт 802.11i существенно поднял безопасность, при его создании опираясь на оригинальный стандарт 802.11, исключив все уязвимости. 802.11i определяет использование стандарта шифрования (Advanced Encryption Standard, AES) вместо WEP. В основе AES лежит реализация алгоритма Рендела. Этот алгоритм существенно лучше своего слабого предшественника RC4, который используется в WEP: он предусматривает использование ключей длиной 128, 192 и 256 разрядов, вместо 64 бит. [4]

Несмотря на надежность протоколов, создаются программы, которые способны обходить их, именно поэтому сейчас так важно постоянно обновлять протоколы. В любом протоколе существуют свои минусы, главная задача разработчиков – быстро устранять возникающие проблемы. Так, в самом начале работы 802.11i никто не предполагал, что необходимо защищать и контрольные сообщения в беспроводной сети. Впоследствии выяснилось, что взломщик может передавать пакеты с запросом на отключение и этим отключать абонента от сети. Для устранения проблемы была оперативно выделена рабочая группа, которая решила данную задачу.

Таким образом, рассмотрены вопросы, возникающие при создании опорной сети связи на основе БЛА, выявлены сильные и слабые стороны имеющихся протоколов.

В дальнейшем планируется разработать модели такой сети, определить ее производительность, зависимость ее характеристик от количества БЛА (узлов сети) и установленного на них оборудования.

Список литературы

1. Чертова, О. Г. Построение опорной сети связи на базе малоразмерных беспилотных летательных аппаратов с отсутствием наземной инфраструктуры [Электронный ресурс] / О. Г. Чертова, Д. С. Чиров // URL: <https://cyberleninka.ru/article/n/postroenie-opornoj-seti-svyazi-na-baze-malorazmernyh-bespilotnyh-letatelnyh-apparatov-s-otsutstviem-nazemnoy-infrastruktury/viewer>.
2. Shifttstas. Wi-Fi Mesh сети для самых маленьких [Электронный ресурс] // URL: <https://habr.com/ru/post/196562/>.
3. Луконин, К. Проектирование Mesh-сетей [Электронный ресурс] / К. Луконин // URL: <https://nag.ru/articles/article/102081/proektirovanie-mesh-setey.html>.
4. Пастоев А. Безопасность беспроводных сетей [Электронный ресурс] / А. Пастоев, Н. Петров // URL: <https://www.osp.ru/cio/2006/04/1156259>.

Коньшева Виктория Юрьевна¹,
аспирант кафедры информационных технологий МАИ

АНАЛИЗ СТРУКТУРНЫХ СВОЙСТВ НЕЛИНЕЙНЫХ ДИНАМИЧЕСКИХ СИСТЕМ

При формировании математической модели объекта управления, в частности нелинейной динамической системы, осуществляется оценка структурных свойств объекта – наблюдаемости и управляемости. Оценка наблюдаемости нелинейной динамической системы предшествует постановке задачи ее идентификации и позволяет выяснить возможность решения задачи управления. Ведь только полностью наблюдаемая нелинейная динамическая система может быть идентифицирована [1, 2].

Выполнение условий наблюдаемости Р. Калмана необходимо также для восстановления координат вектора состояния динамической системы, которые не доступны к измерению по ряду причин. [3]

Для оценки управляемости и наблюдаемости обычно используются уравнение состояния и уравнение выхода объекта в их векторно-матричной форме:

$$\begin{aligned}\dot{X} &= AX + BU; \\ Y &= CX,\end{aligned}\tag{1}$$

где: X – n -мерный вектор-столбец переменных состояния;

Y – q -мерный вектор-столбец выходных переменных;

U – m -мерный вектор-столбец управлений ($m, q \leq n$);

$A (n \times n), B (n \times m), C (q \times n)$ – постоянные матрицы указанных размерностей.

Объект управления (1) с парой матриц (A, B) называется полностью управляемым, если его можно за конечное время $T=t_k-t_0$ перевести из произвольного начального состояния $X(t_0)$ в произвольное конечное $X(t_k)$, применив соответствующим образом выбранное управляющее воздействие $U = U(t)$, определенное на интервале $[t_0, t_k]$.

Для того чтобы иметь возможность произвести оценку управляемости, воспользуемся критерием Р. Кальмана. Для обеспечения полной управляемости матрица управляемости объекта должна обладать полным рангом:

$$\text{rang } N_c = \text{rang } \|B : AB : A^2B : \dots : A^{n-1}B\|_{n \times n \cdot m} = n\tag{2}$$

В случае не полностью управляемого объекта ($\text{rang } N_c = r < n$) неуправляемая часть представляется как источник воздействия, для компенсации которого рассматриваемую систему преобразовываем к разделенному виду и находим передаточную функцию. Данная функция осуществляет взаимодействие между выходом неуправляемой части и выходом системы:

$$Y = Y(t) \text{ [4].}$$

¹ © Коньшева В. Ю., 2020.

Управляемость по выходу – означает возможность перевода выхода объекта из любого состояния $Y(t_0) = Y_0$ в любое другое состояние $Y(t_k) = Y_k$ за конечное время t_k путем приложения допустимого управления.

Критерий управляемости будет иметь вид:

$$\text{rang } \|CB : CAB : CA^2B : \dots : CA^{n-1}B\| = q, \quad (3)$$

где: q – число выходных переменных объекта или количество строк в матрице C . При этом матрица C ($q \times n$) должна быть матрицей полного ранга, т. е. $\text{rang } C = q$, это условие является необходимым, но недостаточным.

Для управления динамическими системами необходимо проводить измерения всех координат их вектора состояния, в которых может содержаться информация о значениях параметров математических моделей, адекватно описывающих их свойства. Необходимо иметь в виду, что измерение координат возможно далеко не во всех случаях, например при отсутствии «точек доступа»; при абстрактности переменных, в этом случае они не имеют физического представления в реальной системе и поэтому не могут быть измерены. Следовательно, возникает задача восстановления не измеряемых координат вектора состояния. Необходимым условием решения этой задачи является наблюдаемость системы. [3]

Наблюдаемость объекта – означает возможность определения первоначального состояния объекта X_0 по результатам наблюдений за его выходом $Y(t)$ на конечном интервале $t \in [t_0, t_k]$, а сам объект называется полностью наблюдаемым. В этом случае необходимо выполнять следующее условие:

$$\text{rang } \|C^0 : A^T \tilde{N}^T : (A^T)^2 C^T : \dots : (A^T)^{n-1} C^T\|_{n \times q \cdot n} = n, \quad (4)$$

где t – символ операции транспонирования матриц.

Другими словами, можно говорить о том, что условие наблюдаемости предполагает, что ранг матрицы наблюдаемости N_c равняется размеру вектора состояния X .

Сложную нелинейную динамическую систему можно представить, как набор функциональных элементов с определенным типом связи между собой. После построения уравнения состояния функционального элемента можно оценить его управляемость и наблюдаемость на основании выведенных теорем [1]. Однако в некоторых случаях при расчете показателей для отдельных функциональных элементов вычислительные затраты значительно меньше, чем в процессе расчета показателей для всей системы в целом.

Управляемость и наблюдаемость важные свойства нелинейной динамической системы, как и ее устойчивость. Для решения задачи восстановления всех координат вектора состояния нелинейной динамической системы необходимым условием является выполнение условия наблюдаемости Р. Калмана. Это, в свою очередь, позволяет осуществлять диагностику системы по заранее заданным или восстанавливаемым входам и выходам функциональных элементов.

Список литературы

1. Кухаренко, Н. В. Управляемость и наблюдаемость объектов : лекция / Н. В. Кухаренко // URL: <https://studydocs.ru/document/626028/3>.
2. Дударенко, Н. А. Математические основы теории систем: лекционный курс и практикум / [Н. А. Дударенко и др.]; под ред. А. В. Ушакова. – СПб. : НИУ ИТМО, 2014.
3. Шаронов, А. В. Методы и алгоритмы обработки результатов экспериментальных исследований / А. В. Шаронов. – М. : Изд-во МАИ, 2004.
4. Беляев, М. Е. Методические указания к выполнению практической работы по курсу «Управление непрерывными и дискретными процессами» / М. Е. Беляев, А. С. Павлов, С. В. Шаветов. – СПб. : Университет ИТМО, 2016.

Кальницкая Валерия Михайловна¹,
курсант факультета по подготовке
специалистов по охране общественного порядка
и обеспечения общественной безопасности
Краснодарского университета МВД России;

Еськов Александр Васильевич²,
профессор кафедры информационной безопасности
Краснодарского университета МВД России,
доктор технических наук, профессор

ОБЗОР РЕАЛИЗАЦИИ РАЗГРАНИЧЕНИЯ ДОСТУПА ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX

В настоящее время совсем необязательно выбирать зарубежное программное обеспечение, в основе которой лежит получение коммерческой выгоды, путем его повсеместной продажи как самого программного обеспечения, так и пакета прикладных сопутствующих программных продуктов, включающих офисные пакеты (Microsoft Office), программы-архиваторы (WinRar), межсетевые экраны, антивирусные программы и т. д. Можно существенно сэкономить и приобрести бесплатную операционную систему отечественной разработки, обладающую при этом довольно высоким уровнем безопасности, проверенного на практике. Таким аналогом на современном рынке программных услуг является Linux. [1]

Linux по сравнению с Windows обладает высоким уровнем надежности, что в свою очередь, не ведет за собой простой оборудования на объекте информатизации. Linux использует и такую файловую систему, в которой предусмотрена строгая иерархия размещения информации: все файлы обычного пользователя хранятся в специально заданном разделе диска: /home/<имя_пользователя>. Для каждого файла в корневой системе можно задать права доступа, представленные следующим образом: чтение (read) – r, запись (write) – w, исполнение (execution) – x. Данные права доступа применимы как к отдельному пользователю системы, ее владельцу, так и к группе пользователей. [1]

Рассмотрим практическое применение прав доступа к файловой системе в операционной системе Linux. Для достижения данной цели установим в виртуальной машине VirtualBox образ системы Linux.

На рабочем столе открываем консоль операционной системы:

¹ © Кальницкая В. М., 2020.

² © Еськов А. В., 2020.



Рис. 1. Рабочий стол среды Linux

Важно отметить, что ранее были созданы пользовательские профили системного администратора и работающих в системе лиц.

Обозначаем путь к необходимой папке путем ввода в консоль: `cd/home/patts/Документы`.

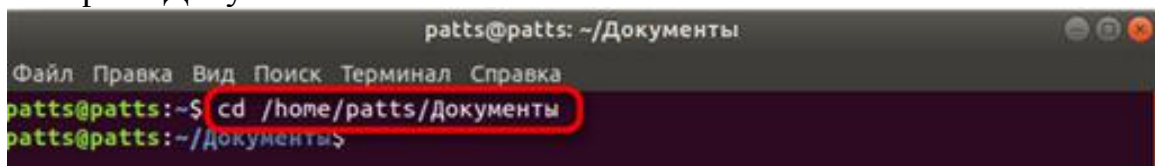


Рис. 2. Задание файла

Для просмотра количества лиц, имеющих право доступа к данному файлу введем утилиту `ls-l`:

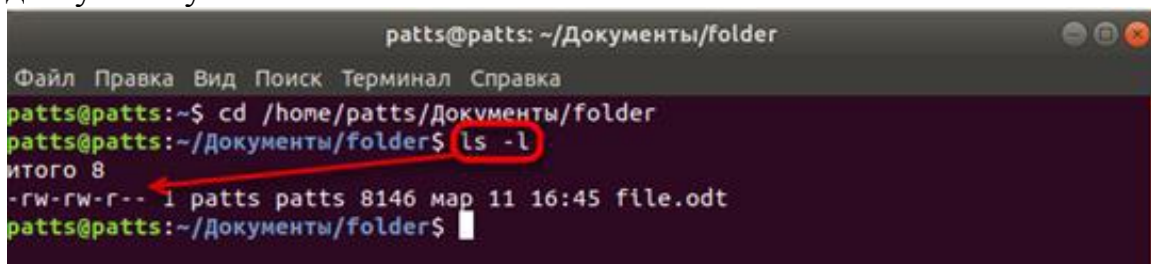
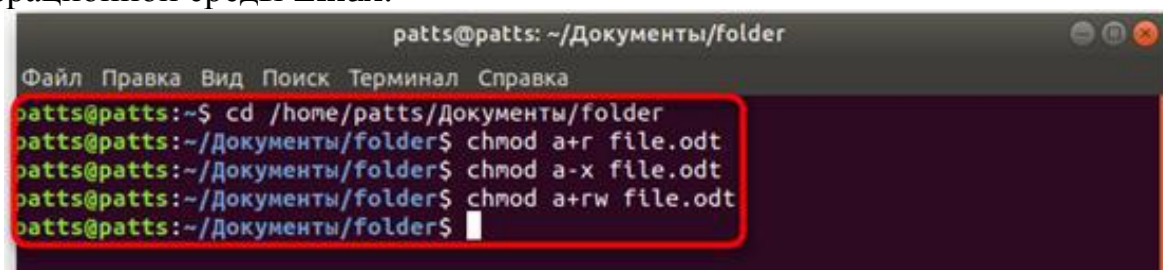


Рис. 3. Результат применения утилиты `ls-l`

В результате выполнения данной утилиты мы видим, что к данному файлу установлены следующие права доступа: `-rw-rw-r-- -l`. Разберемся поочередно в каждом символе данной строки: первый символ (`-`) обозначает признак каталога: если бы вместо данного первого символа был символ `d` (от `directory`), то можно уверенно сказать, что перед нами каталог, но в данном случае мы рассматриваем обыкновенный файл. Последующие три символа (`rw-`) обозначают права доступа владельца рассматриваемого файла: чтение и запись (редактирование) файла. Следующие три символа (`rw-`) указывают права доступа для чле-

нов группы: чтение и запись (редактирование). Последние три символа (r- -) выделяют права доступа для прочих пользователей: только чтение. [2, с. 102]

Далее рассмотрим применение утилит для добавления и исключения прав доступа у субъектов информации к объектам информации в файловой системе операционной среды Linux:



The image shows a terminal window titled 'patts@patts: ~/Документы/folder'. The terminal output is as follows:

```
patts@patts:~$ cd /home/patts/Документы/folder
patts@patts:~/Документы/folder$ chmod a+r file.odt
patts@patts:~/Документы/folder$ chmod a-x file.odt
patts@patts:~/Документы/folder$ chmod a+rw file.odt
patts@patts:~/Документы/folder$
```

The last three lines of the terminal output are highlighted with a red rectangular box.

Рис. 4. Применение утилит добавления и исключения прав доступа

Из представленной иллюстрации видны следующие утилиты:

1. `chmod a+r file.odt` – данной утилитой мы добавляем права на чтения всей группе.
2. `chmod a-x file.odt` – утилита, предназначенная для удаления права на исполнение у обозначенной группы пользователей.
3. `chmod a+rw file.odt` – добавление права на чтение и запись у данной группы пользователей.

В практическом применении разграничения прав доступа в среде Linux для облегчения осуществления данного процесса используют групповой метод разграничения прав доступа, при котором добавляют или исключают права доступа для соответствующей группы пользователей.

Если возникает ситуация, при которой нужно осуществить данные действия в отношении владельца объекта, остальных пользователей, группы или всех перечисленных лиц, то системный администратор будет придерживаться следующего синтаксиса для обозначения субъекта информационного процесса:

- u – непосредственный обладатель файла;
- g – образованная системным администратором определенная группа пользователей;
- o – прочие пользователи информационной системы;
- a – все конечные пользователи данной файловой системы. [2, с. 103–104].

Таким образом, можно сформулировать вывод о надежности применения Linux ввиду того, что для файловой система в данном программном обеспечении зависит от заданных системным администратором конфигураций, результатом которых становится разграничение прав отдельных пользователей от соответствующих информационных объектов.

Список литературы

1. Кенин, А. М. Самоучитель системного администратора / А. М. Кенин, Д. Н. Колисниченко. – 5-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2019.
2. Колисниченко, Д. Н. Linux. От новичка к профессионалу / Д. Н. Колисниченко. – 6-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2018.

Кравцов Олег Геннадиевич¹,
*доцент кафедры юридической психологии
учебно-научного комплекса психологии служебной
деятельности Московского университета
МВД России имени В.Я. Кикотя,
кандидат психологических наук, доцент*

ПАТТЕРНЫ ОТКЛОНЯЮЩЕГОСЯ ПОВЕДЕНИЯ НЕ КРИМИНАЛЬНОГО ХАРАКТЕРА В ИНТЕРНЕТЕ

По мнению многих ученых отклоняющееся поведение стало одной из актуальных проблем современной психологической науки. Само по себе отклоняющееся поведение наносит вред обществу и общественным отношениям, негативно сказывается на самом человеке, его проявляющем и несет для него ряд социальных ограничений. Очевидны деструктивные последствия такого поведения. А в современной социальной ситуации не только увеличивается число людей с отклоняющимся поведением, но и увеличивается сам репертуар такого поведения. Иными словами, в обществе людей с ненормативным поведением становится все больше.

Одним из плацдармов для расширения репертуара отклоняющегося поведения стало интернет-пространство [4]. И особенно важно, что развитие коммуникационных технологий не только предоставило новые средства для реализации старых паттернов отклоняющегося поведения, но породило ряд новых явлений, которые раньше как самостоятельные паттерны поведения не наблюдались. Можно сказать, что перед современной психологией стоят две важные задачи: изучение специфики проявления уже известных паттернов отклоняющегося поведения в новых информационных реалиях и выявление, и описание новых, появившихся относительно недавно, паттернов отклоняющегося поведения. Решение этих двух задач имеет существенное теоретическое и практическое значение. С точки зрения практики изучение новых характеристик отклоняющегося поведения необходимо для выстраивания мер по профилактике коррекции и работы с людьми с таким поведением. Даже просто описание этих явлений бывает важно при определении количественных и качественных параметров для эмпирического изучения. С теоретической точки зрения изучение новых и осмысление ранее известных паттернов отклоняющегося поведения важно для понимания психологической природы этого явления. Без создания единой концепции отклоняющегося поведения невозможно дальнейшее построение исследовательской работы и тем более организации эффективной психологической помощи.

Важно оговориться, что под отклоняющимся поведением не имеется в виду поведение преступного характера. Понятно, что интернет-пространство предоставляет широкие возможности для совершения деяний, за которые предусмотрена юридическая ответственность. Так, согласно официальной статистике

¹ © Кравцов О. Г., 2020.

МВД России в январе – феврале 2020 г. зафиксировано более 60 тыс. преступлений, совершенных с использованием информационно-коммуникационных технологий [1]. Разные авторы по-разному понимают отклоняющееся поведение. В данной статье рассматривается только отклоняющееся поведение не криминального характера.

Отклоняющееся поведение принято разделять на несколько различных форм [6]. Так, не криминальное по характеру отклоняющееся поведение включает асоциальное, зависимое, виктимное и суицидальное поведение. Каждая из этих форм находит свое выражение в условиях интернет пространства.

Зависимое поведение подразделяется на фармакологические и не химические виды зависимостей. Распространение наркотических средств через интернет остаются за пределами данного анализа, так как это относится к криминальному поведению, предполагающему уголовную ответственность. Сравнительно новым в распространении фармакологических зависимостей стала активная торговля через интернет-ресурсы полулегальными или временно не запрещенными веществами. Законодательство по естественным причинам не всегда успевает за бурно развивающейся химической промышленностью. И не все появляющиеся на рынке психо активные вещества можно оперативно внести в список запрещенных, чем активно пользуются злоумышленники, наживающиеся на легальном распространении этих препаратов.

Здесь важным для психологов моментом является вовлечение в эту деятельность большого числа несовершеннолетних, которые помогают в распространении среди своих друзей в социальных сетях, и одной из важных психологических составляющих этой деятельности является созданный Голливудом романтический образ торговца наркотическими веществами. Многие молодые люди вовлекаются в эту полулегальную деятельность именно в силу решения актуальных для них возрастных задач. Так, для достижения чувства взрослости [2], выстраивания своей идентичности или повышения статуса среди сверстников они примеряют на себя роль крутого торговца наркотическими средствами.

Но несколько более интересным, с точки зрения психологии, является распространение в интернет не химических зависимостей. Многие азартные игры переместились в интернет пространство. В интернет-пространстве активно эксплуатируется сюжет легкого и быстрого обогащения. Психологи хорошо знают, что есть определенный психотип людей, который обладает высокой психологической готовностью быть обманутым и вовлеченными в погоню за легкой добычей [3]. Речь идет не только про все возможные онлайн казино. На этом же психологическом принципе построены многие письма от незнакомцев, обещающих предоставление крупных сумм, гуманитарной помощи или наследства. Как отмечают респонденты в нашем поисковом исследовании, не просто все получали подобного рода письма, но для многих это происходит регулярно.

Новые черты приобрело суицидальное поведение в интернет-среде. Еще со времен Э. Дюркгейма (1897 г.) хорошо известно, что одним из очень мощных факторов, порождающих суицидальное поведение, является информирование людей об этих случаях. При этом не важно, в каком контексте подается такое информирование, осуждается ли суицидальное действие или ему придается ре-

кламный лоск. Согласно многократно подтвержденной статистике это значительно увеличивает количество самоубийств в обществе. Современные коммуникационные технологии ощутимо расширяют аудиторию информирования о суицидах. Создаются специализированные сайты, сообщества, закрытые группы, где эта тематика активно накапливается и обсуждается.

Но помимо просто информирования в интернете в свободном доступе существуют фактически «инструкции» по тому, как именно можно спланировать и совершить суицидальные действия. Подобные пошаговые указания также призваны упростить для человека движение в этом драматичном направлении.

Относительно недавно особое внимание психологов стали привлекать так называемые *группы смерти*. Это интернет-сообщества по интересам, в которых участники планируют самоубийство и играют в него. Известны реальные случаи, когда подобные игры приводили к фатальным последствиям. В подобных группах многое построено на эстетике самоубийства, романтизации и воспевании этого действия как высшего проявления воли. Такие сообщества главным образом ориентированы на молодежную аудиторию, в основном школьников. Они эксплуатируют типичные возрастные подростковые проблемы, связанные с чувством одиночества и не выстроенной идентичности. Главная проблема в том, что эти возрастные кризисы переживают так или иначе все люди на соответствующем этапе развития. Не все из-за этого готовы расстаться с жизнью. Но подобные сообщества значительно расширяют группу риска по подростковому, и не только, суицидам.

В интернет-среде широко распространено виктимное поведение. Само по себе виктимное поведение не имеет своего предмета, это не поведение, направленное на что-то, как в случае с зависимостью и суицидом. Но в результате виктимного поведения человек оказывается жертвой, претерпевает урон или получает ущерб. В интернете действует большое число злоумышленников, действия которых направлены на причинение вреда. Чаще всего речь идет про кражи имущества и денежных средств. Для этого активно используются многочисленные программы взломщики и обманные сайты и т. д.

Очень сложно охватить в рамках одного анализа весь репертуар виктимного поведения в интернет пространстве. Яркий пример того, как старые паттерны приобретают новые свойства, — деятельность различных деструктивных культов и сект, а также новых религиозных течений. Раньше привлечение новых адептов в различные религиозные группы во многом строилось на обаянии и коммуникативных приемах конкретных вербовщиков. При этом использовались хорошо известные социальным психологам механизмы убеждения, манипуляции и внушения. Вербовка новых членов культов через интернет-коммуникацию имеет несколько иные особенности, некоторые средства типа личного обаяния не так эффективно работают. Но зато есть множество других инструментов вроде ярких рекламных образов, социальной пропаганды, многочисленных способов удержания на связи. Проще говоря, если на улице подходим человек со странными речами, вы могли просто уйти и не слушать его. В социальных сетях человеку можно присылать сообщения с различных аккаунтов так, чтобы он не смог полностью их игнорировать. То есть навязывание информации приобретает более агрессивный характер.

Еще одна, большая и разнообразная форма отклоняющегося поведения – поведение асоциальной направленности, это многочисленные паттерны поведения, направленные на нарушение социальных нормативов и запретов. Один из самых очевидных вариантов распространение и производство порнографических материалов. И речь не идет о действиях, нарушающих уголовный закон. Интернет пестрит огромным числом разных сайтов с соответствующим контентом.

Происходит активное вовлечение пользователей интернета в создание и распространение собственных пикантных фото и видео материалов. Наибольшую обеспокоенность вызывает вовлечение в индустрию порно-бизнеса несовершеннолетних и молодых людей. Они не прогнозируют возможные последствия для себя и не оценивают риски своих действий.

Другой большой блок асоциального поведения – поведение агрессивного характера. Так, интернет-среда предоставляет широкие возможности для проявления самого разного рода агрессии. Такое явление, как буллинг или травля, может быть реализовано не только при физическом контакте, но и удаленно в виртуальном пространстве. Относительно новое в этом плане явление так называемых *хейтеров* – людей, которые намеренно находят средства, чтобы испортить жизнь в сети своему объекту ненависти. Но кроме одиночных хейтеров есть еще организованные группы по травле и нанесению ущерба другим пользователям интернета. Некоторые из респондентов, участвовавших в нашем опросе, отмечают, что подобная деятельность имеет коммерческую составляющую.

Как показывает даже беглый и поверхностный анализ все хорошо известные формы отклоняющегося поведения находят свое выражение в интернет пространстве. При этом они приобретают некоторые новые черты и механизмы.

Таким образом, важным патогенным действием интернета является, во-первых, предоставление информации о способах и вариантах отклоняющегося поведения. Проще говоря, большое количество людей знают, как совершать самоубийство, какие препараты принимать, как проявлять насилие или совершать обман. Во-вторых, интернет кроме информационной составляющей выступает как источник примеров для подражания. То есть люди получают социальное подтверждение, что они не одни такие и это убеждает их в легальности и допустимости отклоняющегося поведения.

Однако кроме традиционных, известных паттернов отклоняющегося поведения интернет-пространство порождает ряд новых, которые ранее не были знакомы человечеству и точно не изучались систематически. Некоторые из этих форм появились ввиду новых средств коммуникационных технологий, которые существенно расширили возможности обычного пользователя.

К новым формам отклоняющегося поведения можно отнести так называемый *сталкинг*. По сути, это преследование человека. Сама по себе эта активность не запрещена законом, но может доставить много неудобства в жизни жертве преследования. Обычно сталкинг используется как форма запугивания или оказания давления на человека и может стать одной из составляющих доведения до самоубийства.

Большую озабоченность у психологов вызывают различные розыгрыши и задания, которые выполняют пользователи социальных сетей для привлечения

аудитории или поддержания тренда. Проблема в том, что подобные заразительные примеры часто носят угрожающий для жизни и здоровья людей характер. Так, некоторое время назад у школьников, в том числе в Российской Федерации, было популярно испытание «перебежать дорогу перед машиной». Это экстремальное поведение было необходимо заснять на видео и похвастаться перед сверстниками. Наиболее удачные видео набирали большое количество просмотров и приносили своим авторам большую известность. В погоне за этой популярностью молодые люди совершают много опасных и вредных действий, нередко приводящих к увечьям и смерти.

Самое специфическое явление в интернете – насильственные и нелегальные реалити-шоу. По задумке исполнителей, зрители в интернете могут за денежные переводы влиять на то, что происходит в прямом эфире, во время трансляции. При этом сами шоу строятся вокруг насилия и унижения его участников. Известны несколько подобных проектов, когда участники шоу набирались из числа людей с самым низким социальным статусом и не имеющих возможности защищаться. В ходе шоу они должны были выполнять унижительные задания, употреблять в пищу не годные и не съедобные продукты, наносить друг другу различные травмы и фактически пытаться участников. В некоторых случаях подобные шоу фактически сводятся к формату снаффа, т. е. документальной съемки реального убийства человека.

Подобные видео вызывают шок. Но важным психологическим вопросом остаются психологические причины и механизмы вовлечения людей, готовых быть потребителями и активными зрителями таких шоу.

Анализ отклоняющегося поведения не криминального характера не исчерпывающий. Количество паттернов отклоняющегося поведения в интернет-пространстве чрезвычайно велико. При этом количество вовлекаемых в подобное поведение людей также растет с каждым годом и активно насыщается новыми сценариями.

Может показаться, что за этим кроется процесс смены социальной нормы. Однако если появляется некий новый паттерн поведения, то вначале он отклоняющийся, так как не вписывается в представления общества об обычном поведении, но по мере того как все больше людей начинают его реализовывать это поведение из разряда ненормативного становится обыденным. Подобный статистический подход к пониманию нормы не применим к вышеописанным паттернам. Отклоняющееся поведение является отклоняющимся не по тому насколько оно распространено, а по внутренним психологическим особенностям [5].

Так, отклоняющееся поведение отвечает трем качественным критериям:

- наносит вред обществу. Например, зависимое поведение напрямую влияет на количество активных членов общества и настроения, царящие в нем;
- всегда оборачивается для человека, его проявляющего определенными ограничениями со стороны общества. Например, людей с попытками суицида не только ставят на учет в диспансер, но и ограничивают в доступе к ряду профессий.

– отклоняющееся поведение само по себе оказывает психологический вред самому человеку. Например, опыт агрессивного поведения меняет человека внутренне и делает его менее счастливым.

Таким образом, речь идет не о появлении новых паттернов поведения в обществе. Даже без строгого эмпирического анализа можно увидеть, как расширяется репертуар отклоняющегося поведения и как все большее число людей оказываются в него вовлечены. При этом до сих пор в психологической науке отсутствует сколько-либо единая концепция понимания отклоняющегося поведения и его причин. Без такой концепции невозможно решить эту проблему и выстроить эффективную систему профилактики и коррекции отклоняющегося поведения, хотя интернет-пространство представляет возможности не только для реализации отклоняющегося поведения, но и для борьбы с ним и его исправления.

Список литературы

1. Краткая характеристика состояния преступности в Российской Федерации за январь-февраль 2020 года [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации. – URL: <https://xn--b1aew.xn--p1ai/reports/item/19897618/> (дата обращения: 16.04.2020).
2. Божович, Л. И. Проблемы формирования личности: избранные психологические труды / Л. И. Божович / под ред. Д.И. Фельдштейна. – М., Воронеж : Ин-т практической психологии, 1995.
3. Кравцов, О. Г. Проблема личностного развития несовершеннолетних правонарушителей: культурно-исторический подход / О. Г. Кравцов // Культурно-историческая психология. – 2020. – № 1 (Т. 16). – С. 49–56. – DOI: <https://doi.org/10.17759/chp.2020160105>
4. Кравцов, О. Г. Использование психологических познаний для анализа поведения человека в интернете / О. Г. Кравцов // Международный журнал психологии и педагогики в служебной деятельности. – 2018. – № 2. – С. 31–36.
5. Кравцов, О. Г. Психологическое содержание понятия «девиантное поведение» в культурно-исторической теории / О. Г. Кравцов / Психолого-педагогический поиск. – 2016. – № 3 (39).
6. Шарафутдинова, Н. В. Психология девиантного поведения : учеб.-методич. пособие / Н. В. Шарафутдинова. – М. : АРКТИ, 2019.

Кругликова Софья Андреевна¹,
курсант института психологии
служебной деятельности органов внутренних дел
Московского университета МВД России
имени В. Я. Кикотя;

Ульянова Ирина Валентиновна²,
профессор кафедры педагогики учебно-научного
комплекса психологии служебной деятельности
Московского университета МВД России имени В.Я. Кикотя,
доктор педагогических наук, доцент

ПРОФИЛАКТИКА КИБЕРЗАВИСИМОСТИ НЕСОВЕРШЕННОЛЕТНИХ СРЕДСТВАМИ ПОДВИЖНЫХ И ИНТЕЛЛЕКТУАЛЬНЫХ ИГР

В настоящее время проблема киберзависимости становится все более актуальной. Отмечается рост числа научных трудов, посвященных данной проблеме.

Среди отечественных исследователей, которые изучали киберзависимость, следует обозначить работы А. Л. Вегнер, Ю. Д. Бабаева, Д. М. Зиновьева, К. Янга, Н. И. Алтухова, О. В. Рычкова, К. Ю. Галкина, И. Г. Ситкина и других. В зарубежной литературе также отмечаются труды таких ученых, как А. Фрейд, Д. Винникота, М. Кляйн, Б. Спока, М. Маллер, Р. И. Спиз и др.

Перейдем к определению понятия «киберзависимость». Л. Н. Юрьева и Т. Ю. Больбот в монографии «Компьютерная зависимость: формирование, диагностика, коррекция и профилактика» определяют киберзависимость/интернет-зависимость как навязчивое или компульсивное желание войти в интернет, находясь off-line, и невозможность выйти из интернета, находясь online [5].

В современных условиях отмечается все большее количество несовершеннолетних, столкнувшихся с проблемой киберзависимости в своей жизни. На это указывает все большее количество проведенного времени в интернет-пространстве по сравнению с прошлыми годами.

М. Орзак выделил характерные для компьютерной зависимости психологические и физиологические признаки личности:

1. Психологические симптомы: хорошее самочувствие или эйфория за компьютером; невозможность остановиться; увеличение количества времени, проводимого за компьютером; пренебрежение семьей и друзьями; ощущение пустоты, депрессии, раздражения не за компьютером; ложь учителям и членам семьи о своей деятельности; проблемы с работой и учебой.

2. Физиологические симптомы: синдром карпального канала (туннельное поражение нервных стволов руки, связанное с длительным перенапряжением мышц); сухость в глазах; головные боли по типу мигрени; боли в спине; нере-

¹ © Кругликова С. А., 2020.

² © Ульянова И. В., 2020.

гулярное питание, пропуск приема пищи; пренебрежение личной гигиеной; расстройства сна, изменение режима сна.

Несовершеннолетние имеют несформировавшуюся психику, характеризующуюся нестабильностью в силу возрастных особенностей, а также несформированные физиологические данные, что указывает на повышенную подверженность влиянию негативных последствий киберзависимости.

Несовершеннолетние могут иметь различные виды ведущей деятельности, в зависимости от своего возраста; однако с момента поступления в школу игра, как ведущий вид деятельности возрастного периода 3–7 лет, не уходит на второй план, она плавно совмещается преподавателями с учебным видом деятельности, что подчеркивает ее значимость для личностного становления несовершеннолетнего. В школе дети развивают мышление, осваивают чтение и письмо, изучают иностранные языки, сталкиваясь с новой для себя обстановкой. Это дает несовершеннолетнему возможность расширить круг известных ему игр и вызывает повышение интереса к компьютерному пространству, в котором ему необходимо искать информацию. Учитывая, что нарастает распространение компьютерных игр среди детей и ролевая игра вытесняется из жизни младшего школьника, встает вопрос о возможности компенсации нехватки традиционной игры посредством компьютерных игр [2].

Поэтому необходимо осуществлять своевременную и комплексную профилактику киберзависимости у несовершеннолетних. По мнению И. В. Ульяновой, «педагогическая профилактика – это целенаправленная и согласованная педагогическая деятельность учителя, классного руководителя, педагога-психолога, социального педагога, привлекаемых к ней специалистов медицинских и правоохранительных учреждений в школе, включающая устойчивый комплекс взаимодополняющих видов деятельности: медико-санитарное просвещение, воспитательно-разъяснительную деятельность, психодиагностику, оформление технологической карты развития личности и класса» [5].

Профилактику киберзависимости несовершеннолетних необходимо проводить с помощью подвижных и интеллектуальных игр.

Г. К. Селевко так объясняет сущность игры: это определенный вид деятельности, который образуется в ситуативных условиях и служит для наиболее быстрого и эффективного усваивания необходимого опыта общества, включая при этом аспект самоорганизации личности.

Ф. Фребель, один из первых педагогов, выделивших игру как отдельное средство воспитания, предложил свою классификацию игр, среди которых отмечались: умственные (интеллектуальные) игры, сенсорные игры, моторные (подвижные) игры как средства профилактики киберзависимости несовершеннолетних.

О. В. Рычкова в исследовании «Психолого-педагогическая профилактика компьютерной игромании у обучающихся» предлагает в качестве средства профилактики киберзависимости использовать следующую подвижную игру: игра-имитация «Давай с нами!», цель которой – формирование умения противостоять влиянию киберпространства. В процессе этой игры члены группы изображают компанию подростков, собравшихся вокруг компьютера. Кто-то

играет в компьютерную игру, а остальные наблюдают (или играют все вместе по сетевому соединению в компьютерном клубе). Доброволец (мальчик или девочка) изображает подростка, который пытается отказаться от компьютерной игры. Задача группы – уговорить играть, задача добровольца – придумать как можно больше аргументов и способов, чтобы, не провоцируя конфликт в группе (сохранив дружеские отношения), отказаться от компьютерной игры.

Вопросы для обсуждения: Что чувствовали участники? Трудно ли было противостоять давлению группы? Что стало решающим фактором для выбора той или иной стратегии поведения? Какая стратегия поведения в данной ситуации более эффективна? Почему?

Резюме ведущего: Будущее человека – в его собственных руках. У человека всегда есть возможность сказать «нет» тем, чьи предложения не соответствуют его жизненной позиции, убеждениям, интересам или желаниям [2].

Еще пример интеллектуальной игры для профилактики данной проблемы среди несовершеннолетних: игра «Почему появляется компьютерная зависимость?». В процессе этой игры участникам выдают чистые листы бумаги, разделенные на две графы: «Причины играть в компьютер» и «Причины не играть в компьютер». По истечении определенного времени несовершеннолетние обмениваются своими ответами и делятся впечатлениями. В конце педагог подводит итоги игры и организует групповую рефлексию.

В настоящее время, к сожалению, растет процент несовершеннолетних, вовлеченных в киберзависимость с малого возраста. Неотвратимость компьютеризации населения, непосредственное влияние на личность в сфере информационных технологий отмечают многие исследователи. Несовершеннолетние, в силу своих возрастных и физиологических особенностей, наиболее подвержены негативному кибервлиянию, поэтому следует проводить своевременную комплексную профилактику в отношении них, а в процесс данной профилактики целесообразно включить интеллектуальные и подвижные игры, что поможет сбалансировать влияние киберпространства на личность несовершеннолетнего.

Список литературы

1. Зиновьева, Д. М. Психоаналитический взгляд на нарушения поведения детей и подростков: учебно-методическое пособие / Д. М. Зиновьева. – Волгоград : Изд-во ФГОУ ВПО ВАГС, 2010.
2. Рычкова, О. В. Психолого-педагогическая профилактика компьютерной игромании у обучающихся / О. В. Рычкова. – Белгород : ОГУДНППМСИ «БРЦМПСС», 2016.
3. Ситкина, И. Г. Модульная программа профилактики компьютерной зависимости у детей «Эффект бабочки» / И. Г. Ситкина. – Ярославль : ГОАУ ДОД ЯО ЦДЮ, 2014.
4. Ульянова, И. В. Социально-психолого-педагогическое сопровождение подростков с рискованным поведением в условиях смысловжизненноориентационной воспитательной системы школы / И. В. Ульянова, Т. А. Попова, И. Г. Евсеева // Современные проблемы науки и образования. – 2016. – № 5. – С. 272.
5. Юрьева, Л. Н., Больбот Т. Ю. Компьютерная зависимость: формирование, диагностика, коррекция и профилактика / Л. Н. Юрьева, Т. Ю. Больбот. – М., 2006.

Лустин Владимир Иванович¹,
*старший преподаватель кафедры информационной
безопасности учебно-научного комплекса информационных технологий
Московского университета МВД России
имени В.Я. Кикотя*

ВЗАИМОСВЯЗЬ ЦИФРОВОЙ ЭКОНОМИКИ И КИБЕРПРЕСТУПНОСТИ

Указ Президента от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», а также программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства от 28.07.2017 №1632-р позволяют рассматривать цифровую экономику как многогранное понятие. Цифровая экономика – это «хозяйственная деятельность, где ключевыми факторами производства будут данные в цифровом виде, что позволяет повысить ее действенность в отличие от других, более традиционных форм хозяйствования» [1], «в свою очередь, это экономика, основанная на новых методах генерирования, обработки, хранения, передачи данных, а также цифровых компьютерных технологиях» [7], так же «цифровую экономику можно рассматривать как результат трансформационных эффектов новых технологий общего назначения в области информации и коммуникации, которые влияют на все секторы экономики и социальной деятельности» [2].

Цифровая экономика, связанная с передовыми научными достижениями в области высоких технологий, определяемая высоким уровнем развития информационной инфраструктуры, проникает и оказывает влияние на все сферы деятельности общества, в том числе и на совершение преступлений в экономической сфере. преступности. И в частности, особенно быстро развивающейся разновидности экономической преступности – киберпреступности, которая является следствием глобализации информационных коммуникационных технологий и дальнейшего развития международных компьютерных сетей [4].

«Киберпреступность – это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей» [6]. Совершенствование информационно-телекоммуникационных технологий расширяет сферу действия киберпреступности и создает условия для ее дальнейшего существования. Новые технологии изучаются и подстраиваются под определенные механизмы преступной деятельности, что закономерно ведет к усложнению выявления, пресечения и расследования таких преступлений.

При выявлении и расследовании киберпреступлений необходимо учитывать следующие моменты:

преступления могут носить трансграничный характер, так как при совершении хищений и обналичивания денег с использованием информационных

¹ © Лустин В. И., 2020.

технологий злоумышленники могут находиться в диаметрально противоположных местах;

- одним из условий совершения киберпреступлений является высокий уровень познаний в данной предметной области;
- скрытый характер преступных действий, о которых потерпевший узнает через значительный промежуток времени;
- длительность совершения преступления находится в диапазоне от нескольких секунд или суток до месяцев. В следствие этого выявление факта совершения преступных действий, места пребывания преступника, сбора доказательств при осуществлении процессуальных действий затруднительны для правоохранительных органов.

Развитие информационной сферы вызывает совершенствование и появление новых способов совершения киберпреступлений. Раскрывая понятия и уголовно-правовые меры борьбы с преступностью можно определить «киберпреступность как совершенное общественное деяние опасное и уголовно наказуемое при использовании компьютера, интернет-сетей и программ» [5]. Рассматривая влияние цифровой экономики на киберпреступность необходимо отметить, что в УК РФ выделяются в отдельную главу общественно опасные деяния, совершенные с помощью компьютерных технологий.

Проблема квалификации таких составов преступлений состоит в том, что обнаружить эти деяния достаточно сложно, так как выделить совокупность преступлений, которые совершаются с использованием электронной информации, представляется трудной задачей. Решение проблемы с киберпреступностью предлагается законодателем в изменениях, относящихся к главе 28 УК РФ «Преступления в сфере компьютерной информации». Сегодня мошенничество в электронной среде носит многосторонний характер, совершается в компьютерной среде, с применением электронных денежных средств, а также с использованием виртуальных счетов, бирж или банков.

Одно из появившихся в свет преступлений с использованием информационных технологий мошенничество при помощи электронного ключа. Мошенники похищают и применяют против потерпевшего его же персональные данные. С помощью электронного ключа они совершают операции с собственностью и иным имуществом. «Электронный ключ – это аппаратное средство, предназначенное для защиты программного обеспечения (ПО) и данных от копирования, нелегального использования и несанкционированного распространения» [3]. Электронная подпись (ЭП) в сети равносильна подписанию собственноручной подписью юридически значимых документов. Для получения ЭП требуются только данные паспорта и номер СНИЛС, которые получает работодатель или банк при подаче документов при оформлении на работу или оформлении счетов.

Возможны мошенничества с ЭП: операции с недвижимостью физических лиц или регистрация юридического лица на граждан, которые этого даже и не подозревают. Для каждого из таких вариантов мошенничества существуют различные варианты защиты. Это в основном происходит из-за похищения необходимой для мошенничества информации путем взлома компьютерных систем,

тем самым злоумышленники получают доступ к сведениям, которые в дальнейшем используют для совершения противоправных деяний. При этом потерпевший может и не подозревать, что его данные были украдены и использованы в мошеннических целях, но, заметив неправомерное использование персональных данных, вынужден потратить большое количество времени и ресурсов для чтобы предоставить доказательства своей невиновности. Кроме того, найти подозреваемых в сетевом пространстве достаточно трудоемкий процесс, а законодательная база по киберпреступности еще недостаточно подробно разработана. Существуют и другие, более масштабные виды киберпреступлений, связанные с похищением крупных денежных средств со счетов банков и тому подобное.

Развитие информационных технологий влияет на совершенствование способов совершения мошенничества в электронной среде. Для решения проблем борьбы с киберпреступностью требуются: дальнейшее совершенствование законодательной основы регулирующей ответственность за совершение преступлений в рассматриваемой сфере; техническая поддержка правоохранительных органов, занимающихся противодействием киберпреступности; развитие межведомственного сотрудничества как на региональном так и на международном уровне в сфере защиты информационного пространства и борьбы с киберпреступностью.

Список литературы

1. Жиронкин, Д. С. Влияние цифровой экономики на киберпреступность / Д. С. Жиронкин // Молодой ученый. – 2019. – № 30.
2. Криптографические протоколы в системах с ограниченными ресурсами / [Р. В. Мещеряков и др.] // Вычислительные технологии. – 2007. – № 12.1.
3. Складов, Д. В. Аппаратные ключи защиты / Д. В. Складов. – СПб. : БХВ-Петербург, 2004.
4. Тарасов, А. Электронный банкинг и его безопасность / А. Тарасов // Экономическая политика. – М. : Флинта, 2010. – № 5.
5. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т. Л. Тропина. – М. : Прогресс, 2007.
6. Юдина, Т. Н. Осмысление цифровой экономики / Т. Н. Юдина // Теоретическая экономика. – 2016. – № 3.
7. Newsru.com – новостной портал. URL: <https://www.newsru.com/russia>.

*Майорова Ольга Вячеславовна¹,
адъюнкт кафедры основ
экспертно-криминалистической деятельности
Волгоградской академии МВД России*

О НЕКОТОРЫХ АСПЕКТАХ ПРЕСТУПЛЕНИЙ ПРОТИВ НЕСОВЕРШЕННОЛЕТНИХ, СОВЕРШАЕМЫХ В СЕТИ ИНТЕРНЕТ

Защита детей от преступных посягательств и организация качественного и своевременного расследования уголовных дел о преступлениях, совершенных в отношении несовершеннолетних, относятся к числу важнейших задач государства в области борьбы с преступностью.

Потенциальными жертвами преступлений дети были всегда. Причины тому – их доверчивость, открытость всему новому, любознательность, отсутствие страха неизвестности. Все эти факторы способствуют тому, что дети становятся идеальными мишенями для преступников.

Интернет вокруг нас: в кармане в смартфоне со всеми его многочисленными приложениями, сервисами; он в наших домах, на рабочем месте, наши дети с его помощью получают образование, мы совершаем покупки в онлайн-магазинах, узнаем в сети новости, смотрим кинопремьеры, оформляем официальные документы и общаемся с родственниками, живущими за тысячи километров от нас. Варианты использования интернета для незаконной деятельности в отношении несовершеннолетних потерпевших следующие: сексуальная эксплуатация, сексуальные домогательства, порнография (использование несовершеннолетних с целью изготовления порно материалов, либо распространение таковых материалов посредством информационно-коммуникационной сети). Возможность стать жертвой преступления против половой неприкосновенности по своим социальным последствиям для ребенка является наиболее опасной среди всего перечня преступных посягательств в отношении несовершеннолетних.

УК РФ [2] содержит несколько статей, закрепляющих составы преступлений, совершенных против половой неприкосновенности несовершеннолетних (малолетних): ст. 132 «Насильственные действия сексуального характера», ст. 135 «Развратные действия», ст. 242 «Незаконное изготовление и оборот порнографических материалов или предметов», ст. 242¹ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», ст. 242² «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов» Уголовного кодекса Российской Федерации.

Согласно ст. 5 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [1] причиняющей вред здоровью и (или) развитию детей является информация

¹ © Майорова О. В., 2020.

порнографического характера, отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения, содержащая изображение или описание сексуального насилия, представляемая в виде изображения или описания половых отношений между мужчиной и женщиной.

Согласно постановлению Пленума Верховного Суда Российской Федерации 2014 г. «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» [3], развратными могут признаваться и такие действия, при которых непосредственный физический контакт с телом потерпевшего лица отсутствовал, включая действия, совершенные с использованием интернета, иных информационно-телекоммуникационных сетей.

Данные криминальной статистики свидетельствуют о неблагоприятных тенденциях преступности в отношении несовершеннолетних, но в последние годы становится очевидной еще одна немаловажная составляющая детского неблагополучия – противоправные действия в отношении детей и подростков в информационно-телекоммуникационной сети.

По данным ГИАЦ МВД России, в январе-феврале 2020 г. зарегистрировано более 60 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [4].

Интернет развязал преступникам руки, предоставив широчайший арсенал средств для реализации ими своих преступных намерений. Кто знает, довел бы злоумышленник свой преступный замысел до конца, в реальности, если бы интернет не существовал? Стал бы он искать жертву преступления в своем ближайшем окружении, или ограничился лишь сексуальными фантазиями на интересующую его тему?

К сожалению, интернет с его поистине безграничными возможностями смел все препятствия между преступником и его потенциальной жертвой, создав условия для противоправного общения.

Возможности интернет-общения многогранны: 1) переписка в социальных сетях, мессенджерах (сервисах быстрого обмена сообщениями), включающая как текстовую составляющую, так и фото-, видеоконтент, которым обмениваются пользователи, 2) видеозвонки (с помощью Skype, WhatsApp и пр., 3) онлайн-эфир в соцсетях (VK, Одноклассники, Instagram) 4) закрытые форумы по интересам и видео-хостинги (к примеру, закрытые форумы для педофилов со сложной системой доступа).

И речь идет не только о способах реализации злоумышленником своего преступного намерения, которое он выберет в зависимости от типа личности, характера, своих психологических особенностей (к примеру, аудиоформат общения; получение видеоконтента онлайн с целью достижения сексуального удовлетворения либо запись такого рода видеоматериала для просмотра впоследствии; текстовая переписка; фотографии), но и о таких немаловажных преимуществах виртуального общения, как скорость, быстрота получения желаемого (в настоящее время меньше минуты требуется, чтобы посредством поисковых программ найти в сети требуемую информацию) и латентность, «тайность» преступного общения (современные смартфоны и высокое покрытие террито-

рии нашей страны мобильным интернетом позволяют преступнику удовлетворить любой свой интерес).

Функционал интернета как телекоммуникационной сети позволил осуществить преступникам то, что раньше казалось трудно достигаемым. В сеть с целью реализации своих преступных намерений может выйти на охоту как самый закомплексованный преступник, преследующий удовлетворение личного интереса (в случае совершения развратных действий, к примеру), так и хорошо организованная группировка, у которой есть отлаженный механизм по монетизации результата своей преступной деятельности (если речь идет о преступлении, предусмотренном ст. 242¹ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», ст. 242² «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов» УК РФ).

Безграничность интернет-пространства, как цифровой среды совершения преступлений создает определенные трудности в ходе их выявления и расследования. Зачастую с огромным трудом удается установить сведения о потерпевших, данные преступников, а также географическое нахождение места совершения преступления (локацию преступников).

Преступнику не нужно теперь выходить в реальный мир с целью поиска потенциальной жертвы, что, несомненно, в разы рискованнее для него. Смартфон, ноутбук, стационарный компьютер с выходом в сеть – и жертва найдена (и не одна!), общение налажено, процесс пошел, а обнаружится ли преступное намерение – об этом ли размышляет злодей, когда у него в телефоне фото или видеофайлы с несовершеннолетним потерпевшим, к которому он вошел в доверие?

Интернет посредством программных решений сделал возможным одновременное совершение преступного посягательства в отношении множества жертв (к примеру, одновременное общение с несколькими потерпевшими посредством онлайн-видеосервисов, мессенджеров, видеоконференций, онлайн-эфиров и т. д.). Интернет трансграничен, несовершеннолетние потерпевшие могут проживать в любой точке земного шара, главное, чтобы там был выход в сеть.

Стремительное развитие новых коммуникационных технологий и дальнейшее распространение влияния информационных ресурсов на повседневную жизнь граждан будут способствовать совершению преступлений против личности путем использования интернет-пространства. Усиливающаяся виртуализация социальной жизни детей и подростков предопределяет дальнейший рост преступлений против половой неприкосновенности и половой свободы личности несовершеннолетних, что продолжит негативную тенденцию последних лет.

Список литературы

1. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. от 01.05.2019) // СПС «КонсультантПлюс» (дата обращения: 15.04.2020).

2. Уголовный кодекс Российской Федерации (ред. от 07.04.2020) от 13.06.1996 № 63-ФЗ (с изм. и доп., вступ. в силу с 12.04.2020) // СПС «КонсультантПлюс» (дата обращения: 15.04.2020).

3. Постановление Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» // Бюллетень Верховного Суда Рос. Федерации. – 2015. – № 2.

4. Состояние преступности в России // URL: <https://мвд.рф/-reports/item/19412450> (дата обращения: 15.04.2020).

Мандрикова Валерия Вячеславовна¹,
*слушатель факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя;*

Иванов Вячеслав Юрьевич²,
*начальник кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, доцент*

ПРОВЕДЕНИЕ ИССЛЕДОВАНИЯ ПРИ ВЫЯВЛЕНИИ СЛЕДОВ РАБОТЫ ЭКСПЛОЙТОВ

В условиях активного развития информационных технологий перед экспертными подразделениями МВД России встает задача определения незаконного программного обеспечения и/или распространения вредоносного программного обеспечения (эксплойтов) со стороны правонарушителей.

Рассмотрим вопросы обнаружения следов активности эксплойтов в рамках проведения компьютерных исследований экспертными подразделениями МВД России.

В настоящее время преступления в сфере компьютерной информации имеют незначительный удельный в общей структуре преступности, однако прослеживается тенденция к их ежегодному росту. Согласно ведомственной статистике за 2019 г. зарегистрировано 82 185 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 27,2 % выше показателей аналогичного периода прошлого года.

Готовые программные решения не исключают возможности проведения кибератак на пользовательские компьютеры, определяя уязвимость утечки информации как одну из наиболее актуальных проблем в области информационной безопасности.

Взаимодействие органов предварительного расследования с экспертными подразделениями отвечает критериям эффективности в борьбе с киберпреступностью, в рамках которых определено использование незаконного программного обеспечения и/или распространения вредоносного программного обеспечения со стороны правонарушителей.

Одним из подвидов вредоносного программного обеспечения являются эксплойты. Их популярность в среде киберпреступников в отличие от многих других методов заражения компьютеров, предполагает использование методов социальной инженерии, что не всегда приводит к реализации поставленных задач. Методы заражения, использующие уязвимости в системах защиты ПЭВМ, позволяют противникам достигать поставленных целей.

¹ © Мандрикова В. В., 2020.

² © Иванов В. Ю., 2020.

Эксплойт представляет собой программу, набор данных, исполняемый код, часть кода, использующие уязвимости в системных и прикладных программах, предоставляя злоумышленнику доступ к целевой системе.

Для понимания принципа функционирования эксплойта необходимо дать определения понятиям «пейлоуд» и «шелл-код». Shellcode (шелл-код) – набор инструкций, используемый эксплойтом как полезная нагрузка, обеспечивающая доступ к командной оболочке операционной системы. Payload (пейлоуд) – фактический код, используемый на целевой системе после компрометации цели.

Потенциально уязвимая система сканируется на предмет обнаружения доступных портов и запущенных процессов, в результате чего выявляются слабые «точки». Далее на данные точки отправляется эксплойт с прикрепленным к нему пейлоудом, который позволяет определить тип подключения к шелл-коду, а также определить, какие действия необходимо произвести относительно целевой системы после того, как к ней получен доступ.

Первый этап в запуске эксплойтов повышение привилегий, что позволяет выполнять заданные коды, набор действий в которых задается злоумышленниками. После того как эксплойт получает доступ к системе, используя обнаруженные уязвимости, проводится загрузка дополнительных вредоносных программ с серверов злоумышленников, которые могут осуществлять кражу персональных данных, использовать зараженные компьютеры в качестве компонента бот-сети для рассылки спам-сообщений или выполнения DDoS-атак, шифрования дисковых областей и др.

Объекты атаки эксплойтов:

- браузеры с наличием уязвимостей, позволяющих исполнять «произвольные коды», т. е. проводить установку и запуск неких вредоносных программ в системе в фоновом режиме, либо спровоцировать определенное, заложенное в код, поведение системы;
- операционные системы: эксплойты используют уязвимости компонентов операционной системы для исполнения заложенного вредоносного кода. Для пользователей наиболее опасный вариант заражения использование эксплойтов, позволяющих удаленно проводить установку кода в операционную систему;
- приложения MSOffice, Java, объекты flash-анимации, системы просмотра видео-контента, средства работы с файлами pdf и др.

Своевременное обновление программного обеспечения не всегда позволяет обеспечить защиту от активности эксплойтов, причина которой – наличие временного зазора между обнаружением уязвимости и выходом обновления, которое ее исправляет.

В течение данного промежутка времени эксплойты могут свободно функционировать и создавать угрозы безопасности при отсутствии установленных в системе автоматических средств предотвращения атак. Таким образом, успешность атаки определяется наличием версий программного обеспечения, в которых не проведено устранение уязвимостей.

Наиболее часто происходит заражение не одним эксплойтом, а сразу несколькими, так как для обеспечения эффективности атаки злоумышленникам необходимо воздействовать сразу на несколько уязвимостей. В наборах эксплойтов широко используются специализированные методы запутывания кода,

что позволяет избегать обнаружения и определения интернет-адресов с целью помешать процессу их вычисления со стороны аналитиков.

В рамках предварительного расследования необходимо привлечение экспертов и специалистов, которые смогут установить факт создания и применения вредоносного программного обеспечения (эксплойта) конкретным лицом. Однако определение программы как вредоносной, не входит в компетенцию эксперта. В рамках исследования эксперт может раскрыть общий алгоритм работы программы, определить ее функционал, тем самым выводы эксперта носят ориентирующий характер для разрешения вопроса о вредоносности программы.

Исходя из вышесказанного в соответствии с особенностями досудебного производства по уголовным делам о преступлениях в сфере компьютерной информации в рамках производства компьютерных исследований эксперт в пределах компетенций имеет право:

1. Установить время создания вредоносной компьютерной программы, для чего необходимо: синхронизировать время, установленное на электронно-вычислительной машине, с реальным временем; исследовать журнал операций по изменению времени на ЭВМ, которые производились пользователем.

2. Определить место совершения преступления: место написания программного кода вредоносной программы; место компиляции программного обеспечения; место нахождения объекта преступного посягательства.

3. Установить способы совершения преступления, для чего эксперт должен определить, каким способом было произведено «заражение» вредоносным программным обеспечением.

В случае установления использования вредоносного программного обеспечения в совершении преступления, может быть установлена одна из трех версий способа совершения: установка вредоносного программного обеспечения с различных переносных накопителей; распространение вредоносного программного обеспечения через локальную сеть; распространение вредоносного программного обеспечения глобальной сети.

Таким образом, в процессе исследования объекта, поступившего в рамках проведения компьютерного исследования, первоначально необходимо определить:

- место нахождения вредоносного программного обеспечения;
- способы «заражения» вредоносным программным обеспечением;
- пути распространения вредоносного программного обеспечения и установить источник, под которым подразумевается ЭВМ, на которой было скомпилировано вредоносное программное обеспечение, или на котором находилась его копия в момент начала реализации преступного умысла;
- установить источник, от которого произошла передача вредоносного программного обеспечения.

Список литературы

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. – М. : РИОР ИНФРА-М, 2018. – 334.

2. Иванова, А. В. 3D-моделирование места преступления / А. В. Иванова, А. О. Путилов // Борьба с киберпреступностью в условиях развития цифрового общества : сб. науч. статей Междунар. конференции. – 2019. – С. 191–192.

Марков Егор Ильич¹,

*заместитель командира взвода Института подготовки
сотрудников для органов предварительного расследования
Московского университета МВД России имени В.Я. Кикотя;*

Гончар Владимир Владимирович²,

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

НЕКОТОРЫЕ СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В ИНФОРМАЦИОННОЙ СФЕРЕ И ПУТИ ИХ ПРЕДУПРЕЖДЕНИЯ

Из информации ГИАЦ МВД России следует, что с каждым годом количество киберпреступлений неумолимо растет, а преступность в информационной сфере процветает и имеет высокую степень латентности, поэтому с каждым годом уменьшается количество возбуждаемых уголовных дел по данным составам преступления. Поэтому правоохранительным органам и частным компаниям все тяжелее бороться с киберпреступниками, которых с каждым годом становится больше, а способы совершения преступлений все сложнее.

Для эффективной борьбы с преступлениями в информационной сфере и использованием технических средств государственным органам необходимы современная техническая база, должное финансовое и материальное обеспечение, квалифицированные и подготовленные кадры, а также одно из главных – развитую и современную систему законодательства, которая не только идет в ногу со временем, но и опережает его. Поэтому законодательство, а именно глава 28 УК РФ, требует определенных доработок и повышения эффективности использования механизма уголовно-правового регулирования.

Одним из факторов увеличения числа преступлений в сфере компьютерной информации являются неосведомленность и неграмотность определенной части населения нашей страны относительно процессов и сущности информационных компьютерных технологий, что приводит к неосторожности и небрежности при пользовании различными благами информационной среды, что впоследствии именно большинство видов компьютерных преступлений имеют возможность совершаться и существовать лишь благодаря данному фактору.

Сегодня подавляющее большинство банков и кредитных организаций имеют программы банковского банкинга, с помощью которых пользователь с мобильного устройства (смартфон, планшет, смарт-часы и т. д.) может производить различные операции по своему счету в реальном времени, при подключении интернета или же посредством СМС-сообщений. При этом некоторые операторы сотовой связи после смены номера или при отказе владельца от его использования, не отвязывают привязку номера телефона от банковского счета. После этого сотовый оператор может продать данный номер следующему кли-

¹ © Марков Е. И., 2020.

² © Гончар В. В., 2020.

енту, который получает возможность выполнить некоторые удаленные операции по счету, в том числе осуществлять банковские транзакции, без участия реального владельца счета. Тогда может внезапно возникнуть умысел, так как лицо неумышленно приобретает у компании оказывающую услуги связи SIM-карту с номером, привязанному к банковскому счету прежнего владельца, но после прихода СМС-уведомления от банка, например о совершении какой-либо банковской операции, которые зачастую рассылаются пользователям, осознает, что номер используется в качестве привязки к какому-либо пользователю банка, и после этого у данного лица возникает умысел на совершение преступления. Злоумышленники снимают денежные средства небольшими суммами для того, чтобы банк не заблокировал данные операции как подозрительные.

В настоящее время все банки имеют систему 3D-Secure, т. е. защищенный протокол для пользователей CNP-операций, без присутствия карты (чаще всего используется для оплаты в интернет-магазинах, при этом покупатель для оплаты вводит реквизиты банковской карты), который добавляет дополнительный шаг для проведения оплаты, заключающийся в отправке банковской организацией специального кода-подтверждения (может отправляться по СМС-сообщениям либо уведомлением в мобильное приложение банка, который необходимо ввести для проведения транзакции. Очень важно, чтобы интернетсайт и банк были обоюдно подключены к протоколу 3D-Secure [3].

Итак, вернемся к передаче номера телефона другому пользователю сотового оператора. При использовании протокола 3D-Secure код безопасности от банковской организации приходит преступнику, а не старому владельцу номера, который вводит его при оплате товаров и услуг, имея лишь данные вашей карты, которые могут сохраняться на различных сайтах и доступом к номеру мобильного телефона. Такие преступные действия мошенников надлежит квалифицировать по ст. 272 и 159 УК РФ.

Обратиться к судебной практике. Из приговора № 1-287/12 от 19 октября 2012 г. по делу № 1-287/12 Свердловского районного суда г. Белгорода следует: Т., находясь в зоне действия базовой станции сотовой связи, действуя с единым преступным умыслом, направленным на хищение чужого имущества, из корыстных побуждений, используя абонентский номер гражданина И. (который не предоставлял законного права использовать информацию по его банковской карте третьим лицам), подключенный к банковской карте, осознавая, что имеет неправомерный доступ к охраняемой законом компьютерной информации – данным, находившимся на лицевом счете денежным средствам, сформировал и направил на специальный номер оператора мобильной связи БМБ-сообщение для перевода денежных средств на счет мобильного телефона, предоставленное в форме электрического сигнала, осуществив копирование информации с лицевого счета банковской карты И., с последующей модификацией, выраженной в изменении первоначальных данных по движению денежных средств по счету, незаконно списав с лицевого счета банковской карты в свою пользу денежные средства, принадлежащие И., осуществив неправомерный доступ к охраняемой законом компьютерной информации, т. е. произвел ее копирование и модифи-

кацию из корыстной заинтересованности. Данные действия суд квалифицировал по ст. 158 ч. 2 п. «в», ч. 2 ст. 272 УК РФ [4].

Статья 272 не предъявляет требований к «вредоносности» модифицированной информации, т. е. действия преступника будут квалифицироваться по вышеупомянутой статье вне зависимости от причиненного им ущерба [2]. Соглашаясь с позицией Ю. И. Ляпунова, следует считать, что моментом окончания доступа к компьютерной информации будет «момент отсылки пользователем компьютеру последней интерфейсной команды (голосовой, нажатием клавиши и т. д.) вызова хранящейся информации, независимо от наступления дальнейших последствий» [3]. Преступлением это деяние станет только при наступлении указанных в диспозиции последствий. Все действия, выполненные до подачи последней команды, образуют состав неоконченного преступления.

Таким образом, несогласованность действий кредитных организаций и компаний, предоставляющих услуги сотовой связи, а также невнимательность их клиентов ставят под угрозу безопасность банковских счетов людей, сменивших мобильного оператора, или поменявших абонентский номер, развязывает руки злоумышленникам, что приводит к увеличению роста преступности в данной сфере.

Поэтому необходимо обязать операторов сотовой связи сообщать банковским организациям информацию о смене номера или отказа клиента от номера. При этом банк или сотовый оператор должны известить клиента о том, что его номер телефона привязан к его банковским данным и этим могут воспользоваться злоумышленники.

Необходимо также введение в средних образовательных организациях (школах, лицеях, гимназиях, колледжах) занятий по информационной безопасности, так как зачастую дети начинают пользоваться интернетом, компьютером и другими устройствами довольно в раннем возрасте. Дебетовую карту некоторых банковских организаций возможно получить по достижении четырнадцатилетнего возраста и начать ее использовать. Стоит указать на необходимость издания постановления Пленума ВС РФ, касаясь преступлений в сфере компьютерной информации, необходимость которого назревает в течение многих лет и всеми признается целесообразным.

Список литературы

1. Дворецкий, М. Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 уголовного кодекса РФ / М. Ю. Дворецкий // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2013. – № 12 .
2. Ляпунов, Ю. И. Ответственность за компьютерные преступления / Ю. И. Ляпунов // Законность. – 1997. – № 1.
3. Банки.ру // URL: <https://www.banki.ru/wikibank/3d-secure/> (дата обращения: 20.03.2020).
4. Судебные и нормативные акты Российской Федерации // URL: <https://sudact.ru/regular/doc/Vegz2QhJyTY9/> (дата обращения: 22.03.2020).

Михайленко Наталья Васильевна¹,
доцент кафедры административной деятельности ОВД
Московского университета МВД России имени В. Я. Кикотя,
кандидат юридических наук

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Киберпреступность – это явление не одной конкретной страны, а всего мира, цифровые преступления не знают границ и совершаются из любой точки мира. Мировая статистика по совершению киберпреступлений весьма удручающая. Так, каждый час во всем мире совершается около 50 тыс. информационных и цифровых преступлений. Больше всего подобных видов противоправных посягательств совершается в США, на которые приходится около 23 % всех деяний, Китай, с 9 %, Германия и Великобритания делят по 8 % всех цифровых преступлений.

Предполагаемая стоимость ущерба, причиненного хакерами, вредоносными программами и нарушениями данных, по прогнозам, достигнет \$ 6 трлн с 2020 по 2021 г. Более 92 % вредоносных программ доставляется по электронной почте. С помощью правильных информационных кампаний и политики, а также усердия на практике можно устранить более 90 % вредоносных программ, лишь обучая новым навыкам, которые преодолевают укоренившиеся модели поведения.

Особое беспокойство вызывают проблемы, с которыми сталкиваются органы внутренних дел при исполнении своих полномочий и расследовании совершенных преступных посягательств. В частности, повсеместное развитие цифровых технологий приводит к тому, что правоохранительные органы всего мира сталкиваются с проблемами осуществления своей деятельности в условиях повсеместной цифровизации.

Первостепенная проблема всех правоохранительных систем в борьбе с цифровыми преступлениями заключается в том, что подавляющее большинство преступников молоды и соответственно быстрее адаптируются к происходящим изменениям, тогда как в правоохранительных органах картина противоположная, при высоком среднем возрасте сотрудников наблюдаются некоторая заостренность сознания и неспособность использовать передовые технические разработки. Так, по состоянию на 2019 г., преступники в возрастном диапазоне от 16 до 30 лет составляют 35 % общего количества лиц, совершивших преступные деяния. При этом в сфере преступлений, связанных с цифровыми и информационно-телекоммуникационными технологиями процент молодых преступников еще выше, и составляет 90 % для категории возраста от 16 до 35 лет. Вместе с тем средний возраст сотрудников правоохранительных органов 35–40 лет, что, хотя и не говорит о их неспособности раскрывать киберпреступления, однако свидетельствует о низком уровне знаний именно в сфере

¹ © Михайленко Н. В., 2020.

цифровых технологий, что подтверждается приведенной ранее статистикой низкой раскрываемости преступных деяний в области цифровых и телекоммуникационных технологий.

Дополнительной проблемой, которая касается Российской Федерации, ряда стран Восточной Европы и Южной Америки, а также некоторых Восточноазиатских стран, стала недостаточно развитая материальная база правоохранительных органов, особенно это заметно в регионах, которые фактически не способны обеспечить возможность расследования и раскрытия киберпреступлений. К этому можно отнести и общее снижение численности сотрудников во всех структурах, что создает повышенную нагрузку на оставшихся должностных лиц и в некоторых ситуациях не позволяет заниматься сложными информационными преступлениями.

Суть проблемы в том, что как отмечалось ранее киберпреступность не имеет границ и не заключена в рамках одного государства, это вызов всему международному сообществу. Однако на практике, например в Германии, Англии и Франции, ответственность за некоторые категории цифровых преступлений варьируется от двух месяцев до двух лет, в США может достигать даже десяти лет тюремного заключения, а в ряде стран Южной Америки ответственность отсутствует вовсе, а международные офшорные зоны способствуют легализации и отмыванию доходов полученных посредством совершения цифровых преступных посягательств. Вместе с тем, основной международно-правовой акт в сфере борьбы с цифровой преступностью датируется 2001 г., что не позволяет говорить о сколь-либо достойном правовом регулировании в этой сфере. По сути регулирование киберпреступлений отдано, но откуп национальным законодательствам, в корне неверен.

Главенствующей проблемой в подавляющем большинстве стран остается несовершенство уголовного и уголовно-процессуального закона в контексте цифрового развития общества, государства и соответственно преступности.

Наиболее совершенно в вопросе уголовно-правового противодействия посягательствам в указанной сфере законодательство США. В нем криминализирован широкий спектр деяний, совершаемых в финансовой сфере с использованием информационно-телекоммуникационных технологий: мошенничество, совершаемое с использованием «электронных средств платежа, новых методов и услуг», а также создание, распространение и иные манипуляции с электронными средствами доступа и преступления, связанные с «кражей личности». Конструкция юридических норм американского законодательства позволяет привлекать к ответственности за противоправные деяния в финансовой сфере с использованием новых, еще не получивших широкого распространения информационно-телекоммуникационных технологий.

В большинстве стран наблюдаются тенденция по ужесточению ответственности за противоправные посягательства в IT-сфере и непрерывная реформация норм уголовного законодательства как реагирование на возникающие угрозы. Ужесточение ответственности за посягательства с использованием информационно-теле-коммуникационных технологий, учитывая неограниченность круга потенциальных жертв от преступных действий и размеры причиняемого ущер-

ба, должно быть реализовано и в отечественном законодательстве. Интересными для имплементации в отечественное уголовное законодательство представляются реализованные в законодательстве Франции и Литвы нормы, предусматривающие ответственность лиц, принимающих поддельную платежную карту к оплате.

В правоохранительной среде ситуация вообще становится весьма странной, международное законодательство и правовые акты большинства государств хотя законодательно и указывают на возможность и необходимость использования цифровых и современных технологий, однако только общими словами, не существует правового акта, который в полном объеме регулировал работу органов правопорядка с цифровыми и компьютерными технологиями.

В Уголовном кодексе Франции нормы, предусматривающие ответственность за компьютерные преступления, содержатся в двух книгах. Так, в книгу вторую «О преступлениях и проступках против личности», содержащую главу «О посягательствах на личность», включены составы таких преступлений, как незаконные действия с личными данными в телекоммуникационных системах. В книге третьей «Об имущественных преступлениях и проступках» размещена глава «О посягательствах на системы автоматизированной обработки данных», нормы которой предусматривают уголовную ответственность за ее неправомерное использование. Из этого следует, что уголовно-правовой охране подлежат личные данные, а также телекоммуникационные системы. Специальных норм о хищениях, совершаемых с использованием компьютерной информации, Уголовный кодекс Франции не содержит.

Англосаксонская правовая система не предусматривает кодификацию законодательства, поэтому в Великобритании ответственность за совершение компьютерных преступлений устанавливают различные статуты: Закон о неправомерном использовании компьютера, Закон о телекоммуникациях (обман), Закон об электронном сообщении, а также Закон о защите персональных данных, Закон о телевизионных лицензиях (раскрытие информации), Закон о борьбе с обманом в области социального обеспечения. Однако ни один из перечисленных статутов напрямую не устанавливает ответственность за совершение хищений в сфере компьютерной информации. Законом о неправомерном использовании компьютера предусмотрены: ответственность за несанкционированный доступ к компьютерным материалам; несанкционированный доступ с намерением совершить или облегчить совершение дальнейших правонарушений; несанкционированные действия с намерением нанести ущерб в отношении нарушения работы компьютера и т. д.; несанкционированные действия, вызывающие или создающие опасность значительного ущерба; изготовление, поставка или получение изделий для использования в вышеуказанных правонарушениях. Иначе говоря, компьютерная информация в одних случаях объект преступления, в других – предмет и, наконец, средство, способ совершения преступления.

В Уголовном кодексе ФРГ компьютерное мошенничество выделено в отдельное преступление, параграфом 263а установлена ответственность за действия с целью получения для себя или третьего лица противоправной имущественной выгоды, которыми наносится вред имуществу другого лица посред-

ством воздействия на результат обработки данных компьютера путем составления неправильных программ, использования неправильных или неполных данных, несанкционированного применения данных или иного неправомерного воздействия на процесс обработки данных. Компьютерная информация в этом случае выступает способом совершения хищения.

Статьей 246-11 Уголовного кодекса Японии предусмотрена ответственность за противоправное извлечение выгоды посредством изготовления электромагнитной записи, противоречащей истине, а именно установлено, что лицо, которое путем подачи в ЭВМ, используемую в профессиональной деятельности другого лица, сфальсифицированной информации либо неправомерной команды предоставило для использования в ведении дел другого лица противоречащую истине электромагнитную запись относительно приобретения, утраты либо изменения имущественного права и таким образом приобрело противоправную имущественную выгоду или позволило это иному лицу, наказывается лишением свободы с принудительным физическим трудом на срок не свыше 10 лет. Кроме того, в Японии уголовная ответственность за незаконное проникновение в компьютерные системы и информационные сети с целью кражи, порчи информации, а также использование с целью извлечения дохода и причинения ущерба законным владельцам предусмотрена в законе «О несанкционированном проникновении в компьютерные сети»

В современных условиях, кадры действительно решают все, при этом следует обращать внимание и на международный опыт построения работы правоохранительных структур и подбор кадров. Так, например, в Германии и Англии используется позитивный опыт криминальной цифровой разведки, которая в закрытом режиме работает с преступниками и террористами. Исследователи, правоведы и практики, закономерно отмечают, что создание и становление подразделений киберполиции и криминальной разведки являются необходимыми точками роста для всей международной правоохранительной системы, данное условие имеет в том числе прямое отношение и к Российской Федерации.

Щелкина Елена Алексеевна¹,
курсант Института подготовки
сотрудников для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя;

Никулова Екатерина Александровна²,
доцент кафедры юридической психологии
учебно-научного комплекса психологии служебной
деятельности Московского университета МВД России
имени В.Я. Кикотя, кандидат психологических наук

К АНАЛИЗУ ПОВЕДЕНЧЕСКИХ ПРОЯВЛЕНИЙ КУРСАНТОВ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ В КИБЕРПРОСТРАНСТВЕ

Цифровые технологии, мобильные устройства и социальные сети становятся неотъемлемой частью нашей жизни. Так, согласно отчету Digital 2020, количество интернет-пользователей в России составило 118 млн. Это означает, что около 81 % россиян пользуются интернетом, а 48 % всего населения страны – пользователи социальных сетей [4].

Стремительный рост популярности интернета и социальных сетей объясняется тем, что с помощью данных инструментов человек может удовлетворить не только внешние потребности, но и внутренние. Например, за большим количеством «селфи» в личном профиле может скрываться гипертрофированная потребность в признании и одобрении окружающих, а фотографии из путешествий нацелены на демонстрацию своего статуса [5].

Курсанты образовательных организаций МВД России так же активные пользователи интернета и социальных сетей. Они используют данные инструменты и в образовательных целях: например Е. Е. Кургалеева отмечает, что, «используя интернет и электронную библиотечную систему, можно достаточно быстро найти необходимую информацию для написания реферата или научной работы, что целенаправленно повышает кругозор, повышает мотивацию к дальнейшему саморазвитию и активизирует самопознавательную деятельность», так и в личных – создание и ведение профиля в Instagram, ВКонтакте, в которых курсанты удовлетворяют свою потребность в самовыражении и самоутверждении в значимой группе и в социуме в целом.

Обучающиеся не всегда понимают, что тот служебный статус, в котором они находятся, накладывает существенные ограничения на объем информации, возможно транслируемый в социальные сети. Это связано с тем, что опубликованные личные данные курсанта могут нанести ему репутационные потери.

¹ © Щелкина Е. А., 2020.

² © Никулова Е. А., 2020.

У обучающихся 1–3 лет службы еще не в полной мере сформирован образ своей будущей деятельности, потому возможно размещение информации о своем месте жительства, месте работы, о близких лицах. Эта информация может стать предметом шантажа со стороны правонарушителей. Зачастую курсанты не осознают взаимосвязь между публикацией личных фотографий, написанием постов в аккаунтах, некорректное общение с использованием ненормативной лексики в социальных сетях и возможные последствия для создания личного образа будущего сотрудника органов внутренних дел, создания имиджа образовательных организаций и в целом всей системы МВД.

Для глубокого осознания репутационных последствий курсантами руководство образовательных организаций МВД проводит с ними постоянную разъяснительную работу, объясняя, что курсант у большинства членов общества ассоциируется с готовым специалистом, а не со студентом, который только осваивает будущую профессию. Поэтому курсант должен воздержаться от оскорбительных комментариев, фотографий, порочащих честь полицейского сообщества и участия в группах, транслирующих жестокие взгляды и одобряющие противозаконное поведение.

Еженедельно курсанты подписывают инструктажи, в которых говорится «о недопустимости размещения в сети Интернет и социальных сетях (Вконтакте, Facebook, Instagram и т. д.) фотографий и/или видео в форменном обмундировании, а также фотографий и/или видео с оружием, спиртными напитками; любой информации порочащей моральный облик, деловую репутацию, авторитет сотрудника органа внутренних дел и не соответствует нравственно-этическим принципам».

Но, даже несмотря на постоянную профилактическую работу, до сих пор возникают ситуации опубликования фотографий, порочащих моральный облик сотрудника ОВД. Так, по проведенному анализу комментариев в группе «Омбудсмен полиции» социальной сети «Вконтакте»: «и это наше будущее поколение», «что будет дальше», «какое нас ждет будущее». Не всегда на данных фотографиях курсанты находятся в форменном обмундировании. Это фотографии в свободное от службы время, но с демонстрацией алкоголя. Для усиления воздействия на общество, касаясь вопроса воспитания будущих сотрудников правоохранительных органов, авторы данных публикаций прикрепляют фотографию курсанта в форменном обмундировании, которая демонстрирует гордость службы в ОВД, а следом – порочащую первоначальный образ как самого курсанта, так и всех представителей полицейского сообщества.

Нередко подобные записи публикуются анонимами, которые получили их в результате взлома личных страниц курсантов, или людьми, которым отправлялись эти фотографии личным сообщением. Несомненно, подобные публикации негативно отражаются на репутации системы ОВД в целом.

Для недопущения подобных ситуаций курсантам требуется разъяснить, что никто не застрахован от взлома личных страниц в социальных сетях. Поэтому не следует даже в личных переписках отправлять фотографии, которые впоследствии могут быть скомпрометированы злоумышленником.

Не стоит забывать и о базовых способах защиты личных данных в социальных сетях. Во-первых, придумать сложный пароль с сочетанием заглавных и прописных букв, а также знаков препинания. Во-вторых, не использовать одинаковые пароли для своих профилей в разных социальных сетях. Дополнительная мера защиты – двухэтапная аутентификация. После ее настройки при входе в аккаунт у вас будут запрашивать не только пароль, но и код, который придет на ваш номер по SMS [6].

В планируемом исследовании будет продолжен анализ основных мотивов поведения, поведенческие проявления курсантов в цифровом пространстве и факторы, влияющие на непонимание нарушения личного пространства в виртуальном мире. Для повышения имиджа сотрудника внутренних дел необходимо развивать в курсантах духовно-нравственные качества и личную ответственность за поведение в цифровой среде.

Список литературы

1. Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 06.02.2020) «О полиции» // Собр. законодательства Рос. Федерации. – 2011. – № 7. – Ст. 900.
2. Кургалеева, Е. Е. Педагогическая целесообразность и возможности информационных технологий в становлении субъектной позиции курсанта / Е. Е. Кургалеева // Вестник Восточно-Сибирского института МВД России. – 2013. – URL.: <https://cyberleninka.ru/article/n/pedagogicheskaya-tselesoobraznost-i-vozmozhnosti-informatsionnyh-tehnologiy-v-stanovlenii-subektnoy-pozitsii-kursanta-1> (дата обращения: 14.04.2020).
3. Гаврина, Е. Е. Репутационно-правовые риски курсантов образовательных организаций ФСИН России в киберпространстве / Е. Е. Гаврина, Т. А. Симакова // Ведомости уголовно-исполнительной системы. – 2019. – URL.: <https://cyberleninka.ru/article/n/reputatsionno-pravovye-riski-kursantov-obrazovatelnyh-organizatsiy-fsin-rossii-v-kiberprostranstve> (дата обращения: 12.04.2020).
4. Саймон Кемп. Digital 2020 // Глобальный цифровой обзор. – URL.: <https://datareportal.com/reports/digital-2020-global-digital-overview> (дата обращения: 12.04.2020).
5. Что могут рассказать о нас фотографии, которые мы выкладываем в соцсети // ADME. – URL.: <https://www.adme.ru/svoboda-psihologiya> (дата обращения: 15.04.2020).
6. Как защитить себя от взлома и утечки личных данных // informburo.kz.

Платонов Дмитрий Анатольевич¹,

*начальник кафедры физической подготовки учебно-научного комплекса
специальной подготовки Московского университета
МВД России имени В.Я. Кикотя*

ОСНОВНЫЕ МЕТОДЫ ОБУЧЕНИЯ ДВИГАТЕЛЬНЫМ УМЕНИЯМ И НАВЫКАМ КУРСАНТОВ И СЛУШАТЕЛЕЙ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ СИСТЕМЫ МВД РОССИИ

Одно из основных направлений в процессе обучения курсантов и слушателей в образовательных учреждениях системы МВД России организация физической подготовки. Данная дисциплина направлена на выработку и закрепление определенного перечня качеств как физических, так и психологических, которые позволят в дальнейшем осуществлять на высоком уровне основные задачи и функции сотрудника органов внутренних дел, с учетом особенностей профессиональной деятельности. Структура обучения представлена двумя блоками: теоретическим и практическим. В данной статье будет уделено внимание именно практическому блоку, а точнее, основным методам, применяемым сотрудниками кафедр при проведении занятий, направленных на формирование общих и специальных физических качеств.

Профессорско-преподавательский состав кафедр физической подготовки учебно-научного комплекса, опираясь на основной нормативный правовой акт «Наставление по организации физической подготовки в органах внутренних дел Российской Федерации», утвержденное приказом МВД России от 1 июля 2017 г. № 450 [1], осуществляют построение практических занятий по приобретению общих и специальных навыков и умений курсантами и слушателями путем использования следующих основных методов:

- повторный;
- интервальный;
- равномерный;
- моделирования;
- групповой и др.

Рассмотрим каждый из представленных методов подробнее.

Специфика повторного метода: во время проведения занятия преподаватель предлагает выполнить курсантам и слушателям определенный перечень заданий, направленных на развитие двигательных качеств, по окончании выполнения которых, дается достаточное количество времени, позволяющее организму восстановиться, а затем осуществляется повтор данных упражнений. Ключевым отличием от второго метода – интервального, является промежуток времени, выделяемый в качестве отдыха. Так, при организации занятия с помощью интервального метода перед курсантами и слушателями ставится задача о необходимости повтора определенных преподавателем действий спустя избранные временные интервалы.

¹ © Платонов Д. А., 2020.

Равномерный метод применяется практически при каждом проводимом с курсантами и слушателями практическом занятии. Цель – выполнить упражнения в едином темпе, непрерывно. Такая нагрузка позволяет выработать у курсантов и слушателей силовую и скоростную выносливость.

Наиболее специфический – метод моделирования, поскольку он направлен на организацию симитированных ситуаций, с которыми в дальнейшем, учитывая специфику служебной деятельности, могут столкнуться курсанты и слушатели образовательных учреждений системы МВД России. Такой метод применяется в процессе изучения основных навыков и приемов борьбы. С учетом тематики представляется возможным реализовать модель боевой обстановки или модель задержания.

Применение группового метода основано на реализации учебно-тренировочного процесса курсантами и слушателями в составе взвода с целью наделить всех обучающихся едиными базовыми знаниями в области физической подготовки.

Основные методы организации занятий позволяют приобрести необходимые двигательные умения и навыки курсантами и слушателями образовательных организаций системы МВД России. Однако это не весь перечень методов, применяемых профессорско-преподавательским составом кафедр физической подготовки учебно-научного комплекса специальной подготовки. Но эти способы наиболее распространены и эффективны, а также позволяют провести практические занятия по физической подготовке реализуя все поставленные перед курсантами и слушателями цели и задачи.

Список литературы

1. Приказ МВД России от 1 июля 2017 г. № 450 «Об утверждении Наставления по организации физической подготовки в органах внутренних дел Российской Федерации» // Официальный интернет-портал правовой информации. – URL: <http://www.pravo.gov.ru> (дата обращения: 01.06.2020).
2. Карданов, А. К. Значение физической подготовки в профессиональной деятельности современного полицейского / А. К. Карданов А. К. // Теория и практика общественного развития. – 2014. – № 14. – С. 118–120.
3. Мешев, И. Х. Средства и методы развития приоритетных профессиональных качеств сотрудников специальных подразделений в процессе физической подготовки / И. Х. Мешев // Наука и спорт: современные тенденции. – 2018. – № 3. – URL: <https://cyberleninka.ru/article/n/sredstva-i-metody-razvitiya-prioritetnyh-professionalnyh-kachestv-sotrudnikov-spetsialnyh-podrazdeleniy-v-protsesse-fizicheskoy> (дата обращения: 01.06.2020).
4. Факов, А. М. Методы и способы развития физической выносливости у сотрудников спецподразделений МВД России / Факов, А. М. // Теория и практика общественного развития. – 2015. – № 15. URL: <https://cyberleninka.ru/article/n/metody-i-sposoby-razvitiya-fizicheskoy-vynoslivosti-u-sotrudnikov-spetspodrazdeleniy-mvd-rossii> (дата обращения: 01.06.2020).
5. Факов, А. М. Развитие общей выносливости у сотрудников ОВД : учеб. пособие / А. М. Факов. – Нальчик, 2013. – С. 22–24.

Попов Алексей Вячеславович¹,
курсант радиотехнического факультета
Воронежского института МВД России;

Анисимов Сергей Леонидович²,
старший преподаватель кафедры физики
Воронежского института МВД России,
кандидат технических наук

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Сотрудники органов внутренних дел, осуществляя свою деятельность, сталкиваются с большим количеством трудностей, связанных с возникающими угрозами общественной безопасности. На современном этапе развития общества информация представляет большую ценность. Когда речь идет о сведениях конфиденциального характера, в том числе, о Государственной тайне, то нарушение безопасности, целостности, доступности и своевременности ее получения и обработки чревато крайне негативными последствиями для безопасности как населения, так и государства в целом. Широкий спектр выполняемых сотрудниками полиции задач создает необходимость совершенствования механизмов автоматизации обработки большого объема данных, циркулирующего в информационных системах ОВД. Своевременность получения сведений об оперативной обстановке на вверенной территории напрямую влияет на скорость и рациональность принимаемых управленческих решений в целях поддержания общественного порядка и обеспечения общественной безопасности населения.

Одним из таких механизмов является применение искусственного интеллекта (нейросетевых технологий). Основные характеристики [1] таких сетей представлены на рис. 1.



Рис. 1. Основные характеристики нейронных сетей

¹ © Попов А. В., 2020.

² © Анисимов С. Л., 2020.

Информация – один из основных объектов защиты в деятельности ОВД, поэтому функционирование нейросетевых технологий должно быть направлено на: ускорение процессов приема, передачи и обработки информации; противодействие сторонним вредоносным компьютерным программам и DDOS-атакам; минимизацию или исключение вероятности быть подвергнутым интернет-мошенничеству, которое выражается в хищении информационных ресурсов и денежных средств [2].

Анализ статистики преступлений [3], совершенных с использованием искусственного интеллекта (ИИ), свидетельствует о том, что злоумышленники широко используют дроны для транспортировки запрещенных товаров (оружия, наркотиков, донорских органов), получения аудио- и видеоинформации с режимных объектов органов внутренних дел и других ведомств. В преступной деятельности ИИ и нейросетевые технологии для осуществления атак на торговые интернет-порталы, финансовую инфраструктуру коммерческих организаций, инвестиционных компаний; внедрения в структуру программного обеспечения, управляющего финансовыми операциями в интернет-пространстве. Наряду с этим перед сотрудниками правоохранительных органов возникают задачи, связанные с необходимостью разработки нейросетей [4], включающих алгоритмы противодействия каждой из приведенных угроз.

Общая структурная схема нейронной сети ОВД (см. рис. 2):

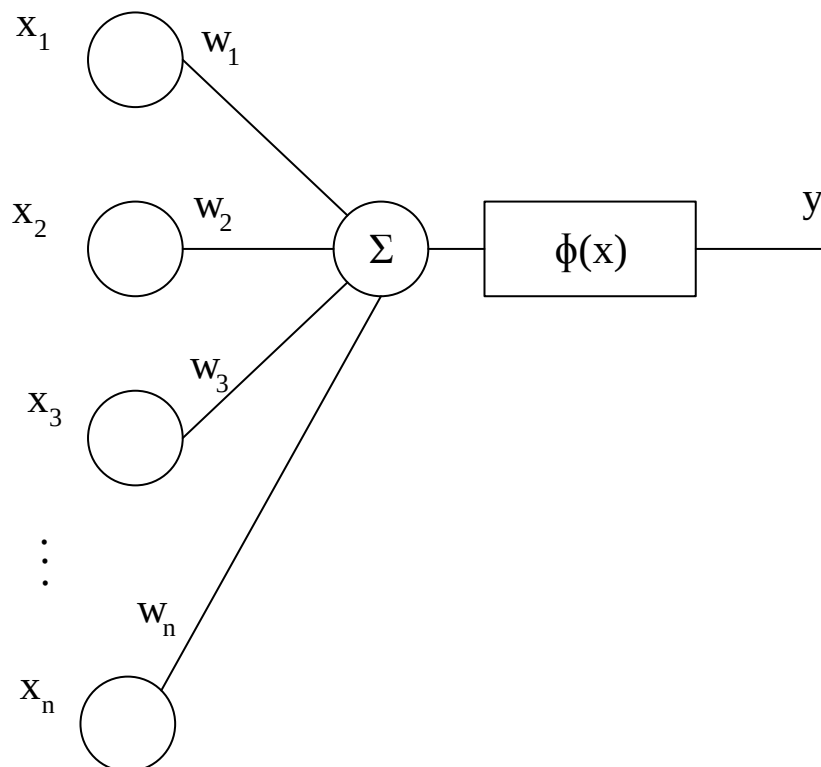


Рис. 2. Структурная схема нейронной сети

На рис. 2 представлена однослойная нейронная сеть, где: множество $\{x_1, x_2, \dots, x_n\}$ представляет собой входную последовательность сигналов, множество $\{w_1, w_2, \dots, w_n\}$ – весовые коэффициенты нейронов, $\varphi(x)$ – активационная функция сети, y – выход нейронной сети.

Основными перспективами развития нейросетевых технологий в деятельности ОВД являются повышение точности распознавания лиц, фото-, аудио- и видеоматериалов, перевод и воспроизведение речи [5, 6]. Технологии автоматического перевода речи позволят сотрудникам полиции в режиме реального времени взаимодействовать с иностранными гражданами без помощи переводчика. Не менее важное достоинство нейросетей – чтение по губам, осуществляемое на 30 % эффективней, чем при помощи специалиста. В результате повышения точности распознавания речи появится возможность воспроизводить и анализировать речевую информацию из видеоматериалов с отсутствующим звуком.

Таким образом, применение ИИ в деятельности подразделений ОВД обеспечит повышение эффективности противодействия киберпреступности в современном обществе; уровня экономической и информационной безопасности. Технологии преобразования информации повысят коммуникабельность правоохранительных органов и обеспечат интеграцию в мировое сообщество

Список литературы

1. Моделирование «разумной» жизни на базе нейронных сетей [Электронный ресурс], 2015. – URL: <https://habr.com/ru/post/265201/> (дата обращения: 10.03.2020).
2. Кузьмин, И. А. Искусственные нейронные сети: перспективы использования в правоохранительной деятельности / И. А. Кузьмин // Криминалистика: вчера, сегодня, завтра. – 2018. – С. 109–116.
3. Киберпреступность в мире [Электронный ресурс], 2016. – URL: <http://www.tadviser.ru/index.php/> (дата обращения: 18.03.2020).
4. Горбачевская, Е. Н. Классификация нейронных сетей / Е. Н. Горбачевская // Вестник Волжского университета им. В.Н. Татищева. – 2012. – С. 42–47.
5. Фаустова, К. И. Нейронные сети: Применение сегодня и перспективы развития / К. И. Фаустова // Территория науки. – 2017. – С. 83–87.
6. Абрагин, А. В. Перспективы развития и применения нейронных сетей / А. В. Абрагин // Проблемы современной науки и образования. – 2015. – С. 12–15.

Рудакова Наталия Константиновна¹,
*курсант факультета подготовки
 специалистов в области информационной безопасности
 Московского университета МВД России
 имени В.Я. Кикотя;*

Клочкова Екатерина Николаевна²,
*доцент кафедры информационной безопасности
 учебно-научного комплекса информационных технологий
 Московского университета МВД России имени В.Я. Кикотя*

РАСПРОСТРАНЕНИЕ В СЕТИ ИНТЕРНЕТ КОНТЕНТА СУИЦИДАЛЬНОГО ХАРАКТЕРА КАК УГРОЗА БЕЗОПАСНОСТИ ОБЩЕСТВА

Проблема совершения самоубийств несовершеннолетними продолжает оставаться актуальной. Среди молодых людей суицид занимает вторую строчку в качестве причины смертности после ДТП, только за последний 2019 г. на территории г. Москвы зафиксировано больше 200 таких происшествий, из них более 50 случаев закончились смертельным исходом, около 90 подростков совершили осознанные попытки совершения самоубийств, и только пять случаев из общего числа были признаны несчастными.

В последние годы увеличилось количество случаев, когда подростков склоняют к принятию решения уйти из жизни, вовлекая их в различного рода игры, которые изначально проходят на просторах интернета, а со временем переходят в реальный мир, и их результат приводит к суициду. Общество пытается бороться с этим явлением. Ситуации, в которых человек лишает себя жизни под влиянием других людей, подпадают под признаки составов преступлений, предусмотренных ст. 110 УК РФ («Доведение до самоубийства»), ст. 110¹ УК РФ («Склонение к совершению самоубийства или содействие совершению самоубийства») и ст. 110² УК РФ («Организация деятельности, направленной на побуждение к совершению самоубийства»).

Наступление общественно-опасных последствий нередко связано с необдуманным поведением самих потерпевших, наличием семейных проблем, возрастными особенностями психики подростков, но, тем не менее, нельзя оставлять без внимания наличие умысла у организаторов и разработчиков подобного рода развлечений. Разработка таких игр основана на знаниях особенностей психологии подростков, технологий влияния на человека и, несомненно, носит социально-деструктивный общественно опасный характер.

Административное законодательство также содержит ряд положений по рассматриваемой проблеме. Например, предусмотрена административная ответственность за нарушение законодательства Российской Федерации (ст. 6.17

¹ © Рудакова Н. К., 2020.

² © Клочкова Е. Н., 2020.

КоАП РФ), а также ответственность по ст. 13.21 КоАП РФ за нарушение средствами массовой информации порядка ее распространения.

Проведенное нами исследование, связанное с выявлением несовершеннолетних пользователей интернета, склонных к совершению самоубийства, а также пользователей, склоняющих подростков к суициду, позволило выявить в социальной сети «ВКонтакте» более сорока сообществ, размещающих контент деструктивного толка, схожего с «группами смерти» (в настоящее время заблокированы).

Проведенные в рамках исследования мероприятия позволили установить, что большинство таких групп создают несовершеннолетние лица, которые проявляют интерес к тематике данного направления, но не имеют намерений склонять к суициду других лиц. В группах смерти используются привычные приемы психологического воздействия, которые крайне усиливаются в совокупности с психологией подростка и средой его нахождения:

1. Использование факторов кризиса идентичности подростка. Протест против заботы родителей и преувеличенное восприятие реальности.

2. Эксплуатация травм и опыта. Эти группы активно вовлекают молодых людей в свою деятельность, пользуясь ситуациями, созданными проблемами последних с родителями, школой, сверстниками и др.

3. Использование транса и вдохновляющего общения. Кураторы общаются с подростками уверенно, категорично, тем самым производят на них сильное впечатление и создают ощущение поддержки наставника. Приобретая, авторитет в глазах подростков, кураторы умело начинают ими манипулировать.

4. Нарушение сна. Во многих группах для выполнения заданий и ритуалов необходимо вставать ночью. Учитывая, что подростки фактически все время проводят в интернете, это практически полностью лишает их сна. Часто в преддверии выполнения неотложных задач участники обязаны не спать всю ночь. Это значительно снижает способность адекватно воспринимать происходящее и значительно повышает внушаемость подростка.

5. Классическая манипуляция «взять верх над слабым». В большинстве случаев для работы этого механизма, не требуется целенаправленной стимуляции извне.

6. Крайний срок для принятия решения. Каждая задача игры ограничена во времени, что не оставляет подростку возможности обдумать свои действия или их последствия.

7. Использование информации.

8. Эксплуатация страха. Участвующих в игре подросток не понимает, какой информацией владеет куратор и как далеко он готов зайти в своих действиях. Кураторы создают иллюзию своего всемогущества и создают вокруг себя атмосферу страха.

9. Создание романтизма и эстетизма вокруг смерти. Смерть преподносится как нечто таинственное и прекрасное, для чего демонстрируются видео с загадочными элементами, особой музыкой, фотографиями и последними словами красивых парней и девушек, которые покончили жизнь самоубийством.

10. Эксплуатация чувства избранности и превосходства, принадлежащие «группам смерти» выше всех остальных.

Одним из основных факторов, способствующих распространению «групп смерти» в интернете, стала анонимность. Зачастую, подросток, общаясь через интернет-сообщества, даже не подозревает, с кем ведет диалог и насколько опасны последствия такого общения. Анонимность становится препятствием для правоохранительных органов для быстрого выявления преступников, использующих завуалированные «ники» в своих сообществах и на страницах. Для решения данной проблемы на уровне Правительства уже звучат предложения о создании единого оператора, который бы мониторил контент для детей в интернете.

Основные виды угроз:

1. Доступность в интернете большого количества материалов, имеющих деструктивный характер по отношению к молодежи.

2. Перенасыщение контента интернет-источников ресурсами, содержащими в себе возможности виртуальной реальности, которая при непрерывном использовании может нанести непоправимый психологический вред молодежи.

3. Недостаточное отслеживание и блокирование ресурсов, содержащих информацию, запрещенную для детей и подростков и наносящую им какой-либо вред.

4. Отсутствие комплексной системы реализации психологических условий профилактики самоубийств среди молодежи.

5. Невозможность привлечения лиц к ответственности, а именно существование пробелов в уголовном и административном законодательстве, в частях, касающихся определения способов и средств доведения до самоубийства, а также возраста наступления ответственности за совершенное деяние данного типа.

6. Молодежь, имеющая психические расстройства, наркотическую или алкогольную зависимость вследствие просмотра контента, наносящего моральный вред и побуждающего к суицидальным действиям.

В средствах массовой информации все чаще появляются сообщения о совершении самоубийств несовершеннолетними, а в интернете распространяются видеоролики, на которых подростки совершают акты самоубийства. Если же рассматривать данное явление в глобальном масштабе, то согласно данным «Парламентской газеты» становится очевидно, что всплеск активности приходится именно на территорию России и близлежащих стран (Казахстан, Кыргызстан, Украина), что свидетельствует о внешнем целенаправленно сформированном информационно-психологическом процессе коррекции чужого информационного пространства в нужном направлении.

Организованные самоубийства происходят во всем мире, но, тем не менее, центр массовых самоубийств сосредоточен именно в России. Данный факт свидетельствует о том, что враждебные Российской Федерации страны, объявили ей информационную войну с целью умышленного истребления русского народа и других народов Российской Федерации с помощью внедрения скрытых специальных деструктивных психологическо-информационных технологий, при-

водящих к изменению разума подростков до уровня, который был бы удобен для манипуляции их сознанием. Таким образом, если будущее поколение России, способное защитить свою Родину, сохранить ее духовное и материальное наследие, развить и возвысить ее, останется и далее подверженным вышесказанному влиянию, то произойдут мощный подрыв и разрушение духовной силы русского народа, что неизбежно приведет к масштабным необратимым негативным последствиям, что и составляет самую главную угрозу.

Представленная тема имеет большой потенциал для дальнейшего развития, так как в настоящее время не существует истории «доведения до самоубийства (ст. 110 УК РФ)», «склонения к совершению самоубийства или содействия совершению самоубийства (ст. 110¹ УК РФ)» и «организации деятельности, направленной на побуждение в совершению самоубийства (ст. 110² УК РФ)» в уголовном законодательстве, а количество преступлений, связанных с суицидами несовершеннолетних, в Российской Федерации с каждым годом возрастает.

Список литературы

1. Закон Российской Федерации от 27.12.1991 № 2124-1 (изд. из 29.07.2017) «О средствах массовой информации».
2. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (в ред. от 29.07.2017) (ред. и доб., соединенный. действует с 26.08.2017).
3. Кадников, Н. Г. Уголовное право России. Общая и Особенная части / Н. Г. Кадников. – М. : Городец, 2006.
4. Шарапов, Р. Квалификация преступлений, связанных с вовлечением в самоубийство и иное опасное для жизни поведение / Р. Шарапов // Уголовное право. – 2017. – № 6.
5. <https://www.gazeta.ru/social/2019/04/25/12321139.shtml>.
6. https://expert.ru/russian_reporter/2019/18/nepreryivnyj-suitsid/.

Савенкова Дарья Дмитриевна¹,
*руководитель направления Управления противодействия
кибермошенничеству Департамента кибербезопасности
ПАО «Сбербанк»*

НОВЫЕ ТРЕНДЫ КИБЕРУГРОЗ: КАК НЕ СТАТЬ ЖЕРТВОЙ

Современный мир стремительно развивается и меняется. Если отбросить стереотипы, то становится, очевидно, что жертвами мошенников могут быть не только пенсионеры и другие незащищенные слои нашего общества. Бесспорно, они первые в зоне риска, в которой находимся все мы.

В последнее время активность кибермошенников в социальных сетях с использованием методов социальной инженерии растет высокими темпами. По данным Сбербанка, самым распространенным видом мошенничества остается социальная инженерия – более 80 % случаев хищения пришлось именно на этот метод получения несанкционированного доступа к конфиденциальной информации.

Преступники умело пользуются доверчивостью и неосведомленностью людей. Аферисты маскируются под сотрудников служб безопасности банков, социальных служб, полиции, прокуратуры, ремонтников, сантехников и даже медиков только для того, чтобы обокрасть своих легковых жертв. Случаев и видов мошенничества – множество, и преступники придумывают все более изворотливые схемы. Рассмотрим наиболее популярные из них.

Кража «личности»

Под кражей личности мы понимаем следующее: 1) кража личных данных жертвы с целью открытия банковских счетов или оформления тарифа у мобильного оператора на имя потерпевшего; 2) получение доступа к существующим учетным записям и счетам без ведома жертвы, чтобы воспользоваться ими в целях личного обогащения.

Злоумышленники различными способами стараются заполучить персональные и иные данные клиентов различных банков, – как правило, через прямой контакт с потенциальным потерпевшим, от которого путем обмана им удастся получить нужную информацию. Если клиент сообщает мошенникам свои данные для проведения операций (номера карт, логин/пароль для входа в личный онлайн-кабинет клиента, одноразовые СМС-пароли), то у злоумышленников появляется полный доступ к счетам жертвы.

Последние полгода злоумышленники при совершении звонков якобы от имени служб безопасности банков стали активно пользоваться услугами дешевой и доступной связи посредством сервисов «Voice over IP» (далее – VoIP). География звонков с сообщениями о том, что карта гражданина якобы заблокирована или по ней происходит операция, которую он не совершал, может быть какой угодно; например IP-телефония позволяет мошенникам имитировать звонки из г. Москвы, хотя сам человек при этом находится в Ростове.

¹ © Савенкова Д. Д., 2020.

Весной 2018 г. в полицию обратились несколько жителей г. Москвы с заявлениями о том, что им поступали звонки от девушки, которая, представляясь сотрудником социальной службы, предлагала гражданам получить путевку на санаторно-курортное лечение либо денежную компенсацию взамен путевки. Граждане выбирали получение денежных средств, сообщали злоумышленнице всю конфиденциальную информацию. Впоследствии с банковских карт были похищены их сбережения другими соучастниками преступной группы. При поддержке Сбербанка подозреваемые были задержаны сотрудниками полиции, ими оказались 23-летняя девушка и трое мужчин в возрасте от 24 лет до 41 года, проживающие в Московской области [1].

Почему пострадавшие все-таки оказались в такой неприятной ситуации? Ответ очевиден – низкая бдительность и киберграмотность. Важно помнить, что только мошенники просят сообщить номер карты, CVV-код, кодовое слово и одноразовые СМС-пароли.

Самопереводы

Из всего разнообразия схем мошенничества самой распространенной по-прежнему остается схема с самопереводами, когда жертва под воздействием третьих лиц самостоятельно совершает операцию по переводу денежных средств мошенникам. В зоне риска оказываются граждане, которые либо что-то продают, или наоборот, которые что-то покупают на сайтах бесплатных объявлений или в социальных сетях, а также те, с кем мошенники вступают в переписку в социальных сетях со странички «взломанного» друга.

Мошенники знают, как вызвать доверие у своих «жертв», – они будут обращаться по имени, вежливо, предоставят все дополнительные фото с товарами, покажут отзывы «покупателей», и ответят на все вопросы.

После того как клиент самостоятельно перевел деньги мошеннику, тот тут же пропадает, а человек не может связаться с ним и жалуется в банк на несанкционированный перевод.

Самопереводы в симбиозе с VoIP дают еще одну популярную схему мошенничества. Под видом сотрудников службы безопасности банков мошенники просят от своих жертв перевести деньги на «резервный счет» для их сохранности. Конечно же, никакого резервного счета у банка нет и быть не может, мошенники пользуются доверчивостью граждан, которые в итоге сами переводят деньги на их счета.

Как ни парадоксально, но в последнее время чаще на эту уловку мошенников стали попадать не пенсионеры, а молодые люди в возрасте от 18 до 30 лет.

Что важно знать: даже если гражданину поступил звонок с номера телефона, похожего на номер его банка, но при этом «сотрудник» просит сообщить конфиденциальную информацию, то надо просто положить трубку и перезвонить в банк по номеру телефона, указанному на сайте банка или обратной стороне вашей банковской карты. Кроме того, нельзя соглашаться перевести деньги за понравившуюся вещь на мобильный телефон продавца, – это элемент мошеннической схемы. Также не стоит обращаться по объявлениям, цена по которым явно занижена, нужно просить подтвердить наличие товара видеосъемкой, сессией по скайпу и т. д.

Обман пенсионеров

Время от времени мы видим в новостной ленте сообщения о том, как мошенники под видом социальных служб или полиции обманывают доверчивых граждан. Вот, например, некоторые случаи за последнее время: выманивали деньги у пожилых людей якобы для поимки мошенников, обещали помочь оправдать осужденных близких родственников, продавали «чудодейственные» БАДы, предлагали получить по акции подарки «почти задаром», установить счетчики на воду и т. д.

Именно в нашей стране сегодня социальная инженерия приобрела особое значение, прежде всего из-за высокого уровня доверия граждан. Тенденция не утешительна, – так исторически сложилось, что люди пожилого возраста имеют высокий уровень доверия во взаимодействии с государственными структурами. Этим и пользуются мошенники, которые понимают, что пенсионеры легко предоставляют свою конфиденциальную информацию фактически любому встречному.

В конце 2018 г. в Сбербанк обратилась пенсионерка, являющаяся клиентом Банка, которая сообщила, что мошенники обманом вынудили ее перевести на их карты почти полмиллиона рублей (деньги бабушка откладывала на похороны) – несколько лет назад она покупала биологически активные добавки к пище (БАДы), которые оказались пустышками.

Примерно за месяц до визита пенсионерки в Банк ей на стационарный телефон позвонил неизвестный мужчина, представившийся сотрудником прокуратуры, и сообщил, что за купленные препараты ей полагается компенсация. Мошенник вызвал доверие клиента тем, что сразу обратился к бабушке по Ф.И.О., знал, какие лекарства она покупала и даже на какую сумму, ему было известно также из какого она города, был очень доброжелателен.

Затем пенсионерке поступали звонки от другого неизвестного мужчины, уже якобы от сотрудника Банка, который сообщал о порядке выплат и необходимости оплатить различные услуги. Сначала это были услуги адвоката, затем страховая комиссия, далее налог и банковские сборы, при этом, мнимая компенсация продолжала расти.

За несколько недель такого обмана мошенники вынудили клиентку перевести им почти все ее сбережения в размере полумиллиона рублей, которые, в свою очередь, они обналичивали в банкоматах Подмосковья.

В феврале прошлого года данная группа «телефонных» мошенников была задержана. [2] На протяжении нескольких лет им удавалось обманом заполучить от пожилых людей денежные средства на суммы от 30 тыс. до 300 тыс. рублей, обещая солидную компенсацию за совершенную ранее покупку лекарственных средств, медицинских приборов или биологически активных добавок (БАДов).

Пенсионеры – одна из наиболее уязвимых категорий граждан России, поскольку восполнить финансовые потери для них практически невозможно. Важно помнить, что, если звонящий мошенник представляется работником прокуратуры, полиции, страхового агентства, нужно обязательно уточнить у него Ф.И.О., занимаемую должность, контакты руководства, данные официаль-

ного сайта. Если злоумышленник замешкается, или что-то покажется подозрительным в разговоре с позвонившим абонентом, нужно незамедлительно обратиться в ближайшее отделение полиции или позвонить в 102! Можно оставить соответствующее заявление и на официальном сайте (МВД РФ, раздел «Для граждан»). [3] Разбираться в этом деле будет Управление «К» БСТМ. В заявлении нужно указать свои данные, номер телефона, а также номер телефона афериста, требуемую сумму, список вопросов, которые задавали, и всю известную информацию о позвонившем.

Вирусное заражение устройств клиентов с операционной системой Android

С развитием технологий компьютерное мошенничество становится все более популярным. Преступники разрабатывают новые методы компьютерных афер как источник прибыли. Но вместе с ростом числа пользователей мобильных устройств по всему миру растут и новые угрозы – вирусы.

Устройства с операционной системой Android наиболее уязвимы к вирусам [4]. Наиболее подвержены вирусной атаке могут быть клиенты банков, использующие СМС-банкинг, и пользователи мобильных банковских приложений.

Вирусы могут распространяться как через СМС/ММС-сообщения, так и через популярные мессенджеры, что резко снижает возможность их выявления и детектирования со стороны операторов сотовой связи.

Владелец смартфона получает сообщение, в тексте которого будет. Ссылка при открытии инициирует загрузку вирусной программы. Как только вирус попадает в смартфон, он начинает рассылать «вирусные» СМС по контактным листам пользователя. Параллельно он делает запрос на номер СМС-банкинга (вид дистанционного банковского обслуживания, при котором доступ к счетам и операциям по счетам предоставляется в любое время и с использованием номера мобильного телефона клиента, предварительно зарегистрированного в банке) и узнает баланс счета владельца смартфона. После этого вирусная программа переводит деньги на счета, подконтрольные злоумышленникам. Вирус способен перехватывать входящие СМС-сообщения, поэтому владелец смартфона может не знать о снятии денег со счета, оповещения о списаниях просто не доходят. Кроме того, вирус может открывать окна браузера, визуально похожие на окна авторизации банковских приложений, и при вводе данных своих карт пользователи отправляют средства напрямую мошенникам. В некоторых случаях вирус может блокировать смартфон.

Для Сбербанка безопасность транзакций клиентов – один из важнейших приоритетов при разработке цифровых сервисов. Поэтому в банке реализована эшелонированная защита, которая включает подтверждение операций с помощью одноразовых паролей, шифрование трафика, встроенные антивирусные решения в приложениях, а также системы фрод-мониторинга. Последние, за счет использования AI-моделей, нацелены как раз на предотвращение кейсов, в которых мошенникам удалось получить доступ к информации клиента.

Несмотря на прикладываемые усилия, понятно, что без участия правоохранительной системы бороться с мошенниками в одиночку невозможно.

Долгое время киберпреступники чувствовали себя практически в безопасности благодаря малозначительным и условным срокам, к которым их приговаривал суд за многомиллионные кражи (например, резонансное дело братьев Попелышей). Сейчас отношение меняется, – например Генеральный прокурор Российской Федерации считает, что актуальность роста числа киберпреступлений говорит о необходимости усиления уголовной ответственности за них [5]. И такие приговоры уже есть – суды их выносят.

Таким образом, новым трендом на государственном уровне должно стать повышение правовой и общей культуры граждан, а также эффективности деятельности государственных органов, прежде всего по профилактике дистанционных (компьютерных) преступлений.

Список литературы

1. URL: <https://77.мвд.рф/news/item/13879698/>.
2. URL: <https://www.group-ib.ru/media/pensionary-vishing/>.
3. Официальный сайт МВД РФ: URL: <https://xn--b1aew.xn--p1ai/>.
4. URL: <https://zen.yandex.ru/media/id/5b7ec863e9d9d000a95451b7/kasperskii-ustroistva-na-android-naibolee-uiazvimy-k-virusam-5bf5175c6b3ce100a9669ce9>.
5. URL: <https://ria.ru/20170426/1493145033.html?in=t>.

Саморока Виктор Анатольевич¹,
доцент кафедры уголовного процесса
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПРИНЦИПЫ ОСУЩЕСТВЛЕНИЯ УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Начавшийся процесс цифровизации современного уголовного судопроизводства имеет тенденцию к расширению, что тенденция подтверждается фактом утверждения Стратегии развития отрасли информационных технологий в Российской Федерации на перспективу до 2025 г., подписание Президентом Российской Федерации Указа от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 г.»), а также принятие Комитетом министров Совета Европы Руководящих принципов в отношении электронных доказательств в гражданском и административном судопроизводстве. Комитет министров Совета Европы (КМСЕ) принял руководящие принципы, касающиеся использования электронных доказательств в гражданском и административном судопроизводстве.

Как указывается в пресс-релизе КМСЕ, эти принципы стали первым международным документом по данной тематике и предназначены для содействия членам Совета Европы в адаптации работы своих «судебных и иных механизмов урегулирования споров» для решения вопросов в данной сфере. В документе отмечается, что руководящие принципы предназначены для создания общей правовой базы государств-членов организации в отношении использования электронных доказательств, а не гармонизации национальных законодательств, что основано на принципе уважения разнообразия правовых систем КМСЕ указал, что, несмотря на значительный прогресс в «цифровизации» судебных систем государств-членов, в них все еще сохраняются трудности, относящиеся к эффективному управлению, в частности отсутствие общих стандартов, а также различие и сложность процедур сбора и использования доказательств в электронной форме. Новые правила предлагают практические решения для ликвидации имеющихся в данной области недостатков законодательства и судебной практики. Руководящие принципы касаются осуществления дистанционного сбора устных доказательств, использования электронных доказательств, а также их сбора, изъятия и передачи. Документ охватывает также вопросы значимости, достоверности, хранения, обеспечения сохранности, и архивирования таких доказательств, касаясь проблем повышения уровня осведомленности, мониторинга, профессиональной подготовки и обучения.

¹ © Саморока В. А., 2020.

Уже год назад Европейская комиссия по эффективности правосудия приняла «Европейскую этическую хартию по использованию ИИ в судебных системах и окружающих их реалиях» [1].

Как считает комиссия ИИ может способствовать повышению качества и эффективности работы судов, но его внедрение должно производиться ответственным образом и не нарушать положений Европейской Конвенции о правах человека и Конвенции о защите личных данных. Отмечается, что эта технология должна не только остаться инструментом борьбы за общее благо, но и отстаивать личные права каждого отдельного человека.

В хартии обозначены пять основных принципов:

1. Уважение фундаментальных прав – разработка и внедрение ИИ не должна нарушать фундаментальные права человека.

2. Отказ от дискриминации, – предотвращение появления или усиления дискриминации в отношении отдельных людей и групп.

3. Качество и безопасность – обработка судебных решений и данных должна проводиться в технически защищенной обстановке, на основании проверенных источников и с применением моделей, разработанных специалистами нескольких научных дисциплин.

4. Открытость, беспристрастность и честность – методы обработки данных должны быть доступными и понятными для возможности проверки третьей стороной.

5. Контроль со стороны пользователей – они должны владеть правом выбора и необходимой информацией.

Указ Президента «О развитии искусственного интеллекта в Российской Федерации» содержит ряд принципов, регулирующих применение таких технологий, например:

– безопасность: недопустимость использования ИИ в целях умышленного причинения вреда гражданам и юридическим лицам, а также предупреждение и минимизация рисков возникновения негативных последствий использования технологий ИИ;

– прозрачность: объяснимость работы ИИ и процесса достижения им результатов.

Даже директор по информационным технологиям министерства обороны США объявил об официальном принятии пяти принципов этического использования ИИ. Ряд сформулированных ими принципов применимы как к боевому, так и не боевому использованию технологий ИИ, сказала Дана Дизи [2]:

– *ответственность*. Персонал министерства обороны США будет проявлять надлежащий уровень здравомыслия и безопасности, оставаясь ответственным за разработку, развертывание и использование возможностей ИИ;

– *беспристрастность*. Отдел предпримет преднамеренные шаги, чтобы минимизировать непреднамеренное смещение возможностей ИИ;

– *доступность для анализа*. Возможности военного ведомства США по ИИ будут разрабатываться и развертываться таким образом, чтобы сотрудники имели надлежащее понимание технологий, процессов разработки и методов работы, применимых к ИИ;

– *управляемость*. Минобороны США будет проектировать и разрабатывать возможности ИИ для выполнения их намеченных функций, обладая способностью обнаруживать и избегать непреднамеренных последствий, а также способностью отключать или деактивировать развернутые системы, которые демонстрируют непреднамеренное поведение.

Цифровые технологии проникают и в уголовное судопроизводство и постепенно получают законодательное оформление. Однако в российском уголовном процессе это пока лишь отдельные, робкие «вкрапления» цифровых технологий в сложную многофакторную деятельность, осуществляемую человеком – следователем, дознавателем, судом.

Между тем опыт применения цифровых технологий в уголовном судопроизводстве зарубежных стран значительно превышает отечественный.

Некоторые страны уже допустили более активное использование новых технологий, например: при регистрации обращений и сообщений о совершенных преступлениях (Казахстан); при производстве предварительного расследования в форме «электронного уголовного дела» (Турция, Украина и др.); при производстве в упрощенных процедурах по незначительным уголовно наказуемым правонарушениям или проступкам (Великобритания); при допуске электронного оформления различных процессуальных документов: протоколов следственных действий, процессуальных решений, в том числе и приговора по делу (Казахстан).

Сегодня в развитии науки и техники и достижений в области ИИ, видится несколько направлений его использования в уголовном судопроизводстве:

– полученные таким путем результаты будут иметь вспомогательный характер (выдвижение и анализ следственных версий, оценка информации для выработки машинных рекомендаций по производству следственных и иных процессуальных действий, подготовка решения о применении мер безопасности и т. д.);

– при должной законодательно регламентации и соответствующей технической реализации, результаты использования ИИ могут иметь доказательственное значение, при этом эти результаты могут подпадать под понятие уже существующих видов доказательств, а также может быть сформировано понятие нового вида доказательств (цифровое доказательство).

Возможности ИИ значительно отличаются от обычных программно-аппаратных комплексов, используемых правоохранителями тем, что он отчасти моделирует умственные (логические) процессы человека и будет сам решать, что ему еще надо получить для формулирования ответа на поставленный вопрос, способен к обучению.

Вопрос не в том, что «машина» сама определит направление поиска данных. Ведь эти данные, информация или «цифровые следы», уже оставлены злоумышленниками, и каким способом мы к ним «придем», не имеет значения. Вопрос в том, как проверить корректность такого получения сведений. Необходимо выработать правовой аспект алгоритмов проверки способов собирания сведений ИИ. Вероятно, что основная часть такой аналитической работы должна осуществляться только под контролем человека (следователя, дознавателя,

судьи). Например, ИИ может помочь проанализировать исходную информацию, существующую в данной криминалистической ситуации, сформировать вопросы, которые надо поставить перед допрашиваемым лицом, и т. д. А далее эти вопросы задает следователь и с учетом ответов развивает дальнейшие вопросы. При этом ИИ анализирует ответы и помогает лицу, осуществляющему следственное действие, формировать последующие вопросы. Данное взаимодействие схоже с участием специалиста в следственном действии с участием кинолога и собаки, руководствуясь их суждениями и принимая на веру как доказательство. Возможность использования ИИ также должна быть законодательно закреплена.

Упреждая критику противников использования новых технологий в уголовном процессе, утверждающих, что данные, полученные таким путем, не будут отвечать требованиям, предъявляемым к доказательствам, что это технически невыполнимо, можно с уверенностью заявить: да, решение, состоящее в требовании обнародования целых алгоритмов или исходного программного обеспечения является утопическим в этом контексте, поскольку частные компании рассматривают свои алгоритмы в качестве стратегического авторского программного обеспечения и обеспечивают им соответствующую защиту. Однако представляется возможным потребовать частичную публикацию важной информации, в частности об использованных алгоритмах, целях, преследуемых при оптимизации алгоритмов, подборе данных для настройки программы, средних значениях и типовых отклонениях в полученных результатах, или же об объеме и типе данных, обрабатываемых алгоритмом. Лица, осуществляющие проверку, могут протестировать достоверность и беспристрастность программы, например путем предоставления различных ложных исходных данных создать большое количество профилей пользователя с определенными характеристиками и т. д.

Сегодня основная задача – формулирование принципов и условий применения ИИ в уголовном судопроизводстве, законодательное закрепление таких положений в УПК РФ и других нормативных актах.

С учетом конъюнктуры правоприменителя специалисты сформулируют технические задания программистам, и те воплотят их в жизнь. Если технически реализовать законодательные предписания не получится, значит еще не пришло время для воплощения таких технологических решений. Но эти предписания должны быть нормативно оформлены уже сегодня. Следует поставить точку в этом философском споре, применительно к рассматриваемой ситуации, и воспользоваться опытом наших предков, которые уже давно решили, что «первым было слово». Этот тезис и нужно реализовать, а не подгонять закон под «сложившуюся практику» (не всегда положительную).

В этой связи можно предложить формулировку ряда ключевых положений, которые будут реализованы в принципах уголовного судопроизводства.

В юридической литературе высказываются различные суждения по поводу определения принципов, но при всех различиях они сходны в одном: принципы – это исходные, руководящие положения (начала), определяющие сущность и предназначение какой-либо теории, науки, мировоззрения, политической ор-

ганизации и т. д. Формулирование данного понятия применительно к сфере уголовного судопроизводства одна из наиболее важных теоретических проблем, так как принципы уголовного процесса представляют собой «...основные положения, определяющие всю систему процессуальных форм, весь строй процессуальных отношений» [3].

Учитывая, что уголовное судопроизводство – это правовая деятельность, имеющая под собой детально урегулированную нормативную основу соответствующие принципы должны носить императивный, властно-повелительный характер и содержать обязательные предписания, выполнение которых обеспечивается арсеналом правовых средств.

Исходя из имеющихся рекомендаций, сформулированных в международных правовых актах, а также внутригосударственном законодательстве, предлагаем дополнить УПК РФ рядом статей. В частности, в главу 2 внести ст. 19.1. Содержание данной статьи можно сформулировать следующим образом:

«Применение искусственного интеллекта в уголовном судопроизводстве.

1. Применение искусственного интеллекта в уголовном судопроизводстве допускается при производстве следственных и процессуальных действий, для содействия в обнаружении, закреплении и изъятии предметов и документов, цифровых доказательств, в исследовании материалов уголовного дела, для постановки вопросов эксперту, специалисту, принятии процессуальных решений, а также для разъяснения сторонам и суду технических вопросов, связанных с его применением, при условии, что полученные таким путем сведения отвечают требованиям, предъявляемым к доказательствам.

2. Доступность для проверки и анализа результатов применения искусственного интеллекта гарантируется. Подозреваемый, обвиняемый, потерпевший, а также другие заинтересованные участники уголовного судопроизводства имеют право на получение информации о факте использовании искусственного интеллекта и проверке полученных таким путем сведений процессуальным способом.

3. Вред, причиненный лицу в результате нарушения его прав и свобод ошибкой в работе искусственного интеллекта, подлежит возмещению по основаниям и в порядке, которые установлены настоящим Кодексом».

Список литературы

1. <https://www.coe.int/en/web/portal/home>.
2. <https://www.gazeta.ru/army/2020/02/28/12980329.shtml>.
3. Строгович, М. С. Природа советского уголовного процесса и принцип состязательности / М. С. Строгович. – М. : Юриздат, 1939. – С. 206.
4. Андреева, О. И. Проблемы использования в уголовном судопроизводстве электронных документов / О. И. Андреева, О. А. Зайцев // Правовые проблемы укрепления российской государственности : сб. статей. Ч. 79. – Томск : Изд. дом Томск. гос. ун-та, 2018. – С. 4–17.
5. Руководящие принципы Комитета министров Совета Европы в отношении электронных доказательств в гражданском и административном производстве: приняты Комитетом министров 30 января 2019 г., на 1335-м заседании за-

местителей министров. URL: <https://www.coe.int/t/ru/web/portal/-/committee-of-ministers-adopts-guidelines-on-electronic-evidence-in-civil-and-administrative-proceedin-1>.

6. Павлушина, А. А. Общие правовые институты процессуального права в информационном обществе: тенденции и перспективы развития / А. А. Павлушина, И. В. Гавриленко // Российский юридический журнал. – 2016. – № 3. – С. 10.

7. Шарипова, А. Р. Направления цифровизации уголовного судопроизводства: применимый опыт арбитражного процесса / А. Р. Шарипова // Библиотека криминалиста. Научный журнал. – 2018. – № 3. – С. 131–135.

Синицын Юрий Юрьевич¹,
адъютант Краснодарского высшего военного училища

ПРИМЕНЕНИЕ АДАПТИВНОГО АЛГОРИТМА КАНАЛЬНОГО КОДИРОВАНИЯ ДАННЫХ С БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ С ИСПОЛЬЗОВАНИЕМ СВОЙСТВ СВЕРТОЧНЫХ КОДОВ

Современные беспилотные летательные аппараты (далее – БЛА) активно развиваются и применяются в различных сферах человеческой деятельности.

Одна из важнейших задач БЛА – непрерывная трансляция потокового видеоизображения в реальном масштабе времени от БЛА на наземный пункт управления (далее – НПУ) [1].

Беспилотные летательные аппараты управляются по средствам командно-телеметрического канала передачи данных. Полезная информация с БЛА на НПУ передается по каналу целевой нагрузки. При необходимости защиты вышеупомянутых каналов передачи данных используются криптографические средства защиты информации.

Для БЛА, использующих криптографические средства защиты информации, одной из наиболее приоритетных задач является обеспечение высоких показателей скорости, надежности и качества передачи информации. Шифрование данных в командно-телеметрическом канале и канале целевой нагрузки на отечественных БЛА происходит в соответствии с алгоритмами криптографического преобразования информации с длинами блоков 128 бит («Кузнечик») и 64 бит («Магма») и длинами ключей 256 бит (ГОСТ Р 34.12-2015). Канал передачи данных должен обладать требуемой помехоустойчивостью, которая характеризует способность канала сохранять заданные количественные и качественные показатели, несмотря на наличие помех в канале связи. На рис. 1 представлена схема защищенного канала передачи данных от БЛА к НПУ с помехами.

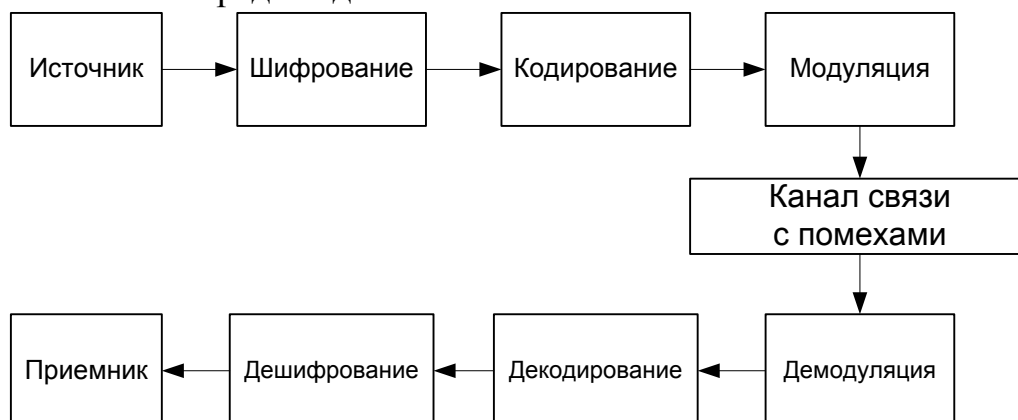


Рис. 1. Схема защищенного канала передачи данных

¹ © Синицын Ю. Ю., 2020.

При воздействии помех на передаваемые данные происходит искажение передаваемых символов, что приведет к искажению данных при получении их приемником.

Для обнаружения и исправления ошибок, вызванных помехами в каналах связи БЛА и НПУ, используются современные алгоритмы канального кодирования. В современных БЛА используются двухкаскадные кодеки с внешним кодом Рида – Соломона и внутренним сверточным кодом [2]. Схема двухкаскадного кодера с внешним кодом Рида – Соломона и внутренним сверточным кодом представлена на рис. 2.

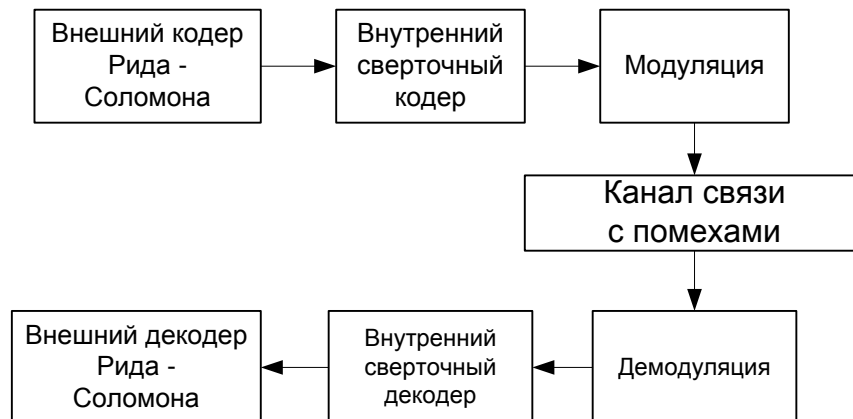


Рис. 2. Двухкаскадный кодек с внешним кодом Рида – Соломона и внутренним сверточным кодом

Код Рида-Соломона используют в качестве внешнего кода, так как он имеет хорошие характеристики как для независимых, так и для пакетированных ошибок, и хорошо устраняет ошибки на уровне транспортного пакета, выдаваемого потребителю. Внутренний сверточный код исправляет ошибки на уровне физической передачи модулированного сигнала, поэтому его часто называют модуляционным кодом. Такое построение двухкаскадного кодера имеет свои особенности.

Поскольку сверточный код работает при умеренно высоких вероятностях ошибки, то для него используют коды с малой длиной кодового ограничения и декодирование по алгоритму Витерби с мягким решением. На выходе декодера Витерби ошибки имеют тенденцию к группированию в пакеты. Поэтому для облегчения работы внешнего декодера Рида-Соломона в состав каскадного кодера вводят устройства перемежения и восстановления структуры передаваемых данных. В случае идеального перемежения ошибки на входе декодера Рида-Соломона будут независимыми, и он реализует свою максимальную исправляющую способность [3].

Предлагается использовать адаптивный алгоритм канального кодирования, основанный на свойствах сверточного кодирования внутреннего сверточного кода двухкаскадного кодера.

Свойства сверточных кодов позволяют обнаруживать и исправлять, как одиночные ошибки, так и пакеты ошибок. Обеспечения требуемой скорости передачи информации, необходимой для непрерывной трансляции потокового видеоизображения в реальном масштабе времени, можно добиться перфори-

ванными сверточными кодами. В соответствии с требованиями качества и сложности системы связи, можно использовать сверточные коды с различными кодовыми ограничениями. Схема адаптивного алгоритма представлена на рис. 3.

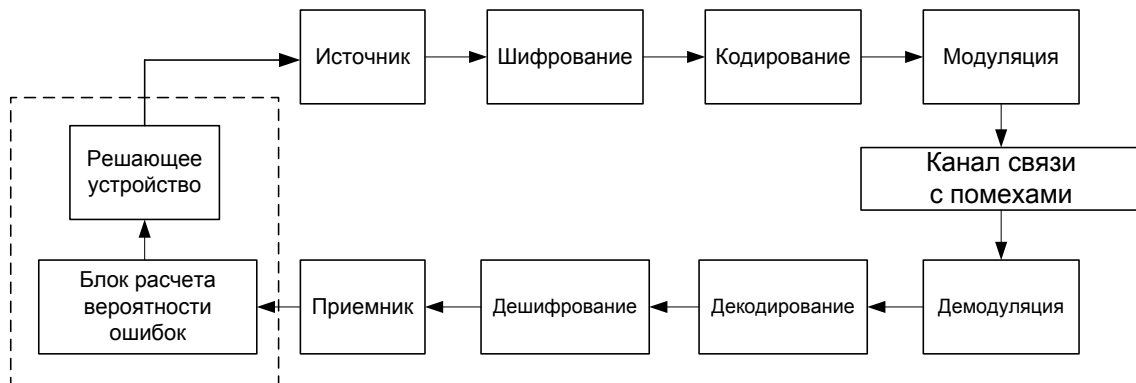


Рис. 3. Схема адаптивного алгоритма канального кодирования

Предложенный адаптивный алгоритм канального кодирования осуществляет расчет вероятности битовой ошибки. Источник передает по каналу связи приемнику тестовую последовательность. Приемник получает тестовую последовательность, заранее ему известную, и передает в блок расчета вероятности ошибок. Блок расчета вероятности ошибок анализирует количество и характер ошибок и передает данную информацию в решающее устройство. Решающее устройство вычисляет отношение сигнал / шум, для текущего момента времени, сравнивает с соответствующими значениями по пятибалльной шкале градаций качества принимаемого изображения, согласно рекомендациям Международного союза электросвязи (см. табл. 1), и выбирает оптимальный сверточный код, способный поддерживать в текущий момент времени требуемое отношение сигнал/шум.

Таблица 1

Шкала градаций качества принимаемого изображения

Качество изображения	Искажения	Отношение сигнал/шум, дБ
Отлично	Незаметно	> 46,6 дБ
Хорошо	Заметно, но не мешает	> 42,3 дБ
Удовлетворительно	Заметно, немного мешает	> 38,0 дБ
Плохо	Мешает	> 33,2 дБ
Очень плохо	Сильно мешает	> 29,2 дБ

Факторами, влияющими на выбор адаптации сверточного кода в двухкаскадном кодеке, являются возможность изменений характеристик внутреннего сверточного кодера (скорость, кодовое расстояние, шаг перфорации), влияющих на распределение ошибок в канале связи, допустимую вероятность ошибок кодовой последовательности, обеспечение требуемой скорости передачи информации.

Внутренняя структура алгоритма сверточного кодирования и декодирования позволяет производить его адаптацию при различных внешних условиях.

Параметры канала связи, требуемые передачи сигнала в текущий момент времени, с текущей помеховой обстановкой можно поддерживать свойствами сверточных кодов: необходимой скорости и оптимальным кодовым ограничением.

Для примера на рис. 4 показаны границы вероятности битовой ошибки P_b для шести сверточных кодов со скоростью $1/2$ и кодовым ограничением K от 2 до 7 [4].

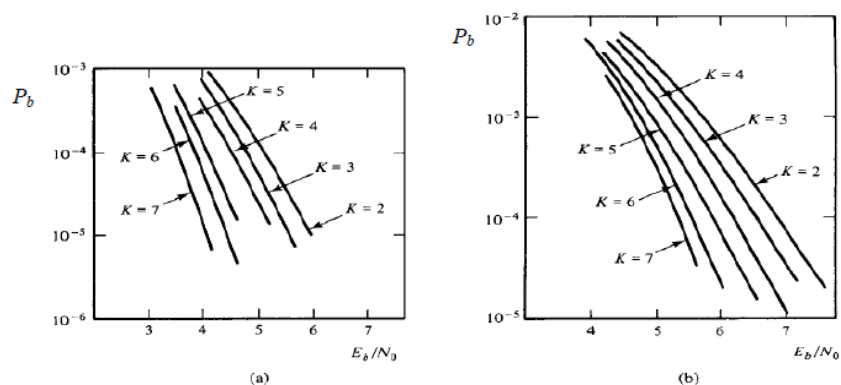


Рис. 4. Границы вероятности битовой ошибки: (а) мягкое решение, (б) жесткое решение

При одинаковом отношении сигнал / шум, данные коды имеют различные вероятности битовой ошибки. Зная вероятность битовой ошибки и значение отношения сигнал / шум в канале связи при помощи свойств сверточных кодов (скорость, кодовое расстояние, шаг перфорации) можно подобрать оптимальный код с необходимыми характеристиками для надежной и качественной передачи информации в текущей помеховой обстановке.

Несмотря на постоянные изменения помеховой обстановки в зоне выполнения беспилотными летательными аппаратами поставленных задач, требования к непрерывной трансляции потокового видеоизображения в реальном масштабе времени увеличиваются. Использование адаптивных алгоритмов помехоустойчивого кодирования позволяет поддерживать высокие показатели скорости, надежности и качества передачи информации.

Список литературы

1. Донченко, А. А. Обоснование требований к системе связи беспилотных летательных аппаратов средней и большой дальности / А. А. Донченко, Д. С. Чиров // Вестник Пермского национального исследовательского политехнического ун-та. Электротехника, информационные технологии, системы управления. – 2011. – № 5. – С. 264–270.
2. Забеньков, И. И. Моделирование цифровой радиосистемы передачи видеоданных с беспилотного летательного аппарата / И. И. Забеньков, М. И. Апанасов // Доклады БГУИР. – 2011. – № 6 (60). – С. 74–78.
3. Мамчев, Г.В. Цифровое телевизионное вещание : учебное пособие для вузов / Г. В. Мамчев. – М. : Горячая линия – Телеком, 2014.
4. Shu, L. Error control coding: Fundamentals and applications / Shu Lin, Daniel J. Costello, Jr // Frenitce-Hall series in computer applications in electrical engineering. – 1987. – С. 603.

Скле́ймин Ю́рий Бори́сович¹,
доцент кафедры информационных технологий
Московского авиационного института,
кандидат технических наук;

Чеботарева Виктория Альбертовна²,
студентка кафедры информационных технологий
Московского авиационного института

ПРИМЕНЕНИЕ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ ДЛЯ ФИЛЬТРАЦИИ ИЗОБРАЖЕНИЙ. РЕАЛИЗАЦИЯ МЕТОДА ВО ВСТРАИВАЕМЫХ СИСТЕМАХ

Благодаря развитию аппаратных средств становится возможным применение технологии обработки изображений в различных отраслях деятельности. Методы цифровой обработки изображений требуют высокой производительности вычислительных систем и применения специальных аппаратных средств.

До недавнего времени использование данных методов было затруднено. С появлением высокопроизводительных процессоров с низким энергопотреблением появилась возможность использовать технологии обработки изображений во встраиваемых системах.

Одной из часто встречающихся задач является фильтрация изображений. Фильтрация необходима при реализации фундаментальных операций компьютерного зрения, распознавания образов и улучшения качества изображений. Существует большое разнообразие фильтров позволяющих решать следующие задачи: сглаживающие фильтры (Гауссовский фильтр, фильтр Баттерворта), контрастоповышающие фильтры, фильтры выделения границ. Фильтрация трудоемкая задача и может быть выполнена с использованием одного из подходов – работа в пространственной области (непосредственно с пикселями изображения) или работа в частотной области с применением различных ортогональных преобразований. Для фильтрации в частотной области широко используется преобразование Фурье. Работа в частотной области позволяет снизить вычислительную сложность алгоритмов фильтрации, но возможна реализация только линейных фильтров. [1] Общая схема фильтрации в частотной области описывается выражением:

$$g(n_1, n_2) = \Phi^{-1}[H(k_1, k_2)F(k_1, k_2)] ,$$

где $F(k_1, k_2)$ – ДПФ исходного изображения $f(n_1, n_2)$ размерами $N_1 \times N_2$, $H(k_1, k_2)$ – передаточная функция фильтра, Φ^{-1} – обратное ДПФ, а $g(n_1, n_2)$ – результат фильтрации (выходное изображение). Функции F , H , и g представляют

¹ © Скле́ймин Ю. Б., 2020.

² © Чеботарева В. А., 2020.

собой массивы размерами $N_1 \times N_2$, как и исходное изображение. Произведение $H(k_1, k_2)F(k_1, k_2)$ формируется как поэлементное произведение массивов. Для ДПФ что существуют эффективные алгоритмы его вычисления. Двумерное ДПФ, задается формулами:

$$F(k_1, k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2) \exp(-j \frac{2\pi}{N_1} n_1 k_1 - j \frac{2\pi}{N_2} n_2 k_2)$$

, для $0 \leq k_1 \leq N_1 - 1$ и $0 \leq k_2 \leq N_2 - 1$. (1)

Если ввести сокращенное обозначение для комплексной экспоненты

$$W_N = \exp\left(-j \frac{2\pi}{N}\right),$$

то

$$F(k_1, k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2) W_{N_1}^{n_1 k_1} W_{N_2}^{n_2 k_2} \quad (2)$$

Прямое вычисление данных выражений не эффективно из-за высокой трудоемкости. Одним из методов снижения трудоемкости служит разбиение двумерного ДПФ на строки и столбцы. Сначала выполняются одномерные ДПФ для всех строк изображения затем для всех столбцов [2]. Еще больше снизить трудоемкость позволяет использование алгоритма быстрого преобразования Фурье (БПФ). Оценка трудоемкости для этих случаев показана ниже.

Для прямого вычисления

$$C_{\text{пр}} = N_1^2 N_2^2,$$

Комплексных сложений и умножений.

Для метода разложения на строки и столбцы прямого вычисления

$$C_{\text{с.с. пр}} = N_1 N_2 (N_1 + N_2).$$

Если числа N_i являются степенями числа два, то можно использовать алгоритм БПФ и число комплексных умножений будет определяться:

$$C_{\text{с.с. БПФ}} = N_1 N_2 \frac{\log_2 N_1 N_2}{2},$$

Необходимое число сложений больше в два раза.

Вычислительная эффективность является достоинством технологии фильтрации изображений в частотной области. К недостаткам относится необходимость работы с комплексными числами, которые будут содержать матрицы $H(k_1, k_2)$ и $F(k_1, k_2)$, кроме того, из-за накопления ошибок округления результат обратного преобразования Фурье может содержать не только действительные значения, но и комплексные величины.

Для устранения этих недостатков предлагается использовать дискретное косинусное преобразование (ДКП). ДКП эффективно используется в алгоритме сжатия изображений JPEG и по своим свойствам аналогично дискретному преобразованию Фурье. Применение ДКП к матрице действительных чисел (исходному изображению) дает на выходе также матрицу действительных чисел. Это свойство дополнительно снижает трудоемкость и упрощает алгоритмы. По аналогии с (1) двумерное ДКП, задается формулами:

$$F(k_1, k_2) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} f(n_1, n_2) \cos \left[\frac{\pi}{N_1} \left(n_1 + \frac{1}{2} \right) k_1 \right] \cos \left[\frac{\pi}{N_1} \left(n_1 + \frac{1}{2} \right) k_1 \right],$$

для $0 \leq k_1 \leq N_1 - 1$ и $0 \leq k_2 \leq N_2 - 1$,

Если ввести сокращенное обозначение для базисной функции

$$W_N^{nk} = \cos \left[\frac{\pi}{N} \left(n + \frac{1}{2} \right) k \right],$$

то получим выражение полностью аналогичное (2).

Для реализации методов фильтрации в частотной области и их возможного применения во встраиваемых системах, необходимо использовать высокопроизводительные платформы. Дополнительной возможностью повышения быстродействия является применение многопроцессорных архитектур. Эффективная реализация параллельных вычислений на многопроцессорных архитектурах требует дополнительных исследований. В качестве платформы для экспериментальной проверки была выбрана демонстрационная плата Parallella Desktop (P1601) [3].

Плата предназначена для построения энергоэффективных вычислительных систем и исследований в области параллелизма, и построена на базе процессора Zynq ARM/FPGA SoC работающего под управлением дистрибутива Ubuntu 15.04, названного Parabuntu, а также 16-ядерного сопроцессора Eriphany. Порты включают microSD, GbE, micro-HDMI, и два USB. Четыре 60-pin разъема служат для расширения ввода-вывода и связаны с FPGA и с чипом Eriphany. Для данной платы доступен набор инструментальных средств, позволяющий выполнить разработку и тестирование алгоритмов фильтрации изображений в частотной области и исследовать возможности их реализации на многопроцессорных системах. В частности, доступны компилятор GCC C/C++ с библиотеками для реализации параллельных вычислений, интерпретатор языка Python и другие средства разработки. Для программ на C/C++ может использоваться отладчик GDB – Eriphany debugger. Имеются примеры реализации алгоритмов быстрого преобразования Фурье.

Экспериментальная проверка показала возможность использования дискретного косинусного преобразования для выполнения фильтрации изображений. Время выполнения меньше, чем при использовании преобразования Фурье. Возможности еще большего сокращения времени обработки за счет использования параллельных вычислений будут дополнительно исследованы В. А. Чеботаревой в рамках выполнения выпускной квалификационной работы.

Список литературы

1. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М. : Техносфера, 2012.
2. Даджион, Д. Цифровая обработка многомерных сигналов / Д. Даджион, Р. Мерсеро. – М. : Мир, 1988.
3. <https://www.parallella.org/> – официальный сайт компании Parallella.

Таланова Надежда Вячеславовна¹,
*адъюнкт факультета подготовки научных
и научно-педагогических кадров Московского
университета МВД России имени В.Я. Кикотя;*

Ульянова Ирина Валентиновна²,
*профессор кафедры педагогики учебно-научного комплекса
психологии служебной деятельности
Московского университета МВД России имени В.Я. Кикотя
доктор педагогических наук, профессор*

ИНДИВИДУАЛЬНАЯ БЕСЕДА С КУРСАНТАМИ КАК МЕТОД ПРОФИЛАКТИКИ КИБЕРЗАВИСИМОСТИ

В настоящее время киберзависимость становится все более распространенной проблемой общества, так как увеличивается количество пользователей интернетом.

Наиболее распространенная аудитория пользователей интернетом молодежь. Интернет стал ее неотъемлемой частью жизни. Курсантские годы относятся к периоду юношества, а значит курсантам образовательной организации МВД России присущи те черты и особенности, что и современным юношам. Это значит, что курсанты 17–23 лет подвержены развитию разного рода зависимостей. Этот возрастной период характеризуется тем, что приобретение новых ценностей начинает носить фундаментальный характер, расширяются социальные контакты и прочее. Следовательно, на данном возрастном этапе становления личности следует уделить особое внимание профилактике зарождения киберзависимого поведения.

Факторы риска, формирующие интернет-зависимое поведение у молодежи:

- склонность к поиску новых ощущений;
- агрессивность;
- тревожность;
- эмоциональная отчужденность;
- низкая коммуникативная компетентность;
- проблемы в социализации [3].

Интернет-зависимость способствует формированию проблем:

- конфликтное поведение;
- хронические депрессии;
- предпочтение виртуального пространства реальной жизни;
- трудности адаптации в социуме;
- потеря способности контролировать время пребывания в интернете [2].

¹ © Таланова Н. В., 2020.

² © Ульянова И. В., 2020.

По мнению Э. Голдберга интернет-зависимость можно констатировать при наличии следующих пунктов:

1. Количество времени, которое нужно провести в интернете, чтобы достичь удовлетворения, заметно возрастает.

2. Если человек не увеличивает количество времени, которое он проводит в сети, то эффект заметно снижается.

3. Прекращение или сокращение времени, проводимого в интернете, приводит пользователя к плохому самочувствию: эмоциональное двигательное возбуждение, тревога, навязчивые размышления о том, что сейчас происходит в интернете, фантазии и мечты об интернете, произвольные или непроизвольные движения пальцами, напоминающие о наборе сообщения [1].

Для предотвращения вышесказанных возможных проблем, с которыми может столкнуться курсант образовательной организации МВД России, педагоги должны проводить индивидуальные беседы, которые помогут глубже изучить духовный мир обучающихся, а также дифференцированно применить те или иные воспитательные воздействия. «Это очень нежное и в то же время ответственное «прикосновение к душе», проникновение во внутренний мир воспитанника», – писал В. А. Сухомлинский.

Сущность индивидуальной беседы заключается в том, чтобы с помощью целенаправленных и умело поставленных вопросов побудить обучающихся к актуализации полученной информации, активизации мышления. Индивидуальная беседа – это метод, способный привлечь обучающегося к выработке правильных оценок и суждений по всем волнующим вопросам. Например, беседуя о природе киберзависимого поведения, обучающийся легче постигает ее суть и значение.

Таким образом, индивидуальная беседа помогает педагогу выявить некоторые отклонения в поведении, привычках обучающегося. Индивидуальная беседа – это возможность организации и проведения коррекции нравственных и ценностных представлений обучающегося, а также диагностика развития личности.

Индивидуальная беседа – часть профилактики киберзависимого поведения, а значит любой педагог, при условии правильного и грамотного подхода к обучающемуся, способен предупредить зарождающиеся предпосылки киберзависимого поведения.

Список литературы

1. Голдберг, Э. Патопсихологические особенности игроманов, зависимых от психоактивных веществ и актуальные аспекты их психологической реабилитации / Э. Голдберг // Наркология. – 2016. – 198 с.
2. Дмитриева, У. Увлечение или диагноз? Психологическое сопровождение компьютерной зависимости / У. Дмитриева // Школьный психолог. – 2008. – 147 с.
3. Егоров, А. Ю. Особенности личности подростков с Интернет-зависимостью / А. Ю. Егоров // Вопросы психического здоровья детей и подростков. – 2005. – 213 с.

Тутынин Игорь Борисович¹,

доцент кафедры уголовного процесса

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ВЛИЯНИЕ СЕТИ ИНТЕРНЕТ НА УГОЛОВНО-ПРОЦЕССУАЛЬНОЕ ПРИНУЖДЕНИЕ ИМУЩЕСТВЕННОГО ХАРАКТЕРА

В настоящий момент бесспорно то, что в постиндустриальный период развития российского и мирового сообщества возникают так называемые цифровые права, представленные в цифровой форме информации. Коммуникационные и информационные технологии изменяют общественные отношения и различные институты, в том числе имеющие отношение к обеспечению прав и интересов личности, общества и государства.

Среди арсенала правовых средств органов и должностных лиц, осуществляющих производство по уголовному делу, совокупность рассматриваемых в данной статье мер занимает специфическое место, обусловленное особенностью характера их воздействия.

Имущественный характер таких мер влияет на основания, условия и порядок применения. Но в новых условиях развития общества и государства, когда информационные технологии уже прочно вошли в обычную жизнь, а в отдельных случаях уже невозможно представить нормальное функционирование институтов государства и права, мерам уголовно-процессуального принуждения имущественного характера предстоит подвергнуться серьезной корректировке, как по вопросам нормативного правового регулирования, так и по вопросам правоприменительной практики.

В частности, в современных условиях упрощается деятельность следователя, дознавателя по поиску имущества, подлежащего аресту, а затем по непосредственному наложению ареста на имущество (исполнение судебного решения), путем задействования в этом третьих лиц. Уже сейчас наложение ареста на отдельные виды имущества затруднительно без участия государственных и негосударственных организаций, осуществляющих регистрацию и учет права (органы учета прав владельцев ценных бумаг, имущественных прав (прав требования) и др.), доверительных управляющих, банковских организаций, операторов электронных платежных систем, осуществляющих операции с электронными деньгами, а также в иных ситуациях с использованием интернета.

В связи с этим предстоит создать единые базы данных, использование которых позволит с использованием интернета выявить разыскиваемое имущество, привести доводы, обосновывающие предстоящее правоограничение, усовершенствовать деятельность по непосредственному аресту имущества.

Предполагаем, что через некоторое время мера уголовно-процессуального принуждения в виде наложения ареста на имущество будет исполняться через

¹ © Тутынин И. Б., 2020.

информационные ресурсы, в том числе с использованием интернета, посредством обращения к «системным администраторам», блокируя возможность изменения во владении, пользовании и распоряжении имуществом.

Искусственный интеллект и нейросети помогут при выборе надлежащей меры процессуального принуждения, когда без обращения к помощи специалистов в области психологии, техническое устройство рекомендует наиболее оптимальный вариант характера и степени принуждения для индивидуального случая по конкретному уголовному делу.

Имущественные права и интересы будут все больше связаны и взаимозависимы с иными правами и интересами, развивающимися в условиях новых технологий. Так называемые цифровые права будут интегрироваться с имущественными правами и интересами. Указанное выше предположение о том, что новые технологии будут способствовать приближению к равным возможностям участникам уголовно-процессуальных отношений в отстаивании своих прав, является условным, идеальным и поэтому вряд ли стопроцентно достижимым.

В данном случае «цифра» и собственность, зачастую «перетекая» друг в друга, обладая сходными качествами, а соответственно, обязанными обладать аналогичными правовыми гарантиями, будут вынуждены совместно подстраиваться под конструкцию, согласно которой уголовно-процессуальное действие, в том числе комплексного (имущественного) характера направляется на упомянутое комплексное право, через влияние на потребность, в конечном итоге вызывая изменение в поведении участника уголовного судопроизводства, обусловленное возможностью или наступлением для него правоограничения.

Применение мер процессуального принуждения имущественного характера будет переустроено в связи с изменениями в объектах собственности. Полный или частичный отказ от наличных денег, преобладание безналичных платежей или электронных денег предоставит все больше возможности влиять, и в какой-то степени манипулировать поведением человека не только государственным органам, коммерческим (банковским) организациям, но и преступным элементам. Неизбежно возникнет необходимость создания соответствующего поисково-блокирующего инструментария, средств, не позволяющих незаконно контролировать и влиять на поведение обывателя. В то же время «блокировки – правоограничения» должны оставлять шансы на равенство в правовых возможностях законного распоряжения своими правами, интересами, свободами.

Помимо перечисленных правоограничений в будущем появятся новые беспечительные меры уголовно-процессуального принуждения, которым придется взаимодействовать с искусственным интеллектом, робототехникой и иными техническими достижениями.

Указанные выше правоограничения станут мерами процессуального принуждения имущественного характера, обладающими соответствующими уголовно-процессуальными гарантиями. При реализации нашего предложения предстоит выстроить реальный и действенный механизм предлагаемого правоограничения посредством введения нового института, отвечающего требованиям кибербезопасности и учитывающего, что противодействие правоохрани-

тельных органов и правонарушителей будет толчком внедрения и развития новых технологий в уголовном судопроизводстве.

Имущественные права и интересы становятся более связанными и взаимозависимыми с тем, что предопределено развитием новых технологий. Доказательством тому служит то, что наиважнейшей особенностью современных имущественных отношений является широкое использование цифровых технологий, цифровые права на цифровые объекты (токены, криптовалюты, иное цифровое имущество) обладают реальной экономической ценностью.

Становится более очевидным, что, так называемые цифровые права интегрируются с имущественными правами и интересами. Например, информация о личности, прежде всего в цифровом формате, приобретает ценность в денежном эквиваленте. В средствах массовой информации все чаще утверждается: «Моя информация – моя собственность». Имущественная состоятельность (наличие личной и частной собственности, кредитные обязательства, транзакции, покупательская активность), пристрастия в выборе товаров и услуг, местоположение и маршруты движения, участие в политической и общественной жизни становятся объектом внимания органов государственной власти, коммерческих и некоммерческих организаций. Проявляет интерес к вышеперечисленной информации криминальный мир. Поэтому уголовно-процессуальное законодательство должно учесть совместное развитие права собственности и зарождающихся новых прав, запланировав соответствующие правоограничения и гарантии.

В дальнейшем появятся новейшие обеспечительные меры процессуального принуждения, действие которых будет связано с искусственным интеллектом, робототехникой, иными возможностями научно-технического прогресса.

Перечисленные правоограничения будут именно мерами процессуального принуждения имущественного характера, обладать надлежащими правовыми гарантиями, отвечать требованиям кибербезопасности.

Использование новых технологий может приблизить к равным возможностям участников уголовно-процессуальных отношений при отстаивании своих прав, к единообразию практики применения правовых норм, что, в свою очередь, приведет к верному и идентичному использованию законодательства, регламентирующего меры процессуального принуждения, к достижению идеалов, предписанных нормативными правовыми актами.

В перспективе возможен переход на исключительно цифровое производство по уголовным делам, функционируемое в интеллектуальных системах, постоянно взаимодействующих с внешней средой. Заинтересованные участники уголовного судопроизводства получают на более высоком уровне доступ к правосудию, иницируя (ходатайствуя) необходимость применения обеспечительных мер имущественного и иного характера, приобретая действенные возможности оказывать влияние на принятие процессуальных решений, с последующим контролем за принятием решений и их исполнением [1].

Цифровые технологии должны использоваться не только для удобства правоприменителей. В режиме реального времени заинтересованные участники получают возможность прослеживать состояние применения мер процессуального принуждения, и в первую очередь упомянутые ранее меры имуществен-

ного характера, в индивидуальном случае (по отдельному уголовному делу), а также в глобальном масштабе (статистика конкретного следователя, судьи, подразделения правоохранительного органа, всего правоприменительного ведомства), что позволит оценить качество оказываемых услуг правоохранительными органами.

Вступив в эпоху всеобщей информатизации и построения информационного общества с единым информационным пространством, с внедрением глобальных информационно-коммуникационных систем, с использованием унифицированных международных протоколов информационного обмена и методов удаленного доступа к базам данных, с преобладанием электронного документооборота, правоохранительные органы с успехом смогут применить для нужд уголовного судопроизводства положения об «информационных системах», «компьютерных данных», «электронных деньгах» и «электронном правосудии».

Список литературы

1. Масленникова, Л. Н. К вопросу о первых результатах реализации научного проекта № 18-29-16018 «Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий» / Л. Н. Масленникова // Lex russica. – 2020. – Т. 73. – № 1. – С. 70–87. – DOI: 10.17803/1729-5920.2020.158.1.070-087.

Ульянова Ирина Валентиновна¹,
*профессор кафедры педагогики учебно-научного комплекса
психологии служебной деятельности
Московского университета МВД России имени В.Я. Кикотя,
доктор педагогических наук, доцент*

АКТУАЛИЗАЦИЯ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ ПРОБЛЕМЫ ФОРМИРОВАНИЯ КИБЕРКУЛЬТУРЫ У КУРСАНТОВ

В современном обществе, характеризующемся как информационное, когда использование гаджетов, взаимодействие посредством интернет-среды стало обыденной действительностью, усиливается проблема формирования у молодежи киберкультуры.

Киберкультура (англ. Cyberculture) – вид современной культуры, который формируется ее носителями с помощью цифровой техники, прежде всего персональных компьютеров, а также гаджетов, порожденных наукой кибернетикой. Англоязычное понятие *cyberculture* определяется Оксфордским словарем как «состояние общества в результате использования средств автоматизации и компьютеризации» [1].

Киберкультура – важная часть культурной жизни современной европейской цивилизации. Для ее формирования у подрастающего поколения развернута широкая образовательная сеть, включая детские сады, школы, образовательные курсы в системе дополнительного образования, а также самообразование, самообучение пользователей.

Однако, принимая во внимание закономерность развития киберкультуры в постиндустриальном обществе, высоко оценивая ее информационный, коммуникативный, технократический потенциалы, следует учитывать и ее масштабные риски.

Так, Г. М. Маклюэн (Канада) назвал конец XX века электронной цивилизацией, аудиовизуальной эпохой, которая восстанавливает нарушенный оральным и визуальным типами культуры сенсорный баланс, а также равномерно и более «физиологично» распределяет нагрузку между зрением и слухом, позволяя человеку находиться в центре событий и эмоционально реагировать на событийность мира. Г. М. Маклюэн подчеркивает позитивное значение современных средств коммуникации, которые способны «расширять сферу» общественной жизни индивида, вовлекать человека во все происходящее и возвращать его в мир целостного восприятия, сокращать расстояние между людьми, что способствует совершенствованию человека и духовного климата в обществе. Вместе с тем он говорил о реальных опасностях информационных технологий, когда «объединенный человек» может стать объектом невидимой эксплуатации и всеобъемлющего контроля, и быть готовым контролировать их влияния на свое сознание [2].

¹ © Ульянова И. В., 2020.

Интенсивное вхождение информационных технологий в жизнь современного человека во многом деструктивно влияют на культуру отношений. Еще в середине прошлого века Д. Белл указывал, что в области культуры в постиндустриальном обществе будут утрачиваться преемственность, традиции, культивируются многообразие, в качестве идеала выбирая синкретизм.

Весьма значимы в данном случае позиции ученых, критически оценивающих сущность постиндустриального общества. Э. Фромм подчеркивал, что индустриальному (постиндустриальному) обществу не нужна полноценная, здоровомыслящая личность, ему требуются «винтик» и «человек-робот» [4]. Согласно Г. Маркузе, в основании современной развитой индустриальной цивилизации лежит определенный исторический проект (отношение человека к миру, определяющее как мышление о мире, так и деятельность в нем), а именно: технологический проект, или технологическая рациональность.

Катастрофичность развития технологической цивилизации заключается еще и в том, что оно вытесняет шансы альтернативы, ибо делает человека неспособным отказаться от благ, предоставляемых этой цивилизацией [3].

Принимая во внимание опасность очевидного расчеловечивания общества под натиском тотального технократизма, важно отыскать те ресурсы, которые обеспечат сохранение социокультурных традиций цивилизации, ее гуманистического базиса (Л. Г. Федотова, Ф. В. Цанн-кай-си и др.), не абсолютизируя исключительность киберкультуры, а принимая ее как эффективное информационно-коммуникативное средство.

Поэтому приобретает актуальность вопрос о формировании этической культуры киберпользователей, прежде всего несовершеннолетних и молодежи.

Этическая культура ориентирует человека на органическое единство этических знаний, моральных принципов, навыков и умений нравственной деятельности. В основе этической культуры лежит нравственная воспитанность личности, опирающаяся на сформированность ее аксиологической и поведенческой сфер. Этическая культура предполагает наличие у человека *гуманистической позиции* как устойчивой системы отношений к окружающим, сторонам действительности, проявляющейся в соответствующем поведении и поступках.

Киберпространство, в которое вовлекаются дети, подростки, юношество, имеет специфику: оно одновременно внешнее и внутреннее, представляет собой новую реальность – виртуальное пространство. Погружаясь в него, несовершеннолетние сталкиваются со значительными рисками, например:

- формирование различного вида аддикций: киберзависимости, лудомании (игровой зависимости) и пр.;
- экзистенциальная деформация (эскапизм как стремление уйти от реальности и погрузиться в приносящие удовольствие действия);
- искажение представлений о норме социальных отношений;
- нарушение реальных коммуникаций с окружающими и др.

Очевидно, что наличие подобных рисков требует комплексного психолого-педагогического сопровождения личности с самого детства, организации соответствующих условий, благодаря которым, взрослея, ребенок развивался бы гармонично и не превращался в манипулируемого субъекта. К сожалению, со-

временная статистика показывает, что число подростков и юношества, проводящих в киберпространстве ежедневно более трех часов, интенсивно растет, составляя сегодня более 70 % общего числа. Как свидетельствуют данные Всемирной организации здравоохранения, зависимость от видеоигр включена сегодня в перечень классификаций болезней (МКБ-11).

Феномен киберкультуры личности включает следующие аспекты:

1. Сформированность гуманистической позиции.
2. Принятие себя как гармоничной личности (развитость интеллекта, эмоций, нравственности, воли, коммуникативности, целеустремленности и пр.).
3. Адекватная сформированность социальных ролей.
4. Осознанность смысложизненных ориентаций.
5. Сформированность учебной/профессиональной и досуговой сфер жизнедеятельности (просоциальные хобби, интересы).
6. Готовность к самоорганизации, самодисциплине.
7. Устойчивые реальные коммуникации.
8. Активная жизненная позиция.
9. Владение навыками эффективного разрешения внутренних и внешних конфликтов.

Предполагается, что курсанты как обучающиеся ведомственного вуза, изначально включенные в служебную деятельность, призванные соблюдать учебную дисциплину, не сталкиваются с проблемой кибераддикции. Однако реалии образовательного процесса демонстрируют другое (что вполне закономерно, так как курсанты – часть современной российской молодежи, массово вовлеченной в киберкультуру), в частности, систематические попытки пользоваться смартфонами во время учебных занятий. Наблюдения, проведенные в течение 2016–2020 гг., показали, что без специальных предупреждений в среднем в аудитории во время проведения лекций, семинаров к мобильным аппаратам обращаются 50 % обучающихся. После предупреждений, замечаний скрытно пытаются выходить в сеть 25–30 % курсантов, после строгих предупреждений остаются 10–15 % курсантов от общего числа учебной группы, скрыто нарушающие запреты.

В связи с этим возникает необходимость комплексного осмысления данной проблемы и разработки специальной профилактико-коррекционной программы. Особое внимание в процессе ее реализации следует обратить на курсантов-первокурсников, которые должны получить установку на участие в занятиях без отвлечений на смартфоны.

Организационную роль на себя должен взять преподаватель-куратор учебного взвода, объединяющий усилия преподавательского и командного составов. Этапы профилактической работы:

1. Профилактическая беседа по проблеме киберзависимости в обществе, молодежной среде: ее риски для профессионально-личностного развития сотрудника ОВД; обсуждение актуальной статистики; презентация официальных документов вуза, регулирующих систему пользования гаджетами; коллективная разработка общих правил для взвода, оформленных в формате специальной «Памятки курсанту»; обсуждение возможных санкций (начало учебного года).

2. Контроль преподавателей за соблюдением правил поведения курсантов на занятиях, включая отказ от пользования гаджетами (в течение учебного года).

3. Системное поддержание кибердисциплины в учебном взводе (в течение учебного года).

4. Формирование у курсантов навыков киберкультуры (в течение учебного года).

5. Периодическое обсуждение преподавателями совместно с курсовым офицером процесса формирования киберкультуры у курсантов каждого учебного взвода (в течение учебного года).

6. Коррекционные мероприятия в случае возникновения острых проблемных ситуаций.

Актуальные формы педагогической деятельности: коллективные (на уровне взвода) в сочетании с индивидуальными.

Актуальные методы педагогической деятельности:

1. Общие: подражание, внушение, убеждение.

2. Частные: методы примера, беседы, дискуссии, диспута; ссылки на авторитетное мнение, внешняя оценка, самооценивание, внешний контроль, самоконтроль, поощрение, похвала, предупреждение, замечание, наказание, эксперимент и пр.

Список литературы

1. Cyberculture, n, OED online, Oxford University Press, December 2001.

2. Маклюэн, М. Понимание медиа: внешние расширения человека / М. Маклюэн // Understanding Media: The Extensions of Man. – М. : Кучково поле, 2007.

3. Маркузе, Г. Критическая теория общества: Избранные работы по философии и социальной критике / Г. Маркузе. – М. : АСТ, Астрель, 2011.

4. Фромм, Э. Бегство от свободы / Э. Фромм; общ. ред. и послесл. П. С. Гуревича.; пер с англ. – М. : Прогресс, 1989.

Ушаков Михаил Андреевич¹,

заместитель начальника кафедры

физической подготовки учебно-научного комплекса специальной подготовки

Московского университета МВД России имени В.Я. Кикотя

СПОСОБЫ ОПТИМИЗАЦИИ УЧЕБНОГО ПРОЦЕССА ПО ФИЗИЧЕСКОЙ ПОДГОТОВКЕ СЛУШАТЕЛЕЙ И КУРСАНТОВ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ

Физическая подготовка занимает важное место в деятельности сотрудников органов внутренних дел, особенно в деятельности подразделений, которые непосредственно участвуют в пресечении и раскрытии преступлений, поскольку нередко от сотрудника требуется применение физической силы для поимки и задержания преступника [1].

Особенности деятельности сотрудников органов внутренних дел обуславливают необходимость получения слушателями и курсантами профессиональных знаний и навыков для успешного выполнения поставленных задач. Для достижения высокого уровня физической подготовки будущих сотрудников подготовка начинается сразу после поступления в образовательную организацию системы МВД России, поэтому перед кафедрами физической подготовки стоят сложные задачи по выработке оптимальных способов проведения занятий, чтобы достигнуть поставленных целей.

Для продуктивной работы на начальном этапе учебных занятий по физической подготовке курсантам необходимо выработать стремление к освоению новых знаний и приобретению новых для них навыков борьбы. Поскольку не для каждого новобранца до поступления в образовательную организацию спорт был неотъемлемой частью жизни, возникает необходимость в стимулировании и развитии у них интереса.

Наиболее распространенной мотивацией среди молодежи, к которой относятся и курсанты, являются соперничество, желание победить, которое также может быть стимулировано какими-то последующими поощрениями.

На занятиях происходит отработка приемов, например, задержания или обезоруживания правонарушителя, однако недостаток заключается в привычной и спокойной для слушателей и курсантов обстановке. Для более эффективного изучения разумно привлекать другие кафедры образовательного учреждения системы МВД России, связанные с действиями сотрудников в особых условиях и личной безопасностью, преподавательский состав кафедры физической подготовки, а также курсантов и слушателей других учебных взводов для моделирования схожих с реальными условиями ситуаций.

Присутствие на занятии новых людей не дает расслабиться, соперничество между разными учебными взводами мотивирует, а моделирование ситуации заставляет обучающегося с большим энтузиазмом отнестись к отработке приемов. Проведение такого рода комплексных мероприятий способствует разви-

¹ © Ушаков М. А., 2020.

тию психологических качеств, необходимых для решения оперативно-служебных задач, что является одной из целей физической подготовки в образовательной организации системы МВД России [2].

Другое направление по оптимизации учебного процесса по физической подготовке – увеличение поступающих на службу в органы внутренних дел девушек.

В нормативных документах, регулирующих физическую подготовку сотрудников ОВД, в том числе и в образовательных организациях системы МВД России, отсутствуют положения по обучению приемам борьбы девушек-курсантов. Кроме того, с каждым годом в образовательных организациях системы МВД России возрастает количество девушек-курсантов [3]. Причем теперь девушки поступают не только на факультеты, которые готовят сотрудников для подразделений ОВД, содействующих раскрытию преступлений, например, психологии служебной деятельности, но также и на факультеты подготовки сотрудников для оперативных подразделений полиции или по охране общественного порядка.

Среди специальных задач при овладении слушателями и курсантами физической подготовки преимущество отдается развитию силовых качеств и силовой выносливости. Поскольку девушки чаще всего обладают меньшей массой и силой по сравнению представителями мужского пола, которые встречаются на улицах в роли правонарушителей, возникает вопрос возможности совершенствования части учебной программы именно для них.

Поскольку представители женского пола превосходят мужчин в координации движений и гибкости, что связано с их анатомическим и физиологическим строением, для девушек-курсантов актуальнее развитие быстроты действий, ловкости, двигательных реакций и пространственной ориентировки. Ловкость относится не к силовым умениям человека, а к умениям, позволяющим быстро оценить обстановку, овладеть сложными движениями, ситуацией, а также направлять ее.

К девушкам-курсантам нужен нестандартный подход, поскольку они не всегда смогут выполнить бросок через спину, как бы правильно они его не выполняли, но изучение болевых точек на теле человека и большего количества болевых приемов позволит иметь преимущество над соперником.

Ежегодно преподавательский состав совершенствует систему обучения в целях поиска наиболее эффективных способов формирования у курсантов и слушателей навыков и усвоения ими знаний, необходимых для решения служебных задач. Развитию интереса к физической подготовке обучающихся способствуют мероприятия по моделированию ситуаций, схожих с реальными условиями, которые встречаются и будут встречаться в практической деятельности сотрудников ОВД, а также другие спортивные соревнования [4]. Кроме того, рост числа девушек-курсантов обуславливает необходимость разработки новых приемов и методов борьбы.

Список литературы

1. Барчуков, И. С. Физическая подготовка личного состава спецподразделений / И. С. Барчуков. – М. : Спор-тАкадемПресс, 2014.
2. Карданов, А. К. Особенности физической подготовки женщин-полицейских / А. К. Карданов // Историческая и социально-образовательная мысль. – 2016. – Т. 8. – № 3–2. – С. 158–161.

3. Приказ МВД России от 01.07.2017 № 450 «Об утверждении Наставления по организации физической подготовки в органах внутренних дел Российской Федерации» // СПС «КонсультантПлюс».

4. Федеральный закон от 04.12.2007 № 329-ФЗ (ред. от 02.08.2019) «О физической культуре и спорте в Российской Федерации» // СПС «КонсультантПлюс».

Орехов Павел Васильевич¹,
старший преподаватель кафедры
специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ВЗВЕШЕННОЙ ОЦЕНКИ ВОЗМОЖНОСТИ УТЕЧКИ ИНФОРМАЦИИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

В современном мире все большую ценность приобретает информация. Оценки экономического ущерба от утечки информации с каждым годом продолжают расти. Так, например, по оценкам специалистов Сбербанка, за 2019 г. ущерб для экономики Российской Федерации от кибератак составил около 2,5 трлн руб. Причем, все эксперты сходятся во мнении, что в последующие годы количество атак на инфраструктуры различных организаций и государственных учреждений будут только расти. В связи с этим актуальна задача защиты информации от несанкционированного доступа как на уровне одной личности, так и на уровне крупной организации и даже целого государства. [1]

Ежегодно совершенствуются технические устройства, предназначенные для негласного съема информации, разрабатываются все новые методы несанкционированного получения информации. Параллельно модернизируются и различные средства для противодействия утечки информации. С целью защиты информации первоначально рассмотрим основные технические каналы утечки информации.

Технические каналы утечки по типу информации делятся на следующие виды [2]:

- а) утечки информации при ее передаче по каналам связи;
- б) утечки речевой информации;
- в) утечки информации, обрабатываемой техническими средствами;
- г) утечки видовой информации.

Безусловно, каждый из этих каналов утечки представляет значительную угрозу утечки информации. Рассмотрим более подробно технические каналы утечки речевой информации. Их подразделяют на виды:

- а) акустические;
- б) виброакустические;
- в) параметрические
- г) акустоэлектрические;
- д) оптико-электронные.

Данные технические каналы утечки возникают при воздействии акустических колебаний на различные строительные конструкции, будь то потолок, стены, пол и др. и инженерно-технические коммуникации, например воздуховоды,

¹ © Орехов П. В., 2020.

металлические трубы отопления, водоснабжения и т. д. Возникающие в описанных выше средах упругие колебания регистрируют различные вибрационные датчики, самые распространенные из них – стетоскопы. Для каждой из типа сред передачи колебаний существуют свои требования по обеспечению уровня защищенности. Но, даже при выполнении всех требований обеспечить абсолютную защищенность от утечки по данному техническому каналу невозможно, требуется разработать модель оценки утечки информации по данному каналу.

В зависимости от типа среды передачи колебаний выделим следующие элементы:

- 1) воздуховоды (передача акустических колебаний по воздушным каналам происходит за счет отражения акустической волны от стенок воздуховода);
- 2) стеновые панели;
- 3) напольные и потолочные перекрытия;
- 4) трубы отопления;
- 5) трубы водоснабжения.

Для оценки вероятности утечки по различным конструкциям опишем модель нахождения взвешенной оценки вероятности утечки.

Обозначим P_1-P_5 – количество объектов, по которым может быть утечка информации соответствующих типов. Однако, указанные показатели очень разнородны и их одновременная оптимизация практически невыполнима. Поэтому нужно определить некоторый интегральный показатель вероятности утечки, представляющий собой свертку показателей P_1-P_5 :

$$P = \sum_{t=1}^5 \alpha_t \cdot P_t,$$

где α_t – значение значимости показателей P_1-P_5 ; P_t – количество каналов утечки информации соответствующих типов t .

Так как α_t не поддается непосредственному измерению, его значение эксперты определяют экспертами методом попарных сравнений с использованием метода Саати [4].

Условимся, что следующие числа будут характеризовать сравнение вероятности утечки информации по различным каналам:

- 1 – P_t и P_s имеют одинаковую вероятность;
- 3 – P_t незначительно вероятнее, чем P_s ;
- 5 – P_t значительно вероятнее, чем P_s ;
- 7 – P_t явно вероятнее, чем P_s ;
- 9 – P_t по своей вероятности абсолютно превосходит P_s .

На основании определенных экспертами рангов строится матрица парных сравнений относительной значимости признаков P^t с элементами $P_{ij}^t = \frac{P_i^t}{P_j^t}$, где

t – индекс, вероятность утечки по различным средам [3].

Следующий шаг заключается в вычислении векторов приоритетов $V_{P^t} = (\alpha_1^t, \dots, \alpha_5^t)$. Для примера рассмотрим вычисление вектора приоритетов, который представляет собой собственный вектор матрицы и может быть найден как решение уравнения:

$$P^t \cdot V_{P^t} = \lambda \cdot V_{P^t} \quad (1)$$

где λ – собственное значение матрицы P^t .

Как видно из формулы (1), для определения собственного вектора матрицы необходимо найти ее собственные значения λ . В рамках данной работы не будем приводить методику расчетов собственных значений и векторов матрицы, а сразу отразим результаты моделирования.

С учетом оценок построена матрица парных сравнений предпочтений экспертов (табл. 1).

Таблица 1

Матрица парных сравнений относительной значимости признаков P_t

	P_1	P_2	P_3	P_4	P_5
P_1	1	1/3	1/5	1/7	1/8
P_2	3	1	1/4	1/6	1/8
P_3	5	4	1	1/4	1/8
P_4	7	6	4	1	1/4
P_5	8	8	8	4	1

Отсюда формула (1) принимает вид:

$$\begin{bmatrix} 1 & 1/3 & 1/5 & 1/7 & 1/8 \\ 3 & 1 & 1/4 & 1/6 & 1/8 \\ 5 & 4 & 1 & 1/4 & 1/8 \\ 7 & 6 & 4 & 1 & 1/4 \\ 8 & 8 & 8 & 4 & 1 \end{bmatrix} \times \begin{bmatrix} \alpha_1^t \\ \alpha_2^t \\ \alpha_3^t \\ \alpha_4^t \\ \alpha_5^t \end{bmatrix} = \lambda \times \begin{bmatrix} \alpha_1^t \\ \alpha_2^t \\ \alpha_3^t \\ \alpha_4^t \\ \alpha_5^t \end{bmatrix}$$

После выполнения расчетов получились следующие показатели значения значимости для каждой из сред утечки информации α_t : $\alpha_1 = 0.024$, $\alpha_2 = 0.044$, $\alpha_3 = 0.104$, $\alpha_4 = 0.249$, $\alpha_5 = 0.577$.

Разработанная выше модель получения взвешенной оценки вероятности утечки информации по различным средам через виброакустический канал с использованием метода попарных сравнений Саати позволяет получить относительную вероятность утечки информации для каждой из сред. Данным методом можно воспользоваться при необходимости повышения защищенности помещения от утечки по виброакустическим каналам, с учетом уже имеющихся средств защиты информации.

Список литературы

1. Сбербанк оценил потери экономики. Информационное агентство «ТАСС» [Электронный ресурс]. – 2020. – URL: <https://tass.ru/ekonomika/7567667> (дата обращения: 15.02.2020).
2. Язов, Ю. К. Защита информации в информационных системах от несанкционированного доступа / Ю. К. Язов, С. В. Соловьев. – Воронеж : Кварта, 2015.
3. Орехов, П. В. Оценка аварийности участков дорожной сети методом Саати / П. В. Орехов // Пожарная безопасность: проблемы и перспективы : сб. статей по материалам VI Всероссийской науч.-практич. конференции с международным участием / 23–24 сентября 2015 г. – Воронеж : Воронежский ин-т ГПС МЧС России, 2015. – Ч.2. – С. 388–392.
4. Саати, Т. Принятие решений. Метод анализа иерархий / Т. Саати. – М. : Радио и связь, 1993.

Пакляченко Марина Юрьевна¹,
*старший преподаватель кафедры радиотехнических
систем и комплексов охранного мониторинга
Воронежского института МВД России,
кандидат технических наук;*

Милютин Роман Викторович²,
*преподаватель кафедры огневой подготовки
Воронежского института МВД России*

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЛАТЕЖНЫХ ТЕРМИНАЛОВ

С развитием науки и техники, с появлением нетривиальных методов, базирующихся на инфокоммуникационных технологиях, регулярно развивающейся аппаратной и программной части возникают оптимальные средства, способы и системы защиты объектов от различных видов угроз, в том числе криминального характера.

Современные технологии без участия человека в полной мере не обладают возможностью обеспечения комплексной защиты объектов охраны, которыми могут быть люди, организации, здания и сооружения, а также отдельные предметы, обладающие особой ценностью, например, платежные терминалы (банкоматы).

Рассмотрим процессы обеспечения защиты и построения технической системы безопасности определенного вида объекта охраны, что носит прикладной характер, заключающийся в разработке и внедрении указанной системы в образовательную деятельность, которая, в свою очередь, способствует успешной подготовке компетентных специалистов правоохранительных органов в области охраны и противокриминальной защиты. Указанная сфера особо актуальна для обучающихся в вузах системы МВД России по техническим направлениям, поскольку специалисты данного профиля подготовки должны совмещать в своей профессиональной деятельности как общие знания и умения нормативного правового содержания, так и компетенции технического и практического характера.

Уход от наличных денег в сторону пластиковых карт привел к увеличению количеству банкоматов. Возможность присутствия в одном подобном аппарате до нескольких миллионов рублей предъявляет ряд значительных требований в части осуществления тактики охраны указанного типа объектов финансового сектора, а также определяет перечень правил проектирования и эксплуатации систем его безопасности.

Мировая статистика позволяет оценить убытки при взломе банкоматов: только за 2018 г. зарегистрировано 4 549 инцидентов, связанных с физическим взломом банкоматов с убытками в размере 36 млн евро. Мошеннические атаки

¹ © Пакляченко М. Ю., 2020.

² © Милютин Р. В., 2020.

на банкоматы, связанные с кардингом, фишингом и скиммингом за 2018 г. оцениваются в 247 млн евро при 13 511 инцидентах.

Приведем пример из недавних негативных событий.

В феврале 2020 г. в Ставропольском крае было утверждено обвинительное заключение в отношении преступной группировки, члены которой с помощью вредоносного программного обеспечения (ВПО) взламывали банковскую систему защиты посредством интернета. Они получили дистанционный доступ к 18 платежным терминалам и похитили денежную сумму в совокупности свыше 13 млн рублей.

В этом же месяце в Красноярске завершилось расследование особо крупной кражи отделения Сбербанка. Способ совершения преступления заключался в том, что мошенники размещали на игрушечных банкнотах – билетах банка сувениров металлизированные защитные полосы, которые распознавались и принимались терминалами (крупноформатной старой версии компании NCR).

Хищение денежных средств из банкоматов на сумму более 8 млн руб., осуществленное с физическим доступом к устройству, произошло в прошедшем году в Нижнем Тагиле. Группировка из трех человек «работала» следующим образом: один из сообщников предварительно искал платежные терминалы, размещаемые на первых этажах зданий. Преступник изучал систему охранной сигнализации, анализировал вероятность взлома с применением специального оборудования, посредством пролома пола или разбора стен. Далее злоумышленники проникали в помещения и отключали систему сигнализации, после чего применяли технические средства, создающие радиопомехи, которые блокировали линии связи банкоматов с пультами охранного наблюдения и мониторинга. Газосварочными приборами разрезали стенки терминалов и изымали денежные банкноты.

2018 год отличился возникновением и частой реализацией атаки «black box», сценарий которой состоял как из действий, осуществляемых с физическим доступом к банкомату, так и операциями, выполняемыми дистанционно. Преступники вскрывали банкомат, подключали его к ноутбуку с определенными драйверами и оставляли его внутри терминала, после чего управление транзакциями осуществлялось с применением ВПО. Злоумышленник подходил к терминалу и имитировал работу с ним, сообщник удаленно подключался к ноутбуку, используя ВПО (например, Cutlet Maker) и запускал на исполнение команды выдачи денег.

Специалисты отмечают, что совершение подобных преступлений опосредовано, как правило, «антикварностью» операционных систем банкоматов. Многие определяют терминалы как наиболее уязвимые компоненты банковской инфраструктуры вообще, поскольку основу программной архитектуры банкоматов составляют обычные компьютеры на базе Windows, часто устаревших версий.

Физический взлом занимает немалую долю атак на банкоматы, производители охранного оборудования подстраиваются под современные тенденции и улучшают выпускаемые технические средства охраны (ТСО), направленные на защиту банкоматов.

В государственном стандарте о вопросах безопасности финансовых (банковских) операций определены базовые составы отдельных защитных мер (см. рис. 1).

В части, касающейся защиты банкоматов среди базового состава указанных мер, можно отметить следующие:

- мониторинг отсутствия, либо выявление аномальной сетевой активности, связанной с несанкционированным информационным взаимодействием между банкоматами и интернетом;
- мониторинг отсутствия и обеспечение оперативного устранения известных уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между банкоматами и интернетом;
- защита от вредоносного кода на уровне контроля банкоматов.



Рис. 1. Базовый состав мер обеспечения безопасности финансовых операций по ГОСТ Р 57580.1-2017

За минувшие несколько лет отмечается динамичное развитие ВПО для банкоматов. Сегодня достаточно просто реализовать удаленную сетевую атаку, используя корпоративную сеть банка (в том числе сегментированную) и не имея физического доступа к терминалу.

Однако это не означает, что преступления, совершаемые путем физического воздействия на банкоматы, перестали совершаться.

В вопросах обеспечения безопасности подобного рода объектов оптимален комплексный подход, состоящий из построения надежных охранных систем (сигнализации, видеонаблюдения, контроля доступа) и передовых программных и сетевых средств защиты.

Кроме того, комплексность требует для реализации симбиоза всего арсенала сил и средств, техники и оборудования, разработки корректных стратегий, а также компетентных исполнителей, воплощающих разнообразные методики защиты в жизнь.

Перспективным видится также внедрение искусственного интеллекта в алгоритмы работы платежных терминалов. О подобной технологии заявили представители японской компании Hitachi-Omron Terminal Solution. Банкоматы их производства с применением искусственного интеллекта распознают пользователя, анализируют его поведение во время денежного перевода и контролируют процессы осуществления транзакций.

Список литературы

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс] // СС «Техэксперт».
2. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (с Поправкой) [Электронный ресурс] // СС «Техэксперт».
3. Информационный портал безопасности SecurityLab.ru. // URL: <https://www.securitylab.ru>.
4. Пакляченко, М. Ю. Анализ киберзащищенности интегрированных систем безопасности / М. Ю. Пакляченко // Актуальные проблемы противодействия органов внутренних дел (полиции) государств - участников Содружества Независимых Государств преступлениям, совершаемым с использованием информационных технологий: сб. науч. трудов Междунар. науч.-практич. конференции, 2019. – С. 66–69.

Курбатова Мария Сергеевна¹,
курсант факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России
имени В.Я. Кикотя;

Поликарпов Евгений Сергеевич²,
начальник кафедры специальных информационных
технологий учебно-научного комплекса информационных
технологий Московского университета МВД России
имени В.Я. Кикотя, кандидат технических наук

ОБЗОР ЗАРУБЕЖНЫХ МЕТОДИК АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Под аудитом безопасности информационных систем принято считать законное действие на право поиска уязвимостей и возможную эксплуатацию найденных уязвимостей. В зависимости от степени доступности аудитору информации об объекте, различают подходы на основе «белого ящика», «серого ящика» и «черного ящика».

«Black Box» или «черный ящик», используется, когда аудитор ничего не знает о параметрах, структуре и принципах функционирования системы. При использовании подхода «серый ящик» аудитор имеет представление о некоторых параметрах исследуемой системы, предполагает, как данная система работает, но остальные данные о системе остаются скрытыми. Этот подход применяется чаще всего. При использовании метода «White Box», или «белый аудит», аудитор получает доступ к полной информации и конфигурации исследуемой информационной системы. Данные методы необходимы для выявления скрытых проблем в безопасности предприятия, а также с их помощью можно оценить возможные риски, угрожающие безопасности в дальнейшем. Именно с помощью аудита безопасности информационных систем можно улучшить защиту данных компании, обеспечить их целостность, а также обеспечить эффективную работу организации.

Основные этапы аудита информационной системы: сбор информации (WWW, DNS, Google) сканирование системы (ping, port scanning), получение доступа к системе, закрепление в системе (backdoor), скрытие следов пребывания (очистка лог-файлов, rootkit) [1]. Выше описанная методика приближительна.

Для оценки состояния информационной безопасности системы применяется ряд зарубежных методик: OSSTMM (The Open Source Security Testing Methodology Manual), ISSAF (Information Systems Security Assessment Framework), PTES (Penetration Testing Execution Standard), OWASP Testing Guide (The Open Web Application Security Project), NIST SP 800-115 и BSI (Study A

¹ © Курбатова М. С., 2020.

² © Поликарпов Е. С., 2020.

Penetration Testing Model). Аудит безопасности информационных систем не может быть выполнен по одному конкретному сценарию, нельзя изначально обозначить исчерпывающий список возможных угроз, поэтому различные специалисты применяют разные методики проведения аудита, с целью более точного и полного описания проведения аудита. Объем информации, доступной аудитору немаловажный фактор в различии перечисленных выше методик.

OWASP Testing Guide – данная методика основана на методе «черный ящик». При проведении аудита информационной системы информация о ее характеристиках является ограниченной или недоступной. Данная методика является полностью бесплатной, воспользоваться ей может каждый, кто проводит аудит безопасности информационных систем. Аудит в данном случае проводится в два этапа, пассивный и активный. При проведении пассивного этапа собирают все необходимые сведения о информационной системе, о ее структуре. Активный этап подразумевает проведение тестов безопасности информационной системы в соответствии с предложенными разделами. Всего таких параметров выделено одиннадцать и все они должны быть проверены. *OWASP Testing Guide* является достаточно хорошо описанной методикой, также широко применяется при обнаружении уязвимостей веб-приложений [2].

OSSTMM – методика основана на экспериментальном подходе проведения аудита безопасности. В данной методике нет упоминания приемов, программ или скриптов необходимых для проверки системы. Предлагается лишь список областей системы, которые должны быть проверены, так называемая «карта безопасности» [3]. Набор элементов содержит шесть основных пунктов, причем в данной методике акцентирования внимания на атаках социальной инженерии. К положительным чертам *OSSTMM* относятся: наличие списка атак, которые необходимо реализовать, частое обновление методики, бесплатный доступ к старым версиям, но в методике отсутствует список необходимых утилит, а также анализ и рекомендации по устранению найденных уязвимостей минимальны.

NIST SP 800-115 – документ разработан национальным институтом стандартов и технологий США, содержит описание общих аспектов проведения аудита состоит из семи разделов: обзор тестирования и экспертизы безопасности; обзор методов; определение цели и техники анализа; техники оценки уязвимости; планирование оценки безопасности; выполнение оценки безопасности; пост-тестовые мероприятия. Согласно данному документу аудит проводится в три этапа: подготовка к аудиту, выполнение тестов, создание отчета. На первом этапе происходят подготовка и исследование системы. Исследование системы включает начало тестирования, анализ найденных уязвимостей. На втором этапе производится атака системы. Необходимо получить доступ к системе, возможность изменить параметры системы, установить дополнительные утилиты. По результатам проведения аудита составляется отчет, в котором указываются найденные уязвимости, а также способы их устранения [4]. Методика основана на методе «серого ящика». *NIST SP 800-115* хорошо описанная методика, имеется список используемых утилит для проведения аудита, однако нет инструкции, как использовать предложенные утилиты.

PTES – методика разработана специально для бизнеса с целью рассмотрения и оценки среды в рамках стандартных отраслевых документов. В методике хорошо разобраны все этапы от определения среды аудита до создания отчетности и вывода по результатам аудита, именно то, что необходимо для организации. Стандарт содержит семь основных разделов и технические рекомендации, которые позволяют проводить аудит от тестирования веб-приложения до полномасштабного тестирования всей информационной системы организации, причем акцент делается на тех областях, в которых уязвимости могут быть наиболее сильными. Технические рекомендации регламентируют процедуры, которые необходимо соблюдать во время проведения аудита.

Подготовительный этап включает разделы: предварительное взаимодействие, сбор информации, моделирование угроз. Этап выполнения тестов состоит из анализа уязвимостей, эксплуатации (обнаружения наилучшего пути атаки), пост-эксплуатации (анализ инфраструктуры, внесение изменений в инфраструктуру, удаление следов присутствия). На заключительном этапе создается отчет, его система должна быть структурирована. Однако у *PTES* отсутствует список рекомендуемых утилит, а также описание их использования, из чего можно сделать вывод, что лицо, проводящее аудит должно обладать достаточными знаниями и опытом [5].

BSI – разработана немецким подразделением Federal Office for Information Security. В отличие от ранее рассмотренных методик, в *BSI* рассматривается не только, как проводить аудит, а также изложены правовые аспекты, которые необходимо выполнить для успешного аудита. В данном документе описаны методы, с помощью которых можно нанести вред ИТ-системе. Проведение аудита по данной методике состоит из этапов подготовки, выполнения тестов и создание отчета. На этапе подготовки собирают сведения о системе, разведке, анализе информации и рисков. Далее выполняют тестирование, представляющее собой попытки активного вторжения в систему [6]. На заключительном этапе создается отчет и производится окончательный анализ системы. Минусы данной методики отсутствие классификации уязвимостей и недостаточно подробно описание используемых утилит.

Таким образом, при выборе методики аудита безопасности информационной системы нужно ориентироваться на различные критерии самой информационной системы, подход проведения аудита, стоимость методики, а также личную профессиональную компетенцию в данном вопросе.

Список литературы

1. Скабцов, Н. В. Аудит безопасности информационных систем / Н. В. Скабцов. – 2018.
2. OWASP Testing Guide v4.0 [Электронный ресурс]. – 2016. – URL: https://wiki.owasp.org/index.php/Penetration_testing_methodologies/ (дата обращения: 20.04.2020).
3. The Open Source Security Testing Methodology Manual [Электронный ресурс]. – 2010. – URL: <https://www.isecom.org/OSSTMM.3.pdf/> (дата обращения: 20.04.2020).

4. National Institute of Standards and Technology: Technical Guide to Information Security Testing and Assessment. Special Publication 800-115 [Электронный ресурс]. – 2008. – URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf/> (дата обращения: 20.04.2020).

5. Standardised penetration testing? Examining the usefulness of current penetration testing methodologies. [Электронный ресурс]. – 2017. – URL: <https://docviewer.yandex.ru/view/565501809/> (дата обращения: 21.04.2020).

6. Federal Office for Information Security: Study A Penetration Testing Model. [Электронный ресурс]. – 2019. – URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.html (дата обращения: 21.04.2020).

Франковская Ксения Дмитриевна¹,
*слушатель факультета подготовки
 сотрудников полиции для подразделений по охране
 общественного порядка Московского университета
 МВД России имени В.Я. Кикотя;*

Куренков Игорь Анатольевич²,
*преподаватель кафедры юридической психологии
 учебно-научного комплекса психологии служебной
 деятельности, кандидат психологических наук*

ПРОТИВОДЕЙСТВИЕ ВОВЛЕЧЕНИЮ НЕСОВЕРШЕННОЛЕТНИХ В СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ И АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЙ ПУТЕМ ИСПОЛЬЗОВАНИЯ СЕТИ «ИНТЕРНЕТ»

Сегодня информационно-телекоммуникационная среда наиболее распространенное средство обмена информацией среди молодежи. За последние десятилетия интернет-пространство совершило большой скачок в развитии. Появились новые социальные сети, мессенджеры, получившие популярность в обществе. Социальные сети Instagram, Telegram, WhatsApp, VKontakte имеют миллионные сообщества по всему миру. По данным статистики более 70 % пользователей социальных сетей представляют несовершеннолетние или лица от 18 до 35 лет.

При этом интернет сегодня – это не просто среда для общения и получения новых знаний, обмена информацией, но и, к сожалению, пространство, открытое для противоправной деятельности. Киберпространство сегодня стало устойчивой платформой для совершения разнообразных противоправных действий, в том числе и связанных с вовлечением несовершеннолетних наиболее распространенные правонарушения: вовлечение несовершеннолетних к совершению различного рода противоправных действий; призыв к участию в несанкционированных публичных мероприятиях, одно из наиболее актуальных и распространенных правонарушений, связанных с привлечением несовершеннолетних к противоправному поведению. За совершение подобного правонарушения предусмотрена административная ответственность по ст. 20.2 («Нарушение установленного порядка организации либо проведения собрания, митинга, демонстрации, шествия или пикетирования») КоАП РФ.

Например, по данным административной статистики ГУ МВД России по г. Москве за период с 1 января по 31 декабря 2019 г. более 30 % правонарушений в сфере общественного порядка и общественной безопасности, в том числе и при проведении публичных мероприятий, совершают несовершеннолетние.

И это лишь один из примеров многочисленных противоправных деяний, совершаемых на просторах интернета с вовлечением в них несовершеннолетних.

¹ © Франковская К. Д., 2020.

² © Куренков И. А., 2020.

К числу таких правонарушений относятся вовлечение несовершеннолетних в табакокурение, употребление некурительных смесей, алкоголя и спиртосодержащей продукции, а также наркотических веществ.

К сожалению, до сих пор открытым остается вопрос и с вовлечением несовершеннолетних в экстремистскую и террористическую деятельность, а также в современные формы противоправной деятельности (А.У.Е.-идеи, stalking, буллинг, радикальный и религиозный экстремизм). Дополнительное беспокойство вызывает и то, что указанные явления общественной жизни для несовершеннолетних представляются как нечто «модное» и абсолютно нормальное. Зачастую несовершеннолетние указанный контент используют для того, чтобы поднять свою значимость и популярность среди своих сверстников.

На заседании расширенной коллегии МВД 26 февраля 2020 г. Президент Российской Федерации В. В. Путин обратил особое внимание сотрудников органов внутренних дел на профилактику правонарушений, особенно среди несовершеннолетних, указав на недопущение распространения радикальных групп в интернет-пространстве, а также на обеспечение комплексной безопасности детских и образовательных учреждений.

В связи с этим наиболее актуально осуществление комплексного взаимодействия между правоохранительными органами и образовательными организациями в целях проведения надлежащей профилактической работы и формирования правовой культуры среди всех категорий несовершеннолетних.

Проведение профилактических бесед, правового информирования, а также индивидуальных средств профилактики с учащимися образовательных учреждений позволит на раннем этапе устранить совершение ряда возможных преступлений и административных правонарушений с их стороны. В профилактическую работу следует в обязательном порядке включить правовое воспитание и основы безопасного общения в интернете.

Немаловажное значение в сфере противодействия противоправным действиям в отношении несовершеннолетних в интернете имеет и реализация программ по повышению уровня компьютерной грамотности и изучения материальных основ вычислительной техники родителями. Повсеместное внедрение соответствующих программ на государственном и региональном уровне (по типу программ «Содействие занятости населения», «Развитие образования» или «Московское долголетие») позволит осуществлять надлежащие профилактические мероприятия правонарушений среди несовершеннолетних не только в рамках, но и вне образовательных и воспитательных учреждений.

Список литературы

1. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 27.12.2019) (с изм. и доп., вступ. в силу с 01.02.2020).
2. Сайт ГУ МВД России по г. Москве. Ссылка на электронный ресурс <https://77.xn--b1aew.xn--p1ai/>.

Харисова Зарина Ирековна¹,
доцент кафедры управления в ОВД
Уфимского юридического института МВД России,
кандидат технических наук;

Файзулова Рузиля Ранисовна²,
курсант факультета подготовки сотрудников
полиции Уфимского юридического института МВД России;

Дюсьмекеева Диана Сергеевна³,
курсант факультета подготовки следователей
Уфимского юридического института МВД России

СОВРЕМЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Проблема противодействия киберпреступлениям актуальна и имеет в настоящее время широкие масштабы, поскольку спектр действия охватывает практически все сферы жизни человека, которые все больше переходят в цифровой формат. Пропорционально бурному развитию технологий и коммуникаций в условиях глобализации информационного пространства прогрессирует и уровень преступности, вследствие чего возникают трудности в процессе выявления, предупреждения и противодействия киберпреступности.

С каждым годом число киберпреступлений растет в геометрической прогрессии. Этому способствуют удобства глобальной сети, которые проявляются в простоте ее использования, широких возможностях дистанционного управления, анонимности пользователей сети, высокой скорости обмена информацией и др. Достижения науки и техники, преследуемые намерения упрощения и ускорения механической деятельности зачастую используются недобросовестными людьми, а также криминальными группировками в преступных целях, нанося вред и обществу, и государству.

Так, в апреле 2019 г. компания Ростелеком заявила об увеличении кибератак по сравнению с прошлым годом в два раза. По аналитическим данным компании Positive Technologies, 27 % кибератак оказались успешными. «Лаборатория Касперского» заявила об увеличении вредоносных программ, распространяемых в последнее время, на треть. По опубликованным Генпрокуратурой данным о преступности в Российской Федерации, количество зарегистрированных преступлений за 2019 г. возросла на 67 %, т. е. отмечается активное развитие киберпреступности – в двукратном размере. За первые 8 месяцев 2019 г. зарегистрировано 180153 киберпреступлений, что превышает показатели прошлого

¹ © Харисова З. И., 2020.

² © Файзулова Р. Р., 2020.

³ © Дюсьмекеева Д. С., 2020.

года на 66,8 %. Первостепенными оказались преступления с использованием ИКТ, также в сфере компьютерной информации. [1]

Согласно докладу Всемирного экономического форума 2019 г. [2], мошенничество с данными и кибератаки выступают на четвертом и пятом местах по глобальным рискам, соответственно, киберпреступления приравняются по ущербу и наносимому вреду к экологическим преступлениям. В официальном ежегодном отчете о киберпреступности (ACR) за 2019 г., говорится о совершении атак каждые 14 секунд, предполагается что к 2021 г. частота возрастет до 11 секунд. [3] Известна тенденция увеличения утечки конфиденциальной информации по сравнению с 2018 г. на 10% во всем мире, в России ориентировочно на 40 %.

За последние годы многие сферы жизни подверглись цифровой трансформации. Образование, политика, государственное управление, банковское дело, экономика, покупки, хранение информации и многое другое отчасти уже перешло в цифровой формат, и каждая из перечисленных областей подвержена посягательству преступников, поскольку информация имеет весьма большую ценность. По этой причине важной проблемой обеспечения информационной безопасности становится изучение форм, методов и приемов выявления и предотвращения рисков возможных утечек в сфере информационных технологий.

К угрозам информационной безопасности относятся: изменение структуры канала передачи данных и его компонентов, связанных с элементом системы доступа, хищения с носителей информации; использование информации, возникающей из-за несовершенства программных компонентов или информационной системы, незаконное подключение различных регистрационных устройств к системным устройствам или линиям связи, введение программных компонентов для изменения программ, намеренное отключение механизмов безопасности.

Сегодня актуальны и потенциально возможны угрозы информационной безопасности: рост атак на IoT («умные») устройства; интерес хакеров к мобильным приложениям и изъятие данных с них; выявление эксплойтов и критических уязвимостей операционных систем, в том числе мобильных; использование технологий нарушения и хищения биометрических данных (голоса, отпечатка пальца, радужной оболочки глаза); появление новых способов распространения вредоносных программ и приложений-двойников для мобильных устройств; рост интереса к приватности данных систем на основе искусственного интеллекта; нарушение персональных граждан государств [4]; внедрение вирусов-шифровальщиков; внедрение фишинговых атак на устройства связи, целевых атак на организации и DDOS-атак на сетевые устройства; возможность маскировки угроз под доверенный трафик; возможность использования кибероружия, например в целях дестабилизации положения страны; дестабилизация оборудования 5-G с целью вывода конкурента с рынка и методы социальной инженерии.

Комплекс мер по предотвращению киберпреступлений состоит из этапов формирования базы на законодательном, нормативно-техническом уровнях, а также непосредственно на уровне организаций. Однако особое внимание следу-

ет уделить новым решениям, способным самостоятельно обучаться и применять методы обнаружения угроз на основе предварительных данных, позволяющих анализировать, выявлять и изолировать угрозы в зависимости от поведенческих признаков, а также учитывать возможные проблемы при использовании облачных технологий.

Пожалуй, большие надежды следует возлагать на переход к отечественным программному обеспечению [5] и операционным системам, что позволило бы в совокупности с российскими средствами защиты реализовать комплекс мер по обеспечению должного уровня информационной безопасности.

Список литературы

1. Ежемесячный сборник о состоянии преступности в России [Электронный ресурс] // Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации, Российская Федерация – 2020. URL:– Режим доступа: <http://crimestat.ru/analytics> (дата обращения: 17.03.2020).
2. The Global Risks Report 2019 14th Edition [Электронный ресурс] // World Economic Forum, Switzerland. – 2020. – URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (дата обращения: 17.03.2020).
3. Global Cybercrime Damages Predicted To Reach \$6 Trillion Annually By 2021 [Электронный ресурс] // Cybersecurity Ventures USA. – 2020. URL: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021> (дата обращения: 17.03.2020).
4. Харисова, З. И. О некоторых проблемах обеспечения информационной безопасности государства и общества от современных киберугроз / З. И. Харисова // Актуальные проблемы права и государства в XXI веке. г. Уфа, 18 апреля 2019 г. : сб. матер. XI Междунар. науч.-практич. конференции. – Уфа : Уфимский ЮИ МВД России, 2019. – С. 388–392.
5. Харисова, З. И. О перспективах перехода органов внутренних дел на отечественное программное обеспечение в рамках импортозамещения / З. И. Харисова, А. А. Катянова // Организация Объединенных Наций и глобальные проблемы человечества в XXI веке : сб. матер. Междунар. науч.-практич. конференции. – г. Уфа : БашГУ, 2019. – С. 250–256.

Химичева Ольга Викторовна¹,
начальник кафедры уголовного процесса
Московского университета МВД России имени В.Я. Кикотя,
доктор юридических наук, профессор,
заслуженный работник высшей школы Российской Федерации;

Андреев Алексей Владимирович²,
старший преподаватель кафедры уголовного процесса
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

НЕОБХОДИМОСТЬ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ КАК ФАКТОР, ОПРЕДЕЛЯЮЩИЙ ЭВОЛЮЦИЮ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Статистика свидетельствует, что по итогам 2019 г., впервые за последние пять лет, на фоне тенденции незначительного роста общего количества преступлений число преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, значительно возросло (+68,5 % по сравнению с 2018 г.) [1]. Это свидетельствует о трансформации преступного поведения и обуславливает необходимость ответных мер в виде адаптации к новым реалиям правоохранительной системы.

Тенденцию роста киберпреступлений отмечают руководители практически всех правоохранительных органов. Так, на серьезный «скачок» указанной категории преступлений обращено внимание на состоявшейся 1 ноября 2019 г. коллегии Министерства внутренних дел Российской Федерации России [2]. Генеральный прокурор России Игорь Краснов отметил, что число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, за последние пять лет возросло в 25 раз, их общая раскрываемость составила менее четверти (24 %), а процент раскрываемости кибермошенничеств крайне низок (9 %) [3].

Негативные социально-экономические явления в жизни общества могут привести к еще большему росту преступлений, связанных с использованием IT-технологий. Так, остается открытым вопрос о достаточности процессуальных мер, направленных на выявление, раскрытие и расследование киберпреступлений, совершаемых в условиях самоизоляции большинства населения страны в связи с неблагоприятной санитарно-эпидемиологической обстановкой.

Вместе с тем при производстве по уголовным делам в этих условиях возникают серьезные проблемы, безусловно отражающиеся на обеспечении прав и законных интересов участников уголовного процесса, интересов общества и государства.

¹ © Химичева О. В., 2020.

² © Андреев А. В., 2020.

Рассмотрим лишь один из примеров [4]: следователь окончил производство по уголовному делу и для реализации права на ознакомление с материалами уголовного дела вызвал обвиняемого и защитника. Однако эти участники отказались явиться для выполнения требований ст. 217 УПК РФ, сославшись на предписания Указа Президента Российской Федерации от 2 апреля 2020 г. № 239 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19)» [5], в соответствии с которыми дни с 4 по 30 апреля 2020 г. объявлены нерабочими, а также положения нормативных правовых актов субъектов Российской Федерации, ограничивающие передвижение населения.

Безусловно, позиция защиты обоснована, однако и позиция следователя находит поддержку в нормах уголовно-процессуального законодательства: ведь согласно ч. 2 ст. 7 УПК РФ следователь принимает решения в соответствии с УПК РФ в случаях противоречия любому другому закону и подзаконному акту, соответственно, он должен выполнить предписания ст. 217 УПК РФ. В свою очередь, сторона защиты не отказывается от осуществления своего права на ознакомление с материалами уголовного дела, но просит перенести его на фактически неопределенный срок (до момента снятия ограничений на передвижение населения). Получается, что предварительное расследование будет фактически приостановлено до момента отмены ограничительных санитарно-эпидемиологических мер, следовательно, его сроки будут превышены. Такие решения должны быть приняты по значительному числу уголовных дел.

Ограничительные санитарно-эпидемиологические меры повлияли и на работу судов, что нашло отражение в постановлении Президиума Верховного Суда Российской Федерации, Президиума Совета судей Российской Федерации от 8 апреля 2020 г. № 821 «О приостановлении личного приема граждан в судах» [6], Обзоре по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 1, утвержденном Президиумом Верховного Суда Российской Федерации 21 апреля 2020 г. [7].

В условиях действия правовых режимов, предусматривающих ограничения свободного перемещения граждан, их нахождения в общественных местах, государственных и иных учреждениях, судам предписано рассматривать дела в порядке упрощенного производства, дела, всеми участниками которых заявлены ходатайства о рассмотрении дела в их отсутствие, если их участие при рассмотрении дела не обязательно, жалобы, представления, подлежащие рассмотрению без проведения судебного заседания, вопросы, для рассмотрения которых не требуется проведение судебного заседания (например, вопросы об исправлении описок, опечаток, явных арифметических ошибок в решении суда). При этом невозможность рассмотрения уголовного дела в связи с введением указанных правовых режимов может стать основанием для отложения и приостановления судебного разбирательства.

Кроме того, Президиум Верховного Суда Российской Федерации в названном выше Обзоре от 21 апреля 2020 г. пояснил, что указы Президента Россий-

ской Федерации в части установления нерабочих дней не распространяются на федеральные органы государственной власти, поэтому нерабочие дни в период с 30 марта по 30 апреля 2020 г. включаются в процессуальные сроки и не являются основанием для переноса дня окончания процессуальных сроков на следующий за ними рабочий день.

Как видим, неблагоприятная санитарно-эпидемиологическая обстановка лишь обострила давно назревшую проблему, несоответствия отечественного уголовно-процессуального регулирования современным реалиям. Действительно, криминальная среда уже вступила в 21 век информационных технологий, разрабатывая и внедряя различные новые способы совершения преступления. В то же время органы и должностные лица, осуществляющие уголовное судопроизводство, имеют в «своем арсенале» лишь те средства и методы борьбы, которые разработаны на рубеже 20 и 21 столетия.

Таким образом, назрела необходимость наделить следователя правовыми средствами собирания доказательств в электронной форме.

Во-первых, следователь должен иметь полномочия получать информацию без изъятия электронного носителя информации.

Для реализации данного положения необходимо закрепить в уголовно-процессуальном законе понятие «запрос в электронной форме» и требования к его составлению и передаче. Такой запрос может быть направлен в государственные организации (медицинские учреждения, суды, различные реестры и др.) и коммерческие организации (банки, учреждения связи и другие организации). Аналогичное понятие уже предусмотрено в ч. 2 ст. 93 Налогового кодекса Российской Федерации.

Помимо запроса в электронной форме следователь должен наделяться полномочиями по получению информации с электронного носителя информации, без фактического изъятия самого носителя информации. Это позволит следователю избежать многих проблем: угрозы уничтожения значимых сведений; получения сведений постфактум, а не в режиме реального времени; устранить зависимость от места хранения информации, находящейся за пределами Российской Федерации и стран, с которыми заключен договор о правовой помощи.

Другими словами, следователю для изъятия информации, содержащейся на электронном носителе, необходимо: знать, что информация, необходимая для расследования, находится на определенном носителе (компьютере, телефоне, накопителе информации и др.); знать местонахождение электронного носителя этой информации; быть уверенным, что информация не будет уничтожена или перемещена на другой носитель информации; законно изъять носитель информации.

Более справедлив другой подход, а именно: следователь устанавливает возможность нахождения значимой для расследования информации на каком-либо носителе, получает на изъятие информации судебное решение, после чего направляет указанное судебное решение вместе с поручением о производстве следственных и иных действий в специализированное подразделение. Указанное подразделение, получая поручение и судебное решение, осуществляет изъятие информации техническим путем без изъятия носителя информации. После производства необходимых следственных и иных процессуальных дей-

ствий, результаты передаются следователю для использования в процессе доказывания. Данный алгоритм действий прежде всего решит проблему того, что информация, имеющая значение для уголовного дела, не будет полностью уничтожена.

Во-вторых, в уголовно-процессуальном законе должно быть урегулировано производство следственных действий в дистанционной форме. Очевидно, что технический прогресс уже позволяет осуществлять допрос без фактического контакта между следователем и допрашиваемым лицом. Однако, дистанционные допросы не производятся из-за отсутствия правовой регламентации. Помимо этого, в дистанционной форме возможно производство и других следственных действий (предъявления для опознания, осмотра предметов и документов, следственного эксперимента).

В-третьих, следует предусмотреть возможность замены некоторых процессуальных действий аналогами в электронной форме. К примеру, в настоящее время применяется только подача заявлений, ходатайств и жалоб через специализированные сервисы в интернете; однако до сих пор процессуальное решение по поступившим в электронной форме обращениям направляется заявителям по почте. В связи с этим необходимо рассмотреть вопрос о направлении уведомлений, повесток, копий процессуальных решений в электронной форме. Ознакомление участников с постановлениями о назначении судебных экспертиз, заключениями экспертов и материалами уголовного дела также можно осуществлять в дистанционной (электронной) форме.

К числу проблем, возникающих в практической деятельности, относится и отсутствие установленных уголовно-процессуальным законом правил собирания, проверки и оценки доказательств в электронной форме, например: в каком порядке изымать криптовалюту, как проверить документы, составленные только в электронном виде и подписанные электронной цифровой подписью.

Повышение уровня киберпреступности, как в количественном, так и в качественном отношении, осложнившаяся социально-экономическая ситуация, связанная с пандемией «коронавируса», показывает несовершенство, а в некоторых случаях нерешаемые правовые коллизии уголовно-процессуального регулирования. Сегодня необходимы эволюция уголовного судопроизводства, введение дистанционных способов собирания доказательств и другие меры по совершенствованию защиты граждан от преступных посягательств.

В нашей стране предпринимаются активные меры по внедрению цифровых технологий во все сферы жизни общества. Так, законопроект «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [8] предполагает, что в отдельных субъектах России и отраслях экономики, будет введен режим экспериментальной цифровой инновации, позволяющий разрабатывать и внедрять новые методы. По итогам данного эксперимента, на основании реестра проблем и достигнутых результатов, будет оценена успешность внедрения методики, данные методы будут закреплены законодательно и внедрены на территории всей Российской Федерации. Отрасли, которые включены в данный проект, достаточно разнообразны: это и медицина, и образование, и экономика, но уголовного судопроизводства, к сожалению, нет в данном списке. Однако возможно создание экспериментального информацион-

ного правового режима и для производства по уголовным делам в отдельных субъектах Российской Федерации, что приведет к колоссальному скачку в развитии уголовно-процессуальных отношений.

Список литературы

1. Комплексный анализ состояния преступности в Российской Федерации по итогам 2019 года и тенденции ее развития : аналитический обзор / [М. В. Гончарова и др.] // ФГКУ «ВНИИ МВД России» / документ обсужден и одобрен на заседании НИЦ № 1 ФГКУ «ВНИИ МВД России» (протокол № 7 от 25 февраля 2020 г.)

2. Решение коллегии Министерства внутренних дел Российской Федерации России от 1 ноября 2019 г. № 3км / Документ опубликован не был.

3. Доклад Генерального прокурора Российской Федерации Игоря Краснова на расширенном заседании коллегии Генеральной прокуратуры Российской Федерации 17 марта 2020 г., посвященной итогам работы органов прокуратуры за 2019 год и задачам по укреплению законности и правопорядка на 2020 год // Новости прокуратуры РФ. – URL: <https://procrf.ru/news/1848173-sostoyalos-rasshirennoe-zasedanie-kollegii-posvyaschenoe-itogam-rabotyi-organov-prokuraturyi-za.html> (дата обращения: 21.04.2020).

4. Бунин, О. Ю. «Вакцина следователя от всех болезней – УПК» / О. Ю. Бунин // СПС «Zakon.ru» / URL: https://zakon.ru/blog/2020/4/13/-vaccina_sledovatelya_ot_vseh_boleznej__upk (дата обращения: 21.04.2020).

5. Указ Президента Российской Федерации от 2 апреля 2020 г. № 239 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19)» // СПС «КонсультантПлюс» / URL: http://www.consultant.ru/document/cons_doc_LAW_349217/ (дата обращения: 21.04.2020).

6. Постановление Президиума Верховного Суда Российской Федерации, Президиума Совета судей Российской Федерации от 8 апреля 2020 г. № 821 «О порядке работы судов в период угрозы распространения на территории России коронавирусной инфекции» // СПС «Гарант». – URL: [https://www.garant.ru/files/2/7/1344672/postanovlenie-prezidiuma-verhovnogo-suda-rossiyskoy-federacii-i-prezidiuma-soveta-sudey-rossiyskoy-federacii-ot-8-aprelya-2020-g\(1\).pdf](https://www.garant.ru/files/2/7/1344672/postanovlenie-prezidiuma-verhovnogo-suda-rossiyskoy-federacii-i-prezidiuma-soveta-sudey-rossiyskoy-federacii-ot-8-aprelya-2020-g(1).pdf) (дата обращения: 21.04.2020).

7. Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 1, утвержденный Президиумом Верховного Суда Российской Федерации 21 апреля 2020 г. http:// СПС «Гарант». – URL: <http://www.garant.ru/hotlaw/federal/1362561/> (дата обращения: 21.04.2020).

8. Проект Федерального закона № 922869-7 «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Система обеспечения законодательной деятельности. – URL: <https://sozd.duma.gov.ru/bill/922869-7> (дата обращения: 21.04.2020).

Черногоров Георгий Викторович¹,
*слушатель факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя;*

Галиев Денис Вадимович²,
*преподаватель кафедры специальных
информационных технологий учебно-научного комплекса
информационных технологий Московского университета
МВД России имени В.Я. Кикотя*

УЯЗВИМОСТИ USB ИНТЕРФЕЙСА

В современном мире информационные технологии проникли практически во все сферы нашей деятельности: работа, передвижение на транспорте, оформление заказов через интернет или же просто фотосъемка – все сопровождается фиксацией информации на устройствах, которыми мы пользуемся. При этом мало кто задумывается о безопасности информации, которая находится на компьютере, имеющем неустранимые без существенных потерь уязвимости.

USB (Universal Serial Bus – универсальная последовательная шина), промышленный стандарт расширения архитектуры PC. Причиной возникновения стандарта для передачи информации послужило желание упростить соединение ПК с периферийными устройствами. Основная цель стандарта: возможность пользоваться таким интерфейсом, который обладал бы максимальной простотой, универсальностью и использовал принцип Plug&Play или горячее соединение. Но вместе с тем есть недостаток: в угоду простоте и удобству использования, USB интерфейс изначально доверяет всем подключаемым устройствам. Из этого появилась уязвимость BadUSB и ее разновидности.

Феномен channel-to-channel crosstalk leakage, который является уязвимостью, а также разновидностью BadUSB, распространяется на USB-устройства, подключенные к соседним портам одного персонального компьютера или хаба. Суть заключается в том, что электрические сигналы, исходящие от USB-портов, можно использовать для хищения данных, так как USB-хаб содержит один чип, в котором логические блоки не изолированы друг от друга. Атакующему достаточно подключить к одному из USB-портов собственное вредоносное устройство, которое отслеживает колебания напряжения на соседних портах, к которым подключены устройства, и тем самым перехватывать разную информацию, например, нажатия клавиш, а соответственно и пароли. В проведенном исследовании использовался ноутбук с подключенным USB-хабом, в который была подключена клавиатура. К USB кабелю клавиатуры на линии D+ и GND были подключены провода, которые, в свою очередь, подключены к ос-

¹ © Черногоров Г. В., 2020.

² © Галиев Д. В., 2020.

циллографу. В соседний порт USB-хаба было подключено USB-устройство, которое снимало сигналы с линий +5V и GND USB порта и передавало их на осциллограф. В результате два сигнала, отображающиеся на осциллографе были идентичны. Так можно перехватывать информацию, интерпретируя сигнал, снимающийся с соседнего USB-порта, который представляет собой кадры, передающиеся последовательной передачей бит по методу NRZI, в данные.

BadUSB – это атака на компьютер через USB-порт посредством подключения устройства с измененной прошивкой или дополнительным кодом на микроконтроллере. При подключении такого устройства, оно может опознаваться как совершенно другое и скрыто выполнять функции, предусмотренные атакующей стороной.

HID-атака – интересная разновидность BadUSB. Ее суть сводится к тому, что в USB-порт вставляется хакерский девайс, эмулирующий устройство ввода. Любая современная операционная система поддерживает Plug&Play и содержит универсальный драйвер устройства каждого класса. Вредоносное устройство автоматически определяется операционной системой как нужный Human Interface Device – HID. Далее операционная система безо всяких проверок принимает его команды. Преимущества HID-атаки – скорость, незаметность и автоматизация. Все необходимые действия выполняются быстрее, чем можно набрать то же на клавиатуре, и без опечаток. В проведенном исследовании, в микроконтроллер платы прототипирования, которая может работать с USB интерфейсом, был прошит вредоносный код. Он содержал библиотеки, которые описывают работу USB-драйвера, содержат файл конфигурации для USB интерфейса, реализуют глобальное манипулирование флагом прерывания и функции для циклов задержки занятого ожидания, предоставляют интерфейсы для программ для доступа к данным, хранящимся в программном пространстве устройства, а также библиотеку, которая использует упрощенный дескриптор отчета клавиатуры, не поддерживающий протокол загрузки. Так же был написан вредоносный код.

При подключении платы к компьютеру происходило ожидание инициализации, только после чего выполнялся дальнейший код, чтобы избежать исполнения кода сразу после подачи питания. Затем происходило открытие командной строки, введение команды для готового эксплойта, который использует оболочку PowerShell (в ОС Windows 10) для скачивания нужных бинарных файлов с сервера. Использовался модуль `web_delivery` из-за низкой вероятности срабатывания антивируса и высокой скорости. Также после окончания работы не останется следов, так как он ничего не пишет на диск. Скачивание происходило через 443 порт. По окончании исполнения кода микроконтроллером был получен удаленный доступ. При этом все было выполнено в автоматическом режиме. За счет того, что действия выполнялись через микроконтроллер и PowerShell, а не программно на атакуемом компьютере, антивирус не сработал.

Данные уязвимости рассматривались как угрозы безопасности информации, ведь интерфейсы USB и USB устройства используется повсеместно и постоянно. Такая угроза будет актуальна до тех пор, пока не изменяется сама концепция и аппаратная часть USB интерфейса, но в таком случае USB может пере-

стать быть именно таким, каким он создавался изначально. В результате могут пострадать устройства, которые будут использовать устаревший формат USB интерфейса, что делает все изменения в отношении USB интерфейса мало осуществимыми, ведь могут пострадать более 1 млрд устройств.

Список литературы

1. Агуров, П. В. Интерфейсы USB. Практика использования и программирования / П. В. Агуров. – СПб. : БХВ-Петербург, 2009.
2. Дмитриев, А. Принцип работы флэш-памяти / А. Дмитриев // Hobbyits.com. – 2012. – URL: <http://hobbyits.com/cifrovyyetehnologii/princip-raboty-i-ustrojstvo-flesh-pamyati.html>.
3. Таненбаум, Э. С. Архитектура компьютера / Э. С. Таненбаум, Т. Остин. – 6-е изд. – ИД «Питер», 2018.

Шарова Ксения Михайловна¹,
курсант факультета подготовки
специалистов в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя;

Поликарпов Евгений Сергеевич²,
начальник кафедры
специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук

СТАТИСТИКА КИБЕРПРЕСТУПНОСТИ ЗАРУБЕЖНЫХ СТРАН

Основу киберпреступлений составляет ограниченное число деяний, которые направлены против целостности, конфиденциальности и доступности компьютерных систем и данных. Но если учитывать преступления, связанные с использованием компьютера для получения личной выгоды, причинения финансового или личного ущерба (также с использованием персональных данных), то их тоже можно включить в более широкое понятие киберпреступности. Однако при этом сложно найти достаточно точное юридическое определение данному понятию. Merriam-Webster так определяет понятие «киберпреступность»: преступная деятельность, совершенная с помощью компьютера специально для незаконного доступа, передачи или манипулирования людьми. На сегодняшний день такие виды преступлений очень распространены, при чем даже на международном уровне; объектом может быть не только отдельный человек, его личные данные, но и компании, и даже страны.

Большую часть киберпреступлений составляет кража данных: персональные, учетные данные, данные платежных карт, медицинская информация, коммерческая тайна, базы данных клиентов, личные переписки и другая информация. Согласно последнему отчету DLA Piper о статистике общего регламента защиты персональных данных по количеству уведомлений о нарушениях данных в первой пятерке оказались Нидерланды, Германия, Великобритания, Ирландия и Дания (см. рис. 1).

По словам начальника центра жалоб, на интернет-преступления ФБР «общее число зарегистрированных киберпреступлений составляет всего лишь 10–12 % фактического числа. Все потому, что пострадавшие граждане или организации, подвергшиеся вымогательству в сети, боятся обращаться за профессиональной помощью для решения вопроса из-за рисков допустить публикацию украденной информации».

¹ © Шарова К. М., 2020.

² © Поликарпов Е. С., 2020.

По результатам опроса о мошенничестве в Америке число жертв кражи личных данных с 2016 по 2019 г. снизилось, чего нельзя сказать о финансовых потерях, которые на 2019 г. составляли 16,9 млрд долл. Этот вывод говорит о том, что преступная направленность больше направлена на хищение материальных средств чем на количество пользователей.

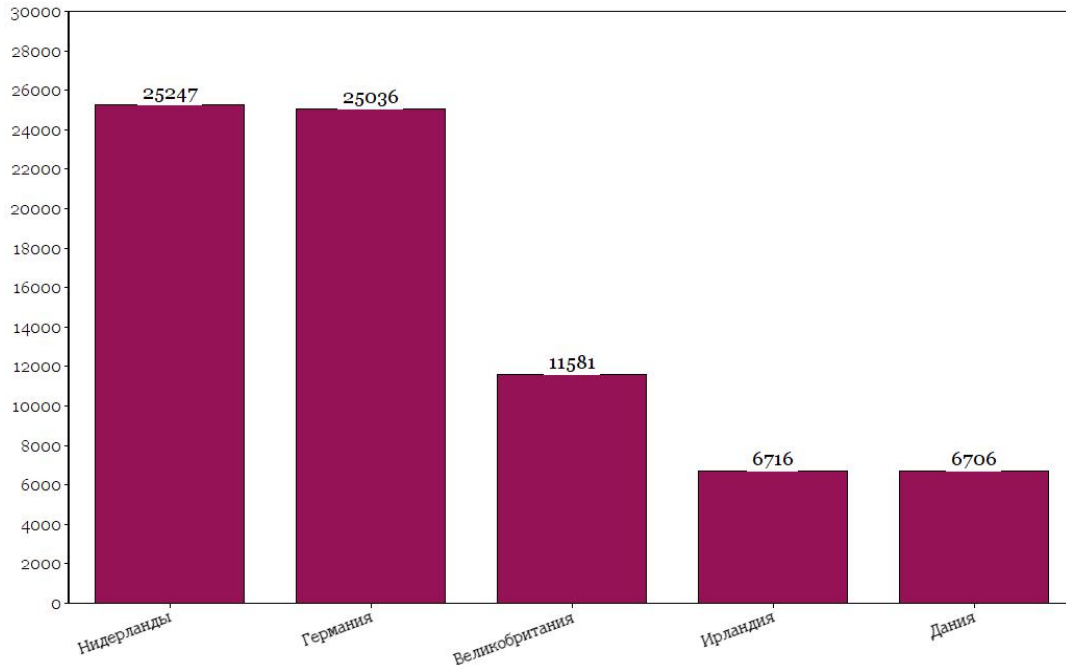


Рис. 1. Количество уведомлений о нарушениях данных стран Европы

Наиболее распространенными способами кибератак считаются использование ВПО, DDoS-атаки, комбинация социальной инженерии и вредоносного кода (в частности, фишинг) и незаконная деятельность (вымогательства, распространение незаконного контента).

Распространение вредоносного программного обеспечения возглавляет рейтинг киберпреступлений за 2019 г., составляя 57,6 % общего количества, на второй строчке захват аккаунта – 24,5 %, на третьей – преступления, совершенные с использованием уязвимостей сети, компьютера 7,5 %, на четвертой – вредоносный спам и внедрение вредоносных скриптов 8 %, и DDoS-атаки с 2,4 %.

В случае с распространением вредоносного программного обеспечения, основными методами доставки их до цели – электронная почта (в 94 % случаев), и веб-пространство (23 % случаев). При этом используются следующие типы файлов Office doc (45 %), приложения Windows.exe (26 %) и другие (22 %). Один из 13 веб-запросов приводит к вредоносным программам.

Говоря о криминальных масштабах распределенных атак отказа в обслуживании, следует сказать, что данный вид наносит очень большой ущерб жертвам (только в 2018 г. ими стали 51 % предприятий). Хотя методы и урон каждой атаки различаются, конечная цель отказа в обслуживании (DoS) и распределенных атак отказа в обслуживании (DDoS) одинакова – затопить ресурс или целевую систему, чтобы лишить доступа тех, кто в нем нуждается. Согласно отчетам, Kaspersky DDoS в 2019 г. на Китай приходилось более 50 % DDoS-атак;

Соединенные Штаты заняли второе место (около 17 %) и Япония на третьем (менее 2 %). В четвертом квартале 2019 г. абсолютное большинство ботнетов (58,33 %) оказалось зарегистрировано на территории США, Великобритании (14,29 %) и Китае (9,52 %). Доля остальных стран в распределении ботнетов менее 2 %.

Распространение социальной инженерии достаточно широко. В среднем, 30 % фишинговых писем открываются пользователями, и 12 % из них переходят на вредоносный сайт или открывают зараженное вложение. В мире за 2019 г. мишенью для таких «посланий» стали США – более 50 %, Германия – 11,7 %, за ней Вьетнам – 5,77 % и Италия – 5,57 %. Статистика стран по доле атакованных пользователей от «Лаборатории Касперского» представлена на рис. 2.

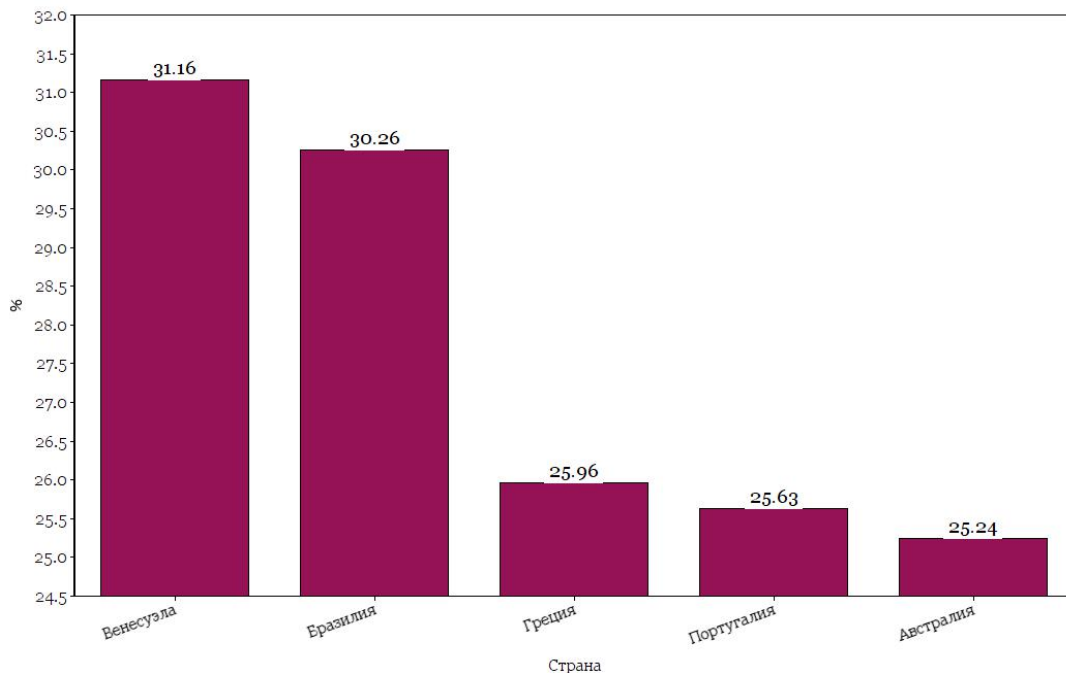


Рис. 2. Доля атакованных пользователей

Вымогатели в сети. Ransomware (трояны-вымогатели) – разновидность зловредных программ, подразделяющаяся на шифровальщиков (которые шифруют ценные файлы, за раскрытие которых нужно заплатить) и блокировщики (ограничивающие доступ к устройству). Средняя стоимость атаки вымогателей на предприятия составляет \$ 133000. Соединенные Штаты занимают самое высокое место с 18,2 % всех атак вымогателей. По факту, 20 % жертв таких преступлений не получают обратно свои данные после уплаты выкупа.

Таким образом, огромное количество статистических данных показывают, насколько сильно распространены киберпреступления. Важно помнить о безопасности в сети, следить, по каким ссылкам переходить, обращать внимание на источник и не поддаваться методам социальной инженерии. Вопросы о кибербезопасности поднимаются на мировом уровне (например, ООН внедряет Глобальную программу кибербезопасности), главы ведущих стран обеспокоены и предпринимают меры, направленные на защиту своих граждан и государств от мошеннических действий, совершаемых с помощью информационных технологий.

Список литературы

1. Fishing as a Cybercrime in the Internet Banking System: Economic and Legal Aspects. – 2019. – URL: <https://www.abacademies.org/articles/fishing-as-a-cybercrime-in-the-internet-banking-system-economic-and-legal-aspects-8441.html> (дата обращения: 20.04.2020).
2. 2019 Cyber Attacks Statistics. – 2020. – URL: <https://www.hackmagedon.com/2020/01/23/2019-cyber-attacks-statistics/> (дата обращения: 19.04.2020).
3. Спам и фишинг в 2019 году. – 2020. – URL: <https://securelist.ru/spam-report-2019/95727/> (дата обращения: 19.04.2020).
4. Must-Know Cybersecurity Statistics for 2020. – 2020. – URL: <https://www.varonis.com/blog/cybersecurity-statistics/> (дата обращения 19.04.2020).
5. 20 Cybersecurity and Phishing Statistics That Matter In 2019. – 2019. – URL: <https://www.appknox.com/blog/cybersecurity-statistics-2019> (дата обращения: 20.04.2020).

Яковлева Кристина Юрьевна¹,

курсант факультета подготовки

сотрудников для органов предварительного расследования

Московского университета МВД России имени В.Я. Кикотя;

Андреев Алексей Владимирович²,

старший преподаватель кафедры уголовного процесса

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

ПРЕДОТВРАЩЕНИЕ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ КИБЕРПРЕСТУПНИКАМИ В СОЦИАЛЬНЫХ СЕТЯХ

С развитием научно-технического прогресса информационные технологии стали неотъемлемой частью нашей повседневной жизни. Ныне день актуальна деятельность по разработке современных криминалистических и уголовно-процессуальных средств и методов работы правоохранительных органов, способствующих раскрытию и расследованию преступлений в социальных сетях. Необходима выработка мер предотвращения преступной деятельности лиц, использующих социальную инженерию в онлайн-платформе, предоставляющей возможность онлайн-общения.

За последнее десятилетие происходит глобальное оцифровывание мира, а уровень правовой грамотности и киберграмотности граждан отстает. В результате проведения социологического тестирования «Лаборатория Касперского» выявила глобальные киберпроблемы. [9] В основном они связаны с тем, что поколения настоящего времени на 92 % ведутся на фишинговые атаки и полностью доверяют информации, хранящейся на серверах интернета, в социальных сетях. Возникла острая необходимость в цифровизации – ускорение и повышение эффективности общественных процессов в сфере информационных технологий. По оценкам Интерпола [4] и Европейской полиции киберпреступность стремительно растет.

Пока еще количество «киберпреступлений» относительно общего количества преступлений имеет низкий удельный вес. В 2018 г. зарегистрировано более 212 060 преступлений [5]. Следственный департамент МВД России отмечает, что количество зарегистрированных «киберпреступлений» за 2018 г. составило – 105 645 [6], это всего 4,9 % общего числа преступлений. Однако ежегодно количество указанных преступлений неуклонно растет.

Стала наблюдаться острая нехватка криминалистических методов и тактических рекомендаций проведения процессуальных и следственных мероприятий, средств для проведения профилактических действий в киберпространстве. Необходимы инновационные уголовно-процессуальные, криминологические,

¹ © Яковлева К. Ю., 2020.

² © Андреев А. В., 2020.

криминалистические разработки с целью предотвращения киберпреступлений в онлайн-платформах, представленных для онлайн-общения субъектов.

Общедоступная информация в цифровом виде востребована обществом для решения различных задач. В настоящее время эффективным средством расследования преступлений является видеозапись. Так, на примере города Москвы, можно просмотреть на сайте [7] доступные в реальном времени веб-камеры, напрямую передающие все происходящее в сеть.

Социальная сеть – актуальная информационная платформой особенно среди молодежи. Анализ информации, размещенной в социальных сетях «Интернет» может способствовать плодотворному расследованию и эффективному проведению профилактических работ, так как все чаще следственной практике известны преступления, связанные с использованием инструментов преступного воздействия социальной инженерии.

Профилактической работой выступает мониторинг веб-страниц с целью выявления и пресечения преступного поведения или призыва к нему. Информация, содержащаяся на веб-страницах социальных сетей, важный объективный источник информации о личности. Фиксация факта общения в сети, общие фотографии могут быть использованы для доказывания мотива преступления, присутствия личной заинтересованности в ходе расследования, может быть достаточным основанием для производства следственных действий.

Компания «Яндекс» запустила сервис для поиска людей в социальных сетях по адресу: yandex.ru/people. Сегодня поиск можно осуществить по 16 социальным сетям: «ВКонтакте», «Одноклассники», «Facebook», а также по различным данным, отраженным в социальной сети. Узнать какие записи человек совершал за последнее время на Facebook, Instagram и других социальных сетях, можно с помощью Social Searcher.

Для того чтобы узнать, что пользователь посетил веб-страничку в Twitter в конкретное время, в социальной сети есть специальный оператор для расширенного поиска – `from:@tim_cook until:2019-10-17`, а с помощью оператора «near:» можно узнать, что пишут люди в конкретном городе или в точке с определенной широтой и долготой: `near:56.35,47.03`.

Пользователь мало информации выкладывает о себе в глобальную сеть, но этого достаточно, чтобы получить совокупность данных о лице. Правоохранительные органы периодически предупреждают граждан посредством правовой справки, чтоб они не стали жертвой информационного преступника. Сотрудники полиции предупреждают, чтобы пользователи не выкладывали в сеть персонифицированную информацию, – отнести паспортные данные, данные банковских карт.

Интернет-ресурсы позволяют получить необходимые и имеющие значение сведения о человеке по графическим данным. Так, имея графическое изображение возможно найти в такой социальной сети, как «ВКонтакте» социальную страничку любого зарегистрированного лица. Необходимо зарегистрироваться в бесплатной программе «Find Clone» [8], добавить фотографию лица человека, которого желаете найти. На данном сайте появится подборка страниц похожих лиц на то лицо, которое представлено на загруженном в систему графическом изображении. С помощью поискового инструмента Yomapic можно увидеть графическую информацию любого указанного места.

Таким образом, целесообразность использования в расследовании преступлений сведений, размещенных на ресурсах социальных сетей интернета и проведения профилактических работ, обусловлена тем, что такого рода информация может существенно облегчить выбор направлений поисковой деятельности и проведения процессуальных действий, а также планирование проведения оперативно-разыскных и следственных мероприятий; поиск информации на открытых информационных ресурсах быстрее, а иногда и более эффективен, чем при добывании ее с помощью негласных мероприятий; в условиях дефицита времени такие источники являются средством быстрого получения необходимой информации, а также блокирования фишинговой атаки. Социальные сети как инструмент в расследовании удобны доступностью, скоростью извлечения и объемом полученной информации.

Целесообразно и важным разработать методические рекомендации для сотрудников правоохранительных органов, устанавливающих механизм непрерывного проведения профилактических мер посредством размещения информации в интернете.

Преступность в киберпространстве имеет высокую степень латентности, поэтому с каждым годом уменьшается количество возбуждаемых уголовных дел по данным составам преступления. Правоохранительным органом трудно бороться с киберпреступниками, которых становится больше, а способы совершения преступлений сложнее. Для эффективной борьбы с преступлениями в информационной сфере и использованием технических средств государственным органам необходимы современная техническая база, должное финансовое и материальное обеспечение, квалифицированные и подготовленные кадры и систематическое проведение профилактических работ.

Список литературы

1. Предварительное следствие в органах внутренних дел : учебное пособие / [А. А. Орлова и др.]. – М. : Щит-М, 2007.
2. Смирнов, И. В. Не надо разбрасываться своими персональными данными / И. В. Смирнов // <http://www.it-weekly.ru/it-news/security/135841.html>
3. Гончар, В. В. Уголовно-процессуальная деятельность в стадии возбуждения уголовного дела: проблемы правового регулирования / В. В. Гончар, М. В. Мешков // Мировой судья. – 2015. – № 4.
4. Официальный сайт Интерпола. Раздел статистика // Interpol. – URL: <https://www.interpol.int/> (дата обращения: 13.09.2019).
5. Состояние преступности за 2018 года // Официальный сайт МВД России. – URL: <http://www.mvd.ru> (дата обращения: 24.09.2019).
6. Аналитический обзор «Правоприменительной практики расследования преступлений, совершенных в сфере информационно-коммуникационных технологий, по итогам 2018 года» // Следственный департамент МВД России. – М., 2018 г.
7. Электронный ресурс. URL: <http://youwebcams.net/online/category/russia/moscow/>.
8. Электронный ресурс. Веб-страница // URL: <https://findclone.ru/>.
9. Официальный сайт АО «Лаборатория Касперского». – URL: <https://www.kaspersky.ru/> (дата обращения: 16.04.2020).