

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

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

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

**Всероссийская научно-практическая конференция
(13 октября 2022 г.)**

Сборник научных трудов

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

Научное электронное издание

Москва

Московский университет
МВД России имени В.Я. Кикотя

2022

© Московский университет МВД России
имени В.Я. Кикотя, 2022
ISBN 978-5-9694-1206-4

УДК 004.9
ББК 16.3
И74

Рецензенты:

начальник кафедры информационной безопасности
Краснодарского университета МВД России доктор технических наук,
профессор **А. В. Еськов**; заместитель начальника 1-го отдела – начальник
3-го отделения ЦИТСиЗИ ГУ МВД России по г. Москве **О. В. Елисеева**

Составитель *И. С. Мельцева*

И74 Информационные технологии в деятельности органов внутрен-
них дел: Всероссийская научно-практическая конференция, 13 октября
2022 г. : сборник научных трудов / [сост. И. С. Мельцева]. – М. : Мос-
ковский университет МВД России имени В.Я. Кикотя, 2022. – 322 с. –
1 электронный оптический диск (CD-R). – Системные требования : CPU
1,5 ГГц ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жест-
ком диске.

ISBN 978-5-9694-1206-4

В сборнике публикуются статьи авторов, принявших участие во Всероссийской научно-практической конференции «Информационные технологии в деятельности органов внутренних дел», прошедшей 13 октября 2022 г. Рассматриваются проблемные вопросы контроля и правового регулирования безопасности государства, анализа угроз обеспечению кибербезопасности страны, а также противодействия преступности в сфере информационных технологий, технологии защиты систем хранения, распространения, обработки и передачи данных, технологий расследования компьютерных преступлений.

Предназначен для курсантов и слушателей очной и заочной форм обучения образовательных организаций системы МВД России, а также научных и практических сотрудников, участвующих в борьбе с преступностью.

Научное электронное издание

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

© Московский университет
МВД России имени В.Я. Кикотя, 2022

Издание подготовлено
с помощью программного обеспечения Microsoft Word

В авторской редакции

Корректор Жукова О. И.
Компьютерная верстка Жукова О. И.

Подписано к изданию 16.12.2022
Объем издания: 4,62 Мб
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-1206-4



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

СОДЕРЖАНИЕ

Клименко А. Б.

Робототехника в деятельности органов внутренних дел 10

Львова А. А.

Использование аппаратно-программного комплекса
«Безопасный город» в деятельности сотрудников
органов внутренних дел.....15

Панфилова А. Д.

Технология блокчейн в деятельности органов внутренних дел.....22

Шишкин И. С.

Использование искусственного интеллекта
правоохранительными органами для выявления
разыскиваемых лиц в местах массового скопления людей 27

Рыбак М. М.

Бесконтактный сбыт фальшивых денежных средств 33

Герцен М. А.

Вопросы управление рисками информационной безопасности.....37

Бочарова А. С.

Цифровые следы в расследовании хищений,
совершенных с использованием сети
Интернет и телефонов.....41

Платов Н. Е., Сизоненко А. Б.

Алгоритм назначения экспертов на процессы аудита
информационной безопасности для эффективного
решения задач по оценке соответствия защищенности
объектов критической информационной инфраструктуры 46

Кияшко С. Е.

Анализ возможностей выявления фактов компрометации
ключа электронной подписи в системах электронного
документооборота на основе методов машинного обучения 50

Баринова А. К.

Защита информации посредством использования
квантовых каналов связи 54

Бедрин В. С.

Информационный экстремизм: его сущность и содержание 59

Бороздина В. Н.

Проблемы выявления и борьбы с запрещенным
контентом в сети Интернет 61

Гавриленко А. А.

Использование информационно-поисковых систем
для решений задач оперативно-разыскной
деятельности ОВД.....65

Овчинский А. С.

Обеспечение информационной безопасности
в гибридной войне 68

Гончар В. В.

Основные проблемы расследования
киберпреступлений и пути их решения 75

Григорьев В. Р., Градосельская Г. В., Жуков Д. О.

Распространение деструктивного контента в социальных
сетях российских пользователей 79

Громова А. В., Ошкуков С. С.

Применение количественных методов в автороведческой
идентификационной экспертизе 92

Данилова Е. А.

Исследование возможности негласного контроля
web-камеры персонального компьютера 100

Коломина А. С.

Механизм выявления ключевых субъектов в «иерархической
модели» дискредитации органов государственной власти
в сегментах сети Интернет 104

Андреев И. В.

Виртуальная и дополненная реальность в ОВД.....107

Лустин В. И.

Повышение защищенности объекта информатизации
от утечки по оптико-электронному каналу 111

Миляев Г. А.

Компьютерная экспертиза при расследовании преступлений
органами внутренних дел 114

Сизоненко А. Б., Титарев А. О., Рудь И. С.

Модель управления ресурсами в социотехнических системах
защиты информации от несанкционированного доступа
на основе теории массового обслуживания.....117

Кудряков Д. Д.

Деанонимизация пользователей пиринговых сетей 121

Калашникова А. А., Ломов М. С.

Место России в компьютеризации: основные
направления и проблемы 124

Стручков И. С., Лапшин И. О., Максимченко А. М.

Автоматизация распознавания парольного ввода
в компьютерную систему 128

Иванов В. А.

Межотраслевой подход в противодействии IT-преступности
в деятельности органов внутренних дел 133

Лукашенко Д. В.

Обучение персонала информационной безопасности
с учетом современных угроз безопасности 137

Андруник А. П.

Интеграция культуры информационной безопасности
в образовательный педагогический процесс 141

Гузеев М. С.

Социальная инженерия в разрезе информационной безопасности.....146

Ермакова А. С.

Обработка персональных данных – возможные
риски угрозы безопасности 149

Борзунов К. К.

Открытые цифровые источники в сокрытии
разведывательных мероприятий 154

Байков Д. В., Паляченко М. Ю.

Проблемы обеспечения кибербезопасности организаций
в условиях цифровизации.....159

Белов Я. М.

Применение экспериментальных правовых режимов
(песочниц) в сфере защиты информации в МВД России.....162

Жиганин А. Я.

Система взаимодействия полиции с гражданами
посредством Telegram-бота 165

Смольянинов В. А.

Информационные и цифровые технологии в деятельности
органов внутренних дел.....168

Рахмонбердиев Б. Б.

Оценка энтропии таблиц кодировок в задаче
оптимальной передачи информации 171

Полюхович А. К.

Вопросы идентификации и аутентификации пользователей
при удаленном электронном обмене в киберпространстве 173

Пузаков А. В.

Анализ криптографических методов в целях
выявления оперативно-значимой информации
в стенографических контейнерах 178

Кашин Ю. О., Булгаков В. В.

Современные способы защиты информации в облачных
хранилищах данных 181

Матюнькин Д. А.

Актуальные вопросы при исследовании компьютерных
вредоносных программ.....187

Дворянкин О. А., Рязанова А. М.

Использование открытых источников информации
при выявлении и пресечении преступлений в сети Интернет,
связанных с торговлей людьми.....191

Корнилов А. А.

Проблемы использования искусственного интеллекта
в деятельности органов внутренних дел 195

Шкинин Д. А.

О негативной роли криптовалюты в условиях
цифровизации экономики.....198

Забавин М. В.

Особенности следообразования при реализации
удаленного доступа к персональному компьютеру 202

Клочкова Е. Н.

Возможности использования открытых источников
информации для поиска криминалистически
значимой информации 206

Кофтина Ю. Н., Екимов А. Ю.

Современные информационные технологии и их использование
в организации кадрового обеспечения органов внутренних
дел Российской Федерации 210

Курбакова Д. О., Задохина Н. В.

Особенности психологического портрета
жертвы киберпреступлений 216

Клочкова А. М., Максимов Н. А.

Проблемы обеспечения безопасности интернета вещей.....220

Поликарпов Е. С., Мурашев А. Е.

Использование цифрового отпечатка устройства
в оперативно-аналитической деятельности 223

<i>Никитин Г. К.</i>	226
Алгоритм программного обеспечения по выявлению фактов продажи технических средств с функцией негласного получения информации	226
<i>Ситникова А. В.</i>	
К вопросу о механизмах образования цифровых следов	230
<i>Цыцурин С. Л., Меликов Э. Э.</i>	
Цифровая безопасность. Недавняя проблема, реальная угроза	235
<i>Шутов О. Н.</i>	
Об использовании технологий Big data в оперативно-разыскной деятельности	238
<i>Гершкович М. А.</i>	
Оптимальное распределение полицейских патрульных нарядов с учетом информации из анонимного сегмента сети Интернет	242
<i>Осипова А. А.</i>	
Специфика распознавания недостоверной информации в социальных сетях	249
<i>Соколова Я. С., Пименова О. В.</i>	
Инновационные инструменты фрод-мониторинга в практике внутреннего аудита информационных систем правоохранительных органов.....	253
<i>Булгаков В. Г.</i>	
Использование биометрических технологий в раскрытии и расследовании преступлений.....	256
<i>Григорькин А. А.</i>	
Использование методов ядерного магнитного резонанса для химического и физического анализа веществ	260
<i>Булгакова Е. В., Лузганов Д. В.</i>	
Оценка степени значимости и устойчивости данных цифрового профиля гражданина Российской Федерации, необходимых и достаточных для идентификации личности.....	267
<i>Тукаева Ф. А.</i>	
Опасности электронной подписи	271
<i>Альховская А. В., Худяков В. В.</i>	
Цифровой профиль человека – объект атаки злоумышленников	274
<i>Чапля Д. Я.</i>	
Цифровая валюта как способ преступления.....	279

Шитов П. М.

Использование открытых источников при выявлении
и пресечении мошенничества в сфере спортивных ставок.....282

Анашкин Ю. Н.

Некоторые проблемы выявления внутреннего
правонарушителя (инсайдера) 286

Чурин Р. А., Ращупкина В. А.

Некоторые проблемы исследования ленточных накопителей
информации в рамках судебной компьютерной экспертизы.....289

Филимонова Ю. В.

Использование сетевых уязвимостей для получения
оперативно-значимой информации 293

Плотников Г. Г.

О надежности систем передачи извещений.....297

Бондарь К. М.

Информационное моделирование криминогенной обстановки 300

Минаев В. А.

Выбор наилучшей модели идентификации деструктивного
контента в социальных медиа 308

Степанов Р. О., Фаддеев А. О.

Информационное обеспечение оперативных служб
при ветровом переносе опасных веществ 317

Клименко А. Б.¹,
*курсант факультета подготовки
специалистов в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Терехов М. Г.,
*преподаватель кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя*

РОБОТОТЕХНИКА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

На данный момент человечество существует в информационном мире, где всем правит техника и информация, проще говоря общество стало информационным, пройдя период информатизации. Российская Федерация так же внедряет информационные технологии во все сферы жизни человека.

Робототехника является одним из приоритетных направлений в развитии науки, технологий и техники в Российской Федерации. Данный термин был образован от слова «робот», которое впервые появилось в 1920 г. в пьесе чешского писателя Карела Чапека «Rossumovi univerzalni roboti (R.U.R.)» [1, с. 125–204]. Так как появляется все большее количество преступлений в информационной среде, органы внутренних дел должны обладать достаточной технической оснащённостью для наиболее успешного раскрытия и предотвращения противоправных деяний. Органы внутренних дел действуют в обстановки недостатка личного состава, и внедрение робототехники поможет решить эту проблему.

Первое предложение о внедрении робототехники в структуры, занимающиеся охраной правопорядка, появилось за рубежом и получило название «police robotics» [2, с. 38; 15], что переводится как «полицейская робототехника».

Вопрос о внедрении технических средств и, в частности, робототехнику можно считать актуальным, ведь с функционированием информационных технологий развивается и преступность. В настоящее время совершается более 300 тыс. преступлений в информационной среде за год, хотя еще в 2011 г. их число составляло всего лишь 11 тыс. [4], и для более высокого процента раскрытия таких преступлений и их успешного предотвращения потребуется техническая оснащённость органов внутренних дел. К такой оснащённости относится и робототехника, но в настоящее время внедрить достаточное количество роботов и поддерживать их в хорошем состоянии весьма проблематично.

¹ © Клименко А. Б., 2022.

Основной целью данной статьи является ознакомление с тем, как робототехника используется в органах внутренних дел.

Для достижения цели необходимо поставить и выполнить определенные задачи:

1. Дать определение термину «робототехника», и ознакомиться с ее основными особенностями.
2. Определить уровень применения робототехники в органах внутренних дел Российской Федерации.
3. Выделить основные проблемы в использовании роботов в системе органов внутренних дел Российской Федерации.
4. Выдвинуть предположение по развитию и применению робототехники в органах внутренних дел в будущем.

Первоначально робототехника не была предназначена для деятельности органов внутренних дел, но со временем ее начали адаптировать под выполнение задач борьбы с преступностью. Полиция использует не только технику, созданную специально для ОВД, но и адаптирует другую технику с учетом специфики задач, которые необходимо решить. Для понимания понятия «робототехника» необходимо дать ему определение. Рассматривая это понятие в общем виде, можно дать такое определение: робототехника – это наука, которая занимается созданием автоматизированных систем, которые предназначены для упрощения работы человека в различных сферах жизни. Техника, созданная таким образом способна лишь выполнять определенные команды, заложенные во время ее создания. Такую технику принято называть роботами. Особенности роботов состоят в том, что ими можно управлять на расстоянии, многие из них способны передвигаться. Контроль над ними чаще всего происходит через камеры [3].

Во всем мире решается вопрос об удачном внедрении робототехники в деятельность военных структур и в полиции. В России так же хотят решить эту проблему.

Потенциальный уровень полезности роботов в деятельности тяжело переоценить, ведь большую часть вещей, которыми занимаются сотрудники, можно передать полицейским роботам. Эта деятельность может быть как очень простой и безопасной (проверка документов), так сложной и опасной, способной нанести вред сотруднику органов внутренних дел или вовсе лишить того жизни. Именно для уменьшения риска разрабатывают роботов, способных заменить человека. В России – одной из первых в мире – в 2007 г. был создан экспериментальный образец телеуправляемого полицейского робота – патрульного «Р-БОТ№1», однако ему не нашли применение в МВД России [5 с. 214]. В 2018 г. был создан еще один робот-полицейский.

Он обладает цифровой камерой с поддержкой функции распознавания лиц, автономными видеорегистраторами с батареями на 2 недели, мониторингом аудиофона и реагированием на слова опасности. Этот робот так же считается провальным проектом, его не используют после испытаний в Казахстане [6]. В настоящее время так же стараются создать роботов полицейских, и в 2022 г. снова представили двух роботов, которые способны распознавать лица, проверять документы и отпечатки пальцев. Хотя разработчик и уверяет в исправной работе

роботов и их полезности, в это верится с трудом, ведь до этого все роботы не прижились в деятельности органов внутренних дел из-за своей бесполезности [7].

Таким образом, за все время существования робототехники роботы не прижились в ОВД. Несмотря на потенциально хорошую идею, направленную на избежание жертв и упрощение работы сотрудников органов внутренних дел, роботы не пользуются популярностью до сих пор. Хотя у использования робототехники есть плюсы, в ней так же много минусов.

Одна из главных проблем создания множества таких роботов – это цена их производства. Стоимость их создания может достигать до 100 тыс. \$, и чтобы их использовать на всей территории страны придется потратить огромную часть бюджета, что на современном этапе негативно отразится на Российской Федерации [8]. Второй немало важной проблемой является дистанционная зарядка и управление роботами.

На данный момент нет возможности эффективно использовать роботов, ибо их негде будет заряжать и нет достаточного количества сотрудников, обладающих необходимыми знаниями и умениями в использовании робототехнических устройств.

Эта проблема уже начинает решаться, ведь в образовательных организациях системы МВД России есть специальности, как раз предназначенные для обучения работы с информационными технологиями и роботами в том числе, однако при этом нет возможности в должной мере обучить сотрудников работать с робототехническими механизмами из-за отсутствия их прототипов. Так же во время создания и исследования таких дорогостоящих вещей, могут совершаться коррупционные преступления. К сожалению такие преступления часто остаются безнаказанными, и нехватка похищенных средств может быть причиной создания, непригодных для использования в деятельности органов внутренних дел, роботов.

Несмотря на все перечисленные проблемы использование роботов может упростить работу сотрудникам ОВД, если исследования в робототехнике будут продуктивными, и помогут в создании, достаточно подготовленных для работы машин. Согласно Федеральному закону от 7 февраля 2021 г. № 3 «О полиции», органы внутренних дел используют в своей деятельности последние достижения науки и техники, современную инфраструктуру [9]. Робототехника однозначно является достижением науки, ее нужно научиться использовать в деятельности органов внутренних дел. Для начала необходимо избавиться от коррупции в создании роботов-полицейских.

Этого можно достичь с помощью увеличенного контроля над исследованиями и созданием роботов. Создание физического тела робота и написание для него задач не самое простое дело и в нем должны принимать участие хорошие специалисты, решения которых должны быть учтены при рассмотрении вариантов создания роботов. Большой ценник в создании роботов получается из-за отсутствия необходимых запчастей, которые государству следует закупать за границей. На сегодняшний день в интересах МВД России применяются беспилотные летательные аппараты в антитеррористических операциях, в целях обнаружения и уничтожения инфраструктуры, передачи полученной информации и т. д. [10, с. 3]

Можно использовать похожие летательные аппараты для патрулирования улиц. Это сократит людские и материальные ресурсы по охране правопорядка на общественных территориях, позволит изменить само содержание и качество этой деятельности посредством повышения уровня профилактического воздействия на граждан, оперативного выявления правонарушений в общественных местах и их пресечение [11, с. 23]. Основным документом, который определяет развитие России в технологическом и информационном плане это «Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.», утвержденная Президентом Российской Федерации. В этом документе определены цели и задачи внутренней и внешней политики страны в сфере применения на развитие информационных и коммуникационных технологий, направленных на развития информационного общества [12].

Повышению эффективности деятельности ОВД с использованием роботов применение ПР и РК для исполнения наиболее сложных и физически выматывающих занятий сотрудников, а не замещение определенных должностей для снятия общей нагрузки и загрузить технические средства. Главное в этом решении обеспечить подразделения комплектациями для обслуживания технических средств и предотвращение их поломок и неисправностей [13, с. 215].

В настоящее время большой упор делается на информатизации общества. Технологии присутствуют во всех сферах человека и достаточно упрощают ему жизнь. ОВД так же стараются максимально быстро развиваться в сфере информации, ведь для предотвращения и раскрытия преступлений необходимо обладать большим количеством знаний и умений чем раньше.

Количество преступлений в информационной среде увеличивается, и ОВД старается поспевать за прогрессом преступного мира, используя для своей деятельности технологии.

На данный момент робототехника – не самая используемая сотрудниками ОВД часть информационного прогресса. Из-за наличия ряда проблем, сотрудники не могут использовать технологии, которые создаются с помощью робототехники, несмотря на это понемногу все к этому идет. Создаются новые роботы для замены патрулей на улицах, для проверки документов и определения личности человека в толпе с помощью баз данных и другие.

В течение какого-то промежутка времени роботы будут присутствовать в деятельности органов внутренних дел, и сотрудники не смогут представить работу без технических технологий, созданных с помощью робототехники, но для достижения этой цели необходимо приложить много усилий и вложить много средств.

Список использованных источников:

1. Чапек К. Собрание сочинений: в 7 т. М., 1976. Т. 4
2. Spilsbury L., Spilsbury R. Robotics. Cutting-Edge Technology. eBook. 2017.
3. Роботы и робототехнические устройства. Термины и определения. 2019.
4. Газета «Tadviser».
5. Число киберпреступлений в России // Сайт «Tadviser». URL: <https://www.tadviser.ru/index.php>.

6. Труды Академии управления МВД России. 2020. №3 (55).

7. Лукашов Н. В. Инновационные технологии оперативного управления в органах внутренних дел России // Труды Академии управления МВД России. 2015. № 3 (35).

8. В МВД показали двух роботов-полицейских // Сайт «Тасс». URL: https://tass.ru/obschestvo/7843191/amp?utm_source=google.ru&utm_medium=organic&utm_campaign=google.ru&utm_referrer=google.ru.

9. Стоимость создания роботов предназначенных для обезвреживания взрывчатых устройств // Сайт «Медуза». URL: <https://meduza.io/amp/feature/2016/07/14/robokopy-uzhe-zdes>.

10. Грибанов Е. В. Перспективные направления развития кибертехнологий предупреждения преступлений // Общество и право. 2021. № 4 (78). С. 21–27.

11. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_216363/.

12. Лукашов Н. В. Организационные и правовые основы применения полицейских робототехнических комплексов в органах внутренних дел Российской Федерации // Труды Академии управления МВД России. 2020. № 3 (55). С. 210–221.

13. Терехов М. Г. Цифровое право // Экономика. Право. Общество. 2021. № 3 (27). С. 68–70.

14. Терехов М. Г. Роль гражданско-правового режима цифровых активов в обеспечении национальной безопасности государств – членов ОДКБ // Защитник закона. 2022. № 13. С. 139–150.

15. Мурадян С. В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право. 2022. № 5. С. 196–201.

16. Михайленко Н. В., Мурадян С. В., Вихляев А. А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях // Аудиторские ведомости. 2022. № 1. С. 140–145.

17. Пушкарев В. В. Феномен уголовного преследования в досудебном производстве: проблемы интерпретации статистических показателей // Органы следствия Министерства внутренних дел Российской Федерации на страже правопорядка (к 56-й годовщине образования следствия в органах внутренних дел) : сборник тезисов и статей Международной научно-практической конференции, Москва, 6 апреля 2019 г. М. : Сирис, 2019. С. 47–50.

18. Вихляев А. А. К вопросу об использовании сотрудниками полиции личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и о допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 г. М. : Университет прокуратуры Российской Федерации, 2021. С. 411–415.

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

Научный руководитель:
Терехов М. Г.,
*преподаватель кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных
технологий Московского университета
МВД России имени В. Я. Кикотя*

ИСПОЛЬЗОВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА «БЕЗОПАСНЫЙ ГОРОД» В ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

На данный момент в мире продолжается четвертая промышленная революция, парадигмой которой является «цифровизация всех сфер человеческой жизнедеятельности». Несмотря на все большее развитие цифровых технологий, уровень преступности в России и мире не уменьшается, а только увеличивается ввиду появления новых категорий преступлений – преступления в сфере компьютерной информации. В данной статье исследуются проблемные аспекты пресечения и предупреждения преступности в городах и сельской местности с использованием аппаратно-программного комплекса «Безопасный город».

Создание и развитие данного комплекса оказало положительное влияние на общее состояние преступности в Российской Федерации – благодаря цифровым технологиям, внедренным для упрощения работы сотрудников органов внутренних дел, преступления стали раскрываться быстрее и эффективнее. Однако работа данного комплекса направлена не только на раскрытие уже совершенных преступлений, но и на пресечение еще не совершенных. Для того чтобы больше углубиться в данную тему мы рассмотрим цели создания данного комплекса, его задачи, а также структуру построения.

В условиях высокого уровня природной, техногенной и других видов опасностей, возросшие требования к системам безопасности, а также тенденции к урбанизации разработка единого многоуровневого комплекса, который посредством использования цифровых технологий, упростит работу органов внутренних дел по обеспечению правопорядка и общественной безопасности, стало важнейшей задачей для властей Российской Федерации.

Автор настоящей статьи отмечает особую актуальность складывающейся проблематики в современном мире по вопросам обеспечения общественной без-

¹ © Львова А. А., 2022.

опасности. Согласно статистике, количество преступлений в Москве увеличивается с каждым месяцем на несколько тысяч, а иногда данный показатель превышает и десятки тысяч преступлений за месяц. Проектирование, а затем и развитие аппаратно-программного комплекса «Безопасный город» существенно упрощает работу сотрудников правоохранительных органов, согласно статистике, свыше 5 тыс. преступлений удалось раскрыть с помощью системы «Безопасный город» в 2020 г., а также свыше 6,8 тыс. преступлений в 2021 г.

Исходя из представленных данных, мы можем сделать вывод, что внедрение «Безопасного города» в работу органов внутренних дел положительно влияет на динамику раскрытия преступлений. В статье автор ставит перед собой цель охарактеризовать причины и условия, складывающейся проблематики по отдельным противоправным деяниям, а также раскрытие и предупреждение преступлений с использованием цифровых технологий аппаратно-программного комплекса «Безопасный город» и научные подходы к разрешению складывающейся проблематики.

Достижение поставленной цели представляется возможным посредством решения совокупности задач:

1. Определить действующие нормативно-правовые акты в исследуемой тематике.
2. Определить основные методы и средства, спроектированные и распространенные для повышения безопасности городов Российской Федерации.
3. Определить практический аспект применения цифровых технологий в деятельности сотрудников полиции.
4. Дать предложения к разрешению складывающейся проблематики.

Методами исследования является анализ и синтез, исходя из полученной в ходе исследования информации и последующего анализа, автор предложит способ разрешения складывающейся проблематики.

Аппаратно-программный комплекс «Безопасный город» – это система правовых, технических, экономических и организационных мер для совершенствования процессов поддержки принятия решений в области обеспечения безопасности среды жизнедеятельности и общественного порядка на территории России.

Единый комплекс обеспечивает обмен информацией между службами и ведомствами при пресечении и ликвидации природных, техногенных и биолого-социальных угроз, угроз общественному порядку и безопасности среды жизнедеятельности.

Данный комплекс утвержден распоряжением Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р.

Специальными целями внедрения комплекса являются:

- повышение уровня управления нарядами органа внутренних дел;
- осуществление взаимодействия различных оперативных служб в охране общественного порядка и борьбе с преступностью;
- получение объективной информации о состоянии правопорядка в целом;
- незамедлительное реагирование правоохранительных органов, УФСБ, МЧС и оперативных служб города (района) при возникновении чрезвычайной ситуации.

Задачами комплекса являются:

- 1) постоянный сбор, анализ, обобщение информации, поступившей посредством цифровых технологий;
- 2) передача актуальной информации, записанной видеокамерами, в различные пункты «Безопасного города» (центр управления, дежурные части органов внутренних дел и др.);
- 3) своевременное выявление нарушений общественного порядка, а также подозрительных предметов, оставленных без присмотра, в перспективе являющиеся опасными для жизни и здоровья людей;
- 4) немедленное реагирование на изменение оперативной обстановки в городе (районе);
- 5) управление сотрудниками органов внутренних дел, осуществляющими контроль за общественным порядком на улицах города(района);
- 6) обработка и анализ поступающей информации, готовность доложить данные об оперативной обстановке руководству УВД, оперативному штабу и пр.;
- 7) обеспечение взаимодействия между администрациями города (района), территориальными подразделениями УВД, УФСБ, УГОЧС, воинскими частями внутренних войск;
- 8) обеспечение хранения видеоданных, а также предоставление доступа к удаленной информации;
- 9) использование и развитие цифровых технологий органов внутренних дел, их объединение в единое информационное пространство, обеспечение информационной безопасности.

Функционирование комплекса осуществляется как в обычном режиме, так и в особых условиях (во время проведения массовых мероприятий, при проведении антитеррористических и профилактических мероприятий, при чрезвычайных ситуациях). Переход работы комплекса из штатного режима в режимы повышенной готовности реализуется действиями дежурных частей органов внутренних дел (сфера оперативного информирования) по специальным оперативным планам.

Работа комплекса строится на некоторых системах, формирующих его особую структуру:

- система видеомониторинга, состоящая из сети видеокамер, а также единого штаба, занимающегося обработкой и анализом поступившей видеoinформации, является основным средством обеспечения и поддержания общественного порядка;
- система архивации информации, обеспечивающая хранение информации в специальных базах данных, которая в дальнейшем может сыграть большую роль в раскрытии преступлений;
- система, отвечающая за сбор, обработку и регистрацию информации, принятой по специализированной связи «гражданин-полиция», а также с помощью оператора «02», обеспечивающая оперативное реагирование на сообщение о преступлении или правонарушении;
- система, взаимодействия между внутренними силами нарядов органов внутренних дел, а также контроль за исполнением ими должностных полномочий, реализация которой происходит посредством их отслеживания;

– система организации слаженной работы оперативных служб в режиме ЧС, представляющая собой объединение сил оперативных служб для скорейшего разрешения сложившейся ситуации.

Слаженная работа всех систем в совокупности составляет основу самого комплекса по ключевым направлениям деятельности органов внутренних дел по поддержанию общественного порядка и борьбе с преступностью, созданию единого информационного пространства для решения этих целей:

1. Обеспечение правопорядка на улицах и в других общественных местах (контроль за обстановкой в общественных местах, своевременное реагирование на выявленные нарушения, оповещение экстренных служб города о сложившейся ситуации). Осуществляется посредством установки видеокамер, отслеживания видеоархивов и передач информации оперативным службам.

2. Обеспечение общественного порядка в местах массового скопления людей с использованием экстренной связи «гражданин – полиция». Осуществляется с помощью установки устройств экстренной связи, также включающей в себя системы видеомониторинга.

3. Регулирование правопорядка в районе объектов особой важности, а также на относящихся к ним территориях (административные здания, объекты жизнеобеспечения, теле- и радиовещательные компании, телеграфы, учреждения Центрального банка Российской Федерации).

4. Обеспечение безопасности дорожного движения (контроль за дорожной обстановкой, своевременное выявление чрезвычайных ситуаций, происшествий, а также реагирование на них, нарушением установленных законодательством правил, розыск автотранспорта, участвующего в совершении происшествия, а также угнанных, похищенных автомобилей).

Осуществляется посредством установки видеокамер разного профиля (для считывания государственного номера, для определения нарушения скоростного режима, для выявления нарушений правил дорожного движения), а также передач информации на сервер «Поток» и ее дальнейшего хранения в транспортных базах данных.

5. Обеспечение личной и имущественной безопасности граждан, различных форм собственности в жилом секторе (беспрерывный контроль за обстановкой, осуществление связи с различными диспетчерами, охрана объектов жилого сектора (лифты, подъезды, подвалы, чердаки и др.), незамедлительное оповещение и реагирование оперативных служб).

Также к работе в этом направлении принято добавлять решение задач коммунальных служб города (контроль освещенности в жилых домах и прилегающей территории, противопожарная безопасность, благоустройство территории и ее своевременная уборка). Осуществляется посредством установки видеокамер на подъездах жилых домов, а также в служебных помещениях.

6. Обеспечение безопасности объектов транспорта и транспортной инфраструктуры (контроль за безопасностью различного вида транспорта (железнодорожный, речной, авиатранспорт), распознавание биометрических данных лица, для последующего розыска, определение оставленных без присмотра вещей и возможность контроля антитеррористической обстановки в транспорте).

7. Создание единой информационной системы органов внутренних дел и поддержание информационной безопасности (объединение различных цифровых технологий для слаженного взаимодействия и контроля обеспечения правопорядка, защита информации от неправомерного доступа, организация хранения информации в базах данных для последующего доступа к ней).

Согласно статистике, предоставленной ГУОООП МВД России в субъектах Российской Федерации функционируют более 200 АПК «Безопасный город» в более чем 750 населенных пунктах установлено 177 тыс. камер видеонаблюдения большинство из них предоставляет информацию в территориальные органы МВД России (рис. 1). Но несмотря на это количество камер, определяющих биометрические параметры лица, а также события и предметы составляют менее 0,1 % от общего количества систем видеонаблюдения.



Рис. 1. Диаграмма данных по выборке регионов

Если рассматривать функционирование АПК «Безопасный город» в г. Москве, то согласно статистике, на 2022 г. установлено более 228 тыс. камер видеонаблюдения. благодаря этому правоохранительные органы успешно раскрыли 22 убийства, 102 случая умышленного причинения тяжкого вреда здоровью, 131 разбойное нападение, а также 335 грабежей. Суммарное количество раскрытых преступлений составило 4,4 тыс.

Благодаря внедрению и совершенствованию АПК «Безопасный город», за первое полугодие в столице сократилось число тяжких и особо тяжких преступлений на 17,1 %, почти на 25 % уменьшилось количество квартирных краж, на 15,3 % – угонов транспортных средств и на 7,1 % – случаев мошенничества.

Предпринятые шаги, которые уже сделаны для комфортного и безопасного проживания людей в городах и поселениях сельской местности, благоприятно сказываются на общем состоянии преступности в городах Российской Федерации. Благодаря цифровым технологиям, внедренным с помощью аппаратно-программ-

ного комплекса «Безопасный город», раскрыть преступления или правонарушения стало гораздо быстрее, проще и доступнее. Также данный комплекс предназначен для пресечения еще не совершенных преступлений. Органам внутренних дел стало легче отслеживать и анализировать обстановку в городах, тем самым их работа каждым месяцем становится еще продуктивнее, чем была до этого.

Однако для еще большего прогресса необходимо решить несколько видов проблем – это организационные и технические проблемы. К первым относятся различные финансовые проблемы. Для построения огромного комплекса нужны немалые затраты, которые к сожалению, сопровождаются коррупционной деятельностью некоторых исполнительных лиц. Также к данному виду проблем относят и нехватку кадрового потенциала. Для успешного дальнейшего развития комплекса необходимы квалифицированные молодые специалисты, готовые разрабатывать цифровые технологии и заниматься их внедрением в комплекс. Еще одной проблемой является устранение межведомственных барьеров.

До создания комплекса каждая спецслужба занималась решением проблем только собственного профиля, но после проектирования «Безопасного города», разграничение проблем невозможно и для обеспечения эффективной деятельности необходимо объединение структур разного профиля. Если говорить о технических проблемах, то они являются следствием организационных проблем, таким образом, автор подчеркивает необходимость решения организационных неурядиц для дальнейшего развития комплекса.

Список использованных источников:

1. Распоряжение Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р (ред. от 05.04.2019) «Об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город"» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_172077/-4ffea2b90b5bab278aea41a0808edb7fb67f43c9/.
2. Ардавов М. М. Эффективность административно-правовых средств принуждения, применяемых милицией : автореф. дис. ... канд. юрид. наук. Ростов-нД., 1998.
3. Указ Президента Российской Федерации от 31 декабря 2015 года № 683 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_38927/.
4. Топольский Н. Г., Качанов С. А., Рыженко А. А. Анализ этапов развития концепции «Безопасный город» // Технологии техносферной безопасности. 2016. № 1. С. 178–186.
5. Методические рекомендации АПК «Безопасный город» построение (развитие), внедрение и эксплуатация. Утверждены МЧС России 22.02.2015 № 2-4-87-12-14. М. : МЧС России, 2015. 72 с.
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (последняя редакция) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61-798/.

7. Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 (ред. от 19.03.2014) «О единой системе межведомственного электронного взаимодействия» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_104665/59a1ee33e6096f0bf3fd23d27eeb41a502ed129e/.

8. Постановление Правительства Российской Федерации от 24 марта 1997 г. № 334 «О порядке сбора и обмена в Российской Федерации в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_13806/9bddbca026155a98a616cc3d4798f706947ccf0c/.

9. Терехов М. Г. Цифровое право // Экономика. Право. Общество. 2021. № 3 (27). С. 68–70.

10. Терехов М. Г. Роль гражданско-правового режима цифровых активов в обеспечении национальной безопасности государств – членов ОДКБ // Защитник закона. 2022. № 13. С. 139–150.

11. Мурадян С. В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право. 2022. № 5. С. 196–201.

12. Михайленко Н. В., Мурадян С. В., Вихляев А. А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях // Аудиторские ведомости. 2022. № 1. С. 140–145.

13. Пушкарев В. В. Феномен уголовного преследования в досудебном производстве: проблемы интерпретации статистических показателей // Органы следствия Министерства внутренних дел Российской Федерации на страже правопорядка (к 56-й годовщине образования следствия в органах внутренних дел) : сборник тезисов и статей Международной научно-практической конференции, Москва, 6 апреля 2019 г. М. : Сириус, 2019. С. 47–50.

14. Вихляев А. А. К вопросу об использовании сотрудниками полиции личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и о допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 г. М. : Университет прокуратуры Российской Федерации, 2021. С. 411–415.

Панфилова А. Д.¹,
 курсант факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Терехов М. Г.,
 преподаватель кафедры противодействия
 преступлениям в сфере
 информационно-телекоммуникационных
 технологий Московского университета
 МВД России имени В. Я. Кикотя

ТЕХНОЛОГИЯ БЛОКЧЕЙН В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Практика показывает, что развитие современных информационных технологий играет очень важную роль для всех сфер жизнедеятельности нашего общества, как положительную, так и отрицательную. Современный мир меняется, развивается наука, появляются новые возможности применения технологий. Положительные тенденции развития информационных и компьютерных технологий, как оказалось, вызывают огромный интерес у преступного общества. В связи с этим появляется проблема совершенствования и укрепления уголовно-правовой защиты, в основном, в экономической и финансовой сферах. Чем быстрее развивается цифровая экономика, тем быстрее возрастает данная проблема.

Так, совсем недавно представителями криминального мира освоились электронные деньги (например, всем известный QIWI-кошелек) и стали основным предметом посягательства правонарушителей. Появление криптовалют (Bitcoin) спровоцировало в настоящее время столкновение мирового сообщества с новейшей технологией реестра блоков транзакций – blockchain («блокчейн»). Возможно ли использование данной технологии не только лицам, находящимся в мире преступности, творящим беззаконие, но и противоположной стороной – органами внутренних дел?

В настоящее время информационные технологии достаточно интенсивно внедряются и играют важную роль в системе государственного управления. Развитие информационных технологий является предпосылкой повышения уровня обеспечения национальной безопасности, суверенитета государства, информационных ресурсов от внешних посягательств.

Современные технологии являются одним из составляющих системы управления во многих сферах: сфера государственного управления, экономика, обороноспособность страны, безопасность государства и обеспечение правопорядка.

¹ © Панфилова А. Д., 2022.

Президент Российской Федерации В. В. Путин в Послании Федеральному Собранию Российской Федерации отметил: «Россия должна стать не только ключевым логистическим, транспортным узлом планеты, но и одним из мировых центров хранения, обработки, передачи и надежной защиты информационных ресурсов». Для этого необходимо создание и оптимизация новых информационных технологий для решения необходимых задач по совершенствованию системы сбора, хранения, передачи и использования информации.

Одной из таких технологий является технология блокчейн.

В статье автор нацелен охарактеризовать причины и условия, складывающейся проблематики по отдельным существующим противоправным процессам с использованием технологии блокчейн.

Достижение поставленной цели представляется возможным посредством решения следующих задач:

- 1) выявить действующие нормативно-правовые акты в сфере использования технологии блокчейна органами внутренних дел;
- 2) рассмотреть мировые практики использования технологии блокчейн;
- 3) определить причины и условия совершения противоправных деяний с применением технологии блокчейн;
- 4) предоставить возможные варианты разрешения складывающейся проблематики.

Автор предложит возможные подходы разрешения сложившейся проблематики, исходя из информации, полученной в процессе исследования, посредством анализа и синтеза. В настоящее время, несмотря на новизну технологии блокчейн, она достаточно хорошо и подробно изучена научными исследователями. Данная технология довольно перспективная в использовании в различных сферах жизнедеятельности человека: торговля, авторские права, реализация избирательного права, банковское дело, бухгалтерский учет и другие.

В первую очередь, по мнению автора, внимание стоит уделить защите информационных ресурсов, обеспечение национальной безопасности от всестороннего вмешательства, включая использование блокчейна в целях совершения противоправных деяний. Такое мнение сформировалось у автора благодаря исследованиям Chainalysis. Согласно этим исследованиям в 2022 г. криптоадреса, относящиеся к преступной деятельности, отправили около 10 % своих средств в криптомикшеры. Автор делает вывод, что количество незаконных переводов с применением технологии блокчейн возросло, так как в 2021 г. адреса отправляли не более 0,3 %.

Таким образом, как можно заметить, процентная доля незаконных переводов действительно выросла. Основываясь также на исследовании Chainalysis, автор подчеркивает, что такие преступные деяния как кража и отмывание денег приобретают тенденцию роста за последние два года. Например, преступления, совершенные с помощью DeFi. Соответственно автор фактически подтверждает свое мнение в пользу защиты информационных ресурсов, обеспечения безопасности государства в первую очередь.

Касаясь использования технологии блокчейн непосредственно органами внутренних дел для борьбы с киберпреступностью или преступностью, связанной с технологией блокчейн. Возможно провести такую параллель – чем более развиваются информационные технологии (в данном случае блокчейн), тем более развивается преступность в изучаемой сфере (как это было представлено автором выше), соответственно, требуется повышать, уровень конкурентоспособности деятельности правоохранительных органов с использованием технологии блокчейн.

Следует заметить, что использование всех преимуществ новых информационных технологий органами внутренних дел способствует не только упрощению своей деятельности, но и повышению уровня эффективности выполнения поставленных перед ними задач.

По мнению автора, все-таки существует несколько методов использования технологии блокчейн органами внутренних дел для борьбы с преступностью в области информационных технологий, такие как:

1. Решение проблемы согласованности и прослеживаемости всей информации о работе органов внутренних дел. Технология блокчейн позволяет создавать устойчивые системы хранения и идентификации данных, непосредственно имеющих отношение к расследованию преступления. Это могут быть цифровые данные, оцифрованные данные материальных предметов (в частности, улики, вещественные доказательства).

2. Поиск лиц, совершивших преступление или как-то связанных с ним, а также транспортных средств, имеющих отношение к преступлению, а также их идентификация на международном уровне.

3. Проверка подлинности доказательства, а также отслеживание действий с ним пользователя. После внесения доказательств в виде цифрового объекта в сеть возможно будет проконтролировать цепочки поставок товаров, а также предостеречь их от подделок.

В некоторых развитых странах достаточно активно внедряется технология блокчейн. Автор рассматривает следующие:

1. США. Предлагается правоохранительным органам использовать «EMS».

2. Индия. Запуск основанного на технологии блокчейн решения для более эффективного управления данными «Police2020».

Технология блокчейн имеет ряд преимуществ и несомненно способна содействовать сотрудникам органов внутренних дел в борьбе с преступностью, основанной на современных, развитых технологиях. В настоящее время блокчейн активно внедряется не только в деятельность правоохранительных органов, но и в другие сферы, обеспечивающие должное функционирование государства. Основываясь на опыте других стран, автор выделяет развитие дальнейшей перспективы блокчейна. Конечно, для полноценного развития этой технологии требуется развивать информационные технологии до более высокого уровня. Но одним из основных преимуществ блокчейна является невозможность изменения данных после их внесения в базу данных, что очень важно для деятельности органов внутренних дел (может способствовать в качестве противодействия коррупции

или же защита от разных видов подделок или исправлений доказательств, имеющих значение в ходе расследования преступления).

Исходя из всего выше сказанного, как отмечает автор, решение поставленных проблем может быть успешно найдено путем дальнейшего развития информационных технологий, в частности, технологии реестра блоков транзакций – технологии блокчейн в деятельности органов внутренних дел, а также не менее успешное внедрение их в процесс осуществления борьбы с преступностью, все более и более развивающейся в XXI в. – веке технологий.

Список использованных источников:

1. Генкин А. С. Криптотехнологии и криминальные риски: есть ли повод для тревоги? // Страховое дело. 2017. № 5.
2. Карцхия А. Оцифрованное право: виртуальность в законе // Интеллектуальная собственность. Авторское право и смежные права. 2018.
3. Кузнецов В. А. О возможных сценариях законодательного регулирования цифровых валют в России / В. А. Кузнецов, Р. А. Прохоров, А. В. Пухов // Деньги и кредит. 2017.
4. Попов Е. В. Оценка готовности отраслей РФ к формированию цифровой экономики // Инновации. 2017.
5. Шпак В. От цифровой экономики к цифровому государству // Электроника: наука, технология, бизнес. 2017.
6. Терехов М. Г. Цифровое право // Экономика. Право. Общество. 2021. № 3 (27). С. 68–70.
7. Терехов М. Г. Роль гражданско-правового режима цифровых активов в обеспечении национальной безопасности государств – членов ОДКБ // Защитник закона. 2022. № 13. С. 139–150.
8. Мурадян С. В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право. 2022. № 5. С. 196–201.
9. Михайленко Н. В., Мурадян С. В., Вихляев А. А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях // Аудиторские ведомости. 2022. № 1. С. 140–145.
10. Пушкарёв В. В. Феномен уголовного преследования в досудебном производстве: проблемы интерпретации статистических показателей // Органы следствия Министерства внутренних дел Российской Федерации на страже правопорядка (к 56-й годовщине образования следствия в органах внутренних дел) : сборник тезисов и статей Международной научно-практической конференции, Москва, 6 апреля 2019 г. М. : Сириус, 2019. С. 47–50.
11. Вихляев А. А. К вопросу об использовании сотрудниками полиции личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и о допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сборник материалов I Всероссийской

научно-практической конференции, Москва, 27 января 2021 г. М. : Университет прокуратуры Российской Федерации, 2021. С. 411–415.

Шишкин И. С.¹,
 курсант факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Терехов М. Г.,
 преподаватель кафедры противодействия
 преступлениям в сфере
 информационно-телекоммуникационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ ДЛЯ ВЫЯВЛЕНИЯ РАЗЫСКИВАЕМЫХ ЛИЦ В МЕСТАХ МАССОВОГО СКОПЛЕНИЯ ЛЮДЕЙ

Каждый день в нашей стране совершаются преступления, наивысшая концентрация которых достигает в городах-миллионниках. Не все из них удастся предупредить или пресечь на месте, что ставит вопрос о возможных путях поиска лиц, совершивших преступления.

Поскольку почти каждый человек в городе должен ежедневно преодолевать различные расстояния для того, чтобы добраться до необходимого ему места, это обуславливает образование массовых скоплений людей, где наравне с законопослушными гражданами может находиться преступник. Данные обстоятельства формируют непосильную задачу для правоохранительных органов, которые не обладают специальными техническими средствами, по выявлению разыскиваемых лиц. Для наиболее своевременного и точного выполнения указанных выше функций в правоохранительные органы активно внедряется искусственный интеллект (далее – ИИ). В данной статье будут рассмотрены основные принципы работы модели, ее сильные и слабые стороны, применяемые технологии и возможный прогресс в будущем.

В данной статье отмечается особая актуальность рассматриваемой темы, поскольку понятие ИИ зародилось не так давно, а если говорить точнее, то в первый раз данный термин был употреблен ученым Джоном Маккарти, который в 1956 г. проводил конференцию в Дартмутском колледже. Там был приведен следующий тезис о том, что «любой аспект человеческой разумной деятельности может быть точно описан таким образом, что машина может его симитировать». И хоть данное высказывание еще далеко от наиболее «правильного» понятия ИИ, но оно послужило основой для всех последующих изобретений.

¹ © Шишкин И. С., 2022.

В наше время ИИ набирает обороты с каждым годом и пока не собирается останавливаться. Его наличие и развитие обуславливает этап информатизации общества, т. е. переход общества на новую ступень, где движимой силой станет информация. Поэтому для наиболее скорого завершения этого процесса необходимо, чтобы не только ученые занимались развитием данной отрасли, но и каждый гражданин принимал активное участие если и не прямо, то хотя бы косвенно. В связи с этим написание статей на тематики информационных технологий помогает поднимать общий уровень образованности населения и увеличивать уже упомянутые темпы развития.

Основной целью данной статьи является: ознакомление с технологиями, позволяющими идентифицировать личность из масс.

Для достижения данной цели необходимо выполнить определенные задачи:

1. Внести определение в понятие ИИ, ознакомится с его основными принципами работы.
2. Определить уровень использования ИИ правоохранительными органами в настоящий момент.
3. Проанализировать систему использования ИИ для этих целей.
4. Выдвинуть предположения по возможному развитию и пути разрешения возникших проблем.

В первую очередь рассмотрим понятие ИИ. Проанализировав огромное количество определений, можно прийти к выводу, что все они подразделяются на два больших направления – с технической точки зрения и с точки зрения научной дисциплины.

Также представляется возможным отметить, что в корне неверно определять понятие ИИ через сравнение его с человеком и человеческим интеллектом. Поскольку в технических определениях нигде не дается понятие интеллекту человека, что очень усложняет проведение аналогий данных категорий. Хотя и по сей день ведется немало споров о возможности реализации человеческого интеллекта в машинном коде. В наше время еще нет таких технологий, которые бы позволили это реализовать, но прогресс не стоит на месте и возможно, что когда-нибудь мы сможем сами прикоснуться к чуду технологического прорыва.

Важную роль в процессе отделения человеческого и технического сыграло введение понятия «агент». Агент – это объект, отличительной чертой которого является автоматизированность и который способен получать информацию из вне, проводить ее анализ и принимать определенные действия, необходимые для решения поставленных задач. ИИ отличается от обычных программ одной очень интересной особенностью – он может обучаться самостоятельно. Отсюда возникает новое понятие – искусственная нейронная сеть (далее – ИНС). ИНС – это математические модели, которые созданы по аналогии с биологическими. Их целью является получение данных, их обработка и принятие решений, получение результата и выборка наиболее благоприятных концепций.

С учетом всех требований дадим определение ИИ – это сложные технологии, основанные на понятии нейронных сетей (машинного обучения), и предназначенные для решения сложных задач, имеющих большое количество переменных факторов.

Принципом работы ИИ является наличие доступа к большому количеству данных, которое возможно быстро обработать при помощи интеллектуальных алгоритмов, что дает программе быстро обучаться, выявляя признаки и закономерности.

Как же все-таки работает система распознавания? Если распознать необходимо лицо, то в первую очередь ИИ нужно найти лицо. Здесь используется метод Виолы – Джонса, созданный в 2001 г. Существуют различные прямоугольники (примитивы Хаара), по которым алгоритм сканирует изображение трижды, чтобы исключить иные объекты. Задача – найти более светлые или темные участки и понять, что это лицо. Если все три раза имелся положительный исход, то программа продолжает действовать. Далее работает биометрический алгоритм, по которому на лице устанавливаются антропометрические точки. Их количество может достигать от 68 до пары тысяч. Затем система «подгоняет» изображение под себя: устраняет наклон и поворот головы, проводит 3D и 2D реконструкцию. Следом нейросеть выстраивает вектор лица, значения которого зависят от личных особенностей, но без учета посторонних факторов: возраст, прическа, макияж. Заключительный этап – сравнение вектора с имеющимися в базе данных. И готово: личность установлена.

Что же касается деятельности правоохранительных органов, хотелось бы отметить, что хоть и процесс информатизации затрагивает их, но в полной мере это пока что не удалось реализовать. Многие данные хранятся на бумажных носителях или в журналах, фотографии преступников также имеются в распечатанном виде. Все это ограничивает скорость и результативность работы.

В настоящее время в процессе идентификации личности участвует не только распознавание лица, но и походка, рост, очки, шляпы и бороды. Об это заявляет гендиректор компании-разработчика Ntechlab Андрей Теленков, с которым тесно сотрудничает Министерство внутренних дел. Известно, что во многих крупных городах России используются камеры с распознаванием лиц. Так в Нижнем Новгороде установлено более 3 тыс. камер, подключенных к одной системе. В Москве же подключено около 140 тыс. камер, данные с которых стекаются в Единый центр хранения данных (далее – ЕЦХД), где и обрабатываются, а далее уже поступают в пользование правоохранительных органов.

В доступе сотрудников Министерства внутренних дел находится подсистема автоматической регистрации сценариев индексирования видеоинформации, которое как раз согласовано с ЕЦХД. Она позволяет подключаться к городской системе распознавания лиц для поиска преступников. Данная нейросеть отслеживает не только передвижения правонарушителя, но и фиксирует его возможных сообщников, если данные лица часто находились рядом с ним. Также появится возможность отследить людей, которые возвращаются на те места преступлений, «где личности преступников не установлены».

На нужды развития данного направления выделяются сотни миллионов рублей и это действительно оправдано, поскольку оказывает невероятную помощь в противодействии преступности. Хотя здесь же и наблюдается проблематика. Если в крупных городах имеется огромное финансирование, то выделение средств на эти нужды является вполне возможным. В то время как в регионах

имеются и более серьезные проблемы требующие внимания, что хоть и не исключает полностью, но значительно уменьшает степень ИИ в повседневную деятельность правоохранительных органов.

Как пример, можно привести приказ от 25 сентября 2008 г. № 610 «Об использовании автоматизированной информационно-поисковой системы идентификации личности по изображению лица (АИПС "СОВА")». Система Оперативного Визуального Анализа, предназначенная для установления личности по признакам внешности в ходе проведения оперативно-разыскных мероприятий.

Далее рассмотрим положительные и отрицательные стороны применения ИИ для выявления разыскиваемых лиц.

Выделим положительные стороны:

1. Скорость. Данная система позволяет быстро собирать и обрабатывать информацию по конкретному лицу, чем значительно опережает человека.
2. Точность. Современные методы почти полностью исключают наличие ошибок, человеческий фактор отсутствует.
3. Круглосуточная доступность. Программа не нуждается в отдыхе, доступ к ней можно получить в любое время.
4. Упрощение поиска. Не нужно будет вручную просматривать камеры и искать преступника, все самостоятельно сделает ИИ.

Серьезными минусами данной системы являются:

1. Высокая стоимость. Довольно закономерный минус, поскольку технология является очень сложной и трудозатратной. Решение: использование отечественной продукции, а также дача образования в сфере информационных технологий.
2. Повышение вероятности атак на серверы хранения данных. Огромное количество персональных данных, которые можно использовать для преступной деятельности – серьезная мотивация для взлома данной системы. Решение: разработка новых средств и методов защиты информации.
3. Рост коррупции. Тот, кто обладает или имеет доступ к таким данным может быть замешан в коррупционной деятельности в силу наличия ценной информации. Решение: Повышение заработных плат лицам, имеющим доступ к соответствующим сведениям, назначение на должности, связанные с данной информацией ограниченного доступа только ответственных и квалифицированных лиц.

Можно заметить, что хоть и у данного способа имеются недостатки, но его плюсы перевешивают. Самое главное в раскрытии преступлений – это оперативность. Если хоть немного промедлить, то можно упустить шанс и уже больше никогда его не получить. ИИ же позволяет решать задачи не только быстро, но и точно, что также особо важно для данного вида деятельности.

Наиболее продуктивный путь по развитию ИИ в целях выявления разыскиваемых лиц в местах массового скопления людей – это привлечение в эту отрасль уже готовых специалистов или подготовка в высших учебных заведениях. Также необходимо своевременно решать вопросы финансирования, чтобы работа не стояла на месте. Еще одним особенно важным аспектом является принятие соответствующих законов по защите прав и свобод, а также приказов для реализации планов в этой сфере. Законодательная база хромает, но это и не удивительно, поскольку мы только погружаемся в сложную сферу ИИ.

Представляется, что ИИ продолжит развиваться, а его значимость в нашей повседневной жизни увеличиваться. Хотя не стоит и забывать про то, что многие будут против глобального внедрения. Для преодоления этого необходимо время и программы по предоставлению населению информации об ИИ.

Сотрудники ОВД и иные государственные служащие должны стать теми, кто активно начнет использовать технологии ИИ, поскольку это позволит им как выполнять свои функции еще лучше, так и показать населению безопасность данных средств.

Список использованных источников:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/.
2. Приказ МВД по Удмуртской Республике от 25 сентября 2008 года № 610 «Об использовании автоматизированной информационно-поисковой системы идентификации личности по изображению лица (АИПС "СОВА")» // АО «Кодекс». URL: <https://docs.cntd.ru/document/428629567>.
3. Брилюк Д. В., Старовойтов В. В. Распознавание человека по изображению лица нейросетевыми методами : препринт. Минск : Институт технической кибернетики НАН Беларуси, 2002. 54 с.
4. Опознать по бороде: МВД взяло на вооружение новую систему слежки // Сайт «Газета.ru». URL: <https://www.gazeta.ru/auto/2021/06/24>.
5. Мэрия Москвы доработает систему распознавания лиц специально для МВД // Сайт «Forbes». URL: <https://www.forbes.ru/tekhnologii/438825-moskovskaa-meria-dorabotaet-sistemu-raspoznavania-lic-special-no-dla-mvd>.
6. Как работает распознавание лиц? // Сайт «Хабр». URL: <https://habr.com/ru/company/droider/blog/568764/>.
7. Умная камера с искусственным интеллектом повышает безопасность, улучшает парковку и дорожный поток // Сайт «Intelvision». URL: <https://www.intelvision.ru/blog/smart-camera>.
8. «Принципы работы искусственного интеллекта и перспектива его использования» // Сайт «Aiconference». URL: <https://aiconference.com.ua/ru/news-printsipi-raboti-iskusstvennogo-intellekta-i-perspektiva-ego-ispolzovaniya-92238>.
9. Терехов М. Г. Цифровое право // Экономика. Право. Общество. 2021. № 3 (27). С. 68–70.
10. Терехов М. Г. Роль гражданско-правового режима цифровых активов в обеспечении национальной безопасности государств – членов ОДКБ // Защитник закона. 2022. № 13. С. 139–150.
11. Мурадян С. В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право. 2022. № 5. С. 196–201.
12. Михайленко Н. В., Мурадян С. В., Вихляев А. А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях // Аудиторские ведомости. 2022. № 1. С. 140–145.

13. Пушкарев В. В. Феномен уголовного преследования в досудебном производстве: проблемы интерпретации статистических показателей // Органы следствия Министерства внутренних дел Российской Федерации на страже правопорядка (к 56-й годовщине образования следствия в органах внутренних дел) : сборник тезисов и статей Международной научно-практической конференции, Москва, 6 апреля 2019 г. М. : Сириус, 2019. С. 47–50.

14. Вихляев А. А. К вопросу об использовании сотрудниками полиции личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и о допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 г. М. : Университет прокуратуры Российской Федерации, 2021. С. 411–415.

Рыбак М. М.¹,
*курсант факультета подготовки
сотрудников для подразделений экономической
безопасности и противодействия коррупции
Московского университета
МВД России имени В.Я. Кикотя*

БЕСКОНТАКТНЫЙ СБЫТ ФАЛЬШИВЫХ ДЕНЕЖНЫХ СРЕДСТВ

На современном этапе стремительно развивается такое направление как информатизация общества. Эта система оказывает благоприятное влияние на жизнедеятельность людей, так как многие системы становятся автоматизированными, что значительно упрощает осуществление и решение определенных задач. Однако, на данный момент все чаще встречаются случаи, при которых информатизация негативно сказывается на экономике страны и формирует криминогенную обстановку, зарождающая новые виды совершения преступлений.

Одним из подобных преступлений является бесконтактный сбыт. Такого рода преступления осуществляются путем использования сети Интернет, посредством различных виртуальных площадок (например, «LegalRC», «Hydra onion»). Подобным способом сбывают различные нелегальные товары, в том числе и поддельные денежные средства.

Причинами повышенного интереса к данному способу сбыта может выступать не только то, что такой процесс сохраняет конфиденциальность данных поставщиков и покупателей, но и возможность реализации других преступных умыслов, например, схем «отмывание денег».

Квалификация бесконтактного сбыта фальшивых денежных средств определяется в зависимости от способа осуществления данного преступления. Например, возможна реализация сбыта высокоорганизованными преступными группами, которые тщательно планируют совершение преступления, сохраняя анонимность и используя различные цифровые технологии, которые и обеспечивают виртуальные площадки с использованием различных платежных систем.

Так, обратимся к Приговору Белгородского районного суда Белгородской области по делу № 1-320/2021, в котором установлено, что С. в составе организованной группы хранил, перевозил и сбывал поддельные деньги. Для того, чтобы осуществляемые действия обеспечивали безопасность участников группы, организаторы разработали схему, в которой подделки передавались через тайники (закладки), координаты и денежное вознаграждение за которые предоставлялись посредством интернет-площадки. Отличительной чертой данной преступной группы было то, что в ней имелся высокий уровень материально-технической оснащенности, то есть каждый участник имел доступ в интернет, что позволяло обладать наиболее актуальной информацией, быть мобильным и оперативно реагировать на различные задачи, а также в случае пресечения незаконной деятельности кого-либо из членов группы, это способствовало остальным, оставаясь

¹ © Рыбак М. М., 2022.

на свободе, скрыть следы преступлений. Действия С. суд квалифицировал по ч. 3 ст. 186 УК РФ, с лишение свободы на 3 года и штрафом в размере 500 тыс. рублей.

По рассмотренному приговору можем заметить, что важной составляющей является хорошо спланированная и разработанная схема, которая позволит обеспечить участникам преступной группы безопасность. Участники понимают, что те действия, которые необходимо осуществить, уже продуманы, поэтому доверительно относятся ко всем членам группы. Говоря о такой квалификации, стоит обратить внимание, что она свойственна только тому бесконтактному сбыту, который был осуществлен организованной преступной группой.

Уголовный кодекс также предусматривает и другие квалификации данного деяния. Например, ч. 1 ст. 186 УК РФ предусматривает ответственность в том числе за бесконтактный сбыт поддельных денег. Особенность подобной квалификации заключается в том, что состав преступления состоит в использовании их в качестве средства платежа при оплате товаров и услуг, размене, дарении, даче взаймы, продажи и т. п.

Стоит отметить, что приобретение заведомо поддельных денег или ценных бумаг в целях их последующего сбыта необходимо будет рассматривать как приготовление к сбыту [1].

Рассмотрим Приговор Октябрьского районного суда г. Ростова-на-Дону по делу № 1-470/2020, согласно которому подсудимый Д. М. Л. обвиняется в совершении преступления, предусмотренного ст. 30, ч. 1 ст. 186 УК РФ. Неустановленные лица, которые были соучастниками по делу, должны были сбывать бесконтактным способом поддельные денежные средства Д. М. Л., который в свою очередь собирался осуществлять сбыт иным лицам. Подобная судебная практика позволяет рассмотреть различные варианты квалификации бесконтактного сбыта.

Также, УК РФ предусматривает ответственность и за бесконтактный сбыт, совершенный в крупном размере, который составляет 2,25 млн рублей, ответственность предусмотрена ч. 2 ст. 186 УК РФ. Состав преступления остается тем же, однако меняется размер, в котором осуществлялся сбыт.

Отличительная особенность бесконтактного сбыта фальшивых денежных средств связана с техническим обеспечением. Речь идет о том, что для осуществления преступного умысла используется интернет, а именно различные мессенджеры и виртуальные площадки. Это обеспечивает высокий уровень конспирации групп и затрудняет процесс расследования подобных преступлений, так как члены преступных групп могут, например, общаться через периодически блокируемые Роскомнадзором «зеркала» сайта Hydra, по которым нельзя определить IP-адрес. Сами же члены группы отличают друг друга по никам.

Осуществление коммуникативной функции позволяет реализовать преступный умысел, для чего используются различные электронные платежные системы, наиболее распространенные в России. Для сохранения конфиденциальности преступники подключают программы, маскирующие IP-адрес, что позволяет скрыть данные об осуществленных денежных переводах.

Для того, чтобы эффективно расследовать преступления данного вида, необходимо изучить возможные механизмы совершения подобного деяния. Различные схемы имеют черты, которые характерны для любого бесконтактного сбыта. Рассмотрим основные из них (рис. 1).

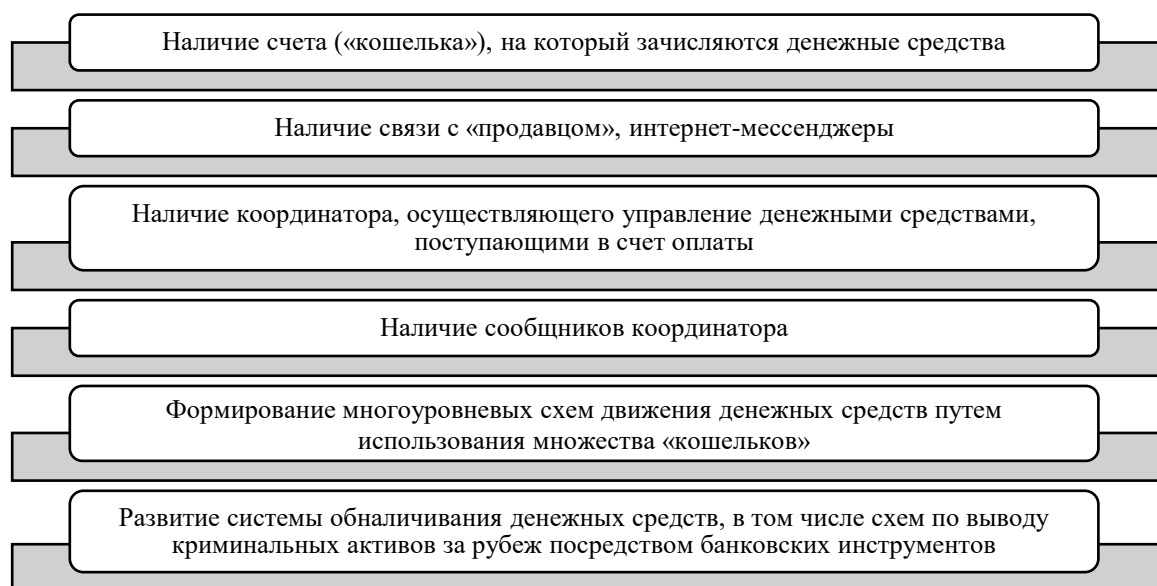


Рис. 1. Базовые условия структуры организации бесконтактного сбыта

На основании рассмотренных выше условий формируются схемы осуществления бесконтактного сбыта. Среди них наиболее распространенными являются следующие:

1. По предварительной договоренности покупатель зачисляет сумму на счет в банке, а продавец осуществляет сбыт поддельных денег бесконтактным путем;
2. Получение продавцом денежных средств через ЭПС, т. е. перевод между банковскими системами, фальшивые купюры оставляют в тайнике;
3. Обмен происходит без открытия счета в банке, но через электронные денежные переводы («Anelik», «Uniastrum» и т. д.). Чаще применяют иностранные продавцы.
4. Наиболее актуальная в современном мире схема бесконтактного сбыта – с использованием интернет-ресурсов. Применяют Qiwi-кошельки, «кошельки-аккумуляторы», расчеты криптовалютой (например, с помощью пиринговой платежной системы «Биткойн»).

Оперативные органы стараются проводится тщательный мониторинг криминальной ситуации бесконтактного сбыта, что позволяет выявить возможные пути совершения данного преступления. Например, в 2022 г. была прекращена деятельность наиболее распространенной виртуальной площадки «Hydra onion». Генпрокуратура Франкфурта-на-Майне, Центральное управление по борьбе с интернет-преступностью и федеральная уголовная полиция сообщили об аресте серверов крупнейшей в мире даркнет-площадки «Гидра» (Hydra Market).

Данная нелегальная площадка являлась русскоязычной, работала через сеть Tor примерно с 2015 г. Там проводилась торговля наркотиками, фальшивыми денежными средствами, личными данными, предоставлялись услуги по сбыту

и взлому аккаунтов и др. В целом на сайте было около 17 млн клиентов и 19 тыс. продавцов. Оборот этого ресурса был самый большой в мире. Виновные в развитии площадки уже установлены.

Однако стоит отметить, что прекращение работы «Hydra onion» не исключает возможность совершения бесконтактного сбыта, так как в современных условиях постоянно разрабатываются новые способы и методы совершения преступлений, которые основываются на различных информационных технологиях, позволяющих скрыть максимально все данные о деянии, что в целом усложняет работы правоохранительных органов, подрывает экономическую безопасность страны и обостряет криминогенную ситуацию.

Список использованных источников:

1. Постановление Пленума Верховного Суда Российской Федерации от 28 апреля 1994 г. № 2 (ред. от 06.02.2007) «О судебной практике по делам об изготовлении или сбыте поддельных денег или ценных бумаг» // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_4040.
2. Терехов М. Г. Цифровое право // Экономика. Право. Общество. 2021. № 3 (27). С. 68–70.
3. Терехов М. Г. Роль гражданско-правового режима цифровых активов в обеспечении национальной безопасности государств – членов ОДКБ // Защитник закона. 2022. № 13. С. 139–150.
4. Мурадян С. В. Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право. 2022. № 5. С. 196–201.
5. Михайленко Н. В., Мурадян С. В., Вихляев А. А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях // Аудиторские ведомости. 2022. № 1. С. 140–145.
6. Пушкарев В. В. Феномен уголовного преследования в досудебном производстве: проблемы интерпретации статистических показателей // Органы следствия Министерства внутренних дел Российской Федерации на страже правопорядка (к 56-й годовщине образования следствия в органах внутренних дел) : сборник тезисов и статей Международной научно-практической конференции, Москва, 6 апреля 2019 г. М. : Сириус, 2019. С. 47–50.
7. Вихляев А. А. К вопросу об использовании сотрудниками полиции личных технических средств при аудио- и видеофиксации противоправного поведения правонарушителей и о допустимости приобщения полученных результатов в качестве доказательств при производстве по делам об административных правонарушениях и в уголовном процессе // Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции : сборник материалов I Всероссийской научно-практической конференции, Москва, 27 января 2021 г. М. : Университет прокуратуры Российской Федерации, 2021. С. 411–415.

Герцен М. А.¹,
 доцент кафедры специальных
 информационных технологий
 учебно-научного комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат химических наук

ВОПРОСЫ УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Управление рисками информационной безопасности является одной из составляющих общих правил информационной безопасности, которые значительно изменились на протяжении десятилетий.

Эти изменения отражают созревание отрасли информационной безопасности в целом. Практика управления безопасностью использовала меньшую сферу действия, которая была сосредоточена на разработке политик и процедур и наблюдении за различными технологиями безопасности, развернутыми в сети с административной точки зрения. В настоящее время управление безопасностью – это разработка корпоративных архитектур, внедрение моделей совершенствования процессов, создание показателей, управление рисками и создание систем управления.

Безопасность стоит денег, а компании должны иметь возможность рационализировать и оптимизировать этот тип расходов. Нарушения безопасности могут привести к опустошению репутации компаний, а не соблюдение различных законов и правил может быстро стать дорогостоящим активом. Эти понятия определяют направления развития организации и точки приложения для управления корпоративной безопасностью, которая стала более дисциплинированной.

По сути, обеспечение информационной безопасности – деловая проблема, которая должна решаться в контексте бизнес-среды предприятия.

Системы управления информационной безопасностью. В конце 1990-х гг. организациям пришлось начать процесс разработки общесистемных программ безопасности в качестве проблем безопасности, связанных с деловыми проблемами. Единственным программным обеспечением безопасности, которое было доступно в то время, был британский стандарт 7799 (BS 7799) [1], в котором описывалось, как должна разрабатываться и поддерживаться система управления информационной безопасностью (ISMS) или программа обеспечения безопасности. Этот стандарт де-факто был усовершенствован на протяжении многих лет Международной организацией стандартизации (ИСО); сегодня организации во всем мире используют серии ИСО / МЭК27000 в качестве своей дорожной карты для внедрения СУБД в вычислительной среде дисциплинированным образом.

¹ © Герцен М. А., 2022.

Стандарты серии ISO / IEC 27000 составлены из передовой практики создания и реализации внутренних программ, таких как управление рисками, управление инцидентами, управление, безопасность приложений, показатели, аудит и многое другое. Организации могут стать сертифицированными на основе этих стандартов, чтобы продемонстрировать свои сильные позиции безопасности для клиентов и деловых партнеров. Основные стандарты, которые составляют серию, включают:

- ISO / IEC 27001: требования к СУИБ [2];
- ISO / IEC 27002: Свод практических правил для управления информационной безопасностью [3];
- ISO / IEC 27003: Руководство по внедрению СУИБ [4];
- ISO / IEC 27004: Руководство по измерению и показателям [5];
- ISO / IEC 27005: Руководство по управлению рисками информационной безопасности [6];
- ISO / IEC 27006: Руководство по аудиту и сертификации [7].

Это всего лишь небольшой список стандартов; новые разрабатываются, утверждаются и добавляются непрерывно.

Структуры архитектуры предприятия. Одним из новейших разработок в области управления информационной безопасностью является интеграция формальных инфраструктур корпоративной архитектуры. Они были введены в связи с трудностями, связанными с отображением методов и процессов обеспечения безопасности для нужд бизнеса.

Серия ИСО / МЭК 27000 используется для разработки общесистемной программы обеспечения безопасности, а корпоративная архитектура определяет, как организации интегрируют эту программу безопасности в бизнес-подразделения, процессы и действия. До использования корпоративной архитектуры организации обнаружили, что их усилия по созданию программы безопасности на основе ISO / IEC 27000 привели к большому количеству документации и меньшему количеству фактических реализаций, чем предполагалось. И хотя безопасность появилась из технического мира, она не легко интегрировалась в бизнес-мир, где требовалась непосредственная поддержка бизнес-драйверов и требований.

Использование модели архитектуры может облегчить для команд понимание того, как темы безопасности, охватываемые различными политическими документами, относятся к потребностям бизнеса, тем самым помогая в реализации необходимых стратегий безопасности. Тем не менее, архитектурные каркасные модели часто сложны по своей природе, и некоторые команды безопасности могут стать перегруженными и «обернутыми вокруг оси». Внедрение сложной модели, такой как корпоративная архитектура, может быть полезно в долгосрочной перспективе, но должно быть сделано методично.

В первые дни многие корпорации уже использовали проверенную инфраструктуру корпоративной архитектуры, которая позволила им понять свой бизнес как с формальной, так и с структурной точки зрения. Эта структура была адаптирована для обеспечения целостности интегрированных в компанию мероприятий по обеспечению безопасности, процессов и стратегий. Это привело

к модели Sherwood Applied Business Security Architecture (SABSA) [8], которая определила требования бизнеса с точки зрения безопасности. Модель состоит из слоев, которые захватывают и представляют стратегические цели, концептуальный дизайн, практическую реализацию, метрическое развитие и шаги аудита.

Оборонные отделы нескольких разных правительств используют свои собственные архитектурные модели для тех же основных целей, как структура архитектуры Министерства обороны США (DoDAF) [9] и структура архитектуры Министерства обороны Великобритании (MoDAF) [10]. Эти структуры архитектуры сосредоточены на том, как интегрировать технологии и процессы информационной безопасности в системы и процессы поддержки военных и оборонных миссий.

Цели управления безопасностью. Системы управления информационной безопасностью и архитектуры корпоративной архитектуры – это конструкции высокого уровня, которые не имеют дело с фактическими элементами управления безопасностью, которые необходимо внедрить для защиты среды. Прежде чем команда безопасности может решить, какие элементы управления необходимо приобрести и ввести в действие, он должен понять, что должен выполнить каждый элемент управления, который называется «контрольной задачей». COBIT [11], ранее известная как Цели контроля для информации и смежных технологий, представляет собой структуру и набор целей управления, разработанных ISACA [12] и Институтом управления ИТ (ITGI). COBIT предлагает рекомендации по закупкам, установке, тестированию, сертификации и аккредитации контроля безопасности, а также обеспечивает структуру, которая позволяет обеспечить управление ИТ-инфраструктурой посредством использования контрольных целей, инструментов внедрения,

Выводы. Новая версия, COBIT 5, развилась, чтобы работать на более стратегическом уровне, чем предыдущие версии COBIT, но общие цели схожи. Так же, как государственный сектор имеет свои собственные структуры архитектуры предприятия, правительство США имеет стандарт NIST SP 800-53, в котором излагается набор средств управления, которые будут использоваться для защиты федеральных компьютерных систем. COBIT фокусируется на задачах управления, а стандарт NIST 800-53 больше ориентирован на сами элементы управления, но оба они обеспечивают аналогичную роль в своих отличительных секторах (COBIT часто используется в коммерческом секторе и стандарт NIST интегрирован в различных правительственных мандатах безопасности).

Важно отметить, что серия ISO / IEC 27000 используется для разработки концептуальной структуры программы безопасности, а корпоративная архитектура используется для интеграции конструкции программ безопасности во всей организации. COBIT используется, чтобы помочь идентифицировать элементы управления, которые необходимо внедрить во всей организации, и предоставляет метод для управления на уровне ИТ-управления.

Список использованных источников:

1. ГОСТ Р ИСО/МЭК 17799-2005 Практические правила управления информационной безопасностью // Сайт «АльтЭль». URL: <https://www.altell.ru/legislation/standards/17799-2005.pdf>.
2. ISO/IEC 27001 Information security management // Official site of ISO. URL: <https://www.iso.org/isoiec-27001-information-security.html>.
3. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls // Official site of ISO. URL: <https://www.iso.org/standard/75652.html>.
4. ISO/IEC 27003:2017 Information technology – Security techniques – Information security management systems – Guidance // Official site of ISO. URL: <https://www.iso.org/standard/63417.html>.
5. ISO/IEC 27004:2016 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation // Official site of ISO. URL: <https://www.iso.org/standard/64120.html>.
6. ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management // Official site of ISO. URL: <https://www.iso.org/ru/standard/75281.html>.
7. ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems // Official site of ISO. URL: <https://www.iso.org/standard/62313.html>.
8. SABSA World Forum at COSAC 2022 // Official site of Sabsa. URL: <https://sabsa.org/>.
9. Полное руководство по DoDAF // Сайт «Кибермедиа». URL: <https://www.cybermedian.com/ru/comprehensive-dodaf-guide/>.
10. Структура архитектуры MOD // Официальный сайт Правительства Великобритании. URL: <https://www.gov.uk/guidance/mod-architecture-framework>.
11. Стандарт CobiT. Управление и аудит информационных технологий. Особенности проведения внешнего аудита ИТ // Сайт «Jetinfo». URL: <https://www.jetinfo.ru/standart-cobit-upravlenie-i-audit-informacionnyh-tehnologij-osobennosti-provedeniya-vneshnego-audita-it/>.
12. Official site of Isaca. URL: <https://engage.isaca.org/home>.

Бочарова А. С.¹,
курсант международно-правового факультета
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Стащенко С. П.,
доцент кафедры противодействия
преступлениям в сфере
информационно-телекоммуникационных
технологий Московского университета
МВД России имени В.Я. Кикотя

ЦИФРОВЫЕ СЛЕДЫ В РАССЛЕДОВАНИИ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ И ТЕЛЕФОНОВ

В данной статье рассматривается механизм следообразования при совершении преступлений с использованием интернет-технологий. Разбираются общие теоретические вопросы, связанные с понятием и классификацией следов. Анализируется механизм следообразования. Выделяются особенности следообразования для преступлений, совершаемых с использованием интернет-технологий, а также зависимости от способа их совершения.

Актуальность темы заключается в резком всплеске преступлений, совершаемых с использованием интернет-технологий. Для 2021 г. характерно незначительное снижение количества данных преступлений (на 1,4 %), но тема остается достаточно актуальной. Активное развитие интернет-технологий и появление новых возможностей отражается на осуществлении преступной деятельности.

Характеризуя преступления, совершаемые с использованием интернет-технологий, с точки зрения криминалистики, позволяет определить совокупность значимых данных о рассматриваемой категории преступлений с целью правильного построения расследования, и выявить типовые следственные версии. Особое внимание для расследования преступлений и изобличения лиц, которые совершили преступление, имеет механизм следообразования.

Побуждение у государства принимать соответствующие меры должно вызывать отсутствие границ у киберпреступности, а также по согласованию мер борьбы с киберпреступностью во всем мире. Опираясь на степень вовлеченности в деятельность, взаимосвязанную с применением цифровых технологий и сети Интернет, и на структуру связей внутри группы, выделяют несколько разновидностей организованных преступных групп.

Во-первых, это группы, чья деятельность нацелена на цифровую среду или на ней сосредоточена. Зачастую это организованные преступные группы со свободной сетевой структурой, действующие на международном уровне непродолжительный период времени. К ним относятся «рои» (взаимодействуют

¹ © Бочарова А. С., 2022.

по принципу сот), представляющие собой диссоциированные, децентрализованные структуры, не имеющие очевидной схемы иерархии; «хабы» – группы с ассоциированной, четкой командной структурой, ключевыми участниками.

Вторая разновидность – группы, объединяющие реализацию преступной деятельности онлайн и оффлайн и имеющие многозвеньевую структуру, кластерный, гибридный характер, определенную степень согласованности в действиях.

Третья разновидность – группы, основная преступная деятельность которых реализуется вне сети, но которыми используются цифровые технологии при координации деятельности или в рамках способа совершения преступления (например, при совершении мошенничества или распространении наркотических средств или психотропных веществ, совершаемые с использованием средств мобильной коммуникации).

Действующий подход законодателя к киберпреступности привел к образованию в криминалистической среде обсуждений по следующему вопросу – понятие и содержание «цифровых следов».

След – это изменения, ставшие результатом совершения преступления. Поэтому именно след отражает специфику совершенного преступления. Также понятие «единство следов», подразумевающее целостность восприятия информации о совершенном преступлении по совокупности следов.

Образование следа является результатом реализации механизма следообразования. В литературных источниках часто упоминается воздействие на механизм следообразования взаимодействием именно материальных объектов. Но следообразование хищений, совершенных с использованием интернет-технологий, имеет ряд специфических черт, для исследования которой необходимо рассмотреть виды следов и их место при совершении данной категории преступлений.

Обычно следы подразделяются на идеальные и материальные. В материальные следы входят следы-предметы, следы-вещества и следы-отображения, представляющие в совокупности традиционный объект криминалистического исследования [3].

В современное время ученые выделяют еще один вид в связи с распространением хищений, совершаемых с использованием интернет-технологий, – виртуальные следы. Значение виртуальных следов не является однозначным: ряд научных исследователей определяют виртуальные следы как результат совершения компьютерных преступлений. Однако, стоит отметить, что для виртуального следа следообразующим объектом будет являться виртуальная среда. К цифровым следам относятся различного рода файлы и данные о их размещении и передвижении на компьютерном устройстве. Обычно, виртуальные среды рассматриваются при непосредственном воздействии на компьютер с целью получения несанкционированного доступа к информации, ее копирования, модификации, удаления и изменения [1].

Рассматривая преступления, совершаемые с использованием интернет-технологий, следует акцентировать внимание на электронные сигналы и коды, которые обозначают наличие источника сигнала, потребителя и основных характеристик среды события. Такие следы относятся к виртуальным, потому что наблюдается сходство в физических свойствах. Кроме того, по своему содержанию

такие следы образуют новую среду- информационную, что позволило выделить информационные следы, которые не могут быть отнесены ни к одной группе традиционных видов следов.

Поэтому возникает проблема доказательственного значения цифрового следа. Преступления, совершенные с использованием интернет-технологий, оставляют за собой совокупность следов, а именно материальные следы, образованные в результате физического воздействия на компьютерное устройство и периферийные устройства, идеальные следы в виде показаний потерпевших, свидетелей и подозреваемых (обвиняемых); виртуальные следы, которые образовались в результате сохранения информации в кэш-файлах, журналах истории и данных о движениях и изменениях файлов. Хотя информационный след, образующийся в результате оставленной в сети Интернет информации, значим при исследовании преступника, его данных, факта взаимодействия потерпевшего со злоумышленником и т. д. [2]

Роль следообразования хищений, совершенных с использованием интернет-технологий, определяется тем, что при уничтожении материальных следов в процессе сокрытия преступления, остается вероятность восстановления картины совершенного преступления посредством виртуальных и информационных следов [5].

При рассмотрении следующей проблемы следует учитывать сложность в обнаружении следов преступлений, совершенных с использованием интернет-технологий, так как в этом случае необходимо учитывать особенные свойства сети Интернет. Следы, которые образовались при взаимодействии с сетью Интернет, распределяются по множеству объектов, к которым чаще всего относится система компьютерного устройства потерпевшего и преступника, информация, хранящаяся у интернет-провайдера, данные в промежуточных сетевых узлах и т. д.

Механизм следообразования интернет-преступлений представляет собой особую форму протекания процесса, обладающая своим результатом образование материальных, идеальных, виртуальных и информационных следов, обусловленных особенностями процесса воздействия на объекты окружающей обстановки и виртуальной среды [2].

В механизм следообразования входят три основных элемента:

1. Преступление.
2. Воздействие преступления на объекты окружающей среды.
3. Следы как результат воздействия преступления на объекты окружающей обстановки.

Процесс следообразования зависит напрямую от реализации объективной стороны хищения, совершенного с использованием интернет-технологий. В контексте данной категории преступлений рассматривается большое количество преступлений, но в совокупности их следует классифицировать на интернет-мошенничества, распространение вирусных программ и противоправной информации в сети Интернет.

При совершении интернет-мошенничеств следы будут образованы в результате взаимодействия преступника и потерпевшего, взаимодействия с интернет-

провайдером, хостинг-провайдером, регистратором доменных имен, в результате чего, необходимо установить регистрационные данные, данные по платежным системам и т. д.

По ходу рассмотрения хищений, совершаемых посредством распространения вирусных программ, важно заострить внимание на следах, образованных в результате воздействия вирусных программ на программное обеспечение, в том числе сохранившийся код вируса, отчет антивирусной программы, зашифрованные файлы и т. п.

Следовая картина противоправного размещения информации в сети Интернет будет складываться из информации в веб-серверах, log-файлах, аккаунтах в социальных сетях, данных о запуске специальных программ и сведений трафика.

Распространенными способами совершения интернет-преступления являются также нюкинг и хакинг, направленные на нарушение оптимальной работы программного обеспечения посредством подачи огромного количества информации или взлома интернет-ресурсов. В подобной ситуации следы будут образованы в результате воздействия на log-файлы, поступления запросов пользователю, изменения данных на веб-сайте.

Совершение интернет-хищений посредством социальных сетей дает возможность злоумышленнику получить необходимые сведения о потерпевшем и использовать «социальную инженерию» для вхождения в доверительный контакт. К тому же в поиске следов необходимо обратить внимание на мобильный телефон, электронную почту, к которым был привязан аккаунт в социальных сетях, статистику активности аккаунта и архив переписок.

Таким образом, важно отметить, что основным элементом следообразования при хищении с использованием интернет-технологий, является информационный след, образованный в результате активных действий пользователей в интернет-пространстве. Тем не менее, несмотря на многообразие следов, образованных в результате совершения интернет-преступлений, попытки скрыть следы преступления не предпринимаются, что говорит, во-первых, о безразличном отношении преступников к содеянному преступлению, а во-вторых, о возможности изначально исказить информацию, что усложняет процесс следообразования.

Список использованных источников:

1. Аскольская Н. Д. Виртуальные следы как элемент криминалистической характеристики компьютерных преступлений // Закон и право. 2020. № 5. С. 173–176.
2. Борисов В. В. Об особенностях фиксации информационных следов в практике защиты информации // Известия ЮФУ. Технические науки. 2019. № 5. С. 23–27.
3. Комиссарова Я. В. Понятие и классификация следов в криминалистике // Вестник Университета имени О. Е. Кутафина. 2019. № 3 (55). С. 131–142.
4. Мазуров И. Е. Методика расследования хищений, совершенных с использованием интернет – технологий : дис. ... канд. юрид. наук : 12.00.12. Ростов-н/Д., 2017.

5. Себякин А. Г. Механизм слепообразования в компьютерных системах с точки зрения теории отражения // Сибирские уголовно-процессуальные и криминалистические чтения. 2021. № 2 (32). С. 87–95.

Платов Н. Е.¹,
адъюнкт Краснодарского высшего
военного училища
имени генерала армии С.М. Штеменко

Сизоненко А. Б.²,
начальник кафедры Краснодарского
высшего военного училища
имени генерала армии С.М. Штеменко,
доктор технических наук, доцент

АЛГОРИТМ НАЗНАЧЕНИЯ ЭКСПЕРТОВ НА ПРОЦЕССЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЭФФЕКТИВНОГО РЕШЕНИЯ ЗАДАЧ ПО ОЦЕНКЕ СООТВЕТСТВИЯ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье рассматривается актуальность качественного распределения членов комиссии (рабочей группы) для проведения аудита информационной безопасности (ИБ) по оценке соответствия защищенности объектов критической информационной инфраструктуры (КИИ) Российской Федерации, ее влияние на эффективность проведения указанных мероприятий. Предложен подход к определению ключевых позиций назначенных экспертов на процессах аудита ИБ.

Цель статьи – разработать алгоритм, позволяющий распределять экспертов в составе рабочей группы для наиболее эффективного проведения аудита ИБ по оценке соответствия защищенности объектов КИИ.

Современное развитие информационных систем, их революционное внедрение в различные сферы повседневной жизни остро ставят вопросы обеспечения информационной безопасности. Одной из составляющих процесса всестороннего обеспечения ИБ является аудит информационных систем. Именно аудит позволяет оценить правильность и адекватность принимаемых мер защиты, внедрения новых способов и средств обеспечения ИБ, и в итоге – дать окончательную оценку достигаемому уровню защищенности [1, с. 7].

Наряду с техническими мерами обеспечения информационной безопасности не меньшее значение придается и организационным, таким как качественный и количественный состав аудиторов ИБ, а также мероприятиям планирования и осуществлению комплекса мер по обеспечению ИБ, организации деятельности и координации взаимодействия сил обеспечения ИБ [2, с. 8]. С этой целью – грамотное распределение экспертов по ИБ в составе аудиторской группы между задачами решает исход по выставлению объективной оценки соответствия защищенности объектов критической информационной инфраструктуры (КИИ) требованиям нормативных правовых актов (НПА) Российской Федерации.

¹ © Платов Н. Е., 2022

² © Сизоненко А. Б., 2022

В ходе подготовки к проведению аудита ИБ эксперты оценивались по таким качествам как трудовая деятельность на должностях по ИБ (стаж), практический опыт в контрольно-надзорной деятельности (количество успешно проведенных аудитов ИБ), наличие ученой степени/звания, наличие у эксперта сертификата как аудитора, количество дипломов / сертификатов / удостоверений о прохождении дополнительного профессионального образования, а также проводились тестирования методом анонимной взаимооценки профессионально-деловых качеств и методом определения компетентности экспертов в предметных областях [3, с. 23]. Исходя из этого формируется качественный вес эксперта, который учитывается при включении в состав аудиторской группы. Таким образом, необходимо разработать алгоритм, позволяющий распределять экспертов по ИБ аудиторской группы для наиболее эффективного проведения аудиторской проверки по оценке соответствия защищенности объектов КИИ.

Обозначим задачу проведения аудита ИБ как множество функций: $F = (f_2, f_3, \dots, f_n)$, $|F| = n$, где n – количество функций аудита ИБ. Множество экспертов, обладающими компетенциями в той или иной предметной области аудита ИБ, обозначим: $Exp = (e_1, e_2, \dots, e_m)$, $|Exp| = m$, где m – количество экспертов.

Применяя подход, изложенный в [4, с. 34], составим для каждой функции вектор-столбец приоритетности привлечения к ее выполнению того или иного эксперта 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 $a_{i,j} \in Q$ (множество рациональных чисел) и понимается как «качество» эксперта в той или иной предметной области для выполнения какой-либо функции. Каждый эксперт обладает определенными ресурсами при проведении аудита ИБ. Обозначим их через вектор ресурсов $R = (r_1, r_2, \dots, r_m)$. Для удобства вычислений примем $r_i \in [0; 1]$. Для проведения аудита ИБ необходимо, чтобы для каждой функции был выделен определенный ресурс. Другими словами, каждая функция обладает определенной трудоемкостью $W = (w_2, w_3, \dots, w_n)$ и $w_j \in [0; 1]$.

Пусть $0 \leq x_{ij} \leq 1$ – доля вклада (количественное значение) ресурса i -го эксперта в j -й процесс, а $\sum_{i=1}^m r_i = \sum_{j=1}^n w_j$.

Тогда задача назначения экспертов, способных провести аудит ИБ с максимальным качеством сводится к классической транспортной задаче [5, с. 70] и имеет сбалансированную (закрытую) форму:

1. Суммарные доли весовых коэффициентов i -того сотрудника, распределяемые между функциями аудита ИБ должны быть равны r_i . Это даст m уравнений:

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

2. Суммарные доли значимостей процессов на выполнение каждой j -той функции должны быть равны w_j :

$$\left. \begin{array}{l} x_{11} + x_{21} + \dots + x_{m1} = w_1 \\ x_{12} + x_{22} + \dots + x_{m2} = w_2 \\ \vdots \\ x_{1n} + x_{2n} + \dots + x_{mn} = w_n \end{array} \right\}; \sum_{j=1}^n w_j = 1$$

3. При этом суммарное значение коэффициентов $a_{i,j}$, определяющих качество выполнения задач (процессов), должно быть максимальное, а следовательно потенциал аудита ИБ принимает вид:

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

Рассмотрим пример: пусть имеются семь функций, которые определены в ходе проведения аудита ИБ на объекте КИИ организации: f_2 – «Возможности внутреннего (внешнего) злоумышленника»; f_3 – «Беспроводные каналы»; f_4 – «Каналы проникновения злоумышленника. Анализ сетевого трафика, журналов регистрации, системных процессов»; f_5 – «Техническая защита информации. Организационный контроль»; f_6 – «Компетентность персонала»; f_7 – «Безопасность персонала. Физическая защита»; f_8 – «Социальная инженерия».

В распоряжении председателя рабочей группы по аудиту ИБ имеется пять экспертов, для которых ранее разработана матрица качества выполнения указанных функций, векторы ресурсов и трудоемкости:

$$A = \begin{pmatrix} 3,34 & 1,63 & 2,73 & 2,94 & 3,24 & 0,32 & 3,47 \\ 0,92 & 3,38 & 1,87 & 2,80 & 3,63 & 1,68 & 1,86 \\ 4,27 & 1,09 & 0,40 & 2,80 & 1,08 & 0,66 & 1,09 \\ 3,92 & 3,50 & 2,50 & 2,81 & 3,92 & 1,41 & 4,07 \\ 3,83 & 3,81 & 1,27 & 3,55 & 2,91 & 2,66 & 0,58 \end{pmatrix};$$

$$R = \begin{pmatrix} 0,17 \\ 0,22 \\ 0,22 \\ 0,20 \\ 0,19 \end{pmatrix}; W = (0,19 \quad 0,11 \quad 0,15 \quad 0,18 \quad 0,17 \quad 0,08 \quad 0,11).$$

Решение транспортной задачи дало следующие результаты:

$$\begin{pmatrix} 0 & 0 & 0,15 & 0,02 & 0 & 0 & 0 \\ 0 & 0,11 & 0 & 0,03 & 0,08 & 0 & 0 \\ 0,19 & 0 & 0 & 0,03 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0,09 & 0 & 0,11 \\ 0 & 0 & 0 & 0,11 & 0 & 0,08 & 0 \end{pmatrix}.$$

Эффективное распределение экспертов на процессы аудита ИБ, а также последовательность переходов между ними представлено в *табл. 1*:

Последовательность переходов экспертов между процессами аудита ИБ

$\begin{matrix} F \\ \text{Exp} \end{matrix}$	f_2	f_3	f_4	f_5	f_6	f_7	f_8
e_1			$\overleftarrow{1}$	2			
e_2		$\overleftarrow{1}$		$\overleftarrow{3}$	2		
e_3	$\overleftarrow{1}$		$\rightarrow$	2			
e_4					$\overleftarrow{2}$		1
e_5				$\overleftarrow{1}$	$\rightarrow$	2	

Таким образом, решение задачи определения состава экспертов для наиболее эффективного проведения аудита ИБ сведено к решению транспортной задачи. Разработанный алгоритм может использоваться в системах поддержки принятия решений, принимаемых руководителями подразделений информационной безопасности. Развитием предложенного алгоритма является определение необходимости привлечения меньшего количества экспертов для проведения аудита информационной безопасности без потери качества его проведения.

Список использованных источников:

1. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями : монография. СПб. : Научно-технологические, 2018. 122 с.
2. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Консультант Плюс». URL: <http://www.consultant.ru>.
3. ГОСТ Р ИСО/МЭК 19011-2021. Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента от 21 апреля 2021 г. // СПС «КонсультантПлюс». URL: <http://www.consultant.ru>.
4. Саати Томас Л. Принятие решений при зависимостях и обратных связях: Аналитические сети. / науч. ред. А. В. Андрейчиков, О. Н. Андрейчикова. М. : ЛКИ, 2008. 360 с.
5. Вентцель Е. С. Исследование операций. М. : Советское радио, 1972. 552 с.

Кияшко С. Е.¹,
*командир взвода (научного) –
младший научный сотрудник роты (научной)
Краснодарского высшего военного училища
имени генерала армии С.М. Штеменко*

АНАЛИЗ ВОЗМОЖНОСТЕЙ ВЫЯВЛЕНИЯ ФАКТОВ КОМПРОМЕТАЦИИ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

На сегодняшний день в своей деятельности практически все организации используют электронный документооборот. Он позволяет повысить оперативность работы, сохраняя при этом аутентичность подписанных документов. Эти свойства реализуются при помощи электронной подписи. Для ее создания необходим ключ электронной подписи, который хранится в тайне от посторонних лиц и известен только его владельцу. Несмотря на все предпринимаемые организационные меры, направленные на обеспечение безопасности ключа электронной подписи, есть риск его компрометации, связанный с человеческим фактором. В данной статье будет представлена концептуальная модель, основанная на методах машинного обучения, на основе которой можно выявлять факты компрометации ключа электронной подписи.

Документооборот является неотъемлемой частью деятельности каждой организации. Различают два вида документооборота – бумажный и электронный. В сравнении с бумажным документооборотом электронный обладает рядом существенных преимуществ: сокращение временных затрат на обработку документов, создание единой базы документов, исключающей дублирование, контроль за движением документов на каждом этапе документооборота и т. д. Для получения юридической силы каждый документ должен быть подписан. В источниках определена альтернатива собственноручной подписи на бумажном носителе – электронная подпись, которая также может использоваться для совершения юридически значимых действий [1, с. 5].

Электронная подпись – это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [1, с. 1]. Для создания и проверки подлинности электронной подписи необходимо иметь ключ электронной подписи и ключ проверки электронной подписи. Владелец первого в связи с недостаточной бдительностью и несоблюдением требований безопасного хранения и использования становится потенциальной целью для злоумышленника, вследствие чего возникает риск компрометации ключа электронной подписи. Актуальность данной проблематики также подтверждается в судебных решениях [2].

¹ © Кияшко С. Е., 2022.

На текущий момент согласно банку данных угроз безопасности информации можно выделить три угрозы, относящиеся к компрометации ключа электронной подписи [3]:

- подмена действий пользователя путем обмана (УБИ-127);
- подмена доверенного пользователя (УБИ-128);
- несанкционированный доступ к аутентификационной информации (УБИ-74).

Также, проведя анализ, можно выделить угрозы, связанные с человеческим фактором:

- хранение ключа электронной подписи на техническом устройстве со свободным доступом;
- передача ключа электронной подписи посторонним лицам;
- отсутствие контроля за использованием носителя ключа электронной подписи.

Обеспечение конфиденциальности ключа электронной подписи – это обязанность участников электронного взаимодействия [1, с. 10], однако если нарушитель завладел ключом электронной подписи и воспользовался им в своих корыстных целях, то способов своевременного автоматизированного обнаружения присутствия угрозы при анализе существующих решений не выявлено. С другой стороны, в Требованиях к средствам электронной подписи и Требованиях к средствам удостоверяющего центра, утвержденных приказом ФСБ России от 27 декабря 2011 г. № 796, сказано, что средства электронной подписи должны противостоять угрозам с целью нарушения безопасности [4, с. 4], что открывает новую область для исследований применения и разработки моделей и алгоритмов обнаружения фактов компрометации нарушителем ключа электронной подписи.

Присутствие нарушителя в системе можно обнаружить по анализу метаданных электронных документов, подписанных электронной подписью наблюдаемого субъекта. Существует большой объем данных, на основе которого нейронная сеть способна обучиться шаблону поведения конкретного субъекта, находить впоследствии отклонения и на основе этого принимать решения о возникновении угрозы.

В качестве исходных данных для обучения нейронной сети целесообразно рассмотреть следующие признаки:

- относительная частота использования электронной подписи;
- время (день недели) подписи электронных документов;
- типичность IP-адреса системы электронного документооборота отправителя и получателя.

На основе метаданных электронных документов, подписанных электронной подписи, можно определить, является ли поведение данного пользователя типичным для него либо имеются отклонения. Так же помимо «интеллектуальных» методов реализовано автоматизированное взаимодействие с кадровым органом, с помощью которого можно проверить легитимность наличия ключа электронной подписи субъекта в соответствии с его занимаемой должностью (*рис. 1*).

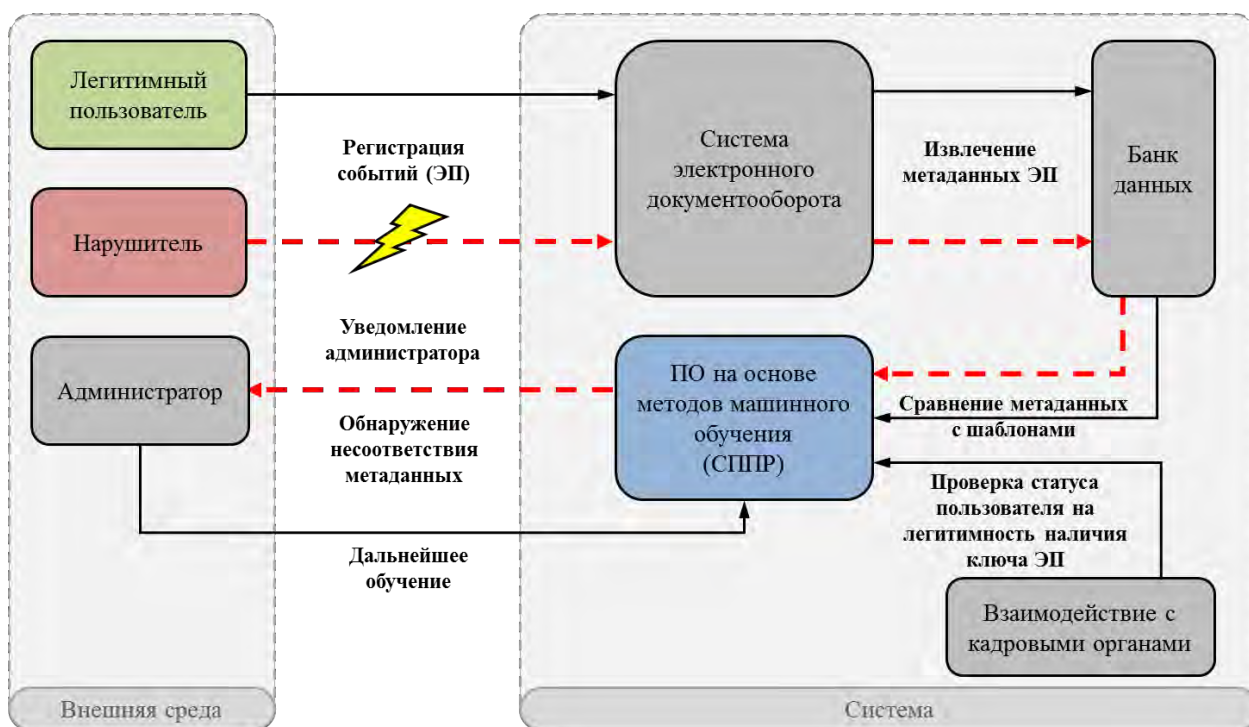


Рис. 1. Концептуальная модель выявления фактов компрометации ключа электронной подписи

В качестве показателей отклонения поведения субъекта системы могут служить такие признаки, как частота подписи электронных документов, типичность использования системы электронного документооборота для приема и передачи электронных документов и время применения электронной подписи. Например, при изменении количества подписанных электронных документов, использовании для приема и передачи документа нетипичного IP-адреса системы электронного документооборота и при использовании электронной подписи после окончания рабочего времени, система примет решение о том, что есть угроза компрометации ключа электронной подписи, о чем сразу уведомит администратора для последующих действий.

Несмотря на предпринимаемые организационные меры, направленные на обеспечение безопасности ключа электронной подписи, есть недостаток – человеческий фактор, при котором остается риск компрометации.

Решить задачу своевременного обнаружения компрометации возможно при помощи построения модели выявления фактов компрометации ключа электронной подписи, использование которой позволяет провести анализ статистических данных пользователей и обнаружить отклонение в шаблонах их поведения. Данное направление исследований является актуальным для разработки специального программного обеспечения и внедрения его в удостоверяющие центры, а применение машинного обучения позволит повысить оперативность выявления и устранения деструктивных воздействий злоумышленника.

Список использованных источников:

1. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_112701/.
2. Российская Федерация. Законы. Судебные и нормативные акты Российской Федерации. URL: <http://sudact.ru/arbitral/doc>.
3. Официальный сайт Банка данных угроз ФСТЭК России. URL: <https://bdu.fstec.ru/threat.doc>.
4. Приказ ФСБ России от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» // Единый портал Электронной подписи. URL: <https://www.iecp.ru>.

Барина А. К.¹,
курсант факультета подготовки
специалистов в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Полянская Е. П.,
преподаватель кафедры информационной
безопасности учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя

ЗАЩИТА ИНФОРМАЦИИ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ КВАНТОВЫХ КАНАЛОВ СВЯЗИ

Информационные технологии и коммуникации в последние годы значительно развились. С информацией сегодня, ее получением и отправлением, связана вся жизнедеятельность современных людей. На данный момент она является тактическим ресурсом государств и общества в целом, который нуждается в сохранении и защищенности от неправомерных действий, приводящих к ущербу. Если говорить о методах обеспечения защиты информации, то их существует немало, но при всем этом возникают новые угрозы для информационной безопасности. Одной из таких является получение информации путем перехвата ее по каналам связи. Решение таких задач требует качественных изменений и перехода научной криптографии на новый уровень информационной безопасности. Ввиду этих проблем и было порождено новое направление в сфере защиты информации – квантовая криптография.

С учетом сложившейся эпидемиологической ситуации в мире за последние годы возникают все новые проблемы, которые становятся более сложными. Квантовая криптография предлагает решение для таких сложных проблем, как моделирование белков. Последний глобальный кризис, вызванный COVID-19, показывает, что ученым нужен другой инструмент для моделирования одного белка и его деактивации. Другим примером экспоненциального роста сложных проблем может быть использование энергии.

Квантовая криптография – технология, использующая квантовую физику для обеспечения надежной защиты информации. В отличие от классической криптографии, которая пользуется математическими методами защиты информации, квантовая криптография сосредоточена на физике и рассматривает случаи, когда информация переносится с помощью объектов квантовой механики. Это открывает много новых возможностей для обработки информации, поскольку можно

¹ © Барина А. К., 2022.

изобрести новые информационные процессы, которые препятствует классической физикой.

Принципы работы квантовой криптографии можно объяснить, рассматривая передачу информации с помощью одиночных фотонов, которые являются квантовыми частицами света, передаваемыми по оптическому каналу, так называемыми кубитами. Особенность кубита заключается в том, что он представляет собой линейную комбинацию состояний квантового бита. При выполнении унитарных операций над кубитовой квантовой системой, которая находится в состоянии суперпозиции, происходит одновременная обработка всех возможных событий. Такой эффект позволяет хранить большое количество информации и дает значительное ускорение вычислительных процессов. Квантовое распределение ключей, которое очень тесно связано с квантовой криптографией, является методом безопасной связи, реализующим криптографический протокол, включающий компоненты квантовой механики. Квантовое распределение ключей и другие протоколы квантовой криптографии используют принципы квантовой механики для обеспечения защищенной криптосистемы с открытым ключом. При этом, если в канале связи будет подслушивающее устройство, которое пытается узнать секретный ключ, то эти протоколы смогут обнаружить его присутствие.

На сегодняшний день большое количество информации, которая передается по каналам связи, шифруется с использованием криптографических систем с открытым ключом. В таких системах ключ состоит из двух частей: открытой и секретной (закрытой). Данные, зашифрованные с помощью открытого ключа, могут быть расшифрованы только с помощью закрытого ключа, а данные, зашифрованные с помощью закрытого ключа, могут быть расшифрованы только с помощью открытого ключа. Безопасность криптографии с открытым ключом основана на предположении о сложности некоторых задач, таких как целочисленная факторизация и дискретная логарифмическая задача. Это делает систему потенциально уязвимой для повышения вычислительной мощности или обнаружения эффективных алгоритмов. Чтобы этого избежать, Чарльзом Беннетом и Жилем Брассаром в 1984 г. был разработан алгоритм кодирования и передачи сообщений, который впоследствии был назван протоколом квантовой криптографии – BB84.

Кратко рассмотрим принцип работы данного алгоритма, который позволяет двум пользователям создать общий криптографический ключ. Он основан на идеях поляризации фотонов. Ключ состоит из битов, которые передаются как фотоны. Базовая модель квантового распределения ключей состоит из двух сторон, называемых Алисой (отправителем) и Бобом (получателем), имеющих доступ как к квантовому каналу связи, который является частным и предполагает совместное использование секретного ключа путем обмена квантовыми частицами, так и к классическому каналу связи, который является открытым и включает в себя базовое согласование, исправление ошибок и протоколы усиления конфиденциальности. Предполагается, что подслушивающий, называемый Евой, может получить доступ к обоим каналам (*рис. 1*).



Рис. 1. Базовая модель квантового распределения ключей

В первой части протокола Алиса берет единичный фотон и поляризует под одним из четырех углов: 0° , 45° , 90° или 135° . Полагается, что Алиса сначала выбирает базис поляризации («+» или «×»), а затем выбирает в этом базисе одно из двух направлений поляризации:

- 0° («↑») или 90° («→») в первом базисе-ортогональном;
- 45° («↗») или 135° («↖») во втором базисе-диагональном.

При этом при битовом вычислении при 0° и 45° будет 1, а при 90° и 135° – 0.

Алиса может закодировать бит распределяемого ключа в состоянии квантовой частицы и отправить Бобу. Перехватчик (Ева) не сможет достоверно узнать, какое состояние было отправлено, а ее попытки произвести измерения и определить какие биты были отправлены, неизбежно приведут к изменениям в состояниях пересылаемых квантовых битов. В результате отправленная Алисой и измеренная Бобом строки бит будут отличаться. Если после сеанса передачи Алиса с Бобом выделяют в битовой строке статистически значимое множество и публично произведут сверку бит, они смогут определить долю ошибок и, руководствуясь моделью, ограничить сверху возможное вмешательство Евы.

В случае, если полученный уровень ошибок не позволяет гарантировать секретность передаваемого ключа, такая строка бит не используется для шифрования. В результате, на руках у перехватчика остается только случайный набор чисел, не имеющий никакого применения (табл. 1).

Таблица 1

Протокол BB84

Битовая строка Алисы	1	0	0	1	1	0	1	0	0	1
Поляризация Алисы	↗	↖	→	↗	↑	→	↑	↖	→	↗
Базис Боба	+	+	×	+	+	×	+	+	+	×
Расшифрованный ключ	0	1	1	0	1	0	0	0	1	0

Квантовая криптография безоговорочно защищена в том смысле, что не делается никаких предположений о неспособности Евы решать сложные матема-

тические задачи, а скорее о ее неспособности нарушать принципы квантовой механики. Однако эти протоколы уязвимы для атаки «человек посередине», когда Ева притворяется Бобом или Алисой. Такие атаки невозможно предотвратить без того, чтобы Алиса и Боб сначала не аутентифицировали друг друга. Кроме того, квантовая криптография не является полностью защищенной при использовании с неисправным оборудованием и в шумной среде. В квантовом канале, подверженном ошибкам, для разработки защищенного ключа можно использовать согласование информации и усиление конфиденциальности. Таким образом, нельзя безоговорочно говорить об идеальности криптографического протокола BB84.

Квантовые каналы связи являются базисом для реализации алгоритмов квантового распределения ключей. Преимущество таких каналов – распределение ключей на большие расстояния между пользователями по открытым каналам связи, при этом у посторонних людей, которые не участвуют в передаче, нет возможности скопировать неизвестное квантовое состояние, прослушать сигнал и различить два не ортогональных квантовых состояния.

Квантовая криптография – метод защиты информации будущего. В настоящее время ни квантовые вычисления, ни квантовая криптография не находятся на той стадии, когда они могут быть практически применены. До сих пор мощное использование квантового компьютера для расшифровки и шифрования информации работает только в теории, поскольку такие компьютеры очень большие по размеру и могут быть изготовлены только на заказ. Так же стоит сказать, что данные алгоритмы работают на ограниченных расстояниях, при превышении 50 км между ними, шум становится настолько великим, что частота ошибок стремительно растет. Сейчас многие государства, в том числе и Россия, вкладывают большие средства в развитие этого направления и решения технических задач, поскольку все понимают, что после создания квантового компьютера классическая криптография станет неэффективным способом защиты информации. Когда же квантовые компьютеры введут в оборот, вычислительные скорости резко возрастут, и математическая сложность алгоритмов классической криптографии станет менее сложной задачей. По всему вышесказанному можно сделать вывод о том, что квантовая криптография – очень перспективное направление, являющееся настоящим прорывом в области информационной безопасности, которое не стоит на месте, развивается и является одним из самых действенных способов защиты информации.

Растущая скорость передачи данных создает все большую потребность в сетевой безопасности. Безопасность данных может стать одной из важнейших проблем, поскольку увеличение объема данных означает больший риск. В частности, одной из основных задач военных технологий является обеспечение безопасной связи.

Говоря об актуальности внедрения квантовых компьютеров, можно сказать, что мощность квантовых вычислений растет экспоненциально с каждым кубитом, а не линейно, как в случае линейных битов, благодаря вычислительным возможностям кубитов с несколькими состояниями. Например, квантовый компью-

тер с 1 кубитом может имитировать 2 классических бита, 2 кубита могут имитировать 4 классических бита, 3 бита могут имитировать 8 классических битов и т. д. Таким образом, это делает возможным экспоненциальный рост мощности квантовых вычислений.

Квантовая технология открывает совершенно новые перспективы для решения проблемы безопасной связи, делая невозможным даже для квантовых компьютеров расшифровку определенных сообщений.

Таким образом, квантовая криптография очень актуальное направление, которое способно решать проблемы из многих и многих областей жизни людей.

Список использованных источников:

1. Леденев А. Н. Физика. Механика. М. : ФИЗМАТЛИТ, 2005. 240 с.
2. Нильсен М., Чанг И. Квантовые вычисления и квантовая связь. М. : Мир, 2006.
3. Дуплинский А. В. Квантовое распределение ключа с высокочастотным поляризационным кодированием : дис. ... канд. физ-мат. наук : 01.04.21. М., 2019. 102 с.
4. Квантовая криптография // Сайт «Se7en». URL: <https://se7en.ws/kvantovaya-kriptografiya-prosteyshie-protokoly-i-chut-chut-kriptoanaliza/>.

Бедрин В. С.¹,
доцент кафедры информатики и математики
Волгоградской академии МВД России,
кандидат юридических наук, доцент

ИНФОРМАЦИОННЫЙ ЭКСТРЕМИЗМ: ЕГО СУЩНОСТЬ И СОДЕРЖАНИЕ

Экстремизму характерны радикализм, нетерпимость, а сознанию свойственны прямолинейность мышления, а также деление мира на две группы – свои и чужие.

Распространение экстремизма в России стало одной из самых серьезных проблем. Особое место занимают экстремистские действия молодежи, связанные с экстремистскими мотивами насильственных действий. Для молодежи характерна психология экстремизма, которая в условиях социального кризиса лежит в основе агрессивности и экстремизма.

Экстремизм среди молодежи представляет собой особенную форму деятельности, выходящей за грани общепринятых правил, форм поведения и типов, подрывающих социальные институты, а также любой их составляющей.

Влияние современных информационных технологий на общество двояко. Между тем, современный человек имеет возможность реализовать их через создание потенциальной информационно-коммуникационной среды, достичь профессиональных и жизненных целей. Через инфокоммуникационную систему будет осуществляться обзор мира, передача социального опыта и культурного наследия, что будет обеспечивать торгово-экономическую деятельность. С другой стороны, он столкнулся с риском манипулирования собственным сознанием – это информация, которую получают террористы и экстремисты.

Экстремизм в информационной среде предусматривает выполнение следующих действий:

- создание, хранение и (или) распространение информации с признаками экстремистской деятельности;
- применение информации, обрабатываемой персональным компьютером, компьютерной сетью и (или) компьютерной системой, в целях воздействия на принятие решения органами местного самоуправления или международными организациями, органами государственной власти, сопряженное с разными формами психического или опосредованного физического насилия (кибертерроризм);
- применение данных, оказывающих деструктивное воздействие на психику человека.

Реализуется экстремизм в информационной среде, как правило, в телекоммуникационной сети Интернет. Данный процесс характеризуется своими разновидностями и особенностями. Имеются ввиду такие интернет-сайты, как микроблоги и форумы, которые среди молодежи в последние годы являются особо

¹ © Бедрин В. С., 2022.

востребованными и активно применяются в экстремистских целях в информационной сфере.

Увеличение фактов информационного экстремизма в телекоммуникационной компьютерной сети Интернет обусловлено «революцией» в сфере коммуникационных технологий, а также результатами современной политики Российской Федерации. Осуществляя контроль за традиционными средствами массовой информации, власти обязали экстремистов удалиться из виртуальной сети телевидения, где контроль был минимальным, а возможности правоохранительных органов были еще меньше. После того, как экстремистские идеи в интернете, распространяясь как вирус, начинают переноситься в области, которым эти идеи даже не свойственны.

Таким образом, проводя профилактические мероприятия среди молодежного экстремизма, следует учитывать увеличение значимости возможностей сети Интернет, а также изменения в коммуникационных системах современного российского общества. Данный фактор зачастую не учитывается представителями различных государственных управленческих структур, а экстремисты уже давно оценили возможности современной системы массовой коммуникации.

Информационный экстремизм является незаметным и нескрытым явлением, а видом преступления, рассчитанным на проникновение в сознание человека, на подрывы его моральных ориентиров для достижения радикальных целей экстремистов.

Таким образом, информационные технологии XXI в. являются невольным распространителем радикальных мыслей и идей, своего рода площадкой для рекламы агрессивно настроенных неформальных организаций разного рода слоев населения.

Список использованных источников:

1. Федеральный закон от 25 июля 2002 г. № 114-ФЗ (ред. от 14.07.2022) «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_37867/.
2. Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_353838/.
3. Указ Президента Российской Федерации от 19 декабря 2012 г. № 1666 (ред. от 06.12.2018) «О Стратегии государственной национальной политики Российской Федерации на период до 2025 года» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_139350/.

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

Научный руководитель
Клочкова Е. Н.,
доцент кафедры информационной
безопасности учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя

ПРОБЛЕМЫ ВЫЯВЛЕНИЯ И БОРЬБЫ С ЗАПРЕЩЕННЫМ КОНТЕНТОМ В СЕТИ ИНТЕРНЕТ

С момента появления сети Интернет ее популярность только возрастает – ежегодно происходит значительное увеличение количества пользователей. Сегодня интернет становится для нас повседневным и привычным явлением, многие уже не представляют без него свою жизнь. Интернет содержит огромное количество разнообразной информации, причем среди этого контента встречается и противоправный, а также фейковый. Распространение такой информации может нанести ущерб как физическим, юридическим лицам, так и государству.

Среди незаконного контента, встречаемого в сети Интернет, отдельное место занимает распространение идей экстремизма и терроризма. Основные угрозы здесь связаны прежде всего с тем, что зачастую целевой аудиторией становятся подростки, которые в силу своего возраста еще не обладают необходимым жизненным опытом и способностью критически оценивать ситуацию, и поэтому достаточно легко подвергаются влиянию и оказываются втянутыми в противоправную деятельность. Суть вербовки в этом случае заключается в вовлечении, как можно большего количества участников в преступную деятельность, не зависимо от возраста и пола.

В качестве одного из способов решения данной проблемы может стать, например, фильтрация контента в образовательных учреждениях. Сегодня многие учебные заведения на своих компьютерах уже устанавливают так называемый «родительский контроль», который блокирует сайты, содержащие вредоносную информацию, а также вводят ограничения на авторизацию в социальных сетях, которые могут выступать не только в качестве площадки для общения, но и местом вербовки в экстремистские, террористические организации, вовлечения в суицидальные группы и т. д.

¹ © Бороздина В. Н., 2022.

Еще один вид противоправного контента, встречающегося в сети Интернет, связан с незаконным сбытом и распространением наркотических средств. Публикуемая информация может быть непосредственно никак не указывать на наличие запрещенного контента, содержать незамысловатые объявления с предложениями о работе. Но в качестве подработки будет выступать доставка наркотических веществ в заданное место, их закладки. Опасность здесь заключается в том, что выявить такую информацию бывает очень сложно, а жертвами зачастую выступают опять же подростки.

К запрещенному контенту, встречающемуся в сети Интернет, также относится распространение детской порнографии. Опасность такого деяния связана с тем, что наносимый ущерб, носит не только материальный, но и психологический характер. Дети могут не помнить, что происходило с ними в детстве, но, если они узнают или видят подобный контент с их участием во взрослом возрасте, это может оставить шрамы на всю их дальнейшую жизнь.

Среди всего многообразия данных, публикуемых в сети, отдельно стоящей категорией становятся сведения конфиденциального характера, являющиеся результатом утечки информации, персональные данные граждан и т. д.

Особенностью современных информационных технологий является то, что информация распространяется с огромной скоростью, а также то, что данные из сети, если они были опубликованы, фактически не могут быть уничтожены. Результатом этого становятся случаи шантажа со стороны злоумышленников снимками, видеозаписями, перепиской интимного характера и т. д.

Самой большой проблемой выявления и борьбы с распространением запрещенного контента стало появления, так называемого Darknet или теневого интернета. Darknet – это собирательное название компьютерных сетей, предназначенных для анонимной передачи информации. Там тоже есть сервисы для торговли, общения и обмена контентом, но их нельзя открыть через стандартный браузер или найти в обычном поисковике.

Помимо легальных сайтов, теневой Интернет наводнили площадки, содержащие детскую порнографию, объявления о продаже наркотических средств, оружия и т. д. При этом вся информация о сайтах и пользователях, включая данные о их местоположении, надежно скрывается через браузер Tor, что делает ее практически недоступной. Анонимность достигается за счет использования промежуточных узлов между клиентскими приложениями и услугами, к которым обращается пользователь, что делает почти невозможным идентифицировать пользователя по его IP-адресу. По этой причине Darknet позволяет распространять, искать и получать практически любой вид запрещенного контента или запрещенных услуг.

Если говорить о методах борьбы с запрещенным контентом, то в Российской Федерации опасный контент зачастую выявляют через анализ обращений граждан, мониторинг интернет-пространства, а также с помощью информации, получаемой от различных ведомств.

Ежегодно усилиями неравнодушных граждан, которые используют ресурсы сети Интернет, выявляется огромное количество противоправного контента. Обращения поступают в Роскомнадзор через официальный сайт или мобильное

приложение. Например, в 2021 г. Роскомнадзором было получено более 900 тыс. обращений. При этом свыше 640 тыс. приходилось на распространение азартных игр в Интернете, 104 тыс. связаны с незаконным оборотом наркотиков, более 50 тыс. жалоб на детскую порнографию, 35 тыс. – на суицидальный контент и призывы к совершению самоубийства. Выявленные противоправные материалы вносят в Единый реестр запрещенной информации. Владелец ресурсов и провайдеру направляют уведомления о необходимости удалить их.

Если говорить о социальных сетях и распространяемой там информации, то разработчики создают и внедряют различные алгоритмы, предназначенные для анализа, фильтрации визуального и текстового контента. Помимо этого, для борьбы с размещением запрещенной информации в социальных сетях также привлекаются простые пользователи, в каждой сети присутствует опция «Пожаловаться на публикацию». Жалобы рассматривают уже не роботы, а служба технической поддержки. И если алгоритмы пропускают целые терабайты визуального и текстового контента, нарушающего все мыслимые и немыслимые правила, то сотрудники техподдержки сразу же удаляют такой контент, накладывая санкции на автора публикации.

Еще одним из способов борьбы с запрещенным контентом стало использование «черных списков» (список ссылок или IP-адресов) для ограничения доступа к сайтам, запрещенным на национальном уровне. Различные интернет-провайдеры проверяют, включен ли сайт, к которому пытается получить доступ пользователь, в список, и в случае положительного результата вместо страницы веб-ресурса открывается информационное сообщение о том, что ресурс заблокирован. Блокировке подлежат не только сайты, нарушающие закон, но и сайты, распространяющие информацию для доступа к запрещенным ресурсам.

В Российской Федерации «черный список» относится к Единому реестру доменных имен, указателю страниц сайтов в интернете и сетевых адресов, который идентифицирует сайты в интернете, содержащие противоправную информацию. При этом Роскомнадзор отвечает за обеспечение актуальности этих данных.

Говоря о блокировке ресурсов, необходимо понимать, что она не является окончательным решением вопроса защиты пользователей от противоправного контента, так как в этом случае зачастую происходит просто перенос информации на другие ресурсы. В качестве примера можно привести попытку блокировки telegram, Instagram (принадлежат компании Meta, признанной экстремистской в Российской Федерации) на территории Российской Федерации. Пользователи все равно, несмотря на наличие блокировки, при желании могут получить доступ к ресурсам через прокси-серверы (VPN) или при помощи других хостингов (зеркал).

Но несмотря на все существующие проблемы, связанные с наличием возможности обхода блокировок, в рамках взаимодействия со службами модерации российских соцсетей за 2021 г. было удалено более восьмидесяти тысяч материалов, содержащих противоправный контент. Статистика показывает, что лидерами по распространению в сети запрещенного и опасного контента являются Darknet, YouTube и группа других социальных сетей, принадлежащих компании Meta, признанной экстремистской в Российской Федерации.

В заключении отметим, что проблемами борьбы с запрещенным контентом занимаются во многих странах мира. Великобритании даже существует организация Internet Watch Foundation (IWF), целью которой является минимизации использования преступного контента в Интернете, включая жестокое обращение с детьми, непристойный контент для взрослых, а также подстрекающий к расизму и преступному поведению. Но в то же время статистика показывает, что, хотя такая борьба ведется, полностью успешной ее назвать нельзя. Основными странами, где размещаются URL-адреса, содержащие информацию о «незаконном контенте», остаются Нидерланды, США, Канада, Франция и Россия.

Список использованных источников:

1. Щурова А. С. Об ограничении доступа к сайтам в сети Интернет, содержащим запрещенную информацию о наркотических средствах // Антинаркотическая безопасность. 2016. №1 (6). С. 30–32.
2. Марценюк А. Г. Запрещенная информация и ее место в системе информационных отношений // Гражданин и право. 2018. С. 69–73.
3. Сидорова Е. А., Кононенко И. С., Загорулько Ю. А., Подход к фильтрации запрещенного контента в веб-пространстве // Аналитика и управление данными в областях с интенсивным использованием данных. 2017. С. 98–100.
4. Кутовой Н. Н., Романова Е. А. Анализ Системы Единого реестра запрещенных сайтов // Наука, образование, общество: тенденции и перспективы развития. 2018. С. 163–169.

Гавриленко А. А.¹,
 заместитель командира взвода
 факультета подготовки сотрудников
 в области информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Аветисян К. Р.,
 старший преподаватель кафедры
 информационной безопасности учебно-научного
 комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ ДЛЯ РЕШЕНИЙ ЗАДАЧ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОВД

Оперативно-разыскная деятельность – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Федеральным законом, в пределах их полномочий посредством проведения оперативно-разыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государство от преступных посягательств. Такое определение дает Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Если углубиться в закон и прочесть задачи, можно установить, что одной из главных задач является выявление и пресечение преступных посягательств.

Изначально любой поиск личности занимал очень много времени и был очень сложен, так как требовал от оперативного сотрудника много знаний, сил и самоотдачи. Необходимо было очень много работать с людьми, наводить справки на человека, подолгу находиться в архивах в поисках необходимой карточки на личность, искать человека по адресам и т. д.

В конце XX в. с появлением первых баз данных процесс поиска информации о человеке стал намного проще, удобнее и быстрее. Не нужно было больше идти в архив и тратить часы на поиск необходимой карточки учета. Теперь требовалось лишь знать данные человека. Достаточно было их внести в поисковую строку, отправить запрос, и в течении нескольких секунд на экране компьютера появлялась учетная карточка на искомую личность. Появление в правоохранительных органах информационно-поисковых систем позволило экономить время сотрудников.

Если начинать рассматривать информационно-поисковые системы, то можно сделать вывод, что самыми первыми и простейшими системами были обычные

¹ © Гавриленко А. А., 2022.

картотеки. Это самый простой способ накопления информации, так как для создания архива необходимо было иметь помещение и картотеку, написанную от руки. Но в тоже самое время архивы были неудобны, ведь приходилось тратить часы на поиск интересующей информации, необходимость вручную создавать карточку на человека, что так же отнимало довольно много времени. Так же с каждым годом количество картотек увеличивалось, что неизменно приводило к увеличению числа архивов, а, следовательно, к затруднению поиска необходимой информации.

Развитие компьютерных систем позволило решить данную проблему. Но для осуществления данной задумки необходимо было решить ряд вопросов. Это и создание своей сети, появление компьютеров у каждого сотрудника, оптимизация всех процессов. Данные вопросы невозможно было решить в короткий промежуток времени, поэтому переход на цифровые информационно-поисковые системы занял довольно много времени. Но данная задача была выполнена, и на сегодняшний день довольно трудно представить деятельность МВД России без данных систем.

На данный момент МВД России ведет большое количество учетов по различным объектам. К объектам учета относятся:

1. Люди – как известные (например, объявленные в розыск), так и неизвестные (лица, скрывшиеся с места преступления).
2. Предметы: к данным объектам можно отнести любые предметы, которые были украдены, утрачены или найдены.
3. Следы: пальцы рук, следы орудий взлома.
4. Орудия преступления.

В связи с большим количеством различной информации, система учетов включает в себя три уровня:

1. Централизованные или федеральные – данные учеты ведет ГИАЦ МВД и ЭКЦ.
2. Местные или региональные – ведутся на региональном уровне, крае, области в информационных центрах, экспертно-криминалистических управлениях или отделах.
3. Централизованно-местные – данные учеты ведутся на местах, т. е. непосредственно в отделах.

Все учеты, которые ведутся на местном и централизованно – местном уровне, направляются в федеральные центры, это позволяет формировать единую учетную базу, увеличению скорости обработки и предоставления необходимой информации.

В МВД России большое количество учетов. Разделение информационно-поисковых систем так же привело к упрощению обращения за информацией, так как весь объем информации разделен на отдельные базы данных, что позволяет выполнить запрос именно в той области, которая интересует пользователя. На данный момент в системе МВД России предусмотрены следующие информационно-поисковые системы:

- «Опознание»;
- «Федеральный розыск – оповещение»;

- «Автопоиск»;
- «Антиквариат»;
- «Вещь»;
- «Сейф»;
- «Досье»;
- «Насилие»;
- «Розыск»;
- «Наказание»;
- «Оружие»;
- «Папилон»;
- «Учет объектов»;
- «Учет фальшивых денежных знаков»;
- «Картотека уголовных дел»;
- «Анализ статистических показателей»;
- «Доказательства»;
- «Постановления».

Появление информационно-поисковых систем в МВД России значительно упростило работу сотрудников. Отпала необходимость вручную перебирать множество бумаг, теперь почти все данные есть в единой базе данных. Теперь достаточно просто зайти в систему ИСОД МВД, выбрать необходимую информационно-поисковую систему, ввести запрос и отправить его. Система автоматически его обработает и выдаст результат, состоящий из результатов поиска по запросу. Появление таких систем так же упростило задачу анализа и обработки информации, что является несомненно важной задачей, так как это позволяет лучше и быстрее анализировать ситуацию и своевременно реагировать на нее.

Список использованных источников:

1. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ (последняя редакция) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_7519/.
2. Официальный сайт МВД России. URL: <https://мвд.рф/>.

Овчинский А. С.¹,
*профессор кафедры информационной
безопасности учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
доктор технических наук, профессор*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГИБРИДНОЙ ВОЙНЕ

Гибридная война. Мы живем в стремительно меняющемся мире: то, что было актуально месяцы назад, быстро уходит в тень под напором новых угроз. Сегодня нашу страну всю глубже втягивают в гибридную войну, которая грозит стать катастрофой для современной цивилизации.

Понятию «гибридная война» придавались разные смыслы. Сейчас уже на нашей территории происходят реальные боестолкновения с применением весьма эффективных средств огневого поражения. Собственно, гибридный или комплексный характер боевых действий можно увидеть в попытках применения противником химических средств поражения (подрыв резервуаров с хлором), бактериологического оружия (опыты по заражению территорий), в угрозах радиационного поражения (обстрелы атомных электростанций), применения тактического ядерного оружия.

Здесь же диверсионные акции (подрывы трубопроводов, энергетических сетей, транспортных коммуникаций и мостов), террористические акты (угрозы, покушения, убийства политиков, идеологов, журналистов). И это все на фоне беспрецедентных по масштабам санкций против нашей страны. Но это не самые серьезные угрозы, с которыми столкнулись наша страна, наше общество, наши люди.

Наиболее опасными представляются информационно-психологические воздействия на сознание людей, сообществ, народов; применение мощи мировых массмедиа и современных цифровых коммуникаций в создании ложных информационных полей.

Это поля психо-исторической войны, когда советские воины-освободители представляются оккупантами и насильниками, а мировые убийцы – идеологи и практики уничтожения миллионов людей – героями, требующими поклонения и прославления.

Одновременно разгорается психо-демографическая война. Сейчас это навязывание гендерного разнообразия и свободы выбирать и менять свою половую принадлежность с раннего детства. Мы помним, как в нарицательные 90-е гг. рождаемость в России была ниже, чем в годы Великой Отечественной войны, а население сокращалось со скоростью более 500 тыс. в год. Маргарет Тэтчер – премьер-министр Великобритании в те годы открыто заявляла: «Нам в России

¹ © Овчинский А. С., 2022.

достаточно иметь 15 млн жителей для обслуживания газо- и нефтепроводов, и добывающей промышленности».

В информационном поле разгорается и идеологическая война. Возрожденная идеология нацизма находит все больше приверженцев и поклонников в европейских странах. Эпицентром бескомпромиссной идеологической войны становятся русофобия, стремление стереть и уничтожить в памяти людей все, что связано с нашей страной.

Противодействие этим угрозам требует переосмысления и качественно новых подходов к обеспечению информационной безопасности, а также общественной и национальной безопасности.

Развитие представления об информационной безопасности. На этапе автоматизации, с появлением ЭВМ и автоматизированных систем обработки данных, информационная безопасность связывалась, в основном, с защитой информации. В те годы информация вышла на арену как объект, требующий внимания в плане обеспечения целостности, доступности, конфиденциальности, и в первую очередь защиты от вредоносных воздействий. Это нашло отражение во многих официальных документах и сохраняется до сих пор.

В последующем на этапе цифровизации с появлением глобальной сети Интернет, с развитием цифровых коммуникаций получение собственно информации становится целью многих видов деятельности.

Так, утвержденная в 2016 г. и ныне действующая Доктрина информационной безопасности Российской Федерации рассматривает обеспечение информационной безопасности как широкий комплекс самых разнообразных мер и мероприятий: разведывательных, контрразведывательных, оперативно-разыскных, аналитических по выявлению и нейтрализации угроз безопасности и ликвидации их последствий.

Сама же информационная безопасность на этапе цифровизации определяется как состояние защищенности личности, общества и государства от угроз в информационной сфере и, согласно Доктрине, основные угрозы связаны не столько с защитой информации, ее производством и оборотом, сколько с защитой сознания людей от вредоносных, криминальных, деструктивных информационных воздействий, несущих угрозу стабильности социальным сферам общества, государству, его суверенитету и целостности.

Информация предстает не столько объектом защиты, сколько целью получения, а главное инструментом воздействия на сознание людей и средством управления социально-политическими процессами.

Последующий этап развития информационных технологий связан с цифровой трансформацией, которая охватила практически все сферы жизни и деятельности людей. И если раньше речь шла об угрозах в сфере получения, обработки и оборота собственно информации, то теперь мы можем говорить об угрозах безопасности социально-информационных сфер, то есть практически всей жизни и деятельности людей. Это сферы семейных отношений, образования, культуры, искусства, науки, духовного подвижничества, политики, управления.

Одна из угроз цифровых технологий – это стирание граней между реальной жизнью и жизнью в сетевом эфире. Погружаясь все глубже в виртуальные миры игр, развлечений, ритуалов, люди становятся все более управляемыми.

Вспомним популярный фильм «Матрица». В нем был дан фантастический образ будущего машинного общества, в котором люди, выполняя предписанные им роли, проживают жизнь не в реальности, а лишь в своих ощущениях.

Но жизнь человека действительно протекает в матрице его личных индивидуальных восприятий, мыслей, переживаний. И личность формируется и реализуется в определенных матрицах отношений: в семье, в образовательной среде, в работе, службе, в культурных и духовных традициях.

Обеспечение информационной безопасности в условиях цифровой трансформации должно было бы быть направлено на создание состояния защищенности социально-информационных сфер жизни нашего общества. Но, и это направление обеспечения информационной безопасности отходит на второй план перед лицом разгорающейся гибридной и, в первую очередь, информационной агрессии против нашей страны, нашего народа, против нашей истории, культуры, духовности, нашего бытия.

Задача сегодняшнего дня – это военная мобилизация всех социально-информационных сфер. Опираясь на исторический опыт нашей страны, можно отметить, что победа в ВОВ, удержание послевоенного мира, достижения в атомной промышленности, в освоении космоса, в образовании и науке были обеспечены мобилизацией всех сил общества в предвоенный период, в ходе войны и в послевоенный период.

Мы же только начинаем движение в этом направлении. И чтобы выдержать военное противостояние и победить требуется провести скорейшую мобилизацию всех сфер общественной жизни уже в новом цифровом мире.

Информация в цифровом мире. Обеспечение информационной безопасности при этом должно опираться на такие представления о самой информации, которые адекватны новым вызовам.

В нормативно-правовом поле информация – это сведения и данные независимо от формы их представления. Это определение было весьма эффективным для решения многих задач на прошлых этапах. Одновременно оно является весьма грубым приближением к пониманию сути информации в условиях возникших угроз.

Дело в том, что на фоне информационного взрыва, когда накопление данных принимает все более сингулярный характер, то есть неуклонно разворачивается в направлении бесконечности, вопрос о том, что собой представляют килобайты, мегабайты и зеттабайты данных и сведений, сообщений и сигналов, остается открытым.

Так, западные эксперты [1] после многочисленных дискуссий сходятся на том, что «информация не нуждается в том, чтобы ее воспринимали и понимали, она не требует умственных усилий для своей интерпретации, ей вообще не обязательно иметь смысл, чтобы существовать».

В такой позиции, образно говоря, нет души и, главное, в ней фокусируется практически вся ложь современного мира. Из этой лжи вырастают двойные стандарты в политике, в праве, в морали. Она все глубже поражает историческую память, питает мировую деструкцию. Ложь была и остается фундаментом чело-веконенавистнических идей, идеологии нацизма.

В фундаментальных подходах к информации выделяются ее атрибутивная и функциональная стороны. Информация выступает атрибутом мироздания, как материя и энергия. Она же обеспечивает функционирование живых и искусственных систем. Сформировался киберцентричный подход, в котором информация выступает в виде данных и управляющих сигналов, и антропоцентричный, в котором информация составляет сведения, знания, жизненные смыслы.

В практическом плане [2] информация – это то, что позволяет реагировать на воздействия на всех уровнях организации живой природы (реактивная проекция информации). Она возникает в сознании человека как функция целевой интерпретации получаемых сообщений. Информация позволяет понимать смысл происходящих событий, оценивать прошлое, заглядывать в будущее.

Именно информация формирует в сознании блоки отношений человека к окружающим событиям. Она создает потенциалы социально-психологической энергии, она же может стать сигналом к разрядке этих потенциалов, приводящих людей к определенным действиям и поступкам.

Получив сообщение о частичной мобилизации, одни люди собираются защищать Родину с оружием в руках, записываются добровольцами, а другие бегут из страны.

Другое сущностное проявление информации – это фиксироваться и накапливаться как на естественных, так и на искусственных носителях (ресурсная проекция информации). Она является необходимым ресурсом эволюции и цивилизации.

Наконец третье сущностное проявление информации, уже атрибутивное, – это отражение окружающей реальности (фоновая проекция информации). Она составляет фон происходящих событий и явлений. Фоновая информация способна обходить защитные функции сознания. На этих свойствах построены технологии визуальной и аудиальной психокоррекции, скрытого тестирования, кодирования и зомбирования. Именно информация (реактивная, ресурсная, фоновая) формирует идеологию.

Борьба идеологий в гибридной войне. Идеологию было принято считать некой «надстройкой» над производительными силами и производственными отношениями. Однако именно идеологии все чаще задают основные векторы как общественных, так и антиобщественных устремлений.

Под идеологией принято понимать систему взглядов и идей, которые отражают наше отношение к окружающей действительности. Идеология может объединять людей или разъединять на враждующие лагеря. Она может оформляться в программных документах.

Главное же, идеология, оказывая влияние на личностные качества человека, образует в сознании некую глобальную матрицу обоснования права на определенные действия и поступки, на образ жизни, на отношение к прошлому, настоящему и будущему.

На разных исторических этапах мир не раз сталкивался с угрозами таких деструктивных идеологий как расизм и терроризм. В русле нацистской идеологии были методично уничтожены миллионы людей, признанных представителями «неполноценных» народов или просто мешавших установлению мирового порядка, основанного на беспрецедентном насилии.

Родовым источником европейского и американского нацизма является, в первую очередь, колониализм, а именно, подъем западной цивилизации за счет ограбления и эксплуатации народов Азии и Африки, американского континента. В этом же ряду труд насильно завозимых рабов на плантациях американских штатов. Обогащение средневековой Европы началось с многочисленных крестовых походов. Только из захваченного в 1204 г. Константинополя драгоценности вывозились более 50 лет.

Базовые ментальные источники нацизма сформированы западноевропейской философией, диалектически обосновавшей могущество человека и поставившей его на место Бога. В русле мальтузианства и социального дарвинизма строились разнообразные теории высших и низших рас, которые воплощались в погромы и массовые убийства жителей «цивилизованных» стран.

Наконец, наиболее глубинные, условно духовные источники нацизма коренятся в древних языческих культах и поклонении идолам силы. Энергия ненависти требует человеческих жертвоприношений и ритуалов, переходящих в кровавые оргии.

Споры мирового нацизма сегодня прорастают иррациональным стремлением к мировому доминированию, новыми волнами шовинизма с пренебрежением жизнью людей и народов, не входящих в «круг избранных», терроризмом с невиданной ранее показной жестокостью.

Сегодня в разгорающейся мировой информационной войне деструктивные идеологии требуют особого внимания со стороны государства, спецслужб, правоохранительных органов.

Идеология истинной человечности. Информационные вирусы деструкции могут проникать в то сознание, в котором образуется идеологический вакуум или идеологический хаос.

Сегодня «эпоха перемен» – это не просто образ нашего времени, это не только отражение стремительных изменений на мировой арене, это неуклонное втягивание в смертельную схватку за будущее нашей страны и всего человечества. В этой схватке мир как никогда поляризован.

Специальная военная операция на Украине высветила ту бездонную пропасть, которая разделяет истинную человечность в жертвенных поступках по спасению и защите жизней людей и нацистско-сатанистскую бесчеловечность в массовых убийствах «не своих» мирных граждан.

Задача идеологической войны – это создание хаоса у противника. В США этому были посвящены фундаментальные исследования в области нелинейных

систем, теории катастроф, синергетики, фракталов, неравновесной самоорганизации. В весьма скрытом, завуалированном режиме специалисты и ученые из разных сфер «трудились» над «управляемым хаосом» в институте Санта Фе, созданном в 1984 г. под эгидой Пентагона и Госдепа. В результате были обозначены такие аттракторы хаоса, которые должны подвести социально-экономическую систему страны к критическому состоянию.

Среди них: содействие либеральной демократии, поддержка рыночных реформ, повышение экономических стандартов, поддержка внесистемных СМИ и, главное, деидеологизация, т. е. уничтожение какой-либо цементирующей обществу идеологии.

Жертвами этих «новаций» стали не только многие «молодые», но и традиционно стабильные государства. Попытки опрокинуть в хаос предпринимались и против нашей страны. В Конституции Российской Федерации, принятой в 1993 г., осталось положение о том, что «никакая идеология не может устанавливаться в качестве государственной или обязательной».

Как бы не было сложно, задачи по демилитаризации, по денацификации Украины, да и всей «недружественной» Европы будут решены. Главный вопрос современности: что мы, наше государство, наша цивилизация сможем предложить миру, какое будущее, какое миропонимание, какую духовность, наконец, какую идеологию?

На самом деле так же, как и многообразие религиозных конфессий в нашей многонациональной стране не исключает единства морально-нравственных начал, так и плюрализм идеологических предпочтений никак не противоречит наличию государственной идеологии, отражающей и объединяющей стремления и чаяния народов нашей страны. Более того, наша идеология должна быть привлекательной и притягательной для жителей других стран и регионов.

Именно государственная идеология должна давать обоснование прав на бескомпромиссную борьбу за суверенитет России, на владение и использование своих природных ресурсов, на твердые позиции в отстаивании исторической правды, на защиту русского мира, на творчество в построении справедливого будущего.

Идеология должна быть стержнем мобилизации социально-информационных сфер. Внедрение государственной идеологии в массовое сознание станет решающим фактором обеспечения как информационной, так и общественной, и национальной безопасности в мире цифровых технологий.

Эта идеология потребует достойного оформления. Также, как герб, гимн, флаг и конституция, она будет необходимым атрибутом государства.

Государственная идеология – идеология истинной человечности необходима для воспитания поколений защитников и творцов.

Список использованных источников:

1. Уэбстер Ф. Теории информационного общества / пер. с англ. М. : Аспект Пресс, 2004.

2. Овчинский А. С., Борзунов К. К., Чеботарева С. О. Информационные координаты. Управление. Противоборство, Безопасность. М. : Горячая линия – Телеком, 2018.

Гончар В. В.¹,
начальник кафедры информационной
безопасности учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ОСНОВНЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ И ПУТИ ИХ РЕШЕНИЯ

Стремительное развитие информационных технологий в значительной степени связано с рисками роста числа преступлений, совершаемых с их использованием.

Показательно, что за истекшие 5 лет уровень преступности в данной сфере увеличился с 90,6 тыс. в 2017 г. до 517,7 тыс. в 2021 г. Зафиксированная негативная тенденция подтверждается увеличением с 4,4 % в 2017 г. до 25,8 % в 2021 г. удельного веса таких преступлений в общем числе зарегистрированных [3].

Изучение информации, поступившей из территориальных органов предварительного следствия МВД России, выявил следующие наиболее распространенные проблемы в расследовании IT-преступлений:

1. Не сформирован действенный инструментарий быстрого получения от операторов связи, кредитных организаций, интернет-провайдеров, социальных сетей и интернет-сервисов информации, имеющей доказательственное значение по расследуемым преступлениям (сведений о биллинге, лице, движении денежных средств по лицевым счетам абонентских номеров и др.).

Длительность получения ответов все еще составляет от нескольких недель до нескольких месяцев. Решение проблемы видится в активном внедрении электронного документооборота.

При формировании запросов в рамках ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» следует четко понимать, о том в какой организации и какие сведения могут быть запрошены.

В целях оказания практической и методической помощи в настоящее время Следственным департаментом МВД России совместно с Московским университетом МВД России имени В.Я. Кикотя разработан и опубликован Сборник образцов типовых запросов, необходимых для расследования IT-преступлений, с указанием контактной информации об организациях и располагаемых ими сведениях.

2. Использование преступниками программ, позволяющих существенно затруднить их идентификацию – TOR, VPN, а также технологий, позволяющих подменять IP-адрес пользователя информационно-телекоммуникационной сети, создавать динамические или нераспознаваемые IP-адреса.

¹ © Гончар В. В., 2022.

Проблема идентификации преступников, использующих программы-анонимайзеры, в настоящее время одна из наиболее актуальных, ее разрешение видится в комплексе законодательных, технических, организационных и научных мер.

Одним из вариантов решения этой проблемы может стать внедрение положительного опыта ГУ МВД России по г. Москве по исследованию информации, содержащейся в Cookie-файлах, важной особенностью которых является их неизменность.

3. Недостаточная компьютерная грамотность населения. Так, в соответствии с вышеуказанными директивными указаниями руководителям следственных подразделений поручено обеспечить принятие действенных мер, направленных на совершенствование методов информирования населения, в том числе с привлечением федеральных и региональных СМИ, социальных медиа о способах совершения IT-преступлений, методах защиты, а также алгоритме действий пострадавшего.

Для решения этой проблемы в большинстве регионов проводятся значительное количество профилактических и просветительских мероприятий. Например, активная профилактическая работа осуществляется в МВД по Республике Башкортостан где кроме всего прочего на официальном YouTube-канале и социальных сетях МВД Республики до населения доводится информация, как не стать жертвой дистанционного мошенничества, при проведении рабочих встреч с представителями финансово-кредитных учреждений отмечена целесообразность нанесения на обратные стороны изготавливаемых банковских карт, около CVV-кода, надписи «СТОП – никому не сообщать», проведены рабочие встречи с руководством волонтерского движения, направлены письма в Министерство молодежной политики республики с предложениями активного привлечения центра волонтерского движения к профилактической и агитационной деятельности, достигнуты договоренности с представителями духовенства о включении информации профилактического характера в ежедневно проводимые мероприятия (проповеди).

4. Необходимость увеличения числа государственных специалистов и экспертов, имеющих право проводить соответствующие исследования и компьютерные экспертизы.

Сегодня в большинстве регионов не сформирована практика привлечения организаций, специализирующихся на обеспечении информационной безопасности, к участию в проведении процессуальных действий, компьютерных исследований и соответствующих экспертиз. Так, в г. Москве представители АО «Лаборатория Касперского» и ГБУ г. Москвы «МИЦ» по резонансным преступлениям систематически проводят компьютерные исследования и экспертизы на безвозмездной основе.

5. Несовершенство механизма, перечня и объема санкций, предусмотренных ст.ст. 272–274.2 УК РФ, не позволяющее достичь целей уголовного наказания.

Согласно информации, представленной территориальными следственными подразделениями системы МВД России, можно сделать вывод, что в подавляю-

щем большинстве при совершении одноэпизодных преступлений, предусмотренных гл. 28 УК РФ, суды назначают наказания в виде штрафа.

Встречаются факты назначения судами наказания за совершение указанной категории преступлений в виде условного лишения свободы.

Анализ приговоров за совершение преступлений данной категории показывает, что наиболее часто судебные органы принимают решения об осуждении лиц к реальному лишению свободы в случаях наличия непогашенной или не снятой в установленном порядке судимости, а также при совокупности с иными преступлениями, прежде всего, предусмотренными гл. 21 УК РФ.

Причиной, способствующей частому применению судами особого порядка принятия судебного решения, является реализация обвиняемым своего права, предусмотренного ч. 5 ст. 217 УПК РФ. В таком случае подсудимому не может быть назначено наказание, превышающее две трети максимального срока или размера наиболее строгого вида наказания, предусмотренного за совершенное преступление.

Кроме того, рассмотрение уголовного дела в особом порядке значительно сокращает время судебного производства, так как отсутствует необходимость в проведении судебного разбирательства в общем порядке.

6. Необходимость совершенствования нормативных правовых актов в области противодействия преступлениям в сфере информационных технологий.

Принятие Федерального закона от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» привело к появлению значительного количества вопросов в части разграничения кражи с банковского счета (п. «г» ч. 3 ст. 158 УК РФ), мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ), а также мошенничества в сфере компьютерной информации, в части вмешательства в процессы нормального функционирования сервисов дистанционного банковского обслуживания (ст. 159.6 УК РФ).

В следственной и судебной практике новый особо квалифицированный вид тайного хищения чужого имущества с банковского счета, а равно в отношении электронных денежных средств получил неоднозначное толкование. По п. «г» ч. 3 ст. 158 УК РФ, обычно, оцениваются действия лица, которое завладело платежной картой потерпевшего и осуществило изъятие денежных средств в наличной форме через устройство самообслуживания клиентов.

Аналогичным образом по п. «г» ч. 3 ст. 158 УК РФ квалифицируются действия лиц, совершивших хищения путем использования сервисов дистанционного банковского обслуживания.

В целях устранения необоснованной конкуренции уголовно-правовых норм, обеспечения единообразия правоприменительной практики целесообразно ст. 159.3 УК РФ исключить.

До настоящего времени законодателем не решен вопрос о сумме причиненного ущерба при квалификации деяний по п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ, что порождает спор органов следствия и органов прокуратуры о применении ч. 2 ст. 14 УК РФ, в части малозначительности деяния при

хищении на сумму менее 2,5 тыс. руб. Возникает необходимость в дополнительном разъяснении порядка определения места совершения подобных преступлений и момента их окончания.

Следует проработать изменения в нормативные правовые акты в части наложения обязательств на финансово-кредитные учреждения хранить фото-видеофайлы из банковских устройств самообслуживания и отделений банков, где они расположены, на срок не менее 6 месяцев.

Несмотря на указанные проблемы, следственные подразделения МВД России принимают действенные меры, для успешного противодействия IT-преступлениям, имеется значительный положительный опыт в данной деятельности.

Автор считает, что указанные обстоятельства представляются значимыми для совершенствования расследования преступлений в сфере информационных технологий, а реализация изложенных предложений позволит существенно повысить эффективность данной деятельности.

Список использованных источников:

1. Информационно-аналитические материалы Следственного департамента МВД России.
2. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Инфра-М, 2023.
3. Официальный сайт Министерства внутренних дел Российской Федерации. URL: <https://мвд.рф/reports/1/>.

Григорьев В. Р.¹,
 заведующий кафедрой КБ – 8
 «Информационное противоборство»
 института кибербезопасности
 и цифровых технологий
 Российского технологического университета,
 кандидат технических наук

Градосельская Г. В.²,
 руководитель факультета социальных наук
 департамента социологии и научно-учебной
 группы «Сетевые методы и модели в анализе
 текстовой информации» Высшей школы экономики,
 кандидат социологических наук, доцент

Жуков Д. О.³,
 профессор кафедры КБ – 8
 «Информационное противоборство»
 института кибербезопасности
 и цифровых технологий
 Российского технологического университета,
 доктор технических наук, профессор,

РАСПРОСТРАНЕНИЕ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ СЕТЯХ РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ

В статье рассмотрено применение методов и технологий лингвистического анализа для определения контента социальных сетей имеющего деструктивную направленность. На основе изложенных методик могут быть выделены речевые маркеры, характеризующие деструктивный контент. Использование этих маркеров позволяет определить характеристики сообщений в социальных сетях и отнести их к одной из заданных категорий. Данный подход позволяет провести анализ семантических сетей комментариев пользователей, построить графы взаимосвязей их речевых маркеров и определить их характеристики (коэффициенты посредничества, плотность и т. д.). Параметры сети (центральность узлов, плотность и т. д.) можно рассматривать как значения элементов вектора, описывающего степень патриотичности, оппозиционности или деструктивности. А сами вектора можно использовать для обучения нейронных сетей при распознавании соответствующих состояний социальных сетей в автоматическом режиме мониторинга или при использовании для этого метода опорных векторов (SVM).

Распространение любого контента в социальных сетях можно рассматривать на основе различных моделей. Однако в них будет общим то, что модераторы этого контента и его пользователи несмотря на возможное различие в своих

¹ © Григорьев В. Р., 2022.

² © Градосельская Г. В., 2022.

³ © Жуков Д. О., 2022.

взглядах образуют единое сетевое сообщество, основанное на сходстве между комментариями, которые образуют связанную сеть.

Поскольку с ростом сети поиск сходства между ее узлами является трудоемким процессом, то для оптимизации процесса решения проблем прогнозирования связей и обнаружения сообществ, исследователи в работе [1] использовали роевые алгоритмы. Методы оптимизации на основе роя, используемые в анализе социальных сетей, сравниваются в этой статье с анализом сообщества и анализом связей на основе традиционно используемых подходов.

В работах [2–4] предложена методика KroMFac, которая проводит обнаружение сообщества с помощью регуляризованной неотрицательной матричной факторизации (NMF) на основе графовой модели Кронекера. KroMFac сочетает в себе методы анализа сети и обнаружения сообщества в единой унифицированной структуре. Данная методика связывает четыре области исследований, а именно обнаружением сообществ на графах, обнаружением перекрывающихся сообществ, обнаружением сообществ в неполных сетях с отсутствующими краями и полных сетей.

Динамику изменения общественных настроений пользователей сети интернет, в значительной степени можно отнести к стохастическим процессам. Присутствие человеческого фактора (множество людей с различными мнениями, предпочтениями и характером поведения) с одной стороны создает случайность изменений (в силу большого разнообразия поведенческих моделей пользователей), а с другой стороны вносит в динамику изменений элементы целенаправленности. Подробное описание использования стохастических методов для моделирования динамики социальных процессов можно найти в [5].

При проведении своих исследований мы хотим рассмотреть более простые модели, однако более детально рассмотреть вопросы использования речевых маркеров для обнаружения и классификации контента определенной направленности.

Критерии отнесения контента к категории деструктивного. При анализе социальных сетей и сетевых масс-медиа основное внимание может быть уделено исследованию текстового контента, как одной из главных форм общения и возможного деструктивного воздействия. В лингвистическом плане деструктивное влияние осуществляется, прежде всего, путем намеренного языкового воздействия на сознание народа, коллектива или отдельной личности.

Критериями отнесения контента к категории деструктивного являются цели, задачи, его назначение, содержание и форма использования контента для достижения желаемых результатов. В зависимости от целевой аудитории, форма, содержание, каналов продвижения используемого контента критерии его отнесения к деструктивному могут быть совершенно различны, весьма разнообразны и в каждом конкретном случае могут варьироваться в широких пределах. Именно по этой причине для выделения соответствующих лингвистических конструкций и параметров контента требуется привлечение экспертов и создание корпусов соответствующих текстов для картирования каждой из групп, на которые направлено воздействие и выявления модераторов деструктивного влияния (т. е. создание экспертной базы перечня и структуры деструктивного контента).

К основным анализируемым лексико-фразеологическим языковым средствам деструктивного влияния относятся специфические политические метафоры, метонимия, перифразы, антифразисы, амплификация, аллюзии, антитезы, гиперболы, риторические вопросы, эмоционально-оценочные эпитеты и предикаты, словесные ярлыки и усиливающие, эти средства, стилистические фигуры.

Идентификация участников дискурса возможна через анализ совокупности дискурсивных практик и характера реализации языковой системы дискурса, включающие в себя тематики и задачи сообщений, знания и способности, квалификация и опыт, взгляды и убеждения, эрудированность и речевые навыки акторов.

Одним из средств оценки деструктивности контента является метод семантического анализа манипулятивного воздействия, на основе исследования используемой лексики, т. е. словарного состава языка, вызывающего либо позитивные, либо негативные ассоциации и таким образом влияющих на восприятие информации. Немаловажным для анализа являются возможности выявления используемых тропеических, фигуральных и иных речевых приемов (например, широкое употребление приема трансформации прецедентного текста как способа искажения информации).

При анализе деструктивности контента важно выявлять объекты воздействия (конкретные персоны, целевые группы, этносы и нации) и мишени воздействия (понятия и представления о связанных с объектом сторонах действительности, которые подвергаются деструктивному воздействию), а для мишеней необходимо выделять наиболее уязвимые места и болевые точки.

Учитывая преобладание иррационального (эмоционального) начала во многих типах деструктивного воздействия, необходимо обращать внимание на значимость категории экспрессивности в текстах, выраженной при помощи различных средств языка (экспрессивной лексики и фразеологии, стилистических фигур и т. д.).

На языковом уровне для текста деструктивного контента прослеживается оппозиция лексем, сочетаний слов и устойчивых конструкций с негативной и позитивной коннотациями.

Можно выделить несколько больших лингвистических групп, применение которых в тексте может служить критерием отнесения контента к деструктивному:

– понятия и термины, связанные с видами психологического воздействия, его технологией и механизмами: агрессия, аргументация и контраргументация, атакующее убеждение, внушение словом, демагогия, духовное помыкание, запутывание ожиданий, защита от манипуляции, зомбирование, манипулирование имиджем (статусом, рангом), манипулирование сознанием, метод «промывания мозгов»; механизм внушения, механизм воздействия, механизм коммуникативного воздействия, мишени воздействия, объект и субъект воздействия, понуждение к действию, порождение информации, программирование поступков, пропаганда, психолингвистическая модель речевого воздействия, психологическая операция, психология политического насилия, психология пропаганды, ролевое управление, семантические психотехнологии, скрытая агрессия, стресс, суггестия, теория

устрашения, техника мифов, технология обмана, технология разрушения сознания, технология скрытого управления, провокация, убеждение, и др.;

– понятия и термины, связанные с условиями психологического воздействия: архетипы, аспекты внушаемости, аттракция, закон духовного единства толпы, захват аудитории, ориентировка в ситуации, отвлекающий фон, поведенческие эффекты, присоединение аудитории, психологические барьеры в общении, психологическое заражение, психология толпы, стандарты поведения, стереотипы, установки, уязвимость подсознания, феномен личного влияния, фрустрация, традиции и ритуалы, ценности, эксплуатация потребностей, эффект когнитивного диссонанса, эффект новизны, эффект ореола, эффект первичности, эффект престижа, эффект стереотипности и др.;

– термины, связанные с конкретными методами и приемами воздействия: вымысел, демонизация имиджа, десенсибилизация (снижение чувствительности); дестабилизация, искажение, «историческая маска», конструирование интерпретаций и воспоминаний, манипулятивная селекция, манипуляция с новостями, метод пробуждения страха, мифы, навязывание повестки дня, переворачивание информации, политическая метафора, символы, создание образа простака, создание псевдособытий, спекуляция на ценностях, уловки (организационно-процедурные, психологические, логические), утечка информации, фальсификация исторических событий, формирование новостей, эффект «нарочитой правдивости» и др.

Выявление и распознавание таких структурных компонентов как речевые жанры (угрозы, брань, оскорбления), речевые стратегии (игнорирование, дискредитация, ложь) и речевые приемы (например, навешивание ярлыков) поможет в решении задач оценки и отнесения контента к деструктивному. При этом необходимо помнить, что некоторые речевые феномены (такие жанры, как порицание, упрек, обвинение, насмешка, ссора, жалоба) могут квалифицироваться как речевая агрессия только в определенной ситуации и при соответствующем подборе лексических средств.

Среди лингвистических характеристик деструктивного контента, которые можно использовать для его выделения, особое внимание нужно обратить на:

1. Использование большого количества экспрессивной и эмоционально окрашенной лексики с негативно оценочной доминантой для усиления эффекта деструктивного контента (для этого очень важен эмоциональный анализ).
2. Включение в ритмическую структуру деструктивного текста ссылок и гиперссылок на сторонние источники (якобы авторитетные и объективные).
3. Формирование “правильной” предустановки, использование заголовков.
4. Использование эгоприманок (фрагмент контента) для привлечения внимания конкретного человека или группы людей и направления информации на нужную аудиторию.
5. Группирование элементов контента по категориям и отсылки к связанным фрагментам, на которых хотят сделать акценты.
6. Создание и продвижение путеводителей по материалам заданной темы.

7. Использование эвфемизмов и приемов генерализации, создание такими единицами вербального уровня, как метонимия (для искажения информации и обезличивания референтов).

8. Любое некорректное (ложное) утверждение можно сопроводить ссылкой (заметкой) о том, что власти (или другие структуры) пока не подтвердили указанный факт.

9. Указание источником искаженных сведений закрытых документов или ссылки на анонимные источники.

10. Для усиления манипуляционного эффекта медиатекста используются графические изображения и/или видео.

К лексическо-фразеологическим средствам, которые могут быть использованы для создания деструктивного контента относятся:

1. Экспрессивно окрашенная лексика, т. е. слова, содержащие в своем лексическом значении отрицательную или положительную эмоциональную оценку предмета речи. В интернет-среде чаще всего в таких случаях используется молодежный или компьютерный сленг.

2. Использование акронимов. Популярность сокращений объясняется тем, что они экономят время (гораздо проще и быстрее написать «спс», чем спасибо), что является важным в условиях живого интерактивного общения.

3. Одним из самых распространенных способов выражения отношения говорящего к чему-либо являются фразеологизмы – устойчивые, лексически неделимые словосочетания, придающие речи яркость и образность. В интернет-общении фразеологизмы рассматриваются в рамках такого явления, как мемы. Принято считать, что пользователь, употребляющий мемы, демонстрирует свою вовлеченность в информационную среду, ведь большинство русских мемов возникают как интернет-реакция на различные социальные, политические и культурные явления современной действительности.

К словообразовательным средствам можно отнести аффиксацию с помощью суффиксов с уменьшительно-ласкательным или уничижительно-пренебрежительным значением и сокращения существующих языковых единиц (примеры: «инет» – «интернет», «акк» – «аккаунт»).

Для выражения различных эмоций используются морфологические средства междометий (хаха, ой, ох, ухфу, фи) и звукоподражания (хнык-хнык, бульк, бац).

Активно используются и синтаксические средства:

1. Парцелляция – расчленение, дробление высказывания, подача информации частями, что свидетельствует, как правило, об эмоциональности, большой взволнованности.

2. Использование эллиптических конструкций – синтаксической фигуры, состоящей в том, что один из компонентов высказывания в речи не упоминается, «опускается» с целью придания тексту большей динамичности; с помощью эллипсиса передается быстрая смена событий, действий, общая динамика сцены, напряженное психологическое состояние автора.

3. Использование повторов (ну прям потеря потерь; обидно, очень обидно) для повышения эмоциональности и усиления акцентов.

Использование поликодовости в тексте с применением многих различных элементов (гибридный, бимедиальный, полимедиальный, мультимедиальный, вербально-визуальный, поликодовый текст) существенно влияют на восприятие текстового смысла. К примерам поликодового текста можно отнести «зачеркнутый текст», который обозначает речь как внутреннюю, с наделением ее при этом определенной коннотацией, а также аудио- или видеоматериалы, служащие для передачи эмоций и настроения.

В целях формирования «правильной» предустановки и повышения спроса на конкретную новость средствами массовой коммуникации, являющимися агентами или коллективными модераторами деструктивного влияния могут придумываться неординарные и провокационные заголовки.

Прагматические типы заголовков зависят от интенциональной установки адресанта:

- фактуальные (передают информацию, эксплицитную по своей природе, транслируют предметно-логическую информацию, и, как правило, без авторских комментариев, оценок, разъяснений);
- персуазивные (содержат умозаключение, выражающее результат осмысления адресантом явлений реальной действительности);
- директивные (директивные заголовки, подобно персуазивным, отражают результат восприятия и осмысления реальной действительности адресантом и отличаются лишь интенцией – стремлением побудить реципиента к совершению конкретных речевых и неречевых действий).

Официальные источники используют первый тип, а оппозиционные – второй и третий типы.

Использование приемов интертекстуальности и интердискурсивности с бесконечными перемещениями, смещениями лиц, голосов, времен, пространств, событий, реальностей и вымыслов дают простор манипулированию информацией.

Исследование характеристик контента на предмет анализа принадлежности авторов к определенному человеческому типу и его влияния на целевую аудиторию нужно проводить по совокупности используемых лексико-стилистических средств с оценкой общего стиля речи, включая выбор слов и построение предложения.

Методы деструктивного воздействия. К основным методам деструктивного воздействия можно отнести:

1. Фабрикация фактов, которая включает в себя следующие приемы:

- замалчивание информации;
- создание информационного шума;
- создание видимости плюралистичности мнений, когда одно и то же событие отражается вроде как по-разному, в то же время выводы делаются одни и те же.

2. Манипулятивная семантика (изменение смысла слов и понятий, важным фактором реализации любого рода манипуляций является воздействие на чувства, а не на разум), которая включает в себя следующие приемы:

- конструирование сообщения из обрывков речей или видео, что меняет смысл сказанного или снятого;

- использование большого количества сложных для восприятия и малознакомых общественности терминов;
- активное использование метафорических лингвистических конструкций;
- разработка и внедрение в информационную среду медиавирусных или лингво-коммуникативных инструментов, создающих информационный повод, призванный с помощью косвенных ассоциаций высветить в подсознании человека тему, которая по какой-либо причине табуировалась, цензурировалась, подавлялась или считалась неприемлемой.

3. Упрощение и стереотипизация, которая включает в себя следующие приемы:

- утверждение и повторение;
- дробление и срочность (информация разделяется на фрагменты, чтобы индивид не смог соединить их в единое целое и у него не хватило бы времени осмыслить проблему);
- сенсационность.

Можно выделить несколько основных стратегий деструктивного воздействия и формирования заданных смыслов:

1. Стратегия размежевания – направлена на выявление противопоставленных друг другу объектов дискурса (расовая, национальная и религиозная рознь).

2. Стратегия позитивной презентации – направлена на представление участников коммуникации в привлекательном виде.

3. Стратегия негативной презентации (дискредитации), в свою очередь, направлена на формирование отрицательного образа объекта, подрыв доверия к нему.

4. Стратегия мобилизации общественного мнения.

5. Стратегия побуждения.

Экспериментальное исследование распространения деструктивного и позитивного контента в социальных сетях российских пользователей. На основе изложенных выше подходов для проведения экспериментального исследования распространения деструктивного и позитивного контента в социальных сетях российских пользователей был разработан набор речевых маркеров для разделения модераторов данного контента и групп пользователей на две группы: «ПАТРИОТЫ» и «ОППОЗИЦИЯ».

По каждой из групп был составлен набор речевых маркеров, которые употребляются в публикациях, комментариях, патриотических и оппозиционных ресурсах.

Для каждого речевого маркера в качестве исходных данных рассчитаны:

- общая частота использования (во всех текстах),
- частоты для каждой группы текстов (патриотических и оппозиционных),
- процент встречаемости данного речевого маркера во всем дискурсе (относительная частота),
- относительные частоты использования для каждой группы текстов (проводится нормировка путем деления частоты речевого маркера на общий объем дискурса в данной группе текстов).

Большие значения абсолютных частот и малые значения относительных частот не позволяют объективно сравнивать преобладание речевых маркеров в том

или ином дискурсе. Необходимо разработать индикатор (систему индикаторов), показывающих преобладание речевого маркера в том или ином дискурсе, а также общий индикатор, позволяющий определять ключевые речевые маркеры, дифференцирующие дискурс групп разной политической ориентации.

В качестве такой системы индикаторов можно использовать следующий набор параметров:

1. Индекс преобладания патриотического дискурса над оппозиционным (Индекс ПО). Рассчитывается как отношение относительной частоты (%) встречаемости речевого маркера в патриотическом дискурсе к оппозиционному. Показывает, во сколько раз данный речевой индикатор преобладает в патриотическом дискурсе по отношению к оппозиционному.

2. Индекс преобладания оппозиционного дискурса над патриотическим (Индекс ОП). Рассчитывается как отношение относительной частоты (%) встречаемости речевого маркера в оппозиционном дискурсе к патриотическому. Показывает, во сколько раз данный речевой индикатор преобладает в оппозиционном дискурсе по отношению к патриотическому.

3. Индекс дифференциации речевых маркеров между дискурсами. Разница между индексами ПО и ОП, возведенная в квадрат и извлечен квадратный корень. Показывает степень расхождения употребимости данного слова в разных дискурсах – патриотическом и оппозиционном. Обычно значимым оказывается размер индекса 1 и более (что соответствует преобладанию в каком-то дискурсе более, чем в 2 раза).

Для понимания количественных тенденций было проведено исследование дискурса патриотов и оппозиционеров в социальных сетях (начиная с 2015 г.).

Было экспертно отобрано более 230 патриотических ресурсов и более 240 оппозиционных ресурсов в социальных сетях. В качестве ресурсов рассматривались открытые страницы и группы, в сетях Facebook (принадлежит компании Meta, признанной экстремистской в Российской Федерации), VKontakte, Life Journal. Было скачано около 100 тыс. сообщений и публикаций в отобранных ресурсах.

Было обработано 35 тыс. самых частотных речевых маркеров и рассчитаны их частотные характеристики. Итоговая база для анализа, содержащая социально значимые и дифференцирующие дискурсы патриотов и оппозиционеров составило более 1,8 тыс. речевых маркеров.

Для определения характерных речевых маркеров был разработан метод дифференциации речевых маркеров характерных для «патриотического» лагеря и «оппозиционного». Представлены ключевые речевые маркеры патриотического дискурса (*табл. 1*) и оппозиционного (*табл. 2*).

Данный подход позволяет провести анализ семантических сетей комментариев пользователей, отнести их к той или иной группе и построить графы взаимосвязей их речевых маркеров и определить характеристики этих графов (коэффициенты посредничества, плотность и т. д.).

Ключевые речевые маркеры патриотического дискурса

№	Речевой маркер	Частота всего	Индекс ОП (доля оппозиции к патри- отизму)	Индекс ПО (доля патриотизма к оппо- зиции)	Индекс диф- ференциации
1	бой	64366	0,099	10,117	10,018
2	донецк	37140	0,119	8,409	8,290
3	танк	42179	0,149	6,691	6,542
4	боевой	67959	0,162	6,166	6,003
5	порошенко	42909	0,169	5,913	5,744
6	ДНР	55316	0,173	5,771	5,598
7	новороссия	41806	0,189	5,299	5,110
8	огонь	40994	0,200	5,010	4,810
9	противник	42848	0,202	4,952	4,750
10	ракета	33553	0,223	4,481	4,258
11	войско	74335	0,246	4,072	3,826
12	армия	93353	0,253	3,951	3,698
13	оборона	42233	0,301	3,327	3,027
14	герой	38318	0,308	3,250	2,943
15	донбасс	72301	0,309	3,236	2,927
16	фронт	37562	0,319	3,131	2,812
17	военный	142767	0,438	2,283	1,845
18	украина	295467	0,482	2,076	1,594
19	американский	79282	0,498	2,007	1,509
20	сила	111356	0,586	1,707	1,121
...	...	...	...	...	...

Ключевые речевые маркеры оппозиционного дискурса

№	Речевой маркер	Частота всего	Индекс ОП (доля оппозиции к патриотизму)	Индекс ПО (доля патриотизма к оппозиции)	Индекс дифференциации
1	суд	34822	4,120	0,243	3,877
2	нефть	25145	3,164	0,316	2,848
3	кремль	21328	3,094	0,323	2,771
4	рубль	47952	3,040	0,329	2,711
5	общество	35268	2,770	0,361	2,409
6	цена	41361	2,756	0,363	2,393
7	выборы	30797	2,743	0,365	2,378
8	сеть	23305	2,504	0,399	2,105
9	акция	25981	2,346	0,426	1,920
10	свобода	28703	2,330	0,429	1,901
11	закон	44680	2,295	0,436	1,859
12	гражданский	31019	2,283	0,438	1,845
13	банк	26569	2,255	0,444	1,811
14	путин	135541	2,083	0,480	1,603
15	компания	40783	2,082	0,480	1,602
16	общественный	26581	2,043	0,490	1,553
17	кризис	28091	1,972	0,507	1,466
18	санкция	42667	1,762	0,567	1,195
19	власть	109463	1,688	0,592	1,096
20	статья	33171	1,634	0,612	1,022
...	...	...	...	...	...

В качестве примера представлено сообщение в одной из групп социальных сетей, относящихся к боевой организации анархо-коммунистов, которая занимается распространением деструктивного контента (рис. 1).

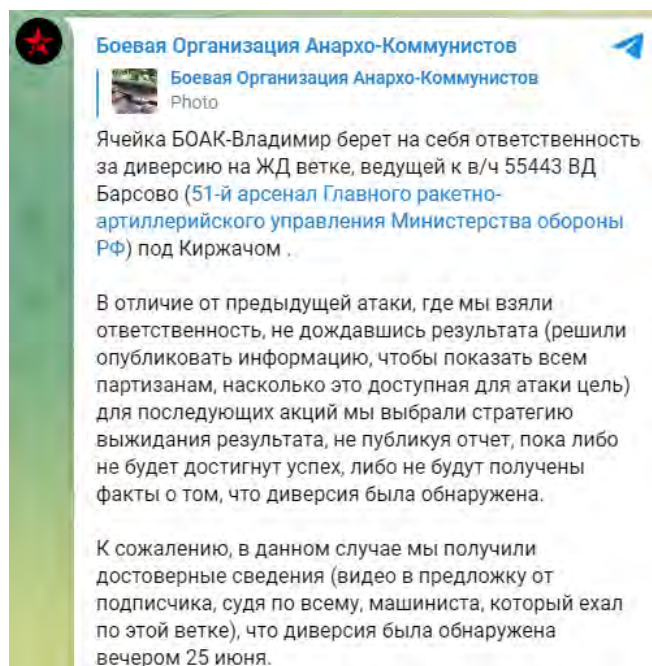


Рис. 1. Пример деструктивного контента, распространяемого в социальных сетях

Анализ данной сети позволяет построить семантический граф ее речевых маркеров (рис. 2).



Рис. 2. Семантический граф речевых маркеров одной из сетей распространения деструктивного контента

Представлена «центральность» некоторых из речевых маркеров семантической сети (табл. 3).

Таблица 3

«Центральность» некоторых из речевых маркеров семантической сети

Node Title	Capability/Semantic Network
жд	0,9933
диверсия	0,9415
рельс	0,9415
акция	0,3646
атака	0,3646
ветке	0,3646
война	0,3646
гайки	0,3646
ответственность	0,3646
результата	0,3646
откручены	0,1589
арсенал	0,0585
барсово	0,0585
берет	0,0585
боак	0,0585
ведущей	0,0585
взяли	0,0585
видео	0,0585
vlадимир	0,0585
вовлечение	0,0585
...	...

Параметры сети (центральность узлов, плотность и т. д.) можно рассматривать как значения элементов вектора, описывающего степень патриотичности, оппозиционности или деструктивности. А сами вектора можно использовать для обучения нейронных сетей при распознавании соответствующих состояний социальных сетей в автоматическом режиме мониторинга или при использовании для этого метода опорных векторов (SVM).

Список использованных источников:

1. Pulipati S. Somula R. Parvathala B.R. Nature inspired link prediction and community detection algorithms for social networks: a survey International Journal of Systems Assurance Engineering and Management. 2021.

2. Cong Tran, Won-Yong Shin, Andreas Spitz Community Detection in Partially Observable Social Networks ACM Transactions on Knowledge Discovery from Data <https://doi.org/10.1145/3461339>.
3. Zhengdao Chen, Lisha Li, and Joan Bruna. Supervised community detection with line graph neural networks. In Proceedings of the 7th International Conference on Learning Representations. ACM. 2019.
4. Till Hoffmann, Leto Peel, Renaud Lambiotte, and Nick S. Jones. Community detection in networks without observing edges. 2020. Science Advances 6, 4 (2020). P. 1–11.
5. C. Gardiner. Stochastic Methods: A Handbook.

Громова А. В.¹,

*начальник управления инженерно-технических
экспертиз ЭКЦ МВД России,
кандидат филологических наук*

Ошкуков С. С.²,

*заместитель начальника отдела фоноскопических,
лингвистических и автороведческих экспертиз
управления инженерно-технических
экспертиз ЭКЦ МВД России*

ПРИМЕНЕНИЕ КВАНТИТАТИВНЫХ МЕТОДОВ В АВТОРОВЕДЧЕСКОЙ ИДЕНТИФИКАЦИОННОЙ ЭКСПЕРТИЗЕ

В целях криминалистической идентификации автора по тексту проводится судебная автороведческая экспертиза, методические основы которой активно разрабатываются 1970-х гг. Объектом идентификационной автороведческой экспертизы является письменная речь, исключая признаки почерка. Развитие информационных технологий формирует новые условия для продуцирования текстов, а также иных форм обмена информацией. В наше повседневное общение прочно вошли приложения для мгновенного обмена сообщениями, за счет этого коммуникация стала более динамичной, а письменная речь приобрела черты разговорной. В связи с этим методы, применяемые в автороведческой идентификационной экспертизе, требуют совершенствования и развития. В статье приведены основные количественные параметры текста и предложен метод идентификации автора текста на их

При расследовании преступлений, носящих дистанционный и опосредованный характер и следами, которых являются тексты интернет-переписки, у органов внутренних дел возникает потребность в установлении автора этих текстов. Данная задача решается в рамках судебной автороведческой экспертизы, которая производится в экспертно-криминалистических подразделениях (ЭКП) системы МВД России более 25 лет [6].

Выделяют две основные группы методов автороведческого исследования:

- качественные (стилистические), основанные на анализе лингвистических характеристик текста (данные методы лежат в основе имеющихся методических рекомендаций по производству автороведческих экспертиз экспертно-криминалистического центра МВД России);
- количественно-статистические (квантитативные), основанные на использовании возможностей автоматизированной обработки данных.

¹ ©Громова А. В., 2022.

² ©Ошкуков С. С., 2022.

Актуальность и научная обоснованность количественных методов исследования определяется развитием корпусной и компьютерной лингвистики, искусственного интеллекта, появление новых методов анализа данных, наличием большого количества научных работ в данной области.

В мировой практике автоматизированной обработки текстов для идентификации авторов к самым простым параметрам текста, поддающимся обсчету, относят количество слов, предложений, слогов, среднюю длину слов, предложений, различного рода *n*-граммы слов и символов и др.

Количественные признаки текста. В целях оценки возможности применения количественных методов в экспертной практике были изучены научные источники, посвященные количественному анализу текстов. В частности, работы, О. В. Загоровской, Т. А. Литвиновой, А. В. Зенкова, А. О. Исхаковой и др., а также работы зарубежных специалистов Upendra Sapkota, Carole E. Chaski, Moshe Koppel, Efsthios Stamatatos и др. [1–14]

В результате анализа источников, а также с учетом экспертного опыта исследования текстов выделены следующие количественные признаки текста: коэффициенты лексического разнообразия (MATTR [2], Jiro [2], Maas [2], Brunet [11], Honore [11], Sichel [11], Simpson [11], Yule [11]), частота предлогов, частота союзов, частота частиц, частота местоимений, индекс прономинализации [1], соотношение глаголов и местоимений к существительным и прилагательным [2], индекс глагольности, индекс субстантивности, индекс адъективности, индекс местоименности, индекс именной лексики, средняя длина слов [5], частота коротких слов (менее 4 символов) [5], частота длинных слов (более 8 символов, более 10 символов), частота служебных слов, частота клавиатурных смайлов, частота графических смайлов (emoji), коэффициент корреляции с законом Ципфа, частота пунктуации.

В качестве признаков *n*-грамм выделены следующие: триграммы слов и пунктуационных знаков (как минимум 1 пунктуационный знак в *n*-грамме), при этом слова заменяются обозначением их грамматических категорий, триграммы слов и пунктуационных знаков (как минимум 1 пунктуационный знак в *n*-грамме), при этом слова заменяются знаком *, триграммы слов и пунктуационных знаков (как минимум 1 пунктуационный знак в *n*-грамме), при этом слова заменяются знаком *, пунктуационный знак заменяется на «PNCT» [1, 13], а также триграммы, полученные путем искажения текста в соответствии с алгоритмами искажения (DVMA, DVSA), предложенными в [14].

Корпус текстов для исследования. Для апробации указанных выше количественных маркеров в ЭКЦ МВД России был собран корпус текстов, состоящий из:

- криминалистически значимые интернет-переписки 45 авторов (мужчин – 30, женщин – 15). На каждого автора 3 и более фрагментов переписок длиной от 1000 символов;
- комментарии на различные новости 27 авторов (мужчин – 7, женщин – 20), имеющих высшее филологическое образование. На каждого автора 2 текста (один положительный комментарий на новость, другой отрицательный) длиной от 1000 символов;

– тексты 21 авторов (мужчин – 11, женщин – 18) из БД RusIdiolect (<https://rusidiolect.rusprofilinglab.ru>), содержащие комментарии на посты, а также переписку в мессенджере длиной от 1000 символов.

Возраст авторов в корпусе составляет от 16 до 53 лет. Общее количество текстов – 940. Общее количество признаков (размер вектора признаков текста), вычисляемых на каждом тексте, составляет 296 (*рис. 1*).

Эксперимент. В дальнейшем на основании модели обучен классификатор (*рис. 2*). На вход модели поступают два текста, а на выходе – вероятность принадлежности текстов одному и разным авторам. Функция расстояния d имеет следующий вид:

$$d = |y_i - y_j|,$$

где y_i – вектор признаков i – текста,

y_j – вектор признаков j – текста.

В качестве классификатора в модели, изображенной на *рис. 2*, выступает полносвязанная нейронная сеть (*FCNN*) со следующими параметрами:

- входной слой – 296 нейронов;
- 1-й скрытый слой – 391 нейрон;
- 2-й скрытый слой – 296 нейронов;
- 3-й скрытый слой – 296 нейронов;
- выходной слой – 2 нейрона;
- функция активации скрытых слоев: LeakyReLU;
- функция активации выходного слоя: Softmax;
- методы регуляризации: L2 и Dropout;
- метод оптимизации: NAdam;
- функция потерь: Crossentropy;
- метод обучения сети: backpropagation.

В ходе обучения классификатора количество сравнений «свой-свой» (сравнения векторов признаков одного автора) – 19710, «свой-чужой» (сравнения векторов признаков разных авторов) – 424443. На *рис. 2* приведен процесс обучения нейронной сети.

Качество работы классификатора, обученного на приведенном выше корпусе текстов, приведено на *рис. 4–6*. Равновероятностная ошибка составила 0,02 (2 %).

Коэффициенты лексического разнообразия:

MATTR - 0.8446
 Maac - 0.0886
 Brunet - 0.8566
 Sichel - 0.0896
 Honore - 0.3915
 Simpson - 0.0069
 Yule - 0.0502

Частоты частей речи:

Частота предлогов - 0.0783
 Частота союзов - 0.0727
 Частота частиц - 0.09
 Частота местоимений - 0.1831

Индекс прономинализации(местоимения : существительные) - 0.9064

Соотношение глаголов и местоимений к существительным и прилагательным - 1.4484

Индекс глагольности - 0.1557

Индекс субстантивности - 0.2055

Индекс адекватности - 0.0324

Частота числительных-прилагательных - 0.00234

Индекс именной лексики (существительных и прилагательных : количество слов)- 0.0572

Индекс аналитичности - 0.24092

Индекс автосемантической - 0.5759

Индекс незначительности - 0.42406

Средняя длина слов - 5.0665

Частота коротких слов - 0.4173

Частота длинных слов - 0.1496

Частота слов длинее 10 букв- 0.0204

Частота структурных слов - 0.5752

Частота клавиатурных смайлов - 0.1391

Частота графических смайлов - 0.272

Коэффициент корреляции с законом Ципфа - 0.9084

Частота пунктуации - 0.0321

Частоты n-грамм деструктурированного текста:

*_*_*	- 0.1272	д_е_т	- 0.0009	з_*	- 0.0002	_)_	- 0	ь_ш_е	- 0.0003
_	- 0.0378	_в_с	- 0.0008	с_е_г	- 0.0006	в_*	- 0.0001	_._в	- 0.0004
_	- 0.0325	ь_*	- 0.0021	_е_г	- 0.0518	_а	- 0.0006	о_з_ь	- 0.0001
_	- 0.0119	_)_	- 0	*_*	- 0.0143	б_ы_л	- 0.0007	з_ь_м	- 0.0001
_	- 0.0109	в_*	- 0.0001	_*	- 0.0018	_в_е	- 0.0007	*_*_*	- 0.0119
,_*	- 0.0015	_а	- 0.0005	_*	- 0.0017	_б_о	- 0.0008	*_*	- 0.0016
_	- 0.0014	б_ы_л	- 0.0006	?_*	- 0.0014	!_*	- 0.0002	*_*	- 0.0013
?_*	- 0.0012	_в_е	- 0.0006	*_*	- 0.0017	у_*	- 0.0013	*_*	- 0.0016
_	- 0.0014	_б_о	- 0.0007	*_в	- 0.0013	б_о_л	- 0.0004	*_*	- 0.0019
в	- 0.0011	!	- 0.0002	*_*	- 0.001	ы_*	- 0.001	*_*	- 0.0009
_?	- 0.0008	у_*	- 0.0011	*_б	- 0.0007	_в_о	- 0.0018	?_*	- 0.0016
_б	- 0.0006	б_о_л	- 0.0004	_	- 0.0011	и_*	- 0.0032	*_*	- 0.0007
_*	- 0.0009	ы_*	- 0.0008	*_*	- 0.0005	*_а	- 0.0	*_*	- 0.0013
*_?	- 0.0004	_в_о	- 0.0015	*_*	- 0.0018	о_л_ь	- 0.0012	_*	- 0.001
_	- 0.0015	и_*	- 0.0027	*_*	- 0.0016	о_т	- 0.0035	*_в	- 0.001
_	- 0.0013	*_а	- 0.0	_в	- 0.0029	_)_	- 0.0003	*_в	- 0.0003
_в	- 0.0024	о_л_ь	- 0.001	в_*	- 0.0013	_б_е	- 0.0004	в_*	- 0.001
в_*	- 0.0011	о_т	- 0.0029	_#	- 0.0008	т_ь	- 0.0044	*_#	- 0.0001
_?	- 0.0001	_)_	- 0.0002	*_*?	- 0.0001	у_д_у	- 0.0004	_*	- 0
#_*	- 0.0003	_б_е	- 0.0003	_#	- 0.0003	б_ы	- 0.0004	*_*#	- 0.0001
*_#	- 0.0001	т_ь	- 0.0037	*_#	- 0.0002	*_б	- 0.0004	_)*	- 0.0013
_)*	- 0.0012	у_д_у	- 0.0003	_)*	- 0.0014	в_с_е	- 0.0007	*_*	- 0.0009
_*	- 0.0	б_ы	- 0.0004	_*	- 0.0	_	- 0.0	*_*	- 0.0006
_	- 0	*_б	- 0.0003	*_*	- 0	_в_р	- 0.0003	а_*_*	- 0.0001
##	- 0.0005	в_с_е	- 0.0006	?_*	- 0.0	!_!_!	- 0.0001	*_*?_*	- 0
?_*	- 0.0	_	- 0.0013	_в_и	- 0.0013	_в_и	- 0.0005	_)*	- 0.0012
#_#	- 0.0004	_в_р	- 0.0003	б_у_д	- 0.0014	*_*	- 0	*_а_*	- 0.0004
_б_у	- 0.0011	!_!_!	- 0.0001	_б_ы	- 0.0013	_а	- 0.0005	?_*_*	- 0
б_у_д	- 0.0012	_в_и	- 0.0004	*_*	- 0	л_ь_ш	- 0.0003	*_*?_*	- 0
_б_ы	- 0.0011	*_*	- 0	т_*	- 0.0025	_*)	- 0.0007	*_*	- 0.0015
_)	- 0	_а	- 0.0004	?_*	- 0.0	_*)	- 0.0002	*_*	- 0.0003
т_*	- 0.0021	л_ь_ш	- 0.0002	?_*?	- 0.0001	*_*!	- 0.0002	*_*_а	- 0.0012
_#	- 0.0003	_*	- 0.0006	а_*	- 0.0037	_*	- 0.0009	в_*_*	- 0.0003
?_*?	- 0.0	*_*!	- 0.0002	_в_о	- 0.0018	_*	- 0.0009	а_*_*	- 0
?_*?	- 0.0001	_*	- 0.0002	_а	- 0.0027	я_*	- 0.0031	*_*_будет	- 0.0001
а_*	- 0.0031	*_*	- 0.0007	?_*?	- 0.0	_в	- 0.0004	_)_	- 0.001
_в_о	- 0.0015	_*	- 0.0007	а_*	- 0.0003	д_у	- 0.0007	*_будет*	- 0.0001
_а	- 0.0023	*_*	- 0.0014	*_в	- 0.0018	_*)	- 0.0016	*_в	- 0
?_*?	- 0.0	я_*	- 0.0026	е_*	- 0.0039	ы_л_о	- 0.0004	*_*_в	- 0.0004
а_*	- 0.0002	_в	- 0.0003	_)_	- 0	_*	- 0	будет*	- 0.0001
*_в	- 0.0015	д_у	- 0.0006	у_д_е	- 0.0012	л_о	- 0.001	_а_*	- 0
е_*	- 0.0033	ы_л_о	- 0.0003	о_*	- 0.0056	в_о_з	- 0.0002	*_б_ы_*	- 0
)	- 0	л_о	- 0.0008	*_а	- 0.0016	е_з	- 0.0003	*_*_а	- 0.0003
у_д_е	- 0.001	в_о_з	- 0.0002	_в	- 0.0007	_*	- 0	_*	- 0
#_#_#	- 0.0001	_*	- 0	_)_	- 0.0025	в_и_д	- 0.0004		
о_*	- 0.0047	е_з	- 0.0003	е_т	- 0.0028	з_*	- 0.0003		
_а	- 0.0014	_	- 0	д_е_т	- 0.0011	с_е_г	- 0.0007		
_в	- 0.0006	в_и_д	- 0.0003	_в_с	- 0.001	м_*	- 0.0015		
)	- 0.0021	з_*	- 0.0002	ь_*	- 0.0025	в_о_т	- 0.0007		
е_т	- 0.0023								

Частоты различных пунктуационных n-грамм:

S_V_? - 0.0019
 A_S_ - 0
 S_S_ - 0
 V_V_? - 0
 S_S_? - 0
 ADV_V_? - 0
 A_S_! - 0
 PR_S_? - 0
 S_V_ - 0.0022
 PART_V_ - 0.002
 PR_S_ - 0
 SPRO_V_? - 0
 V_S_? - 0
 _ - 0.0443
 _? - 0
 _ - 0
 _) - 0
 _ - 0.054
 _ PNCT - 0.1117
 *_ PNCT - 0.11
 PNCT_*_* - 0.1117
 *_ PNCT_PNCT - 0.0178

Рис. 1. Вектор признаков, вычисляемый на тексте

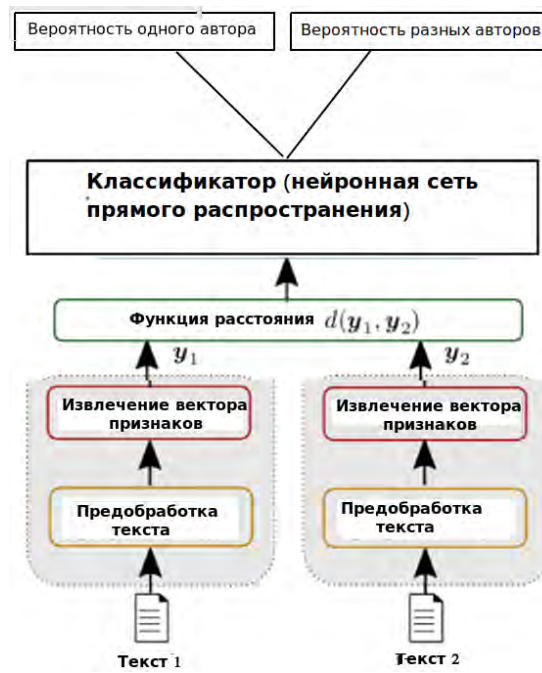


Рис. 2. Модель идентификации автора текстов

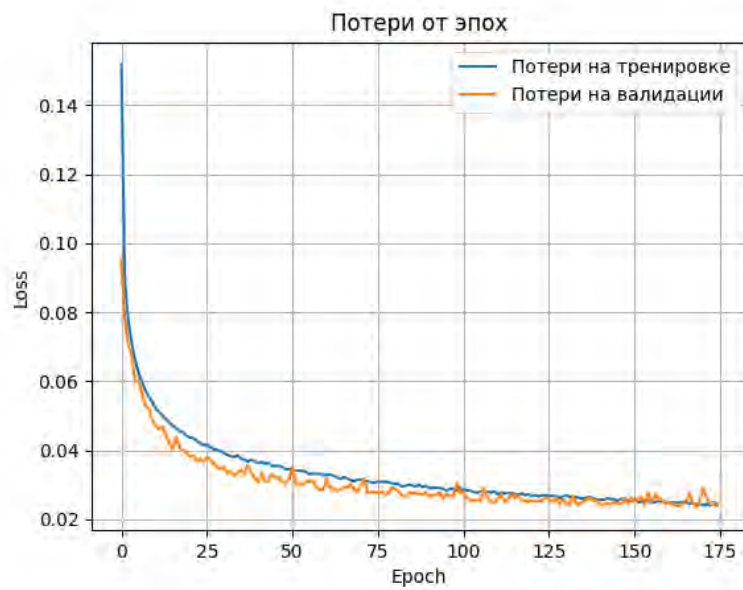


Рис. 3. Процесс обучение классификатора

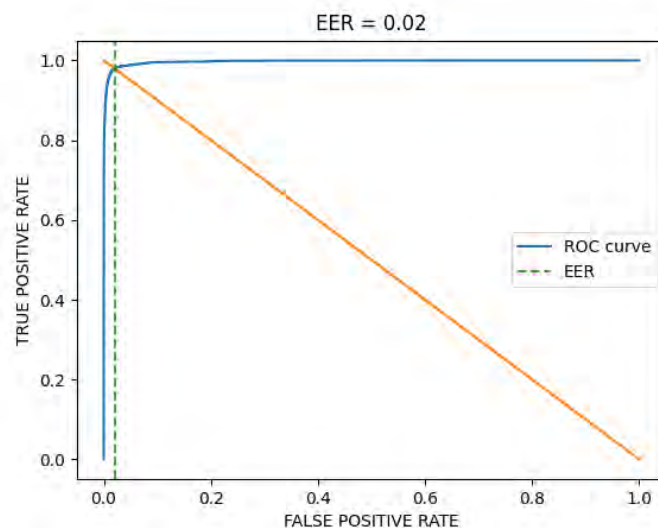


Рис. 4. ROC-кривая (receiver operating characteristic curve) и EER (equal error rate)

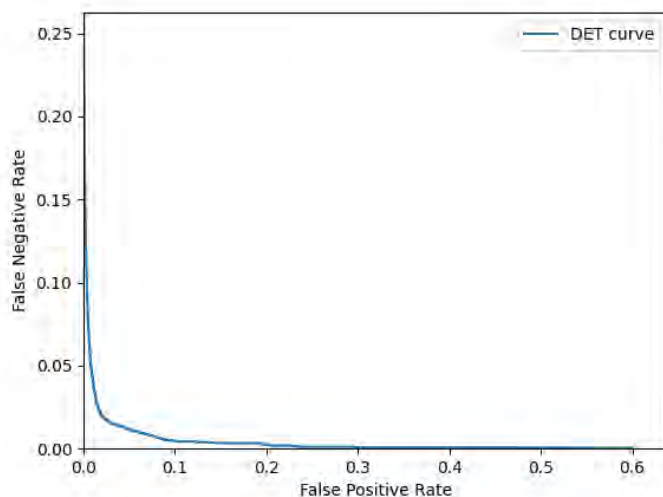


Рис. 5. DET-кривая (detection error trade-off curve)

Таблица 1

Качество работы классификатора

Класс	Precision	Recall	F1-score
«Свой-свой»	0.91	0.91	0.91
«Свой-чужой»	1.00	1.00	1.00

Проведенный выше эксперимент показал, что применение количественных методов в экспертной практике позволит расширить количество признаков, используемых в автороведческом идентификационном исследовании, тем самым повысить объективность данного исследования.

На следующем этапе планируется расширение корпуса текстов и продолжение дальнейших исследований.

Список использованных источников:

1. Диагностирование склонности автора письменного текста к аутоагрессивному поведению / [О. В. Загоровская и др.] // Вестник ВГУ серия: лингвистика и межкультурная коммуникация. 2015. № 3. С. 98–104.
2. Захарова Е. Ю. Лексическое разнообразие текста и способы его измерения // Вестник Тюменского государственного университета. 2020. Т. 6. № 1 (21). С. 20–34.
3. Зенков А. В. Отклонения от закона Бенфорда и распознавание авторских особенностей в текстах // Компьютерные исследования и моделирование. 2015. Т. 7. № 1. С. 197–201.
4. Индивидуально-личностные характеристики автора и количественные параметры его текста: корпусное исследование / [Т. А. Литвинова и др.] // Вопросы психолингвистики. 2015. № 26. С. 98–105.
5. Исхакова А. О. Метод и программное средство определения искусственно созданных текстов : специальность 05.13.17 «Теоретические основы информатики» : диссертация на соискание ученой степени кандидата технических наук. Томск, 2016. 123 с.
6. Литвинова Т. А. Пунктуационные выборы как составляющая ортологического параметра идиолекта носителя современного русского языка в аспекте идентификационной автороведческой экспертизы // Политическая лингвистика. 2019. № 1 (73). С. 114–121.
7. Литвинова Т. А., Громова А. В. Компьютерные технологии в судебной автороведческой экспертизе: проблемы и перспективы использования // Вестник Волгоградского государственного университета. Серия 2, Языкознание. 2020. Т. 19. № 1. С. 77–88.
8. Минаева И. В., Канищева А. В. Закон Ципфа: межстрановой анализ // Экономический анализ: теория и практика. 2018. Т. 17. № 7. С. 1337–1351.
9. Тихомирова Е. А. Статистический анализ в задаче идентификации автора текста, написанного на естественном языке // Наука и Образование. МГТУ имени Н.Э. Баумана. 2017. № 6. С. 131–146.
10. Chaski C. E. Best practices and admissibility of forensic author identification // Journal of Law and Policy. 2013. Vol. 21 (2). P. 333–376.
11. Tweedie, Fiona J. How Variable May a Constant Be? / Fiona J. Tweedie, R. Harald Baayen Measures of Lexical Richness in Perspective // Computers and the Humanities. 1998. Vol. 32 (5). P. 323–352.
12. Koppel M. Computational methods in authorship attribution // Journal of the American Society for Information Science and Technology. 2009. Vol. 60 (1). P. 9–26.
13. Not all character n-grams are created equal: A study in authorship attribution / Sapkota U. [et al.] // Human language technologies: The 2015 annual conference of the North American chapter of the association for computational linguistics. 2015. P. 93–102.

14. Stamatatos E. Masking topic-related information to enhance authorship attribution // Journal of the Association for Information Science and Technology. 2018. Vol. 69 (3). P. 461–473.

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

Научный руководитель:

*Швырев Б. А.,
доцент кафедры специальных информационных
технологий учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат физико-математических наук, доцент*

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ НЕГЛАСНОГО КОНТРОЛЯ WEB-КАМЕРЫ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

На сегодняшний день значительная доля всей эксплуатируемой компьютерной техники оснащается веб-камерами. Это устройство есть во всех без исключения ноутбуках, планшетах и смартфонах. Для многих настольных персональных компьютеров (ПК), которые были приобретены до повсеместного развития видеотехнологий, связанных с Интернет, также докупаются отдельные веб-камеры, чаще всего подключающиеся через USB порт. Такое широкое распространение делает такой объект, как веб-камера, чрезвычайно привлекательным для всякого рода злоумышленников.

Актуальность данного исследования заключается в том, что в настоящее время присутствует стремительное развитие информационно- телекоммуникационных технологий, они широко используются в повседневной, а также рабочей деятельности. С развитием информационной сферы появилось большое разнообразие средств и способов, осуществления несанкционированного получения информации о пользователе, вследствие чего образовалась острая необходимость в обеспечении безопасности пользователей информационной среды.

Целью данной работы является рассмотрение вопроса о возможностях негласного контроля веб-камеры персонального компьютера, применяемом программном обеспечении и соответствующих путях проникновения в компьютерную систему.

Одним из наиболее простых способов снятия информации с веб-камеры является использование API getUserMedia() для современных браузеров, поддерживающих JavaScript. Простота этого языка программирования обуславливает то, что написать соответствующий скрипт для съема информации с веб-камеры может даже начинающий программист. Доступ к камере осуществляется по запросу, и для этого ничего не нужно устанавливать. Сама возможность встроена

¹ © Данилова Е. А., 2022.

в любой современный браузер. Негативным аспектом данного подхода именно для скрытности всего процесса является то, что браузер в самом начале наблюдения, а точнее при подключении камеры, показывает пользователю сообщение о запросе на использование веб-камеры. Но стоит отметить, что данную проблему злоумышленники могут решить с помощью инструментов социальной инженерии, например, злоумышленник связывается с жертвой и сообщает о победе в бесплатной лотерее среди посетителей сайта, где для получения приза надо только позволить сделать свое фото.

Следующей, более продвинутой возможностью по созданию средств негласного использования камеры ПК, является применение одной из универсальных библиотек, связанных с видеонаблюдением или компьютерным зрением. Преимуществом такого подхода является достаточно высокая степень удобства в применении таких средств. Большинство таких библиотек являются высокоуровневыми и не требуют вызова многочисленных команд для настройки веб-камеры и подключения к ней. В качестве конкретного примера можно назвать наиболее популярную библиотеку OpenCV. OpenCV – библиотека алгоритмов компьютерного зрения, обработки изображений и численных алгоритмов общего назначения с открытым кодом, включает следующие компоненты:

- `opencv_video` – анализ движения и отслеживание объектов (оптический поток, шаблоны движения, устранение фона);
- `opencv_highgui` – простой UI, ввод/вывод изображений и видео.

Использование языков общего назначения с применением библиотек для работы с камерой также не слишком сложно с программно-технической точки зрения, хотя и требует больших усилий, чем в выше рассмотренном случае объекта `navigator.getUserMedia()` в языке JavaScript. Однако, важным преимуществом данного подхода является значительно большая гибкость, ведь тут не обязательно использовать браузер в качестве основы.

Получение доступа к веб-камере ПК возможно осуществить с помощью программ, работающих с видеопотоком камеры. Большое количество данных программ допускают скрытый режим работы, т.е. их можно использовать для негласного наблюдения через веб-камеру. Конечно, важной особенностью всех этих программ является необходимость первичного доступа к компьютеру с камерой. Однако, такую установку может провести и сам пользователь, за которым в дальнейшем программа будет следить – для этого необходимо применять методы социальной инженерии. Одними из таких программ является WebcamXP, Хеома, Globoss.

Рассмотрим получение доступа к веб-камере ПК на платформе ОС – Kali Linux. Metasploit Kali Linux – это популярный инструмент, используемый экспертами по тестированию на проникновение. Для подключения к веб-камере ПК необходимо проникнуть в рабочую среду персонального компьютера, для этого может быть использована уязвимость, связанная с протоколом smb. SMB – сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам. В Metasploit Kali Linux необходимо зайти в `exploit`, после чего просмотреть полезную нагрузку, т. е. код или часть вредоносной программы, которая выполняет деструктивное действие. Он запускается на целевой системе после того,

как отработал exploit. Далее злоумышленнику достаточно выбрать необходимую полезную нагрузку, например: `payload/windows/x64/vncinject/reverse_tcp`, она позволяет обеспечить удаленный доступ к графическому интерфейсу ПК. При получении удаленного доступа к ПК появляется возможность беспрепятственно просматривать веб-камеру. Сравнение представленных методов доступа к веб-камере выражено в наглядной форме (табл. 1).

Таблица 1

Сравнение подходов к созданию программ для скрытного наблюдения через веб-камеру ПК

Название /свойства	Использование возможностей JavaScript getMedia	Использование возможностей готовых библиотек (на примере OpenCV)	Использование возможностей программ контролирующие видеопоток камеры	Использование возможностей Metasploit Kali Linux
Степень сложности реализации	Низкая	Средняя	Средняя, возможно сложная, так как необходимо применять методы социальной инженерии	Средняя
Скрытность	Крайне низкая	Средняя	Низкая	Высокая
Гарантия получения информации	Низкая	Средняя	Низкая	Высокая
Количество затраченного времени	Низкое	Среднее	Среднее	Среднее

Проанализируем, представленные технических решений по оценочным показателям (табл. 2). В таблице представлена 3-бальная система оценки, «0» – не соответствует ожиданием; «1» – требует улучшения; «2» – соответствует ожиданиям; «3» – превосходит ожидания.

По приведенным результатам отчетливо видно, что по оценочным показателям Metasploit Kali Linux лидирует на фоне других способов получения доступа к веб-камере ПК. Он является одним из самых сложных в реализации, но при изучении платформы Metasploit возможно получения доступа как к веб-камере ПК, так и рабочего стола ПК, различных ОС.

Перечень программных продуктов, с помощью которых можно проводить негласный контроль веб-камеры ПК достаточно широк, однако основным их режимом работы позиционируется наблюдение за пустой квартирой, за детьми, за постельно больными людьми и т. п.

Анализ использованных методов при помощи оценочных показателей

Название /свойства	Использование возможностей JavaScript getMedia	Использование возможностей готовых библиотек (на примере OpenCV)	Использование возможностей программ контролирующие видеопоток камеры	Использование возможностей Metasploit Kali Linux
Степень сложности реализации	3	2	2	2
Скрытность	0	2	1	3
Гарантия получения информации	1	2	1	3
Количество затраченного времени	3	2	2	2
Суммарный итог	7	8	6	10

Если же говорить об универсальных решениях, то такое ПО должно быть полностью скрытым и маскироваться под системное программное обеспечение компьютера. Механизм распространения такого ПО должен быть родственным компьютерным вирусам; по сути данная программа и должна быть вирусом, основная деструктивная деятельность которого должна быть направлена на получение видеопотока с веб-камеры, подсоединенной к ПК.

Список использованных источников:

1. Georgia Weidman. Penetration Testing: A Hands-On Introduction to Hacking. М. : No Starch Press, 2014. 528 с.
2. Hacking Exposed Web Applications, 3Rd Edition. М. : 2011. 482 с.
3. Поликарпов Е. С. Основы компьютерной разведки. М. : Московский университет МВД России имени В.Я. Кикотя, 2020. 321 с.
4. Эриксон Дж. Хакинг – искусство эксплойта, 2-е издание. М. : High tech, 2009. 510 с.
5. Андрианов В. И. Устройства для защиты объектов и информации. М. : Полигон, 2018. 256 с.
6. Смотри во все глаза. Как взламывают IP- и веб-камеры и как от этого защититься // Хакер – Безопасность, разработка URL: <https://xaker.ru/2017/04/27/hack-cams/>.

Коломина А. С.¹,
 курсант факультета подготовки
 сотрудников в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя,

Научный руководитель:
Аветисян К. Р.,
 старший преподаватель кафедры
 информационной безопасности учебно-научного
 комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,

МЕХАНИЗМ ВЫЯВЛЕНИЯ КЛЮЧЕВЫХ СУБЪЕКТОВ В «ИЕРАРХИЧЕСКОЙ МОДЕЛИ» ДИСКРЕДИТАЦИИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ В СЕГМЕНТАХ СЕТИ ИНТЕРНЕТ

Сложные политические процессы, происходящие в нашем государстве, заставляют задуматься над искусственно создаваемыми и интерпретируемыми событиями, направленными на дискредитацию органов государственной власти в России.

В связи с проводимой СВО на территории Украины, в сегментах глобальной сети все чаще стали всплывать «фейковые» новости о действиях со стороны Российской армии. В виду чего был принят Федеральный закон от 4 марта 2022 г. № 32-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и ст.ст. 31 и 151 Уголовно-процессуального кодекса Российской Федерации».

С этими изменениями в законодатель вводит новое понятие – «дискредитация», а именно «публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан». Из диспозиции статьи можно попробовать дать следующее определение дискредитации – умышленные действия, направленные на подрыв авторитета, имиджа и доверия к кому-либо, умаление его достоинства и авторитета.

Обратимся к ст. 13.15 КоАП РФ «Злоупотребление свободной массовой информации», которая коррелирует со ст. 4 Закона Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации». Здесь говорится что: «Не допускается использование средств массовой информации в целях совершения уголовно наказуемых деяний ... для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань».

¹ © Коломина А. С., 2022.

Однако теперь перед государственными органами появляется новая проблема, а как же выявлять признаки дискредитации?

Для того чтобы разработать механизмы выявления ключевых субъектов в «Иерархической модели» дискредитации органов государственной власти в сегментах сети Интернет выделим следующие признаки дискредитации:

- направленность информации;
- аудитория, на которую направлена информационная акция – «вброс»;
- площадка распространения.

Процедура проверки достоверности сведений занимает определенное время и виду «непрекращающегося» потока информации аудитория не обременяет себя ни анализом распространяемых сведений, ни изучением источника распространения ложной информации.

Целесообразно рассматривать градацию элементов иерархической модели дискредитации государственной власти:

- транснациональный уровень (мировые СМИ, и международные интернет-площадки и др.);
- представители государств, и крупных компаний (Спикеры, руководители корпораций и их официальные представители);
- медийные личности «лидеры мнений».

В настоящее время основная часть населения любой из стран «черпает» актуальную информацию с каналов мессенджеров, сообществ социальных сетей, видео хостингов и т. д. В большинстве случаев люди воспринимают массивы информации по соответствующей тематике без критического анализа поступающих сведений.

Выявлять и анализировать полученную информацию можно посредством нейросетевого классификатора, основанным на семантическом анализе. Все данные полученные из различных источников будут собраны в массив данных для дальнейшего обучения нейронной сети и будут направлены для исследования на предмет дискредитации именно органов государственной власти.

Входные данные для классификатора могут быть собраны при помощи сервисов OSINT. Следует отметить программное обеспечение, используемое для разведки и криминалистики с открытым исходным кодом – Maltego, и применение программных комплексов модульного типа. Посредством которого возможно:

- производить поиск установочной информации по биометрическим признакам;
- исследовать местность по геометкам;
- анализировать сетевой трафик и сетевой адрес;
- проанализировать параметры оконечного сетевого устройства с целью получения геолокаций.

Согласно ст.ст. 21, 38, 73–74, 86 УПК РФ, ст. 26 ФЗ «О связи» № 126 и ст. 26 ФЗ «О банках и банковской деятельности» № 395-1 возможно получить сведения от:

- сотовых операторов;

- интернет-провайдеров;
- кредитных организаций;
- сервисов электронных компонентов;
- сайтов объявлений;
- социальных сетей и др.

Подводя итог, можно сказать, что требуется активное вмешательство в механизмы влияния субъектов, которые дискредитируют государственные органы РФ. Нет никакой абстракции, необходимо осуществлять не пресекающие меры, а превентивные, искоренять на уровне зарождения, основываясь на системном анализе хронологий событий, связей людей, социальных групп. Данные должны анализироваться по определенным ключам, таким как интерпретация событий, потенциал влияния на массовое сознание. Необходимо формирование региональной, государственной повестки, которая будет зависеть от уровня подготовки кадров, специалистов в области информационной безопасности и технического обеспечения.

Список использованных источников:

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34661/.
3. Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 (ред. от 14.07.2022) «О средствах массовой информации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_1511/.
4. Федеральный закон от 4 марта 2022 г. № 32-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_410887/.
5. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_43224/.
6. Федеральный закон «О банках и банковской деятельности» от 2 декабря 1990 г. № 395-1 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_5842/.

Андреев И. В.¹,
курсант факультета подготовки
сотрудников в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Лустин В. И.,
старший преподаватель кафедры
информационной безопасности
учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

ВИРТУАЛЬНАЯ И ДОПОЛНЕННАЯ РЕАЛЬНОСТЬ В ОВД

На сегодняшний день использование технологии виртуальной и дополненной реальности (VR и AR) в органах внутренних дел Российской Федерации (далее – ОВД РФ) имеют большую перспективу применения в профессиональной деятельности.

Общепринятое определение виртуальной реальности – это созданный техническими средствами мир, передаваемый человеку через его ощущения: зрение, слух, осязание и другие. В свою очередь, виртуальная реальность (VR – англ. virtual reality, далее – VR) – создаваемая при помощи компьютерных вычислений трехмерная среда, в которой пользователь может взаимодействовать с ней при помощи специальных манипуляторов, также он полностью или частично погружается в эту среду. Принципы работы данной технологии основаны на помещении человека в симуляцию посредством полноценного или частичного погружения его сознания в имитацию реального мира. Человек оказывается в таком мире при помощи применения очков виртуальной реальности, основой действия которых является проецирование изображения с эффектом трехмерной графики. Для полного погружения также могут использоваться специальные средства – качественное реалистичное звуковое сопровождение взаимодополняет видеокартинку и погружение человека в 3D-пространство; встроенные датчики – гироскоп и акселерометр, они нужны для отображения действий человека в компьютере и взаимодействия с предметами виртуального мира, при изменении положения головы, например, поворот или наклон меняется изображение в очках VR в то направление, куда смотрит пользователь.

Дополненная реальность (англ. augmented reality, AR – «расширенная реальность», далее – AR) – технология, при помощи которой, компьютер или другое устройство, добавляет в окружающий мир объекты цифровой среды, с которыми

¹ © Андреев И. В., 2022.

технологии могут как привносить в реальный мир виртуальные данные. AR ограничивается лишь возможностями устройств и программ. В основе работы AR лежит проецирование виртуальных объектов на реальное окружение, это достигается благодаря видеокамере и устройству вывода изображения, например, смартфон с предустановленным обеспечением, которое позволяет пользователю работать с дополненной реальностью, также наиболее развивающаяся технология очки дополненной реальности.

Система виртуального и дополненного мира предоставляет широкие возможности применения в деятельности сотрудников ОВД. Наиболее простое представление использования – обучение работников и развитие профессиональных качеств. Так VR делает обучение более интерактивным и позволяет помещать пользователя в различные случаи, которые могут моделировать трудные для воспроизведения в реальном мире ситуации, при тренировке которых человек может нанести себе вред. Немаловажную роль в подготовке сотрудника ОВД играет морально-психологическое воспитание. В критических ситуациях он должен оперативно принимать решения, которые могут повлиять на исход [1]. Обучение на основе прочтения лекции занимает основное место в системе образования, но лекция не может предоставить человеку реальную симуляцию, предоставляющую разнообразные виды ситуаций и вариантов их решений. На сегодняшний день технологии VR достигли такого уровня, что могут предоставить сотрудникам эффективную базу для подготовки профессиональных качеств.

Основные причины использования VR в системе обучения:

- способность настраивать различные обстоятельства виртуальной симуляции, которые могут полностью моделировать реальные конфликтные ситуации;
- каждое задание можно отрабатывать многократно, отмечая ошибки при выполнении и мгновенно корректировать неправильные действия сотрудника;
- контролируемая и безопасная среда обучения;
- улучшение профессиональных качеств сотрудников ОВД;
- наличие психологического воздействия, которое влияет на оттачивание навыков и применение правильных решений;
- возможность в перспективе, получения физиологического отклика организмом при помощи специальных костюмов, перчаток с обратной связью.

Выделим преимущества использования VR для подготовки сотрудников ОВД:

- погружение в виртуальный мир, за счет использования VR-шлемов, которые ограничивают пользователя от реального мира тем самым дают эффект погружения;
- достижение и отработка поставленных задач обучения;
- создание различных условий симуляции, которые могут встретиться сотруднику при несении службы.

Несмотря на все достоинства данной технологии, ее распространение на современном этапе невелико. Необходимо привлечение дополнительных средств для финансирования сферы VR в системе подготовки сотрудников ОВД.

Наряду с плюсами VR имеет и недостатки:

- ограниченность из-за привязки пользователя к компьютеру (есть технологии беспроводной связи или шлемы VR с собственной вычислительной мощностью, однако для полного погружения они не могут быть использованы так как качество графики и трекинга не позволяет эффективно использовать в подготовке сотрудников);

- нахождение в виртуальной среде не позволяет получить эмоционального отклика;

- большая стоимость оборудования для полного снабжения образовательных учреждений;

- нахождение в шлемах VR ограничено по времени, из-за воздействия на человеческий мозг может привести к симптомам схожим с морской болезнью, также VR влияет на зрение.

Использование AR технология в учебном процессе позволит облегчить работу сотрудников при патрулировании и выявлении преступников в большом скоплении людей. Приложение для распознавания лиц в очках дополненной реальности основано на действии нейросетей. С их помощью может осуществляться идентификация, что в совместной работе с базами данных МВД России может выявить преступника. Данная технология тестировалась во время проведения Чемпионата Мира по футболу 2018 г. на территории стадионов, были установлены видеокамеры с модулем распознавания лиц, подключенный к ГИС ЕЦХД. Были выданы сотрудникам специальные смартфоны, с предустановленным программным обеспечением. При идентификации видеокамерой лица из баз данных, на устройства полицейских приходило уведомление. Итогом такого тестирования стало задержание около 100 лиц, которые числились в базах правоохранительных органов [2]. В перспективе имеется возможность соединить технологию распознавания лиц и AR устройства. Очки дополненной реальности позволят сотрудникам полиции более эффективно осуществлять охрану общественного порядка.

В основе использования технологий VR и AR в деятельности ОВД лежит Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 21.12.2021) «О полиции», а именно ч. 1 ст. 11, которая гласит: «полиция в своей деятельности использует достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру» [3]. В свою очередь необходимо дальнейшее развитие законодательства, регулирующего саму виртуальную среду и способы ее применения в ОВД.

Дополненная и виртуальная реальность имеет перспективу распространения в ОВД, но для этого нужно сформировать базу, которая позволит распространить большинство подразделений системами обучения сотрудников на основе VR. Наряду с этими технологиями очки дополненной реальности позволят увеличить эффективность работы сотрудников МВД России для идентификации лиц в большом массиве. Таким образом, современные технологии имеют всевозрастающую роль в работе ОВД, и их совершенствование является основополагающим критерием развития данной сферы в Российской Федерации.

Список использованных источников:

1. Грязнов С. А. Использование технологии виртуальной реальности при подготовке сотрудников правоохранительных органов // Вестник Самарского юридического института. 2021. С. 101–105.
2. Московские полицейские получают очки с технологией распознавания лиц // Сайт «RB.ru». URL: <https://rb.ru/news/moscow-police/>.
3. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_11016.

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

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОТ УТЕЧКИ ПО ОПТИКО- ЭЛЕКТРОННОМУ КАНАЛУ

Анализ текущего состояния преступности в сфере информационных технологий позволяет сделать вывод о стремительном развитии средств, методов, доступности технологий для совершения противоправных деяний. Для большого количества организаций одним из важнейших является вопрос обеспечения должным образом защиты информации. На период 2021 г. специалистами компании в области защиты от утечек информации, а также предотвращения внешних целевых атак «InfoWatch», приведены статистические данные по количеству утечек из муниципальных, государственных и коммерческих организаций – зафиксировано 2395 утечек данных [2]. В предыдущие периоды (2018–2020 гг.) наблюдался рост количества зарегистрированных внешних и внутренних утечек информации, имеющих умышленный характер. Ввиду растущих угроз безопасности стоит обратить внимание на возможные каналы утечки информации, для предотвращения потерь.

Защита информации является серьезной проблемой, так как злоумышленники используют информационные технологии как инструмент для совершения преступлений. В свою очередь, использование информационных технологий для сбора, хранения, обработки, передачи и представления сведений стало неотъемлемой частью успешной деятельности органов внутренних. Оптимизация информационных процессов, автоматизированный анализ больших массивов информации, а также оперативный доступ сотрудников к распределенным информационным ресурсам способствует эффективному выполнению служебных обязанностей.

За счет автоматизации целого ряда информационных процессов сотрудники освобождаются от рутинных, трудоемких операций и могут основное время посвятить аналитической работе, повышению профессиональных навыков и дальнейшему совершенствованию своей деятельности. В настоящее время в органах и подразделениях МВД России активно внедряются новые технологии, обеспечивающие связь с Единой системой межведомственного электронного взаимодействия (СМЭВ). Данная система включает в себя информационные базы данных, содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа и взаимодействия с другими информационными системами и электронными ресурсами [1].

¹ © Лустин В. И., 2022.

Ввиду многообразия, важности задач, выполняемых ОВД, а также обработки большого количества информации в ходе их выполнения, возникает потребность в обеспечении сохранности этих данных, а также организации ее передачи наиболее быстрым способом. В настоящее время наиболее используемым источником передачи информации является оптико-электронный канал. Под оптико-электронным каналом понимается использование технических средств, преобразующих электрический сигнал в оптический и наоборот, а также непосредственно использование оптоволоконных сетей связи и его компонентов. Актуальность использования данного способа организации связи заключается в наличии следующих преимущественных характеристик:

- пропускная способность до 10 Гбит/с или более;
- высокая помехоустойчивость, заключающаяся в отсутствии искажения информации в сегменте сети при нахождении рядом с линиями электросвязи, а также отсутствие возможности несанкционированного подключения к сети без физического ее разрушения;
- широкий температурный диапазон не влияющий на работоспособность;
- возможность использования цельного, большого сегмента сети (данная характеристика обуславливается весьма малым затуханием в оптоволокне);
- малый вес проводника;
- долговечность использования;
- приемлемая закупочная цена проводника ввиду технологических особенностей производства [3].

Однако, в силу появления новых технологий и способов осуществления несанкционированного доступа существует необходимость в создании новых методических рекомендаций по защите оптико-электронного канала, а также доработка существующих требований:

1. Систематическое проведение мониторинга состояния целостности кабеля, а также сигналов, циркулирующих вблизи него. Для достижения данного результата необходимо использование оптоволокна в состав которого будут входить специальные волокна, благодаря которым будет осуществляться наблюдение состояния кабеля. Конечно, при внедрении такой технологии в состав оптоволокна, цена кабеля будет значительно выше, однако в случае несанкционированного доступа к такой сети связи и изгибах кабеля будут происходить потери контролирующего сигнала и, как следствие, отправка тревожного сигнала о неполадках в работе в систему мониторинга.

2. Периодическое проведение замеров величины оптически значимой мощности. В процессе работы оптоволоконной сети связи может осуществляться мониторинг уровня оптически значимой мощности. Если величина сигнала будет отличаться от выставленного нормального значения, то система контроля выдаст сигнал тревоги. Однако существует необходимость в проведении соответствующей кодировки сигнала, так чтобы в волокне присутствовал постоянный уровень сигнала, не зависящий от наличия передаваемой информации.

3. Использование оптических рефлектометров. Поскольку подсоединение к волокну забирает часть оптического сигнала, для обнаружения подключений могут использоваться оптические рефлектометры.

4. Использование специальных структур в оптическом волокне. Волокно данного вида имеет низкие потери при процессе передачи данных, а также большой радиус сгиба. В структуру данного вида волокна будут входить фотонные кристаллы, которые составляют фотонно-кристаллические световоды. Большая гибкость в фотонно-кристаллическом виде волокна достигается наличием точечного дефекта в центре симметрии. В основном, при создании проводника используют кварц или песок, а также полые места с воздухом. Некоторое количество таких отверстий может быть заполнено иными жидкими или газообразными веществами, а также жидкими кристаллами. Поэтому за счет наличия таких характеристик, при прохождении пучка света, менее влияют на состояние попытки вытягивания или перекручивания кабеля.

5. Использование шифрования. Несмотря на то, что использование алгоритмов шифрования защищает информацию на программном уровне, а не на физическом, то есть никак не сможет пресечь попытку подключения к сети, однако, повлиять на целостность самой информации может прямым образом, тем самым в случае утечки расшифрованные данные могут иметь минимум полезного содержания.

Список использованных источников:

1. Информационные технологии управления и организация защиты информации : курс лекций / [В. А. Апульцин и др.]. М. : Академия управления МВД России, 2021. 72 с.
2. Аналитический отчет «Россия: утечки информации ограниченного доступа, 2021 год» // Сайт Акционерного общества «ИНФОВОТЧ». URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_Мир_Утечки_2021/.
3. Коротун В. Волоконно-оптический кабель: назначение, конструкция, классификация // Сайт «ASUTPP – заметки электрика». URL: <https://www.asutpp.ru/volononno-opticheskiy-kabel.html/>.
4. Манжос А. С., Дергаус Б. К. Преимущества оптоволоконных линий связи и эффективные пути развития систем телекоммуникаций в оборонной промышленности : статья в сборнике трудов конференции // Научная электронная библиотека elibrary.ru. URL: <https://elibrary.ru/item.asp?id=24090817>.

Миляев Г. А.¹,
курсант факультета подготовки
сотрудников в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Лустин В. И.,
старший преподаватель кафедры
информационной безопасности
учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

КОМПЬЮТЕРНАЯ ЭКСПЕРТИЗА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ

В настоящий момент актуальным остается тот факт, что общество все чаще сталкивается с террористическими проявлениями в информационном пространстве и с применением преступниками информационных технологий. Таких преступников называют взломщиками, которые имеют в своем арсенале большой круг способов для таких незаконных проявлений как: завладение персональными данными, распространение персональных данных дискредитация органов государственной власти и органов местного самоуправления. Отдельно хочется сказать о дискредитации органов власти, ведь на данный момент совершается огромное количество «вбросов» ложной информации как лицами из-за рубежа, так и лицами на территории нашей страны, распространение фейков. Большинство таких преступлений совершается посредством использования информационных технологий, на что МВД России обращает пристальное внимание и быстро пресекает такие деяния.

Помимо этого, преступники имеют широкий спектр технологий для защиты собственных устройств, с которых совершаются преступные деяния, а также накопительных устройств, на которых хранится вся информация.

Когда преступник был обнаружен правоохранными органами или в отношении него имеются веские причины полагать, что именно это лицо совершило преступление, то в отношении него проводятся мероприятия по пресечению противоправных деяний. Однако, в таких ситуациях правоохранные органы не могут быть полностью уверены в виновности лица потому что им нужны вещественные доказательства о виновности этого лица.

Для установления факта совершения преступления с применением информационных технологий правоохранные органы МВД России используют несколько видов компьютерной экспертизы, которая помогает получить доступ

¹ © Миляев Г. А., 2022.

и выявить, совершались ли преступные действия с данного конкретного устройства, а также получить полную информацию с накопительного устройства. Рассмотрим основные виды таких экспертиз.

Информационно-компьютерная экспертиза. Данный вид экспертизы является довольно трудным и трудоемким процессом и заключается в полномасштабном изучении экспертом того как хранятся данные на данном устройстве или носителе информации, каким способом организуется хранение данных. Также она включает в себя установление содержания закодированных файлов, типов файлов, истории действий за определенный период. В ходе проведения экспертизы можно узнать, есть ли на компьютере средства защиты от несанкционированного доступа и для каких файлов, и какого содержания эти средства применяются, и какие программные продукты и средства хранятся и используются на компьютере и каково их назначение. Эксперт может установить то, каков был изначальный вид данных и подробная информация об их использовании. Помимо этого, информационно-компьютерная экспертиза позволяет установить связь между произошедшими событиями, определенными процессами и действиями, совершенными на компьютере.

По результатам информационно-компьютерной экспертизы правоохранные органы получают полное и широкое представление об информации на устройстве и на носителях информации, а также могут установить виновность подозреваемого лица. Однако, по этим результатам невозможно определить, кем именно с данного устройства были совершены противоправные деяния. Например, злоумышленник мог использовать систему удаленного доступа для управления устройством настоящего владельца, прикрыв свою незаконную деятельность [1].

Компьютерно-сетевая экспертиза. Этот вид компьютерной экспертизы направлен на нахождение и комплексное изучение действий лица, совершенных в сети Интернет, а также на исследование информационных следов, которые оставил пользователь. В ходе данного компьютерного исследования эксперт изучает взаимодействие пользователя с сетью и то, какими информационными пакетами происходил обмен в сети, и каким образом это было устроено. Помимо этого, в ходе компьютерно-сетевой экспертизы эксперт решает такие задачи как накопители данных взаимодействовали с сетью. Ими могут быть как внешние, так и внутренние накопители данных. Однако основой уклон эксперта в данной ситуации направлен на изучение действий пользователя в сети, ведь чаще всего террористы и экстремисты совершают незаконное распространение вредоносных программных обеспечений, которые они могут использовать для неправомерного доступа к различному роду данных других пользователей сети или шпионажу [2].

После завершения всего процесса компьютерно-сетевой экспертизы, правоохранные органы получают полный отчет о действиях лица совершенных в сети и могут дать правовую оценку действиям лица, а также использовать результаты этой экспертизы как доказательство виновности лица [3].

Компьютерная экспертиза дает широкий спектр информации для противодействия терроризму и экстремизму в информационной среде. Борьба с информационным терроризмом должна вестись по всем направлениям и роль компьютерной экспертизы в этой борьбе является довольно высокой, так как может подтвердить или устранить виновность лица.

Список использованных источников:

1. Информационно-компьютерная экспертиза // Сайт «Судебный эксперт». URL: <https://sudexpa.ru/expertises/informatcionno-kompiuternaia-ekspertiza/>.
2. Компьютерно-сетевая экспертиза // Сайт «RTM-group». URL: <https://rtm-tech.ru/services/setevaya-ekspertiza/>.
3. Компьютерно-сетевая экспертиза // Сайт «Судебный эксперт». URL: <https://sudexpa.ru/expertises/kompiuterno-setevaia-ekspertiza/>.
4. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // СПС «Консультант-Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_31871/.
5. ГОСТ Р 57429-2017 Судебная компьютерно-техническая. Термины и определения от 1 сентября 2017 г. // АО «Кодекс». URL: <https://docs.cntd.ru/document/1200144960>.

Сизоненко А. Б.¹,
начальник кафедры Краснодарского
высшего военного училища
имени генерала армии С.М. Штеменко,
доктор технических наук, доцент

Титарев А. О.²,
слушатель магистратуры
Краснодарского высшего военного училища
имени генерала армии С.М. Штеменко

Рудь И. С.³,
слушатель магистратуры
Краснодарского высшего военного училища
имени генерала армии С.М. Штеменко

МОДЕЛЬ УПРАВЛЕНИЯ РЕСУРСАМИ В СОЦИОТЕХНИЧЕСКИХ СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ОСНОВЕ ТЕОРИИ МАССОВОГО ОБСЛУЖИВАНИЯ

Рассмотрена проблема администрирования безопасности сложных и/или больших информационных систем (далее – СБИС) как отдельная составляющая проблемы управления правами доступа пользователей в информационным ресурсам (ИР) в информационных системах (ИС). Предложен вариант представления процесса управления правами доступа через математическую модель системы массового обслуживания.

В настоящее время информационные технологии при непосредственном взаимодействии с человеком все больше рассматриваются с точки зрения социотехнических систем, содержание которых составляют люди как активные субъекты, обладающие определенными биопсихосоциальными качествами [1].

Проблема качественного и эффективного администрирования средств защиты информации все больше требует введения такого термина как социотехническая система защиты информации (далее – СТС ЗИ).

Под СТС ЗИ будем понимать – такой элемент техногенной среды, которая являясь одной из подсистем социальной организации, в которой с одной взаимодействующей стороны выступает технико-технологическая база комплексной системы защиты информации, а с другой администраторы безопасности информации, со всем набором характеристик как у отдельной социологической группы.

Важность функционирования информационных систем колеблется от критичности ее для одного отдельно взятого человека до общества или государства. Следовательно, такие системы нужно защищать.

¹ © Сизоненко А. Б., 2022.

² © Титарев А. О., 2022.

³ © Рудь И. С., 2022.

Об актуальности безопасности информации указывается в Доктрине информационной безопасности Российской Федерации, утвержденной указом президента Российской Федерации от 5 декабря 2016 г. № 646, где сказано, что информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [2].

Одним из элементов обеспечения безопасности информации является применение технических мер, а именно использование средств защиты информации, в том числе управление функциями защиты информации, встроенными в информационные (автоматизированные) системы (здесь и далее по тексту под средствами защиты информации (СЗИ) – будут пониматься средства защиты информации, а также функции защиты информации в информационных системах, в том числе механизм разграничения доступа в таких ИС).

Условно применение СЗИ можно разделить на следующие этапы: выбор СЗИ; установка СЗИ; эксплуатация (администрирование) СЗИ.

Безусловно каждый из этих этапов важен для обеспечения информационной безопасности (ИБ) в ИС, но в этой статье будет сделан больше упор на администрирование СЗИ в части управления учетными записями и разграничения правами доступа пользователей к ИР (далее – УПД).

Рассматривая администрирование СЗИ мы видим, что данный процесс неразрывно связан с влиянием человеческого фактора, так как идет управление вида субъект-человек на объект-компьютер[3–6]. При этом основное свое внимание авторы данных исследований направляют на влияние человеческого фактора в ИБ с точки зрения влияния недобросовестных сотрудников (пользователей) компании, на проблемы работы самих администраторов безопасности информации почти не уделяется должного внимания.

Администрирование СЗИ представляет собой сложный и многослойный процесс, сложность которого зависит от множества факторов и параметров. Например, таких как: архитектура, сложность и размерность самой ИС; архитектура, сложность и размерность применяемых СЗИ; количество ИР и вариантов прав доступа к ним; характеристики самого администратора ИБ (количество администраторов ИБ; их компетентность; их моральная, психологическая и физическая выносливость соответствующих нагрузок; их мотивация; благоприятные условия работы).

Формализуем все влияющие факторы на администрирование СЗИ:

$$Dif\_IS = Counts \times Rules \times Config,$$

где Counts – это множество включающее в себя количество пользователей и элементов доступа;

Rules – количество разновидностей прав доступа к ИР;

Config – «коэффициент сложности администрирования», учитывающий сложность назначения того или иного права доступа, а также компетентность администратора.

При назначении прав доступа в нескольких ИС, Dif_IS умножается еще на количество этих ИС.

Данная формула позволяет нам при построении математической модели УПД на основе теории массового обслуживания эмитировать очередь прохождения заявок на предоставление доступа к ИР и администрирования СЗИ в целях предоставления таких прав.

Если построить структурную схему системы массового обслуживания (СМО) в администрировании СЗИ в части управления правами доступа, то получим следующее (рис. 1):

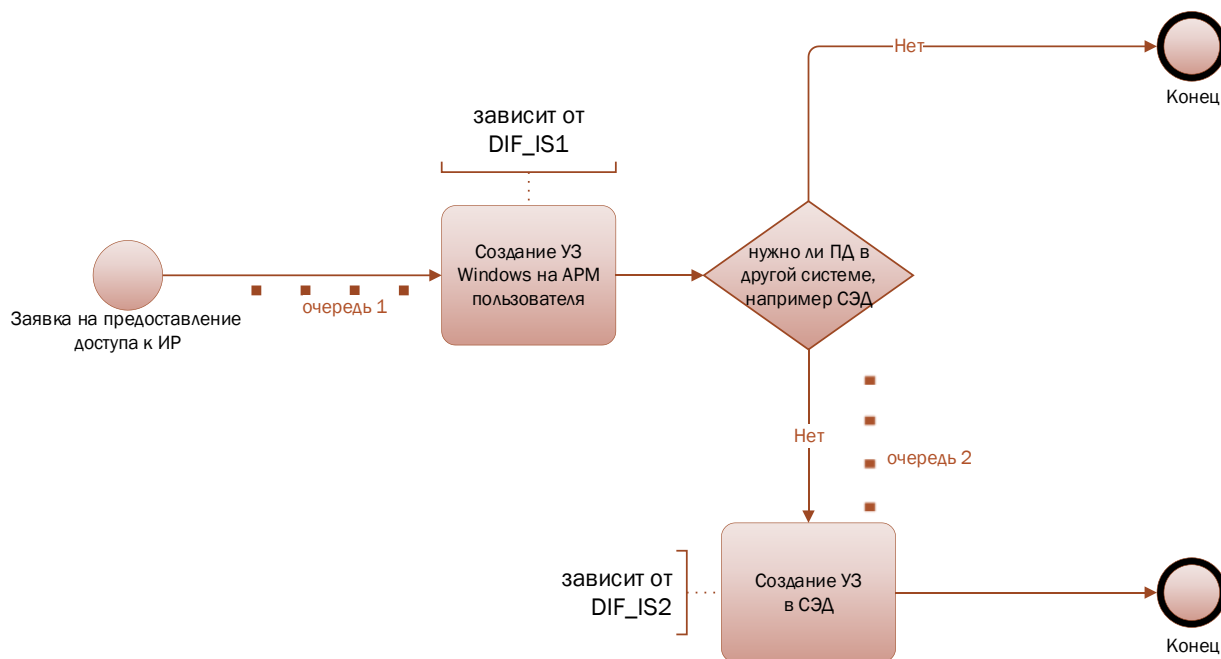


Рис. 1. Структурная схема СМО для УПД

Если построить такую математическую модель и с помощью специального программного обеспечения осуществить множество экспериментов, то можно выявить при каких значениях в формуле (1) наступает критический момент, не позволяющий администрировать СЗИ с надлежащим качеством. Однако определение таких параметров «критичности» является целью дальнейших исследований.

На данный момент проблема влияния человеческого фактора на безопасность информации ИС в части администрирования СЗИ не находит широкого научного изучения. Тем не менее именно от действия администратора зависит качественное и эффективное управление СЗИ, следовательно, и функционирование всей системы защиты информации ИС в целом. При этом администратор ИБ как человек имеет ряд свойственных ему характеристик, влияющих на обеспечение ИБ (компетентность, усталость и т. д.).

Рассматривая администрирование СЗИ в части УПД, мы видим, что при значительных нагрузках администратор ИБ не справляется с поставленными задачами, и они копятся как снежный ком. Например, когда выполнение заявки на предоставление ПД требует более 24 ч., а на следующий день уже приходит новая заявка. В подобных ситуациях снижается качество администрирования СЗИ и повышается вероятность ошибки при назначении прав доступа.

Предложенная математическая модель УПД СМО представляет возможность оценить реальную нагрузку на администратора безопасности и принять решение о поиске решений в целях ее снижения (пересмотр и перестройка системы назначения прав доступа, применение средств автоматизации УПД и т. д.).

Список использованных источников:

1. Социотехническая система как современная форма взаимодействия человека и техники // Сайт «Киберпедия». URL: <https://cyberpedia.su/15xa899.html>.
2. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_208191/.
3. Шаханова М. В., Ле Тхи Ф. Х. Разработка комплексной системы инженернотехнической защиты информации на предприятии // Инновации. Наука. Образование. 2020. № 14. С. 406–411.
4. Маркова Д. Г. Человеческий фактор в информационной безопасности // Известия тульского государственного университета. Технические науки. 2018. № 10. С. 149–152.
5. Жигулин Н. Д., Чеснокова А. А. Проблема человеческого фактора при построении КСЗИ в коммерческой организации // Информационные технологии в моделировании и управлении: подходы, методы, решения : сборник докладов III Всероссийской научной конференции с международным участием. Тольятти, 2021. С. 33–39.
6. Лутфуллина А. Р. Человеческий фактор в системе защиты информации // Неделя науки СПбПУ : материалы научной конференции с международным участием. СПб. : Институт промышленного менеджмента, экономики и торговли, 2018. С. 140–142.

Кудряков Д. Д.¹,
 курсант факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Галиев Д. В.
 преподаватель кафедры информационной
 безопасности учебно-научного
 комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя

ДЕАНОНИМИЗАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПИРИНГОВЫХ СЕТЕЙ

В современных реалиях многие преступления совершаются посредством использования пиринговых сетей, а также onion браузеров, которые позволяют преступникам совершать незаконные действия оставаясь незамеченными. Система работы i2p и p2p сетей не позволяют сотрудникам ОВД напрямую видеть пользователей, которые совершают то или иное действие.

Одной из важнейших проблем деанонимизации пользователей является постоянное совершенствование ПО, а также повышение безопасности протоколов передачи в p2p сетях.

Особое значение в разрешении складывающейся проблематики имеет формирование высококвалифицированных кадров в правоохранительных органах, разработка фундаментальных учебно-методических пособий, рекомендаций по раскрытию противоправных действий, совершаемых в сети Интернет.

Большинство криминальных сделок и незаконного контента в настоящее время располагается в пиринговых сетях. Благодаря анонимности использования p2p многие преступления остаются не выявленными, а лица, их совершившие, не привлечены к ответственности. Ввиду чего деанонимизация злоумышленников, и расследование преступлений, совершенных в пределах пиринговых сетей, остается актуальной для науки и практики темой.

Одним из наиболее популярных средств распространения нелицензионного и запрещенного контента в интернете является многофункциональный кроссплатформенный торрент-клиент для скачивания и раздачи файлов «Utorrent», за счет своего преимущества в скорости и доступности скачивания практически любого контента, для размещения которого необходимо лишь создать определенный торрент-клиент или magnet ссылку. Для пиринговых клиентов раздачи файлов характерно распределенность сети, в которой каждый пользователь является как клиентом, так и сервером для раздачи, благодаря этому отсутствуют очереди на загрузку, а файлы передаются определенными сегментами с разных

¹ © Кудряков Д. Д., 2022.

точек. Система распределяет требуемые сегменты между пирами, чтобы они могли обмениваться недостающими частями файла, при этом большинство данных об ip адресах и передаваемых ресурсах передается в открытом виде, что позволяет их собирать и использовать в целях деанонимизации пользователя.

Для деанонимизации пользователя, пользующегося torrent-трекерами, необходимо отследить его ip. Сделать это можно различными способами, некоторые из которых перечислены в данной статье. Можно воспользоваться сервисом, [iknowwhatyoudownload](#), который по заданному ip может определить большинство публичных торрентов, который данный пользователь качал. Далее необходимо доказать причастность пользователя и получить более детальные данные. Для этого достаточно создать свой torrent-трекер с интересующим злоумышленников контентом, при попытке скачивания к ресурсу создается запрос и остается техническая информация в виде ip, наличия сегментов файла и название пользовательского торрент-клиента, что позволит доказать факт хранения, а с учетом принципа работы torrent-трекеров, распространения и приобретения файла.

Конечно, идентификация у пользователя незаконного файла, несение им полной ответственности не гарантируется. Даже учитывая умышленные действия пользователя, связанные с хранением, распространением файла, нарушающим законодательство, судебская практика разнится. В Москве суды приходят к выводу, что трекеры работающие по принципу bittorrent, автоматически раздают файл желающим, что исключает умысел субъектов, вместе с тем в других регионах суд не видит коллизии и считает, что пользователь знает об автоматической раздаче файлов трекером. Хотя в пользовательском соглашении подобных приложений ничего о механизме работы программы не сказано.

Установив ip адрес и точное время, с которого данный адрес подключался к сети сотрудник сможет вычислить провайдера, к которому можно отправить запрос, для вычисления точного адреса компьютера злоумышленника, с которого тот выходил в сеть. Таким образом для деанонимизации и поимки преступника необходимо лишь узнать его ip адрес и установить его причастность к преступному деянию. Даже если преступник использует vpn, который настроен так, что невозможно совершить соединение в обход него, в руках правоохранительных органов окажется ip-адрес коммерческого vpn сервиса, в который остается подать запрос и получить подлинные данные, хотя, конечно, многие vpn находятся вне юрисдикции Российской Федерации, и находятся за ее границами.

Большинство мессенджеров, в которых есть функция звонков через сеть интернет, используют систему p2p соединения, а значит два пользователя созванивающихся таким образом, подают запросы напрямую к ip собеседника. Используя программу Whreshark – это достаточно известный инструмент для захвата и анализа сетевого трафика, и совершив звонок через мессенджер злоумышленнику, сотрудники смогут без труда отследить ip и вычислить местонахождение преступника. Так как множество преступлений совершаются на основе социальной инженерии, жертва может поспособствовать раскрытию дела, позвонив преступнику, для установления сотрудниками ip.

Большая часть незаконного контента публикуется на доменах в так называемых onion браузерах, которые основаны на принципе i2p сети. Такие браузеры

используется систему трех узлов: входной, точка входа в сеть, промежуточный, который связывает входной и выходной узел, и сам выходной узел, который отправляет трафик к пункту назначения. Анонимность в onion браузере достигается путем шифрования трафика, при передаче каждому узлу. Наиболее интересным для правоохранителей является выходной узел, называемый exit node – он является точкой выхода информации и может стать местом ее утечки. С помощью таких нод можно контролировать трафик, который через них проходит. Для этого достаточно открыть выходную ноду для пропуска трафика по всем портам, после чего запустить любой снифер пакетов. Для примера возьмем достаточно популярный tshark, который осуществит аккумуляцию всей информации в отдельный дамп. Таким образом пассивная разведка сомнительных ресурсов может помочь сотрудникам правоохранительных органов в выявлении готовящихся или уже совершенных преступлений.

Также возможна деанонимизация пользователя путем использования социальной инженерии в рамках орд. Существует возможность создать word или pdf файл, который при открытии будет соединяться с определенным адресом, и соответственно отправлять ему ip-адрес открывшего. Так можно обойти принцип работы tor браузера, так как его анонимность распространяется только на сайты, открываемые в нем. Также данный документ, открытие которого будет в интересах преступника, не будет проявлять никакой вредоносной активности при проверке или открытие его на виртуальной машине, так как виртуальные машины по умолчанию не блокируют соединения.

Ввиду нарастающей тенденции совершения преступлений в интернете, а в частности в сетях, использующих р2р и i2р протоколы, а также использования преступниками tor браузера, который позволяет получать злоумышленникам высокую степень анонимности, предлагается развивать пассивные средства мониторинга в р2р сетях.

Список использованных источников:

1. Информационно-аналитическое обеспечение оперативно-служебной деятельности органов внутренних дел : курс лекций / [Ф. Ф. Анюров и др.] ; под ред. А. М. Кононова, Р. А. Софьиной. М. : ДГСК МВД России, 2011. 298 с.
2. Применение информационных технологий в аналитической разведке : курс лекций / [П. Е. Букейханов и др.] ; под общ. ред. П. Е. Букейханова. М. : Московский университет МВД России, 2012. 215 с.
3. Преступность в СНГ: проблемы предупреждения и раскрытия преступлений : сборник материалов Международной научно-практической конференции. Воронеж : Воронежский институт Министерства внутренних дел Российской Федерации, 2021.

Калашникова А. А.¹,
преподаватель кафедры информатики
и математики Московского университета
МВД России имени В.Я. Кикотя

Ломов М. С.²,
курсант факультета подготовки сотрудников
для подразделений экономической
безопасности и противодействия коррупции
Московского университета
МВД России имени В.Я. Кикотя

МЕСТО РОССИИ В КОМПЬЮТЕРИЗАЦИИ: ОСНОВНЫЕ НАПРАВЛЕНИЯ И ПРОБЛЕМЫ

В статье изучается тематика компьютеризации в современном мире, а также место России в данном процессе в целях обозначить, какое место на сегодня занимает Россия в компьютеризации, а также критически оценить имеющиеся проблемы.

На сегодня Россия занимает достаточно высокие позиции по уровню цифровизации. Наша страна занимает 27 место среди всех стран мира по цифровизации, что является хорошим результатом с учетом того, что позади остаются такие страны как Китай, Швейцария или Австралия [2].

Рейтинг рассчитывается исходя из таких показателей, как: наличие интернета (широкополосного и мобильного), количество пользователей и уровень компьютеризации населения. Составляется данный рейтинг АНО «Диалог» и является достаточно свежим.

Если усомниться в том, стоит ли безоговорочно доверять данному рейтингу и данному источнику, то следует рассмотреть также другие рейтинги, имеющие отношение к компьютеризации. Один из них – рейтинг цифровой конкурентоспособности стран, публикуемый международным информационно-исследовательским порталом Statista [4].

В этом случае рассчитывается рейтинг немного по-другому, поскольку здесь учитываются такие характеристики как цифровые достижения стран, уровень развитости компьютерных технологий, человеческий и интеллектуальный потенциал, способный решать те или иные задачи цифрового характера.

Первое место в этом рейтинге занимают США со 100 из 100 возможных баллов. За ними следует Гонконг, Швеция, Дания, Сингапур, Швейцария. Россия обладает лишь 60,27 баллами, что ставит ее только на 44 место. На одну позицию впереди находится Польша, на одну позицию ниже – Кипр. Из чего можно заключить, что данный рейтинг дает ощутимо более скромные оценки цифровому потенциалу России на сегодня по сравнению с рейтингом цифровизации от АНО «Диалог». С другой стороны, эти рейтинги отталкиваются от разных характеристик.

¹ © Калашникова А. А., 2022.

² © Ломов М. С., 2022.

Другой рейтинг – так называемый Enabling Digitalization Index (EDI), который можно перевести просто как Индекс цифровизации. Ведется рейтинг французской страховой и кредитной организацией Euler Hermes.

Индекс измеряет потенциал и гибкость стран по отношению к цифровым технологиям. Индекс EDI не измеряет внедрение цифровых технологий или цифровую активность (результаты цифровизации), а скорее фокусируется на условиях для трансформации или процветания компаний в цифровом формате.

В этом рейтинге США, опять же, занимают первую строчку, а за ними следуют такие страны как Германия, Нидерланды, Швейцария, Великобритания, Швеция и Япония.

Интересно, что в данном рейтинге Россия также занимает 44 место [5]. Это, впрочем, не означает, что наша страна находится в двух последних иностранных рейтингах ближе к концу списка – скорее, она занимает срединное место. Рейтинг АНО «Диалог», по этой причине, не представляется как рейтинг, дающий какую-то явно завышенную оценку позициям России в цифровизации, хотя, возможно, и стремится подать ситуацию в чуть более благоприятном свете.

Но кроме рейтингов есть такой важный фактор как присутствие страны на рынке информационных технологий, ее потенциал в этой самой компьютеризации. Именно в этой связи в современной России наблюдаются существенные проблемы.

Еще в 2020 г. газета «Взгляд» опубликовала статью, в которой констатируется фактический провал импортозамещения в ИТ-сфере [1]. Авторы подчеркивают отсутствие внятных результатов программы импортозамещения в ИТ и считают, что попытка нарастить конкурентоспособность страны в этой отрасли «не удалась».

Отечественное ПО в данном случае представляет собой просто доработанную или переосмысленную версию зарубежного ПО и вряд ли способно представлять реальную ценность для мирового ИТ-рынка. В перспективе данный продукт не будет пользоваться спросом и на родине, потому что государство не станет жестко регулировать ИТ-рынок на постоянной основе. Импортозамещение – это лишь мера поддержки. На этой базе отечественная ИТ-отрасль должна стать самостоятельной, а ИТ-продукт привлекательным международному рынку.

Ситуация усугубляется фактическим отсутствием нашей страны на рынке ИТ-технологий и оборудования. Не только софт, но и «железо», которое мы приобретаем в личное пользование или которым пользуемся на работе – все это разработано и изготовлено за рубежом. Наиболее известный и востребованный софт разрабатывается в США и Европе. Непосредственно компьютерную технику собирают в Китае, на Тайване, а авторские права на технологии и ноу-хау опять же принадлежать западным странам. Недаром при рассмотрении истории развития компьютерной техники постоянно упоминаются США и западные страны – фактически, они построили современную ИТ-сферу, т. е., Россия на этом рынке фактически не представлена.

Проблем, затрудняющих развитие компьютеризации и информационных технологий в нашей стране, существует целый ряд.

М. В. Тютина, например, выделяет следующие важные, на ее взгляд, проблемы:

- нестабильная политическая и экономическая ситуация;
- слабый рубль, политическая и экономическая неопределенность ускоряют отток капитала из Российской Федерации;
- всплеск инфляции и рост цен на импортную продукцию также существенно тормозят развитие рынка ИТ;
- высокий уровень инфляции подрывает доверие потребителей и негативно сказывается на всем рынке [3].

На наш взгляд, перечисленные проблемы нуждаются в серьезном дополнении, так как есть факторы, мешающие динамичному развитию отрасли и помимо вышеперечисленных.

Во-первых, нельзя не упомянуть непродуктивную конфронтационную политическую линию, которая сложилась между Россией и странами Запада. Страны Запада – важный торговый партнер, источник инноваций и инвестиций. Сотрудничество с ними потенциально было бы полезно не только притоком инвестиций, но и более динамичным развитием информационного рынка. Поскольку сегодня – именно страны Запада являются мировыми лидерами по той же цифровой конкурентоспособности, о которой шла речь выше.

Во-вторых, вследствие достаточно депрессивной социально-экономической ситуации, сложившейся в последние годы, усиливается отток подготовленного, высококвалифицированного кадрового состава. «Утечка мозгов», выливающаяся в отток высококлассных специалистов в те же самые страны Запада, создает не только условия для дальнейшего торможения роста отечественного ИТ-рынка, но и способствует более динамичному развитию цифрового потенциала западных стран.

В-третьих, ситуация на внутрироссийском рынке становится пугающе бесперспективной. Отсутствуют какие-то серьезные драйверы роста, экономика уже много лет не может показать убедительных темпов роста, а реально располагаемые доходы населения последовательно снижаются.

Нет ощущений, что современное правительство намерено принимать радикальные меры для корректировки ситуации. Об этом свидетельствует и анализ нового федерального бюджета на 2022 г., в котором сокращаются расходы на социальную сферу. Все это косвенно повлияет на потенциал инновационного развития в целом и на развитие ИТ-отрасли в частности, поскольку для развития таких высокотехнологичных отраслей должны быть созданы условия.

Красноречив тот факт, что высокие показатели цифровизации, цифровой конкуренции и т.п. характерны именно для стран с высоким уровнем жизни. Это неслучайно, поскольку развитие ИТ-отрасли иногда предполагает и определенную долю привлеченных талантов, которые могут привлекаться из-за рубежа. Для этого в стране нужно создать такие условия, которые будут существенно лучше, нежели те, что предлагают другие страны, из которых эти таланты переезжают в поисках лучшей жизни.

Создание таких условий – это пока весьма существенная проблема для современной России, которая, в том числе, сдерживает более динамичное развитие цифровой конкурентоспособности и компьютеризации.

Следует подытожить изложенное. В целом, согласно рассмотренным рейтингам, Россия занимает «срединное» место как по цифровизации, так и по цифровой конкуренции, а также по условиям развития цифровых технологий. В рейтингах по этим показателям наша страна, как правило, граничит с такими государствами как Польша, Кипр, Китай. При этом, Россия находится достаточно далеко от лидерских позиций и это объясняется рядом проблем.

Среди проблем названы: практически полное отсутствие нашей страны на ИТ-рынке и, в том числе, крайне неубедительные результаты импортозамещения; проблемы с инфляцией; политико-экономическая нестабильность и неопределенность. Свою роль играет и нехватка специалистов в ИТ-сфере, их активный отток за рубеж, а также отсутствие внятных перспектив и драйверов роста для страны.

Список использованных источников:

1. Импортозамещение в ИТ зашло в тупик // Деловая газета «Взгляд». URL: <https://yandex.ru/turbo/vz.ru/s/opinions/2020/5/18/1039123.html>.
2. Россия заняла 27-е место в рейтинге стран по цифровизации // Сайт «РИА Новости». URL: <https://ria.ru/20210903/tsifrovizatsiya-1748459672.html>.
3. Тютин М. В. Анализ и перспективы развития рынка информационных технологий в России // Инновационная экономика : материалы IV Международной научной конференции. Казань : Бук, 2017. С. 9–13.
4. Country-level digital competitiveness rankings worldwide as of 2021 // Statista. URL: <https://www.statista.com/statistics/1042743/worldwide-digital-competitiveness-rankings-by-country/>.
5. Measuring Digitagility: The Enabling Digitalization Index (EDI) // Euler Hermes. URL: https://www.eulerhermes.com/en_global/news-insights/economic-insights/1370.html.

Стручков И. С.¹,
старший преподаватель кафедры
специальных информационных технологий
учебно-научного комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя

Лапшин И. О.²,
заместитель начальника кафедры
специальных информационных технологий
учебно-научного комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя

Максимченко А. М.³,
преподаватель кафедры специальных
информационных технологий
учебно-научного комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя

АВТОМАТИЗАЦИЯ РАСПОЗНАВАНИЯ ПАРОЛЬНОГО ВВОДА В КОМПЬЮТЕРНУЮ СИСТЕМУ

Процессы идентификации и аутентификации личности при доступе к информационным ресурсам тесно связаны между собой и вводятся последовательно.

Идентификация – процесс сравнения идентификатора, вводимого участником информационного взаимодействия, с его идентификатором, содержащимся в компьютерной системе [1].

Аутентификация – это процесс подтверждения подлинности предъявленного идентификатора и проверка принадлежности аутентификатора (секрета, который знают обе стороны взаимодействия) пользователя компьютерной системы [2–4].

Взаимодействие с последующей идентификацией и аутентификацией начинается с включения компьютера и входа в его операционную систему, аутентификацию проходят, чтобы получить доступ к локальной сети и распределенным сетям, системам защиты от несанкционированного доступа, виртуальным частным каналам. Особое место занимает аутентификация при беспроводном, удаленном сетевом доступе к сетям и ресурсам, в том числе при переходе к облачным вычислениям [5–7]. Одним из способов увеличения стойкости компьютерных систем в случае получения пароля и идентификатора посторонними лицом или даже злоумышленником может быть разработка и внедрение в систему безопасности математической модели, описывающей типовое поведение каждого пользователя при прохождении парольной аутентификации [8].

¹ © Стручков И. С., 2022.

² © Лапшин И. О., 2022.

³ © Максимченко А. М., 2022.

Результаты моделирования можно будет использовать для проектирования информационных систем, которые требуют повышенной степени защиты [9].

В частности процедуры, подтверждающую аутентификацию, предоставляющую администраторам информацию о подмене пользователя, передачи пароля постороннему лицу, адекватного психофизиологического состояния пользователя. Для построения математической модели парольного средства аутентификации авторами проведены эксперименты с 30 участниками для изучения изменения скорости ввода пароля различной сложности и структуры в зависимости от времени привыкания к нему.

При этом исследовались режимы спокойного поведения испытуемого при вводе 8-ми символьного пароля, состоящего из цифровых и буквенных символов. Время ввода пароля τ оценивалось до десятой доли секунды с помощью специально разработанной программы.

Кроме того, проведен ряд экспериментов по вводу пароля, когда испытуемый в процессе ввода:

- заменялся на другого пользователя, не водившего ранее используемый пароль;
- подвергался воздействиям стрессовых факторов, когда создавался режим психологически неспокойной обстановки, которая существенно отличалась от обычной ситуации работы пользователя с компьютерной системой.

Представлены примеры, когда пользователь вводит пароли в спокойном режиме (рис. 1–2), далее отражена замена пользователя на другого человека, еще не привыкшего к паролю и ни разу его не вводившего (рис. 3).

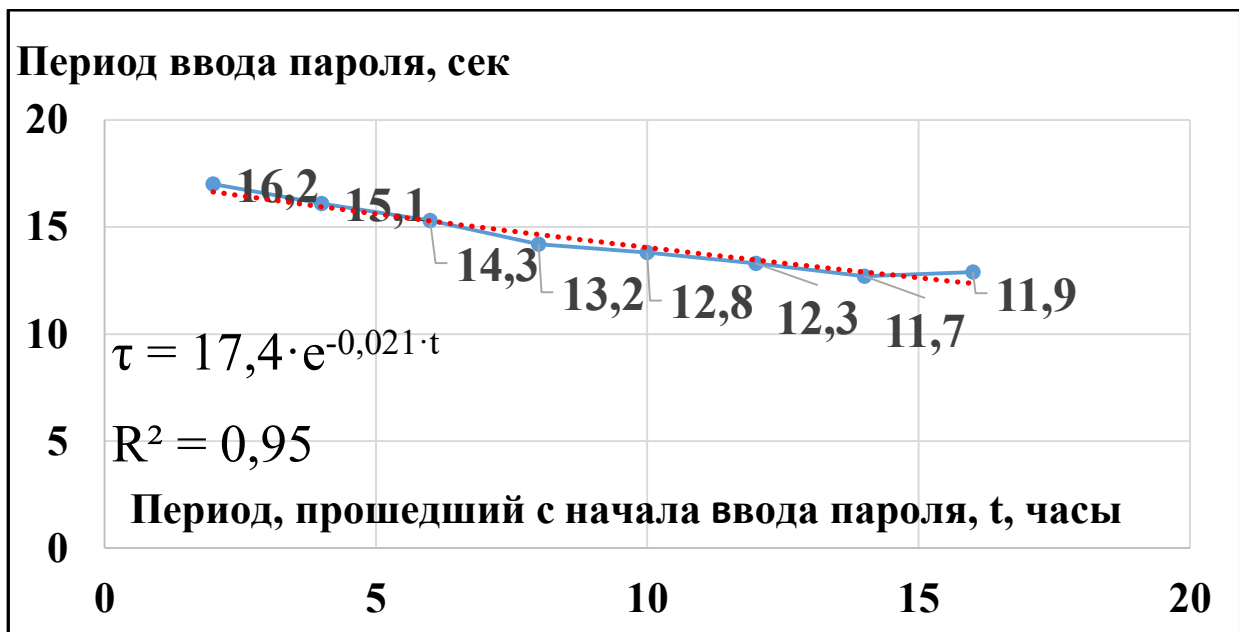


Рис. 1. Зависимость времени ввода пароля от периода его использования, спокойный режим, 1-й пользователь

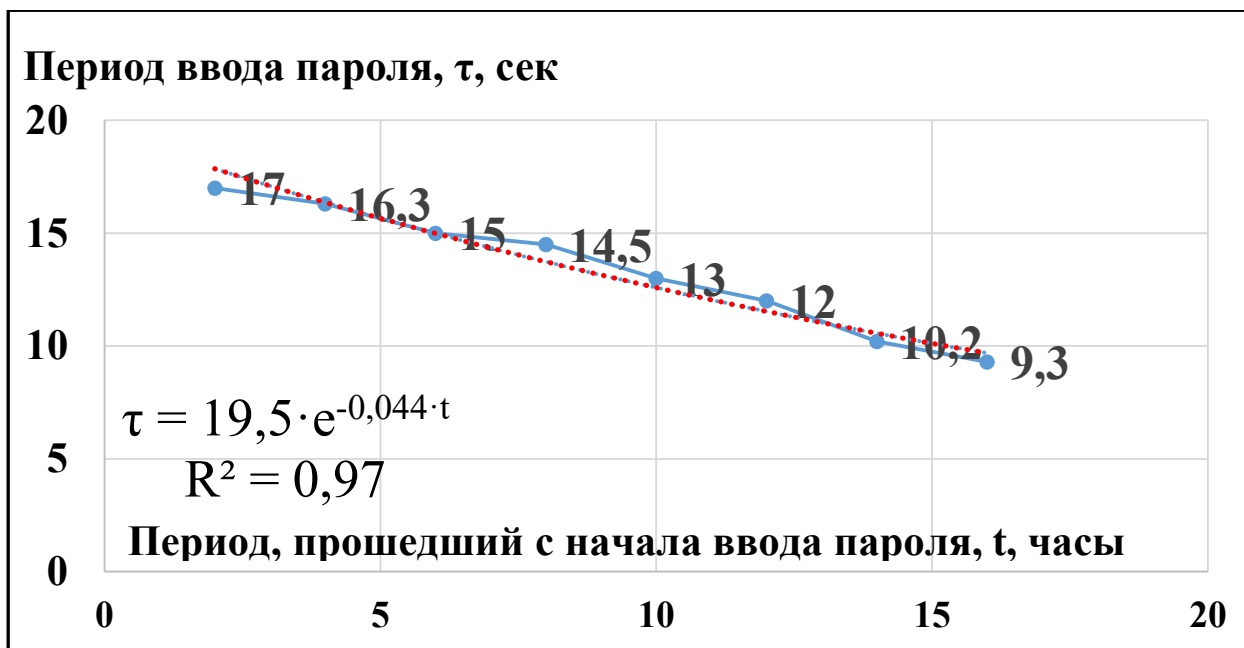


Рис. 2. Зависимость времени ввода пароля от периода его использования, спокойный режим, 2-й пользователь

Анализ периода ввода одного и того же пароля τ , выраженного в секундах, показал, что он снижается в зависимости от времени его использования t в часах по экспоненте вида: $\tau = \alpha \cdot \exp(-\beta \cdot t) + \gamma$.

Такой вид зависимости базируется на результатах исследований кривой «Забытия информации» [10]. Коэффициент детерминации R^2 на рис. 1–2 достаточно высоко соответственно 0,95 и 0,97 где α , β , γ – константы, определяемые экспериментально применительно к каждому пользователю, длине и составу пароля. При этом γ отражает устоявшуюся скорость ввода пароля тем или иным пользователем, определяемую его психофизиологическими характеристиками, отличающимися у разных пользователей.

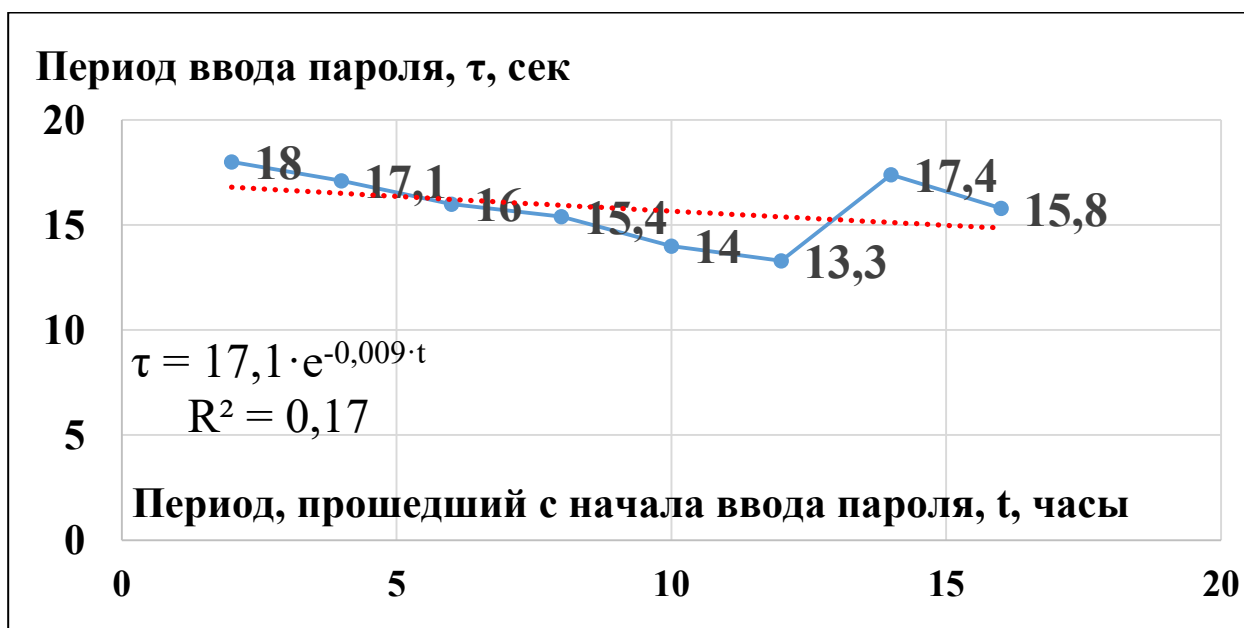


Рис. 3. Зависимость периода ввода пароля от времени его использования, при подмене пользователя в процессе проведения эксперимента

На *рис. 1–2*, отражена зависимость для спокойного режима, одинаковый состав и длины паролей. Сплошной линией отражены эмпирические данные, а пунктирной – теоретическая кривая. При этом коэффициент объяснимости эмпирических данных, выраженный в процентах, весьма высок.

В том случае, когда происходит подмена пользователя или изменение условий ввода (принуждение пользователя, изменение его психологического состояния, изменение пароля и т. п.) в указанной зависимости происходят серьезные изменения и коэффициент объяснимости существенно снижается. Так, на *рис. 3*, отражающем такие изменения, он снижается до 17 %.

Проведенные эксперименты позволили заключить, что, если значение коэффициента R^2 больше или равно 95 %, то аутентификация пройдена успешно и пользователь может приступить к работе на своем компьютере.

Если значение коэффициента R^2 больше 80 %, но меньше 95 %, то администратору информационной системы необходимо обратить на это внимание и разобраться в причинах, почему пользователь не показывает устоявшиеся характеристики аутентификации при тех же условиях ввода пароля, которые были ранее.

Если значение коэффициента R^2 меньше 80 % и система аутентификации не пропускает пользователя, то необходимо тщательно разобраться: нет ли подмены пользователя, нет ли передачи пароля постороннему лицу, соответствует ли психофизиологическое состояние пользователя нормальному для него.

В заключение можно сделать предположение, что значение коэффициента R^2 может служить мерой успешности аутентификации пользователя, вводящего пароль. При его значениях, ниже определенного критерия, происходит отказ в доступе к компьютеру.

Список использованных источников:

1. Минаев В. А., Королев И. Д., Сабанов А. Г. Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4(30). С. 43–49.
2. Бханд А., Десале В., Ширке С. Совершенствование системы аутентификации паролей с использованием графических изображений // Материалы Международной конференции IEEE по обработке информации (ICIP). Пуна, Индия. 16–19 декабря 2015. С. 217–219.
3. Морозова В. И., Гилева В. Д. Обеспечение безопасного доступа и управления идентификацией веб-приложений // Молодой ученый. 2022. № 9 (404). С. 15–18.
4. Стенин С. В., Рак Д. В. Анализ методов аутентификации по используемым средствам // Альманах Пермского Военного Института Войск Национальной Гвардии. 2021. С. 362–366.
5. Усманов С. С-У, Шермухамедов А. Т. За нами будущее: взгляд молодых ученых на инновационное развитие общества // Сборник научных статей 3-й Всероссийской молодежной научной конференции. Курск : Юго-Западный государственный университет, 2022. С. 524–527.

6. Виноградова А. Р., Черепанов С. П. Облачные вычисления и особенности их использования в банковской сфере // Скиф. вопросы студенческой науки. 2020. С. 183–186.
7. Подчасов С. В. Облачные вычисления // Аллея науки. 2020. С. 713–717.
8. Даурбеков С-Э. С. Математические модели: принципы и этапы моделирования// Аудиторские ведомости. 2020. С. 104–106.
9. Рудакова Е. В. Признаки, виды и особенности информационных систем // Духовная ситуация времени. Россия XXI в. 2019. С. 1–4.

Иванов В. А.¹,
*старший оперуполномоченный
Межрайонного отдела № 5
Управления уголовного розыска
МВД России по Удмуртской Республике*

МЕЖОТРАСЛЕВОЙ ПОДХОД В ПРОТИВОДЕЙСТВИИ ИТ-ПРЕСТУПНОСТИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Крайне негативные проявления преступности в Российской Федерации в настоящее время во многом характеризуются тем, что продолжают увеличиваться преступления, связанные с использованием информационно-телекоммуникационных технологий (ИТ-преступность) [5, с. 51–57; 12, с. 133]. Находит это свое подтверждение и в официальных статистических данных о деятельности правоохранительных органов в сфере противодействия данным социально негативным проявлениям. Их изучение и анализ с момента начала официальной регистрации (с 2019 г.) позволяет прийти к достаточно неутешительному выводу о том, что весьма тревожным выглядит увеличение тяжести совершаемых данных преступлений [6]. Так, в 2019 г. из общего числа зарегистрированных таких деяний (294,4 тыс.) тяжкие и особо тяжкие составили 142,7 тыс.; в 2020 г. – 267,6 тыс. из зарегистрированных 510,4 тыс.; в 2021 г. – 288,3 тыс. из зарегистрированных 517,7 тыс.; за период с января по август 2022 г. – 176,4 тыс. из зарегистрированных 334,1 тыс. При этом, немаловажно заметить, что раскрываемость рассматриваемых категорий преступлений остается очень низкой (в 2019 г. – 65,2 тыс., в 2020 г. – 94,9 тыс., в 2021 г. – 118,9 тыс., за январь по август 2022 г. – 94 тыс.).

Отмечают изложенные негативные обстоятельства и в ученой среде. В частности, Т. В. Пинкевич, ссылаясь на совместный аналитический материал ВНИИ и Академии управления системы МВД России от 2020 г., указывает на «увеличение числа такого рода преступлений» [3, с. 79]. К. А. Спехова обращает внимание на рост качественных характеристик киберпреступности [10, с. 52].

Как отметил Министр внутренних дел Российской Федерации В. А. Колокольцев, в своем выступлении 19 октября 2020 г. в ходе «правительственного часа» в Государственной Думе, проблемы борьбы ИТ-преступлениям остаются и сегодня злободневными [1].

По нашему мнению, в качестве одной из существенных проблем в противодействии информационно-телекоммуникационной преступности проявляется, с одной стороны, в отсутствии надлежащего межотраслевого подхода, решение которой нам видится в плоскости осуществления в этом контексте активных теоретических исследований [8, с. 4; 9, с. 200–205; 11, с. 3], с другой – обеспечении эффективного взаимодействия должностных лиц правоохранительных органов

¹ © Иванов В. А., 2022.

в данной сфере борьбы с преступностью на основе положений федерального законодательства и соответствующих ведомственных и межведомственных нормативно-правовых актов. Хотя, справедливости ради, следует отметить, что отдельными авторами делаются попытки решения обозначенных проблем. Так, А. Е. Минаков предлагает создать правовую модель взаимодействия должностных лиц УФСИН России и МВД России при раскрытии и расследовании «телефонных мошенничеств» [7, с. 78].

И все же, полагаем, в виду недостаточных научно-теоретических и прикладных исследований рассматриваемой темы, в практике правоприменения отсутствует и надлежащая нормативная основа для обеспечения совместной упорядочно согласованной деятельности должностных лиц органов внутренних дел во взаимосвязи с иными правоохранительными органами.

По нашему мнению, в этой связи весьма важно учитывать и пусть даже достаточно скромную современную практику. К примеру 18 февраля 2022 г. на базе Университета имени О. Е. Кутафина (МГЮА) семью вузами России подписано соглашение о создании консорциума организаций высшего образования в сфере IP (Internet Protocol). При этом проректор Университета по учебной и методической работе М. В. Мажорина отмечает, что данное «объединение ... позволит выработать наиболее сбалансированное, взвешенное и в то же время инновационное решение по той или иной проблеме» [4].

Для практической правоохранительной деятельности подобное начало, полагаем, тоже есть. В частности, в 2003 г. Р. Н. Зинуровым была выдвинута идея о формировании системы нормативных положений на основе предложенного им проекта Федерального закона «О координации деятельности правоохранительных органов» [2, с. 1–51] для совершенствования объединенных усилий правоохранительной деятельности. А для того, чтобы сделать попытку разрешения рассматриваемой нами проблемы, думается, необходимо вернуться к положениям ст. 8 Федерального закона о прокуратуре Российской Федерации и п. 3 Указа Президента России от 18 апреля 1996 г. № 67 «О координации деятельности правоохранительных органов по борьбе с преступностью» (в ред. от 31.12.2019) и убедиться, что современная российская прокуратура является инстанцией, осуществляющей не только функций надзора за деятельностью должностных лиц правоохранительных органов и, уголовного преследования. Генеральный прокурор Российской Федерации и подчиненные ему прокуроры выполняют и управленческие функции деятельностью данных органов правоохраны. Для убедительности сказанного в логической последовательности нами приведены следующие нормативные положения о функциях российской прокуратуры, которыми в настоящее время они обладают:

- прокурорского надзора (см.: ч. 1 ст. 129 Конституции Российской Федерации; п. 1–5 ч. 2 ст. 1 ФЗ «О прокуратуре Российской Федерации»);
- уголовного преследования (см.: ч. 1 ст. 129 Конституции Российской Федерации; п. 6 ч. 2 ст. 1 ФЗ «О прокуратуре Российской Федерации», п. 31 ст. 5, ч. 1 ст. 37 УПК РФ, ст. 4 Федеральный закон «О введении в действие Уголовно-процессуального кодекса Российской Федерации» от 18 декабря 2001 г. № 177-ФЗ (в ред. от 23.06.2016);

– координации деятельности правоохранительных органов (управленческую функцию) (см.: ч. 1 ст. 129 Конституции Российской Федерации; п. 7 ч. 2 ст.ст. 1, 8 ФЗ «О прокуратуре Российской Федерации»; Указ Президента Российской Федерации от 18 апреля 1996 г. № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью»).

Таким образом, по нашему мнению, в вопросах межотраслевого подхода в противодействии IT-преступности (собственно, также, как и в любом другом направлении борьбы с преступностью в стране) должностные лица органов внутренних дел обязаны руководствоваться изложенным алгоритмом нормативно-правовой регламентации своей правоохранительной деятельности. В свою очередь, именно Генеральный прокурор Российской Федерации и подчиненные ему прокуроры страны на основе приведенных законодательных актов в системной совокупности, полагаем, формируют необходимый и достаточный и эффективно реализуемый механизм управления деятельностью должностных лиц как органов внутренних дел, так и органов правоохраны России в целом, в том числе и по противодействию IT-преступности.

Список использованных источников:

1. Выступление 19 октября 2022 г. Министра внутренних дел Российской Федерации генерала полиции Российской Федерации В. А. Колокольцева на заседании Государственной Думы Федерального Собрания Российской Федерации в рамках «правительственного часа» // Официальный сайт Государственной Думы. URL: <http://duma.gov.ru>.
2. Зинуров Р. Н. Концептуальные основы и научно-практические проблемы координации деятельности правоохранительных органов по борьбе с преступностью (тенденции и закономерности) : автореф. дис. ... д-ра юрид. наук. Уфа, 2003. 51 с.
3. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология : учебное пособие. М. : Академия управления МВД России, 2021. 244 с.
4. Интервью проректора по учебной и методической работе Университета имени О.Е. Кутафина М. В. Мажориной // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 2 (90). С. 10–11.
5. Кобец П. Н. Совершенствование деятельности правоохранительных органов государств – участников СНГ по борьбе с кибертерроризмом в условиях информационной глобализации // Ученые записки Казанского юридического института МВД России. 2022. Т. 7. № 1 (13). С. 51–57.
6. Краткая характеристика состояния преступности в Российской Федерации за период с 2019 по август 2022 гг. // Официальный сайт МВД России. URL: <https://мвд.рф/reports/>.
7. Минаков А. Е. Вопросы межведомственного взаимодействия органов предварительного следствия с учреждениями исполнения наказания при расследовании «телефонных мошенничеств» // Сетевое издание «Академическая мысль». № 1 (10). 2020. С. 78.
8. Наумов В. Б. Институт идентификации в информационном праве : автореф. дис. ... д-ра юрид. наук. М., 2020. 52 с.

9. Потапова С. А. К вопросу о взаимодействии органов внутренних дел Российской Федерации с иными субъектами правоохранительной деятельности // Закон и право. 2021. № 12. С. 200–205.

10. Спехова К. А. Киберпреступность: избирательное правоприменение // Киберпреступность: риски и угрозы : материалы Всероссийского студенческого круглого научно-практического стола с международным участием (Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия» (Санкт-Петербург, 11 февраля 2021 г.) / под ред. Е. Н. Рахмановой. СПб : Астерион, 2021. 236 с.

11. Устинович Е. С. государственная политика в сфере информационных технологий (опыт Российской Федерации) : автореф. дис. ... д-ра юрид. наук. М., 2012. 48 с.

12. Шхагапсоев З. Л. К вопросу о роли органов внутренних дел в предупреждении преступлений, совершаемых с использованием информационных технологий (ИТ-преступлений) // Государственная служба и кадры. 2020. № 2. С. 131–134.

*Лукашенко Д. В.¹,
главный научный сотрудник
Научно-исследовательского
института ФСИИ России,
доктор психологических наук, доцент*

ОБУЧЕНИЕ ПЕРСОНАЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С УЧЕТОМ СОВРЕМЕННЫХ УГРОЗ БЕЗОПАСНОСТИ

В статье рассматривается образовательный процесс на курсах повышения квалификации по направлению информационная безопасность. Определены особенности разрабатываемой программы. Были определены, исходя из актуальных угроз, тематика занятий, порядок и последовательность их проведения. В статье приводится краткое описание каждого тематического образовательного периода. Выделена целевая аудитория и определены целевые умения, на формирование которых направлено обучение. Уделяется большое внимание практическим занятием при освоении курса.

Разработка учебной программы по информационной безопасности для курсов повышения квалификации требует глубокого знания предметной области и современного ее состояния, а также знать, уметь и владеть педагогическими приемами и методами, направленными на эффективное обучение за ограниченное время. Отличительной особенностью всех курсов повышения квалификации от классического обучения по программам высшей школы является ограниченный промежуток времени [1, с. 29], в который необходимо уложить актуальные очищенные от лишней академичности знания, при этом не скатываясь к сухому изложению информации и развитию навыков без осознания материала, а наоборот формируя опережающее эвристическое понимание проблем информационной безопасности.

Рассмотрим программу повышения квалификации по направлению Информационная безопасность с названием «Выявление и противодействие компьютерным инцидентам». Данное направление нацелено на системных администраторов, администраторов безопасности, сотрудников занимающихся обработкой инцидентов и других сотрудников ИТ отделов, занимающихся защитой информации, реагированием на атаки и угрозы.

Интернет полон мощных хакерских утилит, и злоумышленники широко их используют [2, с. 24]. Если в организации есть подключение к интернету и один или два недовольных сотрудника, то информационная система гарантированно будет атакована. Начиная с единичных проверок интернет-инфраструктуры организации до сотен в день и злонамеренного инсайдера, злоумышленники медленно и скрытно проникают в самые важные информационные ресурсы, минуя системы защиты и обнаружения [3, с. 25]. Для противодействия этим вторже-

¹ © Лукашенко Д. В., 2022.

ниям обучающиеся должны понимать инструменты и методы взлома компьютерных сетей. Они должны детально понимать тактику и стратегию злоумышленников, и для этого недостаточно теоретических занятий необходим практический опыт поиска уязвимостей и обнаружения вторжений, а также осознание комплексного плана обработки инцидентов [4, с. 93]. В нем рассматриваются последние передовые коварные векторы атак, классические атаки, которые все еще распространены, и достаточно часто встречаются. Эффективность обучения по данному направлению как ни с каким другим тесно переплетается с практическими занятиями. Вместо того, чтобы просто учить нескольким приемам хакерской атаки, эффективен пошаговый процесс реагирования на компьютерные инциденты и подробное описание того, как злоумышленники взламывают системы, чтобы системный администратор мог подготовиться, обнаружить и противостоять атакам. Отдельным направлением является рассмотрение правовых вопросов, связанных с реагированием на компьютерные атаки, включая мониторинг сотрудников, взаимодействие с правоохранительными органами и сбор, и сохранение доказательств. Апогеем обучения по этой программе будет наличие знаний и умений, позволяющих обнаружить брешь [5, с. 57] в системе информационной безопасности организации раньше злоумышленников и устранить их.

Примерная программа может иметь вид.

ДЕНЬ 1: Пошаговое расследование инцидентов и расследование компьютерных преступлений.

В этом разделе рассматривается пошаговая модель обработки инцидентов, которая была отработана на практике с участием опытных специалистов по обработке инцидентов и доказала свою эффективность в сотнях организаций. Этот раздел предназначен для того, чтобы предоставить обучающимся полное погружение в процесс обработки инцидентов, используя шесть этапов (подготовка, идентификация, локализация, уничтожение, восстановление и извлеченные опыта), необходимых для подготовки к компьютерному инциденту и борьбы с ним. Во второй части этого раздела рассматриваются практические примеры из практики. В этом разделе представлена информация о шагах, которые может предпринять системный администратор для повышения шансов на поимку и преследование злоумышленников.

ДЕНЬ 2: Компьютерные и сетевые хакерские атаки (часть 1).

На первый взгляд безобидная утечка данных из сети организации может дать ключ, необходимый злоумышленнику для взлома системы. Этот однодневный курс охватывает первые две фазы многих компьютерных атак связанные с разведкой и сканированием.

ДЕНЬ 3: Компьютерные и сетевые хакерские атаки (часть 2).

Компьютерные злоумышленники постоянно совершенствуют свои методы и по-новому атакуют сети и системы. Этот день посвящен третьей фазе многих хакерских атак – получение доступа. Злоумышленники используют различные стратегии для перехода систем от уровня сети до уровня приложения. В этом разделе подробно рассматривают атаки, от переполнения буфера и методов форматной строковой атаки до перехвата сеансов предположительно безопасных протоколов.

ДЕНЬ 4: Компьютерные и сетевые хакерские атаки (часть 3).

Этот учебный день начинается с изучения одной из любимых техник злоумышленников для взлома систем: червей. Рассматривается эволюция червей за последние два года и экстраполяция этого процесса в будущее для анализа грядущих суперчервей, с которыми в будущем можно столкнуться. Обучение плавно переходит к веб-приложениям, часто используемым злоумышленниками. Поскольку самодельные веб-приложения большинства организаций используют открытое программное обеспечение, злоумышленники внедряют SQL запросы, осуществляют межсайтовый скриптинг, клонируют сеансы и множество других механизмов.

ДЕНЬ 5: Компьютерные и сетевые хакерские атаки (Часть 4).

Этот день обучения охватывает четвертый и пятый этапы многих хакерских атак: поддержание доступа и отслеживание следов. Компьютерные злоумышленники устанавливают черные ходы, применяют руткиты, а иногда даже манипулируют самим ядром системы, чтобы скрыть свои преступные следы. Каждая из этих категорий инструментов требует специальной защиты для базовой системы. В этот день рассматриваются наиболее часто используемые образцы вредоносного кода, а также обсуждаются будущие тенденции развития вредоносных программ, в том числе возможности вредоносного ПО на уровне BIOS и комбинированные вредоносные программы.

ДЕНЬ 6: Мастерская хакерских инструментов.

За прошедшие годы индустрия безопасности стала умнее и эффективнее противостоять хакерам. К сожалению, хакерские инструменты становятся умнее и сложнее. Один из наиболее эффективных способов остановить врага – это на самом деле проверить окружение с помощью тех же инструментов и тактик, которые атакующий может использовать против вас. Этот семинар позволит обучающимся применить на практике то, чему они научились за пройденный курс.

По окончании обучения слушатели должны уметь:

- для защиты корпоративной среды применять углубленные процессы обработки инцидентов, включая подготовку, идентификацию, локализацию, ликвидацию и восстановление;
- проанализировать структуру общих методов атак, чтобы оценить распространение атакующего по системе и сети, предвидя и предотвращая дальнейшую активность атакующего;
- использовать инструменты и доказательства для определения типа вредоносных программ, используемых в атаке, включая руткиты, трояны и бэкдоры, выбирая соответствующие средства защиты и тактику реагирования для каждого из них;
- использовать встроенные средства командной строки, такие как Windows tasklist, wmic и reg, а также Linux netstat, ps и lsof, чтобы обнаружить присутствие злоумышленника на компьютере;
- анализировать таблицы ARP маршрутизатора и системы вместе с таблицами CAM коммутатора для отслеживания активности злоумышленника по сети и идентификации подозреваемого;

- использовать дампы памяти и инструмент Volatility для определения действий злоумышленника на компьютере, установленного вредоносного ПО и других вычислительных машин, которые злоумышленник использовал в качестве опорных точек в сети;
- получать доступ к целевой машине с помощью Metasploit, а затем обнаруживать артефакты и последствия эксплуатации с помощью анализа процессов, файлов, памяти и журналов;
- проанализировать систему, чтобы увидеть, как злоумышленники используют инструмент Netcat для перемещения файлов, создания бэкдоров и создания ретрансляторов в целевой среде;
- запустить сканер портов Nmap и сканер уязвимостей Nessus, чтобы найти дыры в целевых системах, и применить такие инструменты, как tcpdump и netstat, для обнаружения и анализа последствий сканирования.

Список использованных источников:

1. Вилкова А. В., Литвишников Б. А., Швырев Б. А. Проблемы непрерывного обучения персонала информационной безопасности // Мир науки, культуры, образования. 2019. № 4 (77). С. 29–31.
2. Гузеев М. С., Швырев Б. А. Информационная безопасность дистанционной работы в условиях пандемии // Уголовно-исполнительная система: право, экономика, управление. 2022. № 3. С. 21–27.
3. Ковалев О. Г., Вилкова А. В., Швырев Б. А. Методология формирования знаний об информационной и компьютерной безопасности учреждений УИС // Уголовно-исполнительная система: право, экономика, управление. 2022. № 4. С. 25–27.
4. Швырев Б. А. О безопасности в киберпространстве // Международный журнал гуманитарных и естественных наук. 2021. № 1-1 (52). С. 93–97.
5. Власенко А. В. Управление информационной безопасностью на предприятии / [А. В. Власенко и др.]. Краснодар : Новация. 2020. С. 231.

*Андруник А. П.¹,
главный научный сотрудник
Научно-исследовательского
института ФСИИ России,
доктор педагогических наук, доцент*

ИНТЕГРАЦИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫЙ ПЕДАГОГИЧЕСКИЙ ПРОЦЕСС

Деятельность государственных организаций сильно связана с информацией и ее использованием. Повышенный уровень информатизации организаций и связанных с ними процессов также представляет интерес для киберпреступников. Оценка информационной безопасности организации и управление рисками играют важную роль в противодействии угрозам. Приоритетные меры направлены на улучшение управления информационной безопасностью и дальнейшее бесперебойное функционирование организации. Для достижения этих целей необходимо иметь хорошо обученный персонал знаниям не только производственного процесса, но как минимум основам информационной безопасности и в дальнейшем формировании культуры информационной безопасности. Получения новых знаний и усвоения их взрослыми людьми с сформированными жизненными принципами и взглядами не является простой и легко реализуемой задачей. В работе рассматривается модель планирования и оценки устойчивого развития культуры информационной безопасности.

Объем доступной информации и ее важность для организаций выросли в геометрической прогрессии за последние несколько лет. До недавнего времени существовала ситуация, когда получение информации считалось скудным и труднодоступным, а решения принимались на основе относительно небольшого объема информации. Благодаря автоматическому сбору данных объем информации увеличился, и дефицит стал избыточным. По мере роста оцифровки информации организации сталкиваются с возрастающими проблемами в обработке и эффективном использовании данных для улучшения факторов производства и производительности [1, с. 15–21].

Деятельность государственных организаций сильно связана с информацией и ее использованием. Информационные системы и информация, которую они содержат, являются ключевой частью операций, а услуги организаций все чаще становятся электронными и автоматизированными [2, с. 31]. Информация все теперь передается между организациями в электронной форме, а автоматизированные процессы открывают новые перспективы для использования и развития знаний.

Повышенный уровень информатизации организаций и связанных с ними процессов также представляет интерес для киберпреступников [3, с. 4–10]. Организации обременены постоянными угрозами безопасности, реализация которых

¹ © Андруник А. П., 2022.

должна быть устранена и снижена в первую очередь за счет упреждающих, но, в конечном итоге, также и активных средств.

Оценка информационной безопасности организации и управление рисками играют важную роль в противодействии угрозам. Приоритетные меры направлены на улучшение управления информационной безопасностью и дальнейшее бесперебойное функционирование сервисов и факторов производства. Для достижения этих целей необходимо иметь хорошо обученный персонал знаниям не только производственного процесса, но как минимум основам информационной безопасности и в дальнейшем формирования культуры информационной безопасности [4, с. 29–30]. Получения новых знаний и усвоения их взрослыми людьми с сформированными жизненными принципами и взглядами не является простой и легко реализуемой задачей [5, с. 22–23].

Ознакомление с информацией недостаточно для формирования устойчивых навыков и понимания основ информационной безопасности [6, с. 27]. Применения полученных знаний как производственном процессе, так и в быту.

Рассмотрим модель планирования и оценки устойчивого развития культуры информационной безопасности.

Устойчивое развитие следует принимать во внимание на каждом этапе педагогического процесса (подготовительное обучение, обучение на рабочем месте, оценка профессиональных навыков, взаимодействие с трудовой жизнью). С этой целью была разработана модель процесса устойчивого развития культуры информационной безопасности в дополнительном профессиональном образовании взрослых слушателей. Критерии устойчивого развития культуры информационной безопасности в дополнительном профессиональном образовании взрослых слушателей, основаны на модели процесса [3, с. 7].

Учреждения, которые проводят дополнительное обучение для достижения профессиональных целей, могут использовать модель процесса для повышения качества процесса планирования обучения, а также для подготовительного обучения и возможностей получения степени (квалификации и специальности).

Модель процесса начинается с того факта, что при персонализации демонстрационной степени компетенция выпускника также определяется и оценивается с точки зрения устойчивого развития. Это важно для планирования необходимого развития навыков. В то же время можно повлиять на отношение обучающихся к вопросам устойчивого развития.

Требования к компетентности для устойчивого развития критериев степени должны быть открыты для конкретных целей и содержания, чтобы обеспечить их реализацию в подготовительном образовании. Обучение может также соответствовать требованиям к компетентности для устойчивого развития профессий и рабочих навыков, которые не включены напрямую в критерии степени, но их компетентность не может требоваться для демонстрации в новой степени.

Собственная профессиональная деятельность и учебная среда образовательного учреждения должны поддерживать достижение целей компетентности в области устойчивого развития. Следовательно, ключевые аспекты окружающей среды, безопасности, благополучия и культуры рабочей среды должны быть

озвучены обучающимся и приняты во внимание при разработке и руководстве рабочих методов.

Краеугольными камнями опыта устойчивого развития являются [7, с. 94–97]:

- осведомленность о целях устойчивого развития и их значении;
- управление устойчивыми методами работы в профессии;
- приверженность продвижению устойчивого развития в своей профессии и рабочем коллективе.

Увеличение этих знаний требует систематического использования методов обучения, которые способствуют достижению целей обучения в области устойчивого развития [4, с. 29]. Эти методы обучения включают, например, укрепление навыков критического мышления, навыков опережающего мышления и методы драматической и театральной педагогики. Качественное образование также требует, чтобы преподаватели обладали достаточными знаниями о содержании и решениях устойчивого развития в их соответствующих профессиях, а также о педагогических подходах.

Ориентированное на дополнительное профессиональное обучение образование взрослых в основном осуществляется на рабочем месте [5, с. 27]. Для достижения компетентных целей устойчивого развития важно, чтобы цели и реализация обучения на рабочем месте планировались вместе с выпускником и руководителем рабочего места. Таким образом, можно положительно повлиять на осведомленность об устойчивом развитии на рабочих местах и на развитие передовой практики.

Для качественной оценки навыков устойчивого развития на учебных мероприятиях требуется, чтобы все участники оценки четко понимали критерии оценки. Достижение этой цели требует, где это необходимо, раскрытия требований к профессиональному развитию и критериев оценки для устойчивого развития критериев степени и их регистрации в качестве конкретных критериев оценки. Они рассматриваются в ходе ориентационных дискуссий между участниками оценивания и выпускником.

Чтобы обеспечить постоянное улучшение качества образования, организатор демонстрационного экзамена должен собрать информацию о реализации содержания устойчивого развития в подготовительном образовании для получения степени, во время обучения на рабочем месте и на мероприятиях для получения степени. Важно, чтобы информация об оценке и обратной связи передавалась между преподавателями и использовалась при разработке содержания и методов обучения.

На основе модели процесса, ориентированного на получение дипломов дополнительного профессионального образования взрослых разработаны восемь критериев устойчивого развития культуры информационной безопасности, относящихся к различным этапам процесса персонализации. Критерии оцениваются, и действия, соответствующие критериям, могут быть разных уровней. Критерии устойчивого развития перечислены ниже поэтапно.

Фаза подачи заявки. Критерий 1: Организатор экзамена на степень гарантирует, что персонализация степени определяется и оценивается на основе требований к компетентности критериев степени.

Этап приобретения необходимых навыков / подготовительное обучение.

Критерий 2: Учтены содержание и реализация подготовительного тренинга.

- требования к профессиональной компетентности для устойчивого развития в соответствии с критериями степени, открытыми для конкретных требований;

- другие ключевые аспекты профессионального развития и профессии, определенные отдельно, и требования к ключевым компетенциям, которые не включены в критерии степени.

Этап приобретения необходимых навыков / планирование и контроль обучения на рабочем месте. Критерий 6: Ключевые аспекты устойчивого развития профессий и рабочих мест были приняты во внимание при обучении а рабочем месте. Цели обучения для устойчивого развития обучения на рабочем месте были запланированы и решены вместе с консультантами на рабочем месте.

Этап завершения. Критерий 7: Требования к профессиональной компетентности для устойчивого развития в соответствии с критериями степени оцениваются на мероприятиях для получения степени. При необходимости требования профессионального развития для устойчивого развития, объекты оценки и критерии оценки открываются и фиксируются как конкретные критерии оценки и обсуждаются вместе с участниками оценки.

Оценка и обратная связь. Критерий 8: Организатор демонстрации изучает и оценивает реализацию содержания устойчивого развития культуры информационной безопасности в подготовительном образовании и обучении на рабочем месте, а также компетентность выпускников в области устойчивого развития в мероприятиях на получение степени. Информация об оценке и обратной связи используется при разработке процесса получения степени.

Критерии и инструмент самооценки предоставляют образовательным учреждениям инструмент для разработки программ дополнительного профессионального образования взрослых для формирования культуры информационной безопасности. Они также служат основой для распространения сертификации учебных заведений в области устойчивого развития на дополнительное профессиональное образование взрослых.

Целью самооценки является изучение реализации целей и мер, установленных в программе устойчивого развития в учреждении, а также состояния проблем устойчивого развития в целом. Цель оценки - выявить операционные сильные стороны, передовой опыт и потребности в развитии, чтобы улучшить работу по устойчивому развитию. Для каждого критерия создаются описания уровня на основе модели для конкретного критерия, такие как отсутствующий, начатый, разработанный или установленный. Основываясь на списке вопросов, организатор экзамена сможет оценить свой уровень по всем критериям. Критерии позволяют включить дополнительную профессиональную подготовку с ориентацией на получение степени в сертификационные аудиты в области устойчивого развития.

Список использованных источников:

1. Bernd W. Wirtz et al. Strategic Development of Business Models // Long Range Planning. 2010. Vol. 43. №. 2-3. P. 272–290.
2. Jones, B. Web 2.0 Heroes: Interviews with 20 Web 2.0 Influencers. Wiley, 2008. 273 p.
3. Pedley, D. Understanding the UK cyber security skills labour market / D. Pedley, D. McHenry, H. Motha, J. Shah. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf.
4. Вилкова А. В., Литвишков В. М., Швырев Б. А. Проблемы непрерывного обучения персонала информационной безопасности // Мир науки, культуры, образования. 2019. № 4 (77). С. 29–31.
5. Гузеев М. С., Швырев Б. А. Информационная безопасность дистанционной работы в условиях пандемии // Уголовно-исполнительная система: право, экономика, управление. 2022. № 3. С. 21–27.
6. Ковалев О. Г., Вилкова А. В., Швырев Б. А. Методология формирования знаний об информационной и компьютерной безопасности учреждений УИС // Уголовно-исполнительная система: право, экономика, управление. 2022. № 4. С. 25–27.
7. Швырев Б. А. О безопасности в киберпространстве //Международный журнал гуманитарных и естественных наук. 2021. № 1-1 (52). С. 93–97.

*Гузеев М. С.¹,
старший научный сотрудник
Научно-исследовательского
института ФСИИ России,
кандидат педагогических наук*

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В РАЗРЕЗЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Многие компании тратят сотни тысяч долларов на обеспечение корпоративной компьютерной безопасности. Система безопасности защищает секреты компании, помогает соблюдать федеральные законы и обеспечивает конфиденциальность клиентов компании. К сожалению, с помощью социальной инженерии можно обойти даже самые лучшие механизмы безопасности. Социальная инженерия использует очень дешевые и низкотехнологичные средства для преодоления препятствий, создаваемых мерами информационной безопасности. В завершении приводятся рекомендации по минимизации угроз социальной инженерии.

Миллионы долларов тратятся как на меры информационной безопасности, так и на исследования и разработки в этой области. Эти меры предназначены для предотвращения доступа посторонних лиц к компьютерным системам, а также для предотвращения получения авторизованными пользователями дополнительных привилегий [1, с. 12]. Надлежащие технические меры безопасности могут эффективно противостоять практически любой технической угрозе, исходящей от постороннего лица. К сожалению, самая серьезная атака может иметь не технический характер.

Социальная инженерия - это термин, который хакерское сообщество связывает с процессом использования социальных взаимодействий для получения информации о компьютерной системе «жертвы». Во многих случаях хакер наугад звонит в компанию и спрашивает у людей их пароли. В более сложных обстоятельствах хакер может рыться в мусоре или выдавать себя за охранника, чтобы получить важную информацию. Хотя эти методы кажутся смешными и, возможно, даже смешными, они чрезвычайно эффективны. Социальная инженерия предоставляет хакерам эффективные короткие пути и во многих случаях облегчают атаки, которые были бы невозможны с помощью других средств. Например, мастера обмана, которые значительно проникли в телекоммуникационную систему Соединенных Штатов, смогли сделать это только после получения информации, найденной в мусоре Нью-Йоркской телефонной компании [1, с. 22].

Основные способы защиты от атаки с приемами социальной инженерии.

Несмотря на строгие меры безопасности, злоумышленники могут добиться огромного успеха за очень короткий период времени. Хотя атака может показаться очень сложной и требующей много времени, она может быть проведена за короткое время и стоить очень мало. Многие уязвимые места, используемые злоумышленниками, являются общими для большинства компаний. Выявление

¹ © Гузеев М. С., 2022.

недостатков поможет компаниям преодолеть их и защититься от методов социальной инженерии.

Время от времени злоумышленники просят подтвердить свою личность как настоящих сотрудников, указав свой номер сотрудника или учетное имя компьютера корпоративной сети [2, с. 29]. Компании должны иметь отдельный идентификатор для своей компьютерной поддержки [3, с. 24]. Наличие отдельного идентификатора для компьютерной деятельности отделит функции персонала от функций поддержки и обеспечит дополнительную безопасность как для персонала, так и для компьютерной деятельности.

Многие атаки можно было бы предотвратить, если бы сотрудники компании проверяли личность звонящего, перезвонив им по правильному номеру телефона, указанному в телефонном справочнике компании. Эта процедура создает минимальные неудобства для законной деятельности, однако по сравнению с объемом потенциальных убытков, неудобства в значительной степени оправданы. Если сотрудники обязаны перезвонить любому, кто запрашивает личную или конфиденциальную информацию, компрометация любого характера будет сведена к минимуму. Для этой цели также могут быть приемлемы услуги идентификации вызывающего абонента.

Реализуйте программу повышения осведомленности о безопасности.

Если сообщать свой пароль незнакомому человеку может показаться нелепым для профессионалов, это кажется безобидным для многих пользователей компьютеров. Компании тратят миллионы долларов на приобретение современных аппаратных и программных устройств безопасности, но при этом игнорируются программы общей осведомленности. Компьютерные профессионалы не могут предполагать, что базовые методы обеспечения безопасности являются базовыми для непрофессионалов [4, с. 25–26]. Хорошая программа повышения осведомленности о безопасности может быть реализована с минимальными затратами и может сэкономить компании миллионы рублей убытков.

Каждый сотрудник компании должен быть лично знаком с компьютерным аналитиком. На более чем 60 пользователей должен приходиться один аналитик. Аналитики должны быть координационным центром всей компьютерной поддержки и должны быть единственными людьми, напрямую контактирующими с пользователями. Пользователи должны быть проинструктированы немедленно связаться со своим аналитиком, если к ним обратится кто-то другой, утверждающий, что он из службы поддержки компьютера [5, с. 94–97].

Во время атак злоумышленники осознают, что даже если они будут обнаружены, у сотрудника не будет возможности предупредить других сотрудников о возможной атаке. Это означает, что даже если в атаке был обнаружен компромисс, атака могла продолжиться с минимальными изменениями. По сути, компромисс только улучшил бы атаку, потому что злоумышленники узнали бы, что не работает.

Социальная инженерия – единственно возможный метод проверки политик безопасности и их эффективности. В то время как многие оценки безопасности проверяют физические и электронные уязвимости, немногие анализы уязвимо-

стей изучают человеческие уязвимости, унаследованные от пользователей. Следует отметить, что эти атаки должны выполнять только квалифицированные и заслуживающие доверия люди.

Даже самые лучшие технические механизмы не смогут предотвратить нападение. Атака социальной инженерии выявляет уязвимости в политиках безопасности и осведомленности, которые нельзя обнаружить другими способами. В целом атаки социальной инженерии обнаруживают проблемы во многих организациях. Однако каждая атака вызовет проблемы, специфичные для исследуемой организации. Именно по этой причине каждая оценка угрозы должна включать тщательную социальную инженерию, выполняемую квалифицированными и надежными людьми.

Сотрудники подразделений информационной безопасности должны учитывать нетехнические аспекты компьютерной безопасности наряду с техническими мерами. Слишком часто компьютерные профессионалы считают, что основные принципы компьютерной безопасности известны каждому. Это опасное предположение, и слишком часто оно оказывается неверным. Должна быть комплексная программа обеспечения информационной безопасности, которая включает постоянную программу повышения осведомленности о безопасности.

Список использованных источников:

1. Швырев Б. А. Основные понятия национальной кибербезопасности государств, входящих в Северо-Атлантический альянс : монография. М., 2018. 114 с.
2. Вилкова А. В., Литвишков В. М., Швырев Б. А. Проблемы непрерывного обучения персонала информационной безопасности // Мир науки, культуры, образования. 2019. № 4 (77). С. 29–31.
3. Гузеев М. С., Швыряев Б. А. Информационная безопасность дистанционной работы в условиях пандемии // Уголовно-исполнительная система: право, экономика, управление. 2022. № 3. С. 21–27.
4. Ковалев О. Г., Вилкова А. В., Швырев Б. А. Методология формирования знаний об информационной и компьютерной безопасности учреждений УИС // Уголовно-исполнительная система: право, экономика, управление. 2022. № 4. С. 25–27.
5. Швырев Б. А. О безопасности в киберпространстве //Международный журнал гуманитарных и естественных наук. 2021. № 1-1 (52). С. 93–97.

Ермакова А. С.¹,
*курсант Института-факультета
подготовки сотрудников для органов
предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Худяков В. В.,
*доцент кафедры информатики
и математики Московского университета
МВД имени В.Я. Кикотя*

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ – ВОЗМОЖНЫЕ РИСКИ УГРОЗЫ БЕЗОПАСНОСТИ

Современный мир с каждым днем все больше и больше движется в сторону цифровизации общественных отношений, развития новых информационных систем. В этом огромном массиве данных, которые человечество обрабатывает каждую минуту, особую роль играют персональные данные человека. Каждый раз при использовании банковских программ либо сайтов государственных организаций мы соглашаемся на обработку наших персональных данных. Тогда возникает закономерный вопрос: обработка персональных данных – это некий рудимент, доставшийся нам в наследство от предыдущих поколений, либо острая необходимость, обусловленная вызовами современной реальности? Ответить на эти вопросы мы постараемся в рамках данной статьи.

Практически каждый день мы сталкиваемся с таким понятием, как персональные данные, но мало кто задумывается о том, что же подразумевается под этим понятием. Рассматривая данный термин с научной точки зрения, можно сказать, что персональные данные представляют собой совокупность сведений о субъекте правоотношений, которые в свою очередь хранятся в установленном законом порядке и подлежат установленной законом защите. Интерпретируя данное определение более простым языком, можно сказать так: персональные данные – это совокупность каких-либо данных о конкретном лице, которые охраняются в соответствии с законодательством Российской Федерации.

На практике персональные данные принято разграничивать по критерию отнесимости к различным сторонам жизни человека. Так, выделяют всего пять видов персональных данных [4]:

1. Общие – т. е. данные, которые просто дают общую характеристику лица, например, пол, возраст, ФИО.
2. Биометрические – данные, которые непосредственно связаны с биологической стороной жизни человека. В данную группу относятся все данные медицинского характера: наличие каких-либо заболеваний у лица, дактилоскопические базы данных, и т. д.

¹ © Ермакова А. С., 2022.

3. Специальные – данная группа непосредственно связана с духовной стороной жизни человека, так, например, в данную группу относятся сведения о расе, национальности, принадлежности человека к каким-либо религиозным течениям и т. д.

4. Общедоступные – т. е. данные, которые лицо само распространило о себе, например, сведения о месте работы или учебы, родственные связи и т. д.

5. Обезличенные – данные, которые не позволяют идентифицировать человека, без наличия каких-либо дополнительных данных. Зачастую такие данные представляют собой зашифрованные сведения, представленные в виде таблиц.

Подобное разнообразие персональных данных обязывает государственные органы, осуществляющие сбор и хранение персональных данных, принимать меры к защите персональных данных. Защита данных – один из краеугольных камней в вопросе обработки персональных, поскольку от того, как будет организована защита персональных данных на прямую зависит безопасность тех лиц, которым эти данные принадлежат.

В настоящее время наиболее распространены следующие способы защиты персональных данных:

1. Ограничение доступа лиц в помещения, где хранится оборудование, содержащие в себе персональные данные – речь идет об ограничении доступа лиц в помещения серверных комнат, где находятся сервера с персональными данными.

2. Ограничение доступа пользователей к определенным видам компьютерной информации – говоря иными словами, установление паролей на те программы и файлы, к которым есть доступ только у определенного круга лиц.

3. Использование средств антивирусной защиты – поскольку одним из основных средств взлома доступа к персональным данным являются различного рода шпионские и вредоносные программы, то использование защитного программного обеспечения является ключевым способом защиты данных.

4. Использование особых технических средств, позволяющих обеспечить защиту данных в пределах той территории, где они хранятся – данными техническими средствами могут быть различного рода камеры видео наблюдения, кодовые замки и т. д.

Как мы можем видеть в настоящее время применяется весьма широкий перечень средств обеспечения безопасности персональных данных. Изучив механизмы защиты у обыкновенного человека, может возникнуть закономерный вопрос: зачем необходимы такие меры безопасности? Какие угрозы влечет за собой утечка персональных данных?

Подобные меры безопасности сформировались не сразу, а постепенно, с учетом международного опыта. Сама по себе утечка данных как таковых угроз не несет, если не располагать достаточными знаниями и опытом. В случае же если персональные данные становятся известны криминальным структурам, то последствия для лиц, чьи данные были взломаны, могут быть печальными.

Так, например, получение третьими лицами данных о банковских счетах пользователя может повлечь потерю денежных средств со счетов. Раскрытые паспортные данные позволяют злоумышленникам осуществлять различного рода

манипуляции с денежными средствами в микро финансовых организациях, без ведома лица, чьи данные были взломаны, что в конечном итоге повлечет существенный материальный ущерб для этого лица.

Однако утрата денежных средств не является самым главным последствием утечки персональных данных. Так, при получении третьими лицами полных сведений о лице, становится возможным создать цифровой образ человека, и через такие фальшивые лица осуществлять экстремистскую деятельность.

Именно по причине того, что распространение персональных данных может повлечь за собой ряд неблагоприятных, с точки зрения закона, последствий, были выработаны меры предосторожности, при обработке персональных данных. Например, должностные инструкции, предписывающие исключать доступ компьютерных устройств, на которых хранятся персональные данные, к сети Интернет. Подобная мера призвана исключить неправомерный доступ к охраняемой информации. Или же, например, одной из мер можно считать необходимость авторизации пользователя при использовании аккаунтов, на которых хранятся персональные данные.

Все вышеперечисленные меры предосторожности и способы защиты наталкивают еще на один достаточно очевидный вопрос: а так ли нам необходим процесс обработки персональных данных? Ведь на данный процесс затрачивают огромные ресурсы и средства.

По моему мнению процесс обработки персональных данных лиц является неотъемлемой частью современной жизни. Развитие баз данных существенно упростило работу во многих отраслях. Так, например, в органах внутренних дел достаточно активно развиваются всевозможные виды учетов, которые также содержат в себе персональные данные о лицах, ранее привлекаемых к уголовной и административной ответственности.

Наличие баз данных упрощает процесс сбора необходимой информации о лице. Так, органы лицензионно-разрешительной системы располагают обобщенными базами данных, позволяющие в короткий период времени принять решение о возможности предоставления лицу разрешения на хранение огнестрельного оружия. Службы безопасности дорожного движения в процессе своей деятельности также используют базы персональных данных, в которых отображаются штрафы и ограничения конкретных лиц, что позволяет оперативнее выявлять нарушителей на дорогах. Банки, в свою очередь, собирают персональные данные о заработной плате своих клиентов, что позволяет им быстрее принимать решение о выдаче или отказе в выдаче потребительского кредита.

Современный мир все больше уходит в сферу цифрового документооборота, что несомненно является более удобной альтернативой привычным нам бумажным документам и многотомным архивным делам. В каждой сфере деятельности создаются базы данных, аккумулирующие в себе персональные сведения о лицах. Но в то же время подобное развитие информационных систем требует повышенной защиты этих самых данных, поскольку оцифрованные персональные данные на много более уязвимы для внешнего воздействия, нежели привычные нам бумажные документы.

По моему мнению, в настоящий момент обработка персональных данных является жизненной необходимостью для всех сфер государственного управления. Однако следует принимать меры по совершенствованию систем защиты данной информации, а именно:

1. Качественно повысить профессиональный уровень сотрудников, работающих с персональными данными – т. е. обучить их всем тонкостям работы с компьютерной техникой. Данная мера позволит избежать допуска необученных лиц к охраняемой законом информации.

2. Разработка новых защитных программ, с многоуровневой системой защиты – подобным направлением в нашей стране занимается лаборатория Касперского. Именно их программное обеспечение позволяет избежать большинства утечек информации.

3. Создание особого регламента хранения всех типов персональных данных – т. е. усиление охраны зданий и помещений, где происходит обработка персональных данных.

Подводя итог, следует отметить, что обработка персональных данных в настоящее время является необходимым элементом функционирования всех государственных органов, поскольку на базах персональных данных выстроены все процессы государственного управления. От необходимости собирать, хранить и обрабатывать персональные данные человечество уйдет еще не скоро, а следовательно, нам необходимо принимать все возможные меры по защите персональных данных от утечек и взломов, а для этого нам необходимо существенно повысить текущий уровень защиты.

На наш взгляд, государство должно серьезно задуматься над тем, чтобы усилить подготовку профессиональных кадров, осуществляющих обработку персональных данных, а также повышать уровень компьютерной грамотности среди населения. Только благодаря таким действиям мы сможем получить относительно безопасную компьютерную среду. Помимо работ в направлении повышения уровня владения компьютером, что является не мало важным при работе с персональными данными, государство также должно быть заинтересованно в развитии систем защиты компьютерной информации, а для этого необходимо усиливать государственную поддержку тем институтам, которые занимаются разработкой защитного программного обеспечения.

По нашему мнению, вопрос обеспечения безопасности персональных данных, является вопросом из сферы интересов обеспечения национальной безопасности, именно по этой причине необходимо проведение целого комплекса мероприятий, направленных на искоренение существующих угроз. Только в случае проведения таких мероприятий мы сможем осуществлять безопасную обработку персональных данных, которая является жизненной необходимостью в современных реалиях.

Список использованных источников:

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных законами о поправках к Конституции Российской Федерации от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ,

от 14.03.2020 № 1-ФКЗ, с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_28399/.

2. Конвенция о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_121499/.

3. Конвенция Содружества Независимых Государств о правах и основных свободах человека от 26 мая 1995 г. // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_6966/.

4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.

5. Загородников С. Н., Максимов Д. А. Чужие тайны и их защита: нормативно-правовые аспекты // Российский следователь. 2014. № 3. С. 40.

6. Трудовое право : учебник / [В. М. Лебедев, Д. В. Агашев, А. А. Белинин и др.] ; под ред. В. М. Лебедева. М. : Норма : Инфра-М, 2018. 464 с.

7. Лушников А. М. Российское трудовое право: вызовы XXI века // Lex russica. 2014. № 3. С. 284–293.

8. Семенихин В. В. Кадровое делопроизводство. М. : ГроссМедиа, РОСБУХ, 2015. 624 с.

9. Терещенко Л. К. Правовой режим персональных данных и безопасность личности // Закон. 2018. № 6. С. 37–43.

10. Трофимова И. А. Обработка и хранение персональных данных // Делопр-изводство. 2015. № 3. С. 107–110.

11. Яковец Е. Н. Своеобразие состава защищаемой конфиденциальной информации // Право и кибербезопасность. 2014. № 2. С. 51–58.

Борзунов К. К.¹,
*доцент кафедры информационной
безопасности учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук*

ОТКРЫТЫЕ ЦИФРОВЫЕ ИСТОЧНИКИ В СОКРЫТИИ РАЗВЕДЫВАТЕЛЬНЫХ МЕРОПРИЯТИЙ

Информационные сферы, связанные с современным состоянием общества и государства, является результатом таких глобальных процессов, как информационный взрыв, цифровизация, цифровая трансформация и др.

Плоды этих революционных преобразований – виртуальные киберпространства, возникшие на основе компьютеризации, активного развития и широкого распространения телекоммуникаций и информатизации практически всех сфер жизнедеятельности общества и государства. Обращают внимание на себя такие информационные сферы, как государственная, коммерческая и торговая, производственная и общественная.

Информационные сферы цифрового мира. Информационные сферы общества изобилуют персональными данными (в виде отчасти обезличенной некоторой текстовой информации, идентифицирующих данных и признаков, картотечных учетных данных и т. д.) населения по причинам нестрогого соблюдения требований конфиденциальности; отражением неограниченного многообразия событий жизни людей (в виде фотографий, аудио- и видеозаписей, текстовых сообщений, заметок, комментариев и т. д.); следами коммуникативных связей людей (в виде их участия в блогах, чатах, широкого использования мессенджеров, электронной почты, социальных страничек и др.).

Информационные сферы коммерции и торговли, производства, оказания широчайшего спектра услуг (юридических, медицинских ..., найма и обслуживания, путешествий и развлечений) аккумулируют данные и сведения, относящиеся косвенно к полному спектру тайн, представляющих область конфиденциальности; отражают успехи и неудачи (публичные отчеты), сотрудничество и соперничество среди юридических и физических лиц (взаимные претензии, рейтинги репутации); раскрывают интересы в этой сфере различных социальных слоев (статистические данные, социологические опросы).

В информационных сферах государства, ведомств и министерств накапливаются соответствующие ресурсы, предназначенные для удовлетворения потребностей граждан, содержащие, в частности, перспективы решения социальных проблем и официальные публичные отчеты в области государственной деятельности (отчеты правительства, министерств и ведомств, налоговые и финансовые, крупного и среднего бизнеса); публичные материалы в области судопроизвод-

¹ © Борзунов К. К., 2022.

ства (решения, постановления, частные определения) и, в частности, транспортных рейсов (воздушных, морских, автомобильных и железнодорожных) по магистралям, геопространственных данных по разнообразным местам планеты (города, природные парки, исторические места, деловые и развлекательные центры, транспортные узлы).

Информационные ресурсы цифрового мира. Ресурсы СМИ впитывают в себя и распространяют новости, факты, события. Позволяют комментировать происходящее и зафиксированное, вести дискуссии, формируя общественное мнение. Однако следует учитывать, что в условиях информационных войн, проведения информационно-психологических акций в отношении населения и отдельных социальных слоев, массового вброса дезинформации на основе технологий дипфейков (технология дипфейк – технология создания и замены элементов на существующих видео при помощи искусственного интеллекта и нейронных сетей) одурманивания и одурачивания населения, состояние достоверности, надежности и адекватности ресурсов СМИ становится неопределенным. Использование этих ресурсов несет угрозы.

Отдельно обращают на себя внимание информационные ресурсы так называемой «желтой» или «бульварной» прессы, впитывающие в себя «весь брак и все отходы» журналистики – слухи и сплетни, сенсации (действительные и мнимые), скандалы. При этом материалы данного ресурса предстают в виде «коктейлей» лжи и правды, недостоверности, неподтвержденности и надуманности, нарочитой вульгарности.

На фоне этого взрывного накопления данных в самое последнее время отмечается тенденция взрывного появления алгоритмов обработки данных и доступа к данным. Результат уже этого процесса – широчайший спектр условно бесплатных программных продуктов (пока еще «полуфабрикатов»), так называемых инструментов OSINT (от англ. Open Source INTelligence) [1] или, по-русски, инструментов разведки по открытым источникам.

Легальная разведка в цифровом мире. Отметим, что акцент этой практической деятельности переносится именно на открытые источники данных и сведений, сообщений о разнообразных фактах. Они анализируются в ходе реализации специфического комплекса мероприятий, инструментов и методов [2; 3], который может быть применен в отношении конкретных людей, организаций, а также событий, явлений.

Однако грань того, что отделяет OSINT от шпионажа достаточно тонкая и размытая. Некоторые оппоненты апеллируют к такому качеству OSINT, как легальность, отмечая, что «сбор и анализ информации, находящейся в общественном достоянии, не противоречат нормам международного законодательства, а также законам большинства государств, хотя некоторые источники и способы их исследования могут находиться на грани законности». Второй довод данных оппонентов в отношении такого качества OSINT, как доступность, – обращение внимание на допустимость «мониторить и анализировать общедоступные источники любой организацией и даже отдельным человеком без использования специализированного оборудования или «связей» в органах госбезопасности».

Однако технологии сведения воедино разрозненных порций данных, сведений, фактов, сообщений о каких-либо объектах в сочетании с их анализом как раз и позволяют получить новое качество – информацию, а не механическую сумму полученного. Более того, возникает возможность определить идентифицирующие признаки и данные конкретных объектов.

Второй аспект упомянутой тонкой и размытой грани связан и с «мягкостью (не строгостью)» обеспечения конфиденциальности данных и сведений в информационных ресурсах сети Интернет, и с появления алгоритмов доступа к данным, а для неподготовленных пользователей и специфических инструментов OSINT.

Уровни глобальной сети. В контексте использования информационных ресурсов следует отметить особенности глобальной сети [4], существенные в рамках обозначенной темы. Вообще-то существуют на текущий момент времени три уровня глобальной сети, которые необходимо принимать во внимание.

Уровень «видимая сеть». Этот уровень еще иногда называют «чистая сеть». Данный уровень сети доступен любому пользователю в любое время за счет того, что он содержит индексируемые страницы, доступ к которым осуществляется через соответствующие браузеры и поисковые системы. При этом администраторы сайтов этого уровня управляют доступом к цифровым источникам, а именно доступом к файлам фронтенда и к файлам бэкенда.

Таким образом, пользователь этого уровня сети имеет доступ к файлам фронтенда и не имеет доступ к файлам бэкенда, в частности, к страницам учетных записей и архивам.

На примере онлайн-магазинов: пользователю можно просматривать каталоги продуктов, но он при этом ограничен в просмотре и действиях до входа в учетную запись. Вход в учетную запись означает, что пользователь переходит на следующий уровень «глубинной сети».

Уровень «глубинная сеть». Этот уровень является частным и, как правило, защищен паролем. Ресурсы этого уровня по объему составляют по оценкам экспертов около 96 % интернета. На этом уровне не возможен доступ к страницам через обычный поиск, поскольку здесь поисковые системы не индексируют страницы. Пользователь должен заранее обладать конкретной ссылкой или данными для входа, в частности URL-ссылкой и соответствующим паролем. Объектами данного уровня являются: облачные хранилище или диски; базы данных различных организаций, учреждений, предприятий, фирм, компаний; страницы учетных записей на разных сайтах, в частности: медицинские записи, данные банковских карт, отчеты и другие подобные страницы.

На уровнях «видимая сеть», «глубинная сеть» применяются, как говорят, обычные браузеры, в частности такие, как: Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Яндекс.Браузер и некоторые другие. Пользователь, работая с тем или иным браузером, имеет возможность обратиться к соответствующей поисковой системе. И, наконец, третий уровень, который сложнее всего обнаруживается.

Уровень «даркнет». Имеет и другие названия: темный интернет, темная сеть, теневая сеть, темный веб и другие. Суть этого уровня в том, что эта часть сети

скрыта. Она состоит из сайтов, к которым доступ реализуется с использованием не обычных браузеров, ранее упоминавшихся, а специализированных браузеров, а, точнее, специальных программ, среди которых популярным до сих пор является Tor. Но, известны и другие точки входа на уровень скрытой части сети: Freenet, Riffle, I2P.

Аналоги Tor: ExpressVPN – скоростной аналог Tor; NordVPN – обеспечивает оптимальный обмен файлами по протоколу P2P, защиту от DDoS-атак, использует двойное шифрование VPN; FreeNet – объединяет технологии OpenNet и DarkNet, функционирует, собирая данные в одноранговых узлах, а затем загруженный контент отправляет через его же различные узлы; I2P (*сверка выражения: I+I+P*) – невидимый интернет – проект, обеспечивающий анонимную сеть, которая позволяет реализовать безопасную связь между пользователями путем создания программным клиентом пользователя дискретного количества безопасных «туннелей», через которые и передаются сообщения «внутри» или «наружу».

Итак, фактически эта скрытая часть сети не регулируется и не контролируется, хотя, конечно же, попытки со стороны правоохранительных органов и специальных служб многих государств предпринимаются. По причине бесконтрольности в скрытой части сети организованы и действуют как законные, так и незаконные сайты.

Естественно следует отметить, что упомянутые браузеры уровня «*даркнет*» предоставляют весьма ограниченную и сомнительную защиту в том, плане, что даже интернет-провайдер фиксирует использование скрытой части сети. Это происходит потому, что браузеры выступают только в роли шлюзов для входа в скрытую часть сети и предоставляют доступ к сети. И при этом личные данные пользователя остаются уязвимыми для заинтересованных субъектов (любопытных глаз, хакеров, киберпреступников, оперативных сотрудников и др.), несмотря даже на то, что пользователь применяет дополнительный уровень безопасности через VPN-подключение.

Рассмотренные уровни глобальной сети вполне очевидно показывают слабость аргумента легальности OSINT в части касающейся того, что цифровые источники уровня «*глубинная сеть*» и в намного большей мере уровня «*даркнет*» фактически в действительности находятся на грани законности и более того способны доступа к ним также на грани законности.

Уменьшение тонкости и увеличение размытости грани, отделяющей OSINT от разведывательных мероприятий, связано и с фактическим наполнением неиндексируемыми данными информационных ресурсов сети. Как правило, эти данные по своей сути являются результатом либо утечки информации ограниченного доступа, либо изначального формирования данных с таким статусом, когда данная задача решалась путем использования информационных технологий, не соответствующих общепринятым международным стандартам сбора, хранения и передачи данных для глобальной сети Интернет.

В качестве итога можно сделать вывод о том, что реальна и возможна скрытая реализация разведывательных мероприятий. Она прикрыта цифровыми источниками, сомнительной открытости или легальности.

Причинами этой реальности и возможности стали: произошедшие глобальные процессы: информационный взрыв, цифровизация, цифровая трансформация. При этом возникает виртуальное киберпространство на базе глобальных телекоммуникаций и цифровых источников, а также взрывное увеличение количества алгоритмов обработки данных и доступа к данным, приводит к разработке на их основе многочисленных так называемых инструментов OSINT.

Список использованных источников:

1. OSINT (Open Source INTelligence) // Сайт «SkillFactory.блог». URL: <https://blog.skillfactory.ru/glossary/osint/>.
2. Инструменты OSINT 2022 (Часть 1) // Сайт «Advisor». URL: <https://www.advisor-bm.com/osint-tools>.
3. Инструменты OSINT 2022 (Часть 2) // Сайт «Advisor». URL: <https://www.advisor-bm.com/osint-tools-catalog-part2>.
4. Deep web, dark web, darknet и surface web – в чем разница? // Сайт «Каспеский». URL: <https://www.kaspersky.ru/blog/deep-web-dark-web-darknet-surface-web-difference/30044/>.

Байков Д. В.¹,
*слушатель факультета подготовки
специалистов в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Пакляченко М. Ю.²,
*доцент кафедры специальных информационных
технологий учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук*

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Грамотная разработка и эффективная реализация долгосрочных планов, как правило, не относятся числу простейших в исполнении видов деятельности государственного управления, однако, в современной ситуации наблюдаются существенные изменения. Ясно обозначена национальная цель – цифровая трансформация экономики и государственного управления [1].

Реализация цифровых решений должна сократить нагрузку на служащих и работников государственных структур, повысить скорость предоставления услуг гражданам, обозначить действительную проблематику и предложить конструктивные ее разрешения, которые существенно улучшат существование и развитие общества и государства, реализацию организациями управленческих, социально-культурных или иных функций.

Цифровизация страны на всех уровнях государственного управления – значимая характеристика ее конкурентоспособности и результативности как в локальных, так и во внешних действиях. Очевидно, что цифровые технологии принесут беспрецедентные изменения в социальную и экономическую область существования нашего общества.

COVID-19 обнажил недостатки скороспелых цифровых проектов и продемонстрировал насколько значимым на этапе его планирования является определение в архитектуре цифрового решения функционала, ориентированного на обеспечение информационной безопасности, цифровой этики, информационно-технической инклюзии. Непродуманное внедрение информационных технологий в деятельность государственных структур и организаций провоцирует проблематику на стыке права, этики и безопасности (государства, граждан, общества).

¹ © Байков Д. В., 2022.

² © Пакляченко М. Ю., 2022.

Можно обозначить ключевые приоритеты в аспекте обеспечения информационной безопасности в рамках цифровой трансформации государственных органов и организаций:

- сохранение цифрового суверенитета государства как элемента национальной безопасности;
- модификация методик государственного администрирования, ориентированная на высококачественные данные, для минимизации издержек при оказании государственных услуг и исполнении функций и для достижения иной степени безопасности общества (в том числе информационной);
- исключение угрозы национальной безопасности на уровнях государственного регулирования и правоприменения в направлении использования аппаратного и программного обеспечения иностранных государств путем создания отечественной инфраструктуры, внедрения в учреждениях и организациях культуры безопасной работы с информацией;
- выявление и исключение правовых ограничений для внедрения и применения цифровых технологий, разработка стандартов безопасности для органов власти и государственных организаций по информационной инфраструктуре, программному обеспечению, работе с данными, электронному документообороту;
- формирование единого инфо-пространства для реализации прав людей в отношении получения объективных, достоверных и защищенных сведений.

Указами Президента Российской Федерации [2], цифровая трансформация определяется как одна из национальных целей развития страны, а задачами [3], требующими своего обеспечения являются:

- формирование оперативной и защищенной цифровой образовательной среды, реализующей эффективность и доступность образования;
- приобретение всеми желающими компетенций в сфере цифровой экономики;
- совершенствование кадрового обеспечения на базе информационных и коммуникационных технологий и платформенных решений;
- формирование и исполнение новых стандартов и требований обустройства инфраструктуры государства на основе цифровых технологий.

Согласно [4] отмечается, что применение цифровых решений стало элементом современных административных систем в сферах государственного управления, обороны и безопасности страны, обеспечения правопорядка, а также в большинстве отраслей экономики. В утвержденной данным указом Президента Российской Федерации Стратегии развития информационного общества реализация прав общества на непредвзятую, подлинную и безопасную информацию и формирование обстоятельств для довольствования необходимостью в обрете-нии качественной и подлинной информации, в том числе посредством цифровых решений, выступает первоочередной задачей.

Таким образом, актуальны выявление, анализ и систематизация препятствий на пути цифровой трансформации государственных органов и организаций, равно как и востребованы инициативы в части минимизации или исключения имеющихся и возможных затруднений на пути цифровизации.

Список использованных источников:

1. Распоряжение Правительства Российской Федерации от 22 октября 2021 г. № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru>.
2. Указ Президента Российской Федерации от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru>.
3. Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru>.
4. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru>.

Белов Я. М.¹,
*слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель:
Пакляченко М. Ю.,
*доцент кафедры специальных информационных
технологий учебно-научного
комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук*

ПРИМЕНЕНИЕ ЭКСПЕРИМЕНТАЛЬНЫХ ПРАВОВЫХ РЕЖИМОВ (ПЕСОЧНИЦ) В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ В МВД РОССИИ

В последние годы в МВД России стремительно развивается политика обеспечения информационной безопасности, что обусловлено применением современных комплексных систем защиты и созданием новых центров и отделов, которые обеспечивают безопасность данных. Разные подразделения в структуре ГИАЦ МВД России, ДИТСиЗИ МВД России и ГЦСиЗИ МВД России занимаются не только применением инновационных отечественных продуктов и цифровых решений, но и разработкой предложений в нормативно-правовые источники, регламентирующие вопросы внедрения и эксплуатации указанных технологий в служебную деятельность подразделений министерства.

Снизить юридические неопределенности и некоторые нормативные риски в связи с применением передовых технологий, за которыми не успевает законодатель, призвано явление экспериментального правового режима, который регламентируется законом [1]. Данные режимы еще называют «регуляторные песочницы», которые формируют собой ограниченную среду для проведения организационных экспериментов с технологиями без угрозы нарушения норм права.

Вместе с тем существуют иные «песочницы» – в программно-аппаратном поле, которые представляют собой системы для детектирования вредоносных программ, продолжающих быть одной из основных угроз для безопасности любой информационной системе, в том числе автоматизированным системам МВД России.

Для борьбы с вирусами могут быть использованы решения, работающие по технологии песочница: Kaspersky Anti-Targetted Attack (КАТА) [2], MaxPatrol и др.

Рассмотрим КАТА. В данном продукте реализована песочница, которая является прослойкой между атакуемым ресурсом и атакующим, предназначена для те-

¹ © Белов Я. М., 2022.

стирования различной информации, среди которой может быть письмо, отправляемое на служебную почту, установленное программное средство, несертифицированное для работы на аттестованном АРМ, а также многое другое.

Для юридического сопровождения реализации цели обеспечения защиты информации в России принят закон о семи проектах для «цифровой песочницы». Воплощение указанных мероприятий возможно посредством применения киберполигонов, которые представляются как технологическая база для моделирования реальных участков информационной инфраструктуры, позволяющая проводить учения по вопросам обеспечения информационной безопасности.

Подробно определим, как Kaspersky позиционирует свою песочницу. Это система, которая выполняет анализ подозрительных объектов в виртуальной машине, ограниченной от реальной инфраструктуры, определяя в объекте наличие опасных артефактов и сигнатур, на основании наличия которых делается вывод о зловредности и возможные варианты работы на контролируемом АРМ.

Около двух лет назад вендор разработал собственную песочницу (рис. 1), которая используется как основной инструмент для анализа вредоносных программных объектов и для сохранения сигнатур в антивирусную базу. Помимо этого, песочница является частью огромного комплекса по обеспечению защиты информации, позволяющего классифицировать файлы и URL-адреса на вредоносные и безопасные, накапливать сведения об активности вредоносного программного обеспечения, с целью разработки действий и правил, направленных на детектирование и сопровождение вредоносных проявлений как на отдельных машинах, так и в сетевом периметре.

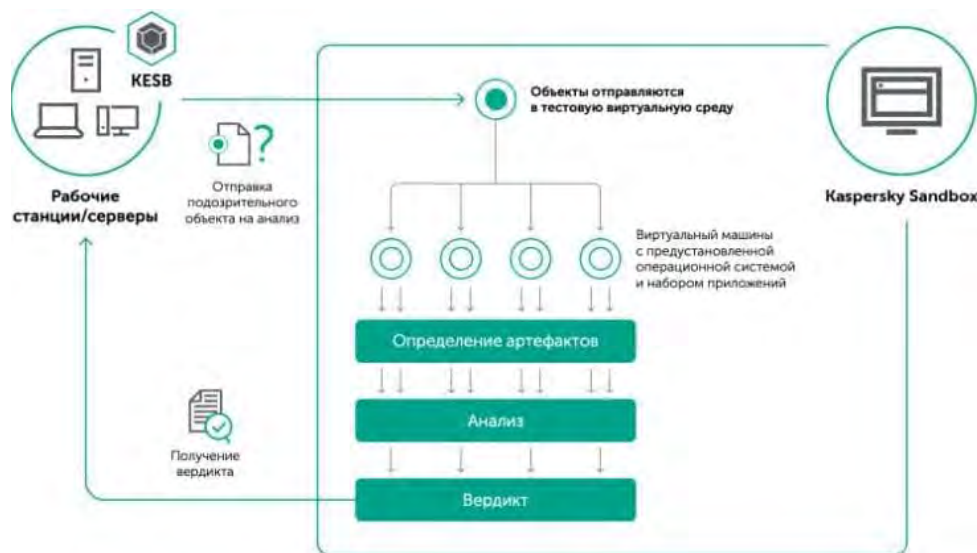


Рис. 1. Схема функционирования Kaspersky Sandbox

На рисунке можно проследить как работает песочница, которая тестирует подозрительный объект, проверяя его на наличие артефактов и различных опасных сигнатур. Данная технология позволяет в эффективно обеспечивать защиту информации.

Отметим, что для защиты информации в МВД России используется целый комплекс программных средств от Kaspersky. Работа с продуктами от указанного

производителя позволяет реализовать эффективное отслеживание и реагирование на все компьютерные события, происходящие на АРМ сотрудников.

Отметим, что перспективы экспериментальных правовых режимов достаточно значимы, так как предоставляется возможность подстроиться под современные реалии в правовом и техническом поле, адаптироваться под актуальные угрозы и атаки. Достоинства экспериментальных правовых режимов проявляются в гибкости и неординарности в сравнении со стандартными нормативно-правовыми источниками [3]. С другой стороны, важно указать на явный минус: многие сотрудники не привыкли к такому явлению и воспринимают его неимперативным, однако это и является преимуществом, так как технические специалисты и разработчики, которые борются с вредоносным программным обеспечением и прочими актуальными угрозами не имеют четко формализованных границ своих возможностей, следовательно, требуют экспериментальности, творчества и оригинальности в любом направлении своей деятельности.

Список использованных источников:

1. Федеральный закон от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/document>.
2. Обзор Kaspersky Sandbox – песочницы для обнаружения целенаправленных атак // Сайт «Anti-malware». URL: <https://www.anti-malware.ru/reviews/Kaspersky-Sandbox#part2>.
3. Экспериментальные правовые режимы в сфере цифровых инноваций в России // Сайт «Tadviser». URL: <https://www.tadviser.ru>.

Жиганин А. Я.¹,
 курсант факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Пакляченко М. Ю.,
 доцент кафедры специальных информационных
 технологий учебно-научного
 комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат технических наук

СИСТЕМА ВЗАИМОДЕЙСТВИЯ ПОЛИЦИИ С ГРАЖДАНАМИ ПОСРЕДСТВОМ TELEGRAM-БОТА

В XXI в. технологии стали охватывать все больше сфер жизнедеятельности человека. В наше время сложно представить себе современного человека без смартфона или компьютера, все больше людей в настоящее время находятся в виртуальном пространстве, в котором они обмениваются информацией друг с другом. Нельзя не отметить роль 2020 г., а именно начавшейся во время него эпидемии коронавируса, послужившей катализатором в процессе повышения активности людей в виртуальном пространстве. Учебные заведения перешли на дистанционный формат учебы, работники различных организаций не посещали офисы, а работали, не выходя из дома.

Однако с февраля 2022 г. внутри виртуального пространства произошли большие изменения. 21 марта 2022 г. Тверской районный суд г. Москвы вынес решение о том, что компания «Meta Platforms», которой принадлежат «Facebook», «Instagram», считается экстремистской организацией, а ее деятельность запрещена в России. В связи с этим, многие пользователи данных площадок перешли в мессенджер «Telegram». Стоит обратить внимание, что к данному мессенджеру особый интерес вызывают новостные каналы, и люди заходят в него скорее для того, чтобы посмотреть актуальные новости, поделиться ими с друзьями и начать дискуссию.

Для того, чтобы иметь более четкое представление о значимости мессенджера Telegram, обратимся к статистике: в 2022 г. Telegram посещают 40 млн российских пользователей в месяц [1], что составляет 1/3 от тех людей, которые пользуются сетью Интернет в России [2]. Помимо этого, на просторах интернета существует перечень российских государственных Telegram-каналов [3], среди которых – личный канал Д. А. Медведева, а также такие ведомства, как МИД России, МЧС России, Министерство обороны Российской Федерации и многие

¹ © Жиганин А. Я., 2022.

другие. К слову, 21 сентября 2022 г. в России была объявлена частичная мобилизация, а на следующий день Правительство Москвы запустило в Telegram чат-бот [4], который помогает горожанам получить ответы на основные вопросы, касающиеся проведения частичной мобилизации в столице.

Указанные преимущества и популярность мессенджера могут быть применимы в процессах оптимизации правоохранительной деятельности, в частности, для разрешения необходимости создания в полиции системы взаимодействия с гражданами в мессенджерах, которая обеспечит связь подразделений МВД России с широкой аудиторией Telegram. Данная система может представлять собой встроенного в Telegram чат-бота, который будет наделен следующими возможностями:

1. Вызов полиции. В Telegram есть возможность отправлять свои номер телефона и местоположение собеседнику, в том числе, чат-боту. Используя данные возможности, граждане могут вызывать на место происшествия сотрудников полиции, присылая все необходимые данные в дежурную часть, которая будет определяться системой исходя из местоположения лица. Граждане смогут вызывать полицию путем отправки текстового или голосового сообщения. В случае с голосовым сообщением, система будет преобразовывать речь человека в текст. Помимо этого, можно предусмотреть возможность отправки фото/видео материалов с места происшествия дежурному.

2. Подача заявления в полицию. Приказ МВД России [5] предусматривает возможность приема, регистрации и разрешения заявлений и сообщений граждан. Система взаимодействия с гражданами может быть наделена возможностью оставления заявления в электронном виде, путем отправки всех необходимых сведений чат-боту. Стоит отметить, что в Telegram есть возможность отправки документов.

3. Оставление обращения. Официальный сайт МВД России обладает сервисом приема обращений, в котором указывается подразделение, в которое должно быть адресовано сообщение, данные об адресанте и текст самого обращения. Данный сервис также может быть встроен в систему взаимодействия полиции с гражданами посредством мессенджера.

4. Публикация новостей из ресурса МВД Медиа. При помощи чат-бота, заинтересованные граждане смогут читать публикации ресурса МВД Медиа, а также отчеты о состоянии преступности текущего года.

5. Уведомление граждан. Чат-бот может уведомлять граждан о криминогенных обстановках, о чрезвычайных ситуациях и происшествиях, происходящих в регионе, в котором проживает гражданин. Следует понимать, что система сможет уведомлять только тех граждан, которые ранее пользовались функционалом данного чат-бота.

Таким образом, система взаимодействия полиции с гражданами посредством Telegram-бота расширит возможности подразделений полиции в области непосредственного взаимодействия с гражданами. Программный модуль данной системы может переписываться и дорабатываться новыми возможностями, построенными под текущую обстановку.

Список использованных источников:

1. Бурный рост Telegram, сговорчивые бондхолдеры «Яндекса» и новые чистки в «Сбере» // Сайт «The Bell». URL: <https://thebell.io/burnyy-rost-telegram-sgovorchivye-bondkholdery-yandeksa-i-novye-chistki-v-sbere>.
2. Интернетом в России пользуются 89 % населения // Сайт «Trashbo». URL: <https://trashbox.ru/link/2022-02-15-digital-2022-russia>.
3. Список российских государственных Telegram-каналов // Сайт «Onff». URL: <https://onff.ru/spisok-rossiiskikh-ghosudarstviennykh-tielieghramm-kanalov/>.
4. Мобилизация 2022 : Telegram-бот // Мессенджер «Telegram». URL: <https://t.me/MobilizationmskBot>.
5. Приказ МВД России от 29 августа 2014 г. № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» (с изменениями и дополнениями) // НПП «Гарант». URL: <https://base.garant.ru/70791976/>.

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

Научный руководитель:
Пакляченко М. Ю.,
*доцент кафедры специальных информационных
технологий учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук*

ИНФОРМАЦИОННЫЕ И ЦИФРОВЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

С каждым днем число угроз, направленных на дестабилизацию кибербезопасности, постоянно растет. Благодаря информатизации общества деятельность киберпреступников больше не сдерживают территориальные границы, поэтому вопросам, связанным с применением цифровых технологий и информационных систем в деятельности органов внутренних дел для оптимизации служебной деятельности в части обеспечения общественной и собственной безопасности, уделяется все больше внимания.

Органы внутренних дел в своей работе используют различные типы информационных, в том числе цифровых, технологий. Примерами таковых могут быть: системы биометрии, системы графической визуализации пространственных данных, средства имитационного и предикационного моделирования, технологии детектирования и оценки объектов. Министерство придает большое значение широкомасштабному развитию инфокоммуникационных технологий и их внедрению в подразделения полиции, примером данного направления может служить единая система информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России) [1].

При помощи представленной системы была реализована возможность объединения разрозненных информационных систем, занимающихся автоматизацией отдельных направлений деятельности полиции. В аспекте кибербезопасности можно отметить, что в архитектуре ИСОД МВД России существует подсистема обеспечения информационной безопасности, состоящая из следующих элементов: криптографические средства защиты; инструментарий электронной подписи; программное обеспечение для предотвращения заражения автомати-

¹ © Смолянинов В. А., 2022.

зированных рабочих место вредоносными программами; сервисное разграничение доступа к ресурсам и системам инфо-инфраструктуры; индивидуальные электронные идентификаторы и др.

Если исходить из концепции применения технологий машинного обучения [2] в повседневную служебную деятельности структур МВД России, ИСОД МВД России может поспособствовать внедрению указанной технологии в систему, что в свою очередь расширит ее путем масштабирования и адаптации под современные требования, позволит автоматизировать типовые и рутинные процедуры, выполняемые сотрудниками полиции, дополнит функционал интеллектуальными системами поддержки принятия решений, построения аналитики и прогнозов, значительно повысит уровень информационного обеспечения учреждений МВД России, поспособствует росту качества проводимой сотрудниками оперативной и аналитической работы.

Затрагивая вопрос цифровых технологий в работе органов внутренних дел, стоит обратить внимание на главный информационный аналитический центр (ГИАЦ МВД России), который в прикладном аспекте выступает наиболее масштабный репозиторий оперативно-справочных и розыскных сведений в системе МВД России, что вводит понятие больших данных (Big Data) [3] в служебную деятельность полиции. В задачи ГИАЦ входит обеспечение органов и учреждений статистическими данными, а также информацией о криминалистической, оперативной, производственной, научно-технической, документарной и архивной деятельности. Данный центр располагает разнообразными формами и видами учетных документов, исчисляемых миллионами единиц, что требует определения надежных технологий защиты больших данных, включая проверку их целостности и достоверности, работу с мета-данными. Объем и скорость передачи данных из существующих источников, таких как устаревшие приложения и электронная коммерция, быстро растут, возникают новые разновидности типов и источников данных, такие как социальные сети и потоки устройств Интернета вещей (IoT). Для того, чтобы соответствовать современным реалиям, стратегия обеспечения конфиденциальности больших данных также должна расширяться.

Таким образом, анализ текущей ситуации МВД России в отношении информационных и цифровых технологий позволяет определить, что в ближайшем будущем в планах развития и внедрения основными направлениями будут выступать технологии Big Data, искусственного интеллекта и машинного обучения, аппаратной и программно-технической поддержки решений для руководства на всех уровнях иерархии, планирования и управления деятельностью, работы исполнителей, оптимизированного единого комплекса в инфраструктуре цифрового и технического обеспечения деятельности подразделений МВД России.

Список использованных источников:

1. Вермеенко Я. С. Современное состояние и перспективы развития ИСОД МВД России // Академическая мысль. 2021. № 3 (16). С. 75–78.
2. Воронов М. В., Пименов В. И., Небаев И. А. Системы искусственного интеллекта : учебник и практикум для вузов. М. : Юрайт, 2022. 256 с.

3. Советов Б. Я., Цехановский В. В. Информационные технологии : учебник для вузов. 7-е изд., перераб. и доп. М. : Юрайт, 2022. 327 с.

Рахмонбердиев Б. Б.¹,
 слушатель факультета подготовки
 иностранных специалистов
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Плотников Г. Г.,
 профессор кафедры информационной
 безопасности учебно-научного
 комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат технических наук

ОЦЕНКА ЭНТРОПИИ ТАБЛИЦ КОДИРОВОК В ЗАДАЧЕ ОПТИМАЛЬНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Информация в современном мире представляет большую ценность, чем раньше представлялось, однако с использованием высокопроизводительных электронно-вычислительных машин не все обращают внимание на объем обрабатываемой и передаваемой информации. В данной статье рассматривается информация с точки зрения оптимальности ее обработки и передачи.

Рассматривая данную задачу, стоит обратить внимание на то, что каждый символ, прежде чем преобразоваться в удобную для обработки и передачи форму, преобразуется в соответствии с таблицей кодировок, где каждый символ имеет свой номер, который в дальнейшем переходит в выбранную систему исчисления. Данная таблица представляет из себя кодировочный алфавит, и определяет информационную емкость системы (энтропию). И так перейдем к вычислениям, данный процесс можно реализовать математическими подсчетами с применением определенного алгоритма действий, а также формул. За меру информации математика считает:

$$I = \log_2 \left(\frac{1}{p} \right) = -\log_2 p.$$

Стоит отметить, что в теории информации использует двоичный (битовый) логарифм:

$$lb a = \log_2 a.$$

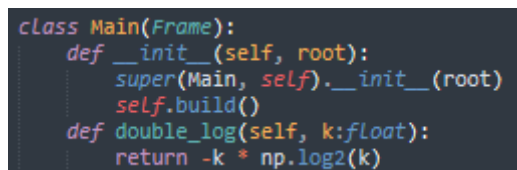
Однако есть тонкость при расчетах на ЭВМ, там необходимо перевести из $\log_2 a$ в $\ln a$, процесс перехода выглядит так:

$$lb a = \log_2 a = \frac{\log_e a}{\log_e 2} = \frac{\ln a}{\ln 2}.$$

Исходя из выше сказанного можно следует, что процесс высчитывания энтропии заключается в правильном восприятии поставленных задач. Благодаря синтаксису языка программирования python и использованию математической

¹ © Рахмонбердиев Б. Б., 2022.

библиотеки `numpy`, появилась возможность написать калькулятор рассчитывающий энтропию (рис. 1).



```
class Main(Frame):
    def __init__(self, root):
        super(Main, self).__init__(root)
        self.build()
    def double_log(self, k:float):
        return -k * np.log2(k)
```

Рис.1. Часть кода калькулятора энтропии на языке Python

Таким образом предлагается расширить границы энтропии информации в качестве изменения формата преобразования битового логарифма, а именно как было сказано выше, в итоге вычисления преобразуются в двоичную систему. При переводе из одной системы в другую используется определенная кодировка, например, windows 1251, которая имеет 255 символов, каждый символ имеет свой порядковый номер.

Взяв на рассмотрение данную таблицу кодировки можно понять, что одно слово будет представлять из себя сумму нулей и единиц, например, слово Университет будет иметь следующий вид 226229240241232242229242, так как энтропия исключает часто повторяющиеся символы, то следующий ее вид таков – 211237232226229240241242 (Универст) далее ЭВМ переводит из кодировки в двоичную систему она выглядит так 1100010111110001100110111011101110001000000000000000000000000000, если рассмотреть $\log_2 a$, в виде $\log_{20} a$, а так же $\log_{200} a$, то появляется возможность передавать большой поток информации с минимальным количеством символов, что будет эффективнее. Смысл предлагаемого варианта заключается в том, чтобы брать за основу кодировочного алфавита не определенные знаки и буквы, а, например, слоги. Так в результате объемный текст будет скомпилирован так, что объем передаваемого пакета будет минимальным. Следует отметить, что при данном подходе размер самого алфавита будет возрастать, что при передаче незначительно объема исходной информации не даст существенного эффекта.

Список использованных источников:

1. Плотников Г. Г. Вероятностная модель передачи сообщений в условиях воздействия помех в радиосистемах передачи извещений // Вестник Воронежского института МВД России. 2006. №1 (26). С. 99–104.

Полюхович А. К.¹,
 слушатель факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Минаев В. А.,
 профессор кафедры специальных информационных
 технологий учебно-научного
 комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 доктор технических наук, профессор

ВОПРОСЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ПРИ УДАЛЕННОМ ЭЛЕКТРОННОМ ОБМЕНЕ В КИБЕРПРОСТРАНСТВЕ

Информационные системы критической инфраструктуры предоставляют услуги, от которых зависят основные функции государственных органов и его экономики, и в конечном итоге – благосостояние общества [1]. Поэтому такие системы становятся все более распространенной мишенью для преступлений и атак в киберпространстве. Одной из основных причин, угрожающих безопасности указанных систем, является недостаточный контроль удаленного доступа, связанный с издержками управления идентификацией и аутентификацией пользователя при удаленном электронном обмене в киберпространстве. Управление идентификацией и аутентификацией зависит от назначения прав пользователя в цифровом пространстве.

В последние годы активно развиваются методы двухфакторной цифровой аутентификации (2FA) для удаленного доступа к информационной системе критической инфраструктуры. Результаты тестирования устойчивости системы к кибератакам показали, что такие методы надежно защищают от опасных HTTP-запросов и несущих угрозы входных данных.

Аутентификация – это процесс проверки и подтверждения личности как законного пользователя системы. По сути, в процессе аутентификации указывается идентификатор пользователя – имя, код, адрес электронной почты и др. [2] Затем пользователь предоставляет свои личные данные для идентификации, например, пароль. Если предоставленные данные подтверждаются, пользователь получает доступ к системе.

Обмен SMS-сообщениями – один из наиболее распространенных методов двухфакторной аутентификации [3]. Пользователь, который связывает свои учетные данные для входа с активным номером мобильного телефона, получает

¹ © Полюхович А. К., 2022.

SMS-сообщение с паролем из 5 – 10 цифр в процессе аутентификации. Пароль необходимо ввести в форму входа для успешного завершения процесса аутентификации.

Метод аутентификации на основе SMS зависит от состояния мобильного соединения. Во время нахождения за рубежом SMS-сообщение с кодом доступа не отправляется [4]. Очевидно, что при утере мобильного телефона с SIM-картой аутентификация невозможна. Кроме того, связь GSM ненадежна, и ее результатом может быть утечка SMS-кода доступа с использованием вредоносного программного обеспечения, внедренного в мобильное устройство. Аутентификация с помощью SMS уязвима для атак методами социальной инженерии, когда киберпреступники применяют поддельные SIM-карты с номером мобильного телефона жертвы. На вредоносную SIM-карту будут отправлены SMS-сообщения, а само мобильное устройство жертвы отключается от мобильной сети. В связи с этим NIST объявил [5], что методы двухфакторной аутентификации на основе SMS устарели, став ненадежными (рис. 1).

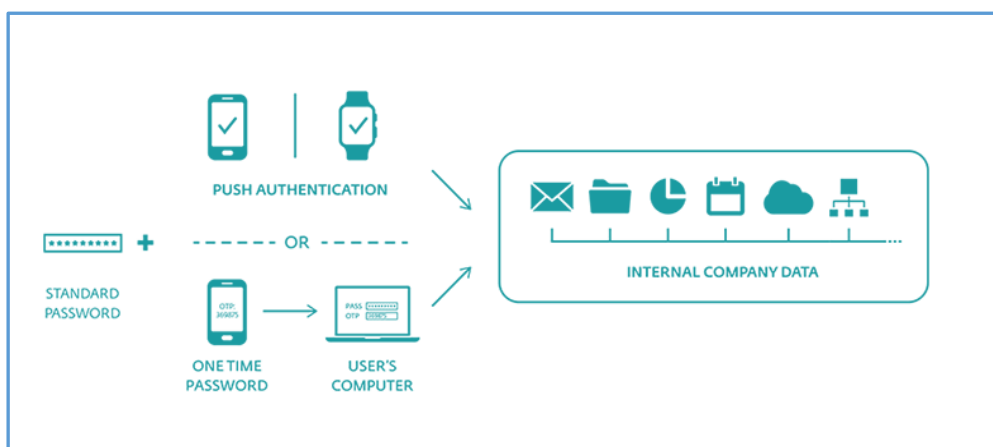


Рис. 1. Пример построения двухфакторной аутентификации

В процессе двухфакторной аутентификации также может использоваться электронная почта. Как и в случае использования SMS, на электронную почту отправляется одноразовый пароль из 5–10 цифр. Пароль может быть представлен пользователю несколькими способами: в виде текста – пользователь должен скопировать код в форму входа, или в виде ссылки – пользователь должен войти в ссылку, чтобы завершить процесс аутентификации. Однако такая аутентификация имеет существенные недостатки: электронные письма не всегда успешно доходят, кроме того, злоумышленники могут взломать учетную запись электронной почты.

Аутентификация на одноразовых паролях базируется на HMAC или одноразовом пароле на основе TOTP-алгоритмов. Эти алгоритмы позволяют генерировать пароли, которые активны только для одноразового использования или в течение фиксированного периода времени. Алгоритм TOTP генерирует одноразовый пароль, используя специальную криптографическую функцию. SHA-256 – это одна из часто используемых для этого криптографических функций. Но и такая аутентификация имеет недостатки. Во-первых, пользователь не может аутентифицироваться, если физическое устройство, например, смартфон, выключено.

Во-вторых, необходимо обеспечить синхронизацию времени между мобильным устройством и сервером системы. Кроме того, злоумышленники могут сгенерировать коды доступа, перехватив общий секрет; также возможна атака методом грубой силы, когда количество доступов не проверяется.

В процессе двухфакторной аутентификации мобильные устройства могут использоваться не только как генераторы паролей или токенов, но и при реализации метода аутентификации «push authentication» [6]. Этот метод базируется на получении сообщения/запроса на сопряженное мобильное устройство, с помощью которого можно подтвердить или отклонить вход в учетную запись в определенной системе. Стоит отметить, что в случае утери или кражи мобильного устройства пользователь должен как можно быстрее отвязать аккаунт от него. Более того, пользователи могут непреднамеренно принимать незаконные запросы на вход в систему, а все запросы на вход могут быть перехвачены и автоматически проверены вредоносным программным обеспечением, работающим на телефоне. В связи с этим на мобильном устройстве необходимо установить безопасное и надежное мобильное приложение.

Местоположение пользователя также может быть использовано в процессе аутентификации. Учитывая, что местонахождение пользователя – личная информация, он может отказаться ее раскрывать. В этом случае информация о местоположении может быть сфальсифицирована на нескольких уровнях – оборудования, операционной системы, приложения.

Другой способ аутентификации пользователя основан на распознавании изображений [7]. Во время такой аутентификации пользователю предоставляется несколько изображений, и он должен выбрать те из них, которые были выбраны во время первоначальной настройки его учетной записи. При этом пользователю требуется время, чтобы выбрать изображения из достаточно длинного списка. А у злоумышленника есть возможность подобрать изображения, исходя из увлечений и психологического портрета человека.

Universal 2nd Factor (U2F) – открытый стандарт, упрощающий двухфакторную аутентификацию за счет использования специализированных устройств USB или NFC и технологий безопасности смарт-карты [8]. Стандарт U2F использует криптографическую защиту с открытым ключом для аутентификации человека. Это – новая технология, которая еще не получила широкого распространения, ее поддерживает ограниченное количество существующих веб-браузеров: Google Chrome, Opera и Firefox. В то же время браузеры Internet Explorer и Edge не поддерживают ее.

Биометрия – еще одно решение для процесса аутентификации. Голос, лицо, радужная оболочка глаза, геометрия руки, отпечатки пальцев – персональные биометрические данные, которые можно использовать в процессе аутентификации. Такие биометрические данные уникальны и могут использоваться для надежной аутентификации человека. Следует отметить, что в процессе биометрической аутентификации используются разные устройства ввода, различающиеся ценой, иногда – значительной. Поэтому, как правило, реализация такого метода достаточно сложна и требует значительных материально-экономических

вложений. При этом точность метода не стопроцентная - возможны ошибки первого и второго рода.

Для улучшения процесса аутентификации можно использовать методы машинного обучения. Их реализация дает возможность следить за поведением пользователя и изменениями в нем. Сложные методы машинного обучения используют ряд различных поведенческих факторов для аутентификации: географическая локация пользователя; время суток, когда он обычно входит в систему; как быстро пользователь вводит пароль; динамика нажатия клавиш; что делает пользователь, ошибаясь при вводе пароля.

Следует отметить, что беспарольные методы аутентификации требуют больше усилий для злоумышленников, пытающихся обойти защиту компьютерных систем. Однако и такие методы также зависят от различных данных пользователя, например, биометрических. Все это свидетельствует о необходимости поддержания баланса между удобством использования, безопасностью и затратами на внедрение и эксплуатацию конкретного метода аутентификации.

В заключение подчеркнем, что надежность процесса аутентификации может быть усилена за счет двухфакторной аутентификации (2FA). Во время этого процесса пользователь должен указать два разных фактора для подтверждения своей личности.

Помимо аутентификации 2FA, может использоваться многофакторная аутентификация (MFA). В этом случае процесс аутентификации основан как минимум на двух факторах для подтверждения личности пользователя, получающего доступ к критической системе. Как правило, многофакторная аутентификация разрабатывается на основе цифровых личных или одноразовых данных пользователя, данных применяемого физического устройства (планшета, смартфона и т. п.), а также биометрических данных (отпечатки пальцев, голосовые шаблоны, геометрия руки и т. д.).

Список использованных источников:

1. Кибератаки, нацеленные на критически важную инфраструктуру // Сайт «E-tech». URL: <https://etech.iec.ch/issue/2019-02/cyber-attacks-targeting-critical-infrastructure>.
2. Чандрашекер А., Банги А., Санджана Б. Обзор полезной и безопасной двухфакторной аутентификации / Материалы 2-й Международной конференции IEEE по последним тенденциям в области электроники, информационных и коммуникационных технологий (RTEICT). 19–20 мая 2017 г., Бангалор, Индия. С. 842–846.
3. Ali, F.A.B.H.; Hanza, M.Z.B.M.; Sukri, M.A.B.M. Two Factor Authentication by Using SMS for Web Based Application. Int. J. Inf. Technol. 2020, No 9. P. 21–24.
4. Минаев В. А., Королев И. Д., Сабанов А. Г. Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия // Вестник УрФО. Безопасность в информационной сфере. 2018. № 4 (30). С. 43–49.
5. FATF (2020), Guidance on Digital Identity // Site «FATF». URL: <https://www.fatf-gafi.org/publications/documents/digital-identity-guidance.html>.

6. Пернпрунер М., Карбон, Р., Ранис С. Хорошее, плохое и (не очень) уродливое использование внеполосной аутентификации с помощью карт eID и push-уведомлений: дизайн, формальный анализ и анализ рисков / Материалы 10 конференции ACM по безопасности и конфиденциальности данных и приложений. Новый Орлеан. Луизиана. США. 16–18 марта 2020. С. 223–234.

7. Бханд А., Десале В., Ширке С. Совершенствование системы аутентификации паролей с использованием графических изображений / Материалы Международной конференции IEEE по обработке информации (ICIP). Пуна. Индия. 16–19 декабря 2015. С. 217–219.

8. Das S., Dingman A., Camp L. J. Why Johnny Doesn't Use Two Factor a Two-phase Usability Study of the FIDO U2F Security Key // Site «Ifca.ai». URL: [https://-www.111.pdf\(ifca.ai\)](https://www.111.pdf(ifca.ai)).

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

Научный руководитель:
Аветисян К. Р.,
*старший преподаватель кафедры информационной
безопасности учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя*

АНАЛИЗ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ В ЦЕЛЯХ ВЫЯВЛЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ В СТЕНОГРАФИЧЕСКИХ КОНТЕЙНЕРАХ

Тема стеганографии очень востребована, о чем говорят большинство современных публикация, конференций, да и в повседневной жизни обычного обывателя уже может встретиться один из методов сокрытия информации благодаря методам стеганографии.

Стеганография – это способ передачи или хранения информации с учетом сохранения в тайне самого факта такой передачи (хранения). Этот термин ввел в 1499 г. аббат бенедиктинского монастыря Св. Мартина в Шпонгейме Иоганн Тритемий в своем трактате «Стеганография».

Стеганографию необходимо рассматривать в купе с криптографией, хоть это совсем разные вещи. Задачей стеганографии можно отметить сокрытие самого факта существования секретного сообщения. Тогда как криптография просто скрывает это самое секретное сообщение. Стеганография позволяет представить секретное сообщение в различных видах, например, как изображение, статья, список покупок или даже простой кроссворд. Однако стеганография неразрывно связана с криптографией. Нельзя уверенно говорить о стеганографии, не затрагивая никаким образом методы криптографической защиты и шифровки сообщений.

В настоящее время не существует ни одного документа, который регламентировал бы основные термины, методы и классификации в области стеганографии. Стеганографию можно поделить на несколько подвидов для удобства и помощи в ее изучении и развитии.

Первый из таких подвидов – это цифровая стеганография. Она основана на избыточности пересылаемых мультимедийных данных, представленных в цифровом виде, изначально имеющих аналоговую природу (изображения, видео, звук). На эту стеганографию и будет упор в данной работе.

¹ © Пузаков А. В., 2022.

Второй подвид – это компьютерная стеганография. Она в свою очередь подразумевает внедрение качеств форматов данных, обрабатываемых и передаваемых в инфокоммуникационных сетях.

И последний подвид, возникший самым первым и давший начало всей системе стеганографии – это классическая стеганография. Суть такой стеганографии представляет собой сокрытие информации окружающей природы, используя некомпьютерные методы.

В нынешнее время начинают набирать популярность и распространяться в свободном доступе огромное количество приложений, которые позволяют как встраивать в сообщения скрытой информации, так и приложения позволяющее провести обследование сообщения на наличие такого встроенного сообщения.

Скрытой (стеганографической) передачей информации называют процессы, реализующие методы передачи информации, при которых возможна передача дополнительной информации в структуре данных, представленных в цифровом виде и используемых в качестве контейнера, преимущественно за счет их избыточности. Контейнер – цифровые данные, которые позволяют передавать дополнительную информацию, используя принцип избыточности. Существует пустой контейнер (который не содержит никакой информации) и заполненный контейнер (с добавленной информацией), его еще называют стего. Сообщение, которое встраивается в контейнер называется встроенное сообщение или скрытое. Стежоключ – это ключ, который известен только получателю и отправителю, и позволяющий скрыть добавленную информацию. При необходимости дополнительной защиты можно добавлять несколько стегоключей.



Рис. 1. Схема стенографической передачи данных

Стеганография в цифровых изображениях – раздел стеганографии, изучающий проблему сокрытия данных в цифровых изображениях.

Стеганографией цифровых изображений могут пользоваться правонарушители в своих каких-либо неправомерных планах. Поэтому в ответ существует такая деятельность, как стеганоанализ цифровых изображений, которая позволяет обнаружить сам факт сокрытого сообщения в изображении.

На данный момент в открытом доступе имеется большое количество программного обеспечения, позволяющего осуществить внедрение стегоконтейнера не только в изображение, но также и в видеозапись, аудиозапись и так далее.

Каждая эта программа находится в интернете совершенно бесплатно. И каждый желающий может попробовать себя в роли стеганографа.

В стеганографических приложениях используются криптографические методы шифрования, такие как IDEA, AES128, AES256 и т. д.

Соккрытие текстовой информации в изображении благодаря бесплатному ПО осуществляется всего в 2 клика. Необходимо просто создать текстовый документ, который мы хотим спрятать и выбрать непосредственно изображение, в котором будет сокрыто сообщение. После этого нажать кнопку «сокрыть», в зависимости от своего приложения. И программа выдаст вам новую картинку уже с спрятанным сообщением.

Важно грамотно выбрать себе программу для работы, потому что некоторые не смогут использовать ваше расширение, а некоторые будут уж слишком очевидно шифровать, что даже ребенок, посмотрев на свойства файла

поймет, что в нем что-то не так. Например, ПО Openstego позволяет осуществлять как стеганографию цифровых изображений, так и стеганоанализ, но размер полученного изображения будет весить больше на пару Мб.

Так же можно проверить наличие сокрытого сообщения в изображении побайтовым сравнением исходного изображения и полученного с помощью программы.

Тема стеганографии становится все актуальнее и актуальнее с каждым днем. Не удивительно, ведь это очень важно, как для информационной безопасности всего государства, так и для органов внутренних дел, которые смогут пресекать новые правонарушения в области цифровых преступлений.

Список использованных источников:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.

2. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_7519/.

3. Аветисян К. Р. Повышение криптостойкости конечного приложения на основе применения принципов динамического полиморфизма. // Сборник материалов деловой программы «Интерполитех-2015». М., 2015.

4. Поликарпов Е. С. Основы компьютерной разведки : учебное пособие. М. : Московский университет МВД России имени В.Я. Кикотя, 2020.

5. Гончар В. В. Совершенствование государственной политики по противодействию преступлениям в сфере информационных технологий. // Вестник экономической безопасности. 2017. № 3.

Кашин Ю. О.¹,
курсант факультета подготовки
специалистов в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Булгаков В. В.³,
ученик ГБОУ «Школа Свиблово»

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

СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ ХРАНИЛИЩАХ ДАННЫХ

На сегодняшний день технологии облачных вычислений это огромный прорыв в мире IT. Она дает людям огромные возможности из разных преимуществ, таких как управление данными и их хранением, и автоматизацией всего процесса в бизнесе или учреждении. Сейчас у специалистов информационных технологий возникают вопросы о том, как решить задачу по сохранению в безопасности данных в облачных вычислениях. Поэтому сегодня это направление работы по безопасности данных и защиту конфиденциальности является как никогда актуальным. Решение проблем в этой деятельности является основным фактором для дальнейшего развития технологий облачных вычислений во всех видах ее применения.

В контексте облачных вычислений организации и компании, как правило, избегают привязки к поставщикам, применяя подход с участием нескольких поставщиков. Допустим, ваши данные распределены между несколькими популярными общедоступными облачными платформами, такими как Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform (GCP). Лежит ли на них ответственность за то, чтобы хранить ваши данные подальше от посторонних глаз? Или вам нужно взять на себя ответственность за безопасность ваших данных, размещенных в облаке? Ответ - и то, и другое. Когда организации используют общедоступное облачное хранилище, они соглашаются с моделью совместной ответственности. В этой модели четко определены средства контроля безопасности, за которые отвечает компания-владелец данных, и те, за которые

¹ © Кашин Ю. О., 2022.

³ © Булгаков В. В., 2022.

отвечает компания-оператор данных. Эта ясность помогает организациям лучше понять, для чего именно им нужны инструменты кибербезопасности.

В настоящее время выделяются следующие виды проблем, возникающие при хранении и обработке данных в облачных сервисах:

Репликация данных. Снимки и резервные копии данных в организациях делаются постоянно, сохраняясь в облаке. Но никто не может дать четкого ответа, где эти данные были сохранены и кто их может просматривать и получать к ним доступ. Владелец данных не может в таком случае идентифицировать и контролировать несанкционированное копирование своих данных.

Небезопасные API. Интерфейс программирования приложений позволяет пользователям настраивать свои методы облачных вычислений. API-интерфейсы могут представлять угрозу для облачной безопасности из-за их «природы». API предоставляют разработчикам инструменты для создания решений по интеграции своих приложений с другим программным обеспечением. Уязвимость API и заключается в этом взаимодействии, которое происходит между приложениями. Хотя оно и помогает разработчикам и предприятиям, но вместе с этим возникают серьезные проблемы с безопасностью.

Внутренние угрозы. Нельзя списывать данную угрозу со счетов. Возможно, владельцы считают, что данные, находящиеся в зоне контроля – в безопасности. Но это одна из самых больших проблем – недобросовестные сотрудники, с которыми могут столкнуться разработчики и компании. Сотрудники организации могут использовать свой доступ к облачным сервисам для неправомерного использования или доступа к информации, связанной с финансами, персональными данными и т. д.

Стандарты защиты облачной информации – отечественные и зарубежные. В нашей стране основные положения по обеспечению безопасности данных в облачных хранилищах содержатся в ГОСТ Р ИСО/МЭК 27018-2020, который в свою очередь идентичен иностранному ISO/IEC 27018:2019 «Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors». В данном документе содержатся основные понятия, рекомендации и правила обращения с оборудованием, используемым для облачных вычислений, правил обращения с информацией а так же ссылки на многие другие смежные документы ИСО/МЭК, регламентирующие защиту информации.

Утечка данных у Amazon. За прошедший время произошло большое количество утечек, следствием которых явились незащищенные хранилища Amazon S3. В результате было похищено огромное количество данных о различных организациях. По словам исследователей безопасности, в очередной раз обнаруживших три открытых хранилища AWS, платформа July System используется несколькими известными компаниями, включая CNN, ESPN, Intel, Toys «R» Us, CBS, Fox и NBC Universal. Данные содержат учетные записи безопасности для приложений iPhone/Android и репозитория, которые потенциально могут позволить кому-либо получить доступ к персональным данным клиента и трекинга, а также внутренние сборки и средства разработки для различных клиентов,

включая NFL, CBS, Amex, NBA, FOX, PGA и другие. Все три хранилища являются частью одной экосистемы, называемой EMSP. EMSP – это платформа Enterprise Mobility Services Platform, которая может получать ценную информацию о клиентах и персонализировать мобильных пользователей, используя Wi-Fi-сеть. В базах данных также были представлены файлы с именами и брендами, такими как Katy Perry, NFL, NBA. В одной из папок содержались более 1 тыс. имен пользователей и паролей менеджеров Unilever в Индии. Реальная проблема заключается в том, что обнаруженное является частью гораздо более крупной инфраструктуры и утекшие пароли могли быть использованы киберпреступниками для доступа к ее защищенным областям.

Почему защита данных в облаке необходима. Защита облачных данных и другие вопросы конфиденциальности рассматриваются как существенные риски при хранении личной информации в облаке. Опасности или риски, связанные с хранением данных в облаке, включают:

- несанкционированный доступ;
- убытки или ущерб, причиненные поставщиком услуг и их работниками;
- действия, направленные против поставщика услуг – взлом или отправка вредоносных программ и троянов;
- слабые методы обеспечения безопасности, связанные с защитой данных;
- нарушение регулятивного контроля.

Прежде чем выбирать службу облачных вычислений, нужно провести анализ рисков, чтобы оценить любое потенциальное влияние на организацию. Поскольку значительная часть приложений и данных размещается в инфраструктуре сторонних производителей, существует несколько типов рисков, например:

1. Неспособность отслеживать, где хранятся приложения и данные.
2. Отсутствие понимания того, как поставщик облачных услуг хранит и защищает данные.
3. Пренебрежение признанием того, что облачная безопасность является общей ответственностью. Как правило, большинство облачных провайдеров имеют самую современную систему безопасности; однако она может быть ограничена.
4. Игнорирование того, что облачные провайдеры имеют разные возможности, и неспособность устранить несоответствия в защите облачных данных путем разработки собственной политики безопасности.

Организациям также приходится решать ряд других проблем в области безопасности, таких как:

- нарушения безопасности;
- неправомерное использование и кража данных;
- системные уязвимости и заражения вредоносными программами.

Следовательно, несмотря на множество преимуществ облачных вычислений, существуют и подводные камни, которые необходимо устранить, чтобы обеспечить безопасность и защиту конфиденциальных данных.

Как защитить свои данные?

Не хранить конфиденциальные данные. Звучит очень странно. Но технологии меняются. Бизнес также меняется в соответствии с технологией. Сегодня данные

играют важную роль в бизнесе. Таким образом, конфиденциальность данных является одним из основных аспектов любого бизнеса. Но если что-то есть в Интернете, трудно поверить, что это безопасно. Поэтому следует избегать хранения наиболее важных файлов или информации в облаке. Необходимо в облачной платформе хранить только те файлы, к которым вы часто обращаетесь, и избегать размещения информации, связанной с финансовыми данными, данными о конкурентах, данными о клиентах, контактными данными, такими как номер телефона или адрес и т. д.

Шифрование данных. Один из лучших способов защитить данные при использовании облачного хранилища – это шифрование данных. Это лучшая форма безопасности, поскольку перед доступом к данным требуется расшифровка. Это также защитит данные от поставщиков услуг и пользователей. **Чтобы сделать их более защищенными, следует обеспечить облачное шифрование на этапах загрузки и выгрузки.**

Зашифрованный облачный сервис. Существует несколько облачных сервисов, которые обеспечивают локальное шифрование и дешифрование файлов и информации внутри них, кроме хранения и резервного копирования. Это означает, что сервис заботится как о шифровании файлов, так и о их безопасном хранении в облаке. Это гарантирует, что никто, включая поставщика услуг или администраторов, не сможет получить доступ к вашим файлам и данным. На рынке доступно множество бесплатных, а также пробных версий.

Использование пароля. Первое, что можно сделать, это ввести надежный пароль, который может выдержать взлом. Очень важно часто менять свой пароль и никогда не использовать один и тот же пароль для всех учетных записей или папок. Можно выбрать двухшаговую проверку для входа в систему, если облачный сервис предлагает такую возможность. Google Drive использует двухфазный вариант входа в систему, состоящий из пароля и кода, отправленных на зарегистрированный номер. Эта дополнительная защита сделает данные намного безопаснее.

Ограничение доступа. Предоставлять доступ следует только тем пользователям, которые действительно нуждаются в нем. **Внутренние пользователи и сторонние поставщики должны получать доступ только к тем файлам, которые необходимы им для работы.** При необходимости нужно использовать ключи шифрования. Также необходимо регулярно проверять пользователей и поставщиков, и добавлять или удалять пользователей в соответствии с требованиями.

Непрерывное обновление системы. Безопасность облачных данных повышается благодаря регулярному исправлению и обновлению систем и прикладного программного обеспечения в облачной платформе. Для поддержания высокого уровня безопасности и поддержки новых версий, требуются новые исправления, обновления и пакеты обновления для операционной системы. Здесь важно определять тенденции рынка и новые версии программного обеспечения, а также сообщать о пробелах в безопасности, которые могут возникнуть в установленных системах и приложениях.

Защита от программ-вымогателей. Программа-вымогатель – это форма кибератаки, при которой преступники шифруют ваши документы, весь ваш диск

или всю сеть серверов вашей компании. Затем вам будет закрыт доступ ко всем вашим файлам и приложениям до тех пор, пока вы не заплатите выкуп, обычно в криптовалюте. Проверьте, предлагает ли ваш провайдер обнаружение и восстановление программ-вымогателей. Если они это сделают, вы можете быть спокойны, зная, что все ваши облачные файлы и локальные файлы, синхронизированные с облаком, будут в безопасности в случае атаки.

Многонациональная структура конфиденциальности и безопасности. Чтобы обеспечить каждому бизнесу и стране все преимущества облачных вычислений, разные страны должны сотрудничать в разработке многонациональной структуры конфиденциальности и безопасности данных в облаке. По мере развития облачных вычислений и потоков данных из одной страны в другую. Например, данные были созданы в Индии с использованием программного обеспечения, размещенного в Великобритании, и хранятся в США у пользователей из Австралии. Облачный провайдер должен координировать весь этот процесс, чтобы обеспечить бесперебойную и безопасную передачу данных.

Правила трансграничной передачи данных. Для повышения эффективности и безопасности облачных решений, и получения быстрых результатов поставщики облачных услуг должны иметь возможность управлять центрами обработки данных в нескольких местах и свободно передавать данные между ними. Плавный поток данных позволяет облачным провайдерам оптимизировать свои услуги и предлагать лучшие бизнес-решения. Однако ограничения на трансграничную передачу данных могут создать неопределенность, если не соблюдаются правила или правовые рамки.

Чтобы защитить данные в облачной платформе, необходимо помнить обо всех вышеперечисленных вещах.

В заключении следует сказать, что облачный рынок имеет множество поставщиков, каждый из которых предлагает широкий спектр услуг. Это позволяет предприятиям и организациям оценивать несколько облачных провайдеров, чтобы найти тот, который наилучшим образом соответствует вашим потребностям в области безопасности, конфиденциальности и защиты данных.

Таким образом, облачные вычисления – одна из наиболее перспективных технологий для следующего поколения ИТ-приложений. Основной проблемой ускоренного роста облачных сервисов являются вопросы безопасности и конфиденциальности данных. Главной целью любой компании является сокращение объема хранения данных и связанных с этим затрат. Поскольку мы все знаем, что данные играют большую роль в принятии бизнес-решений, ни одна компания не будет размещать все свои бизнес-данные в облаке, если они не доверяют им полностью. Существует множество методов, которые были внедрены ИТ-исследователями для защиты данных и достижения наивысшего уровня безопасности данных. Тем не менее, все еще существуют определенные пробелы, которые необходимо заполнить, сделав эти методы более эффективными. Требуется больше знаний в области облачных вычислений, чтобы сделать их приемлемыми.

Список использованных источников:

1. Утечка данных через незащищенное хранилище Amazon // Сайт «SecurityLab». URL: <https://www.securitylab.ru/blog/personal/bezmaly/343140.php>.
2. Ванина М. Ф., Ерохин А. Г., Фролова Е. А Применение облачных технологий в компаниях малого и среднего бизнеса // Век качества. 2015. № 1. С. 61–64.
3. Лучшие практики по безопасности хранилищ данных // Сайт «SecurityLab». URL: <https://www.securitylab.ru/analytics/502751.php>.
4. Средства защиты данных // Сайт «Библиофонд». URL: <https://www.bibliofond.ru/view.aspx?id=66834>.
5. Облачные вычисления // Сайт «Хабр». URL: <https://habr.com/ru/post/11-1274/>.
6. Что такое безопасность облака? // Сайт «Kaspersky». URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security>.
7. Серикулы О. Информационная безопасность облачных вычислений // Вестник магистратуры. 2019. № 6-5 (93). С. 17–23.

*Матюнькин Д. А.¹,
слушатель факультета подготовки
специалистов в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

*Научный руководитель:
Сергеева Е. Ю.,
преподаватель кафедры специальных
информационных технологий учебно-научного
комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

АКТУАЛЬНЫЕ ВОПРОСЫ ПРИ ИССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

Стремительные темпы развития информационных технологий приводят к появлению новых возможностей для преступных посягательств на информацию с использованием вредоносного программного обеспечения (далее – ПО). Однако и средства борьбы с ПО, представляющими угрозу информации пользователей в компьютерных системах, развились в направлении исследования программного обеспечения.

Исследование недеklarированных возможностей ПО – это исследование функциональных возможностей ПО, не описанных или не соответствующих описанию в документации, при использовании которых возможно нарушение безопасности информации.

Цель исследования недеklarированных возможностей ПО часто состоит в том, чтобы разобраться в программе, исходный код которой недоступен. Перечислим типичные ситуации:

- 1) анализ вредоносного ПО [1];
- 2) анализ программ с закрытым исходным кодом на уязвимость;
- 3) анализ интероперабельности программ с закрытым исходным кодом.

Анализ вредоносного ПО, если только это не скрипты, редко оказывают нам помощь, предоставляя исходный код. А в отсутствие исходного кода наши возможности понять, как ведет себя вредоносное ПО, крайне ограничены. Есть два основных вида анализа: динамический и статический. Динамический анализ подразумевает выполнение вредоносного кода в среде виртуализации, когда за все аспекты поведения контролируются с помощью различных инструментальных утилит. Статический анализ – это попытка понять, что делает программа, читая ее код, который в случае вредоносного ПО чаще всего состоит только из листинга дизассемблера и, возможно, листинга декомпилятора.

¹ © Матюнькин Д. А., 2022.

Для простоты анализа на уязвимости, можно разбить весь процесс аудита безопасности на три этапа: обнаружение уязвимости, анализ уязвимости и разработка эксплойта [2]. Одни и те же шаги выполняются вне зависимости от того, есть исходный код или нет, однако объем усилий резко возрастает, если имеется только двоичный код. Сначала необходимо найти место в программе, потенциально допускающее эксплуатацию. Для этого часто применяются динамические методы, например, фаззинг, но то же самое можно сделать (обычно с гораздо большими усилиями) с помощью статического анализа. После того как проблема выявлена, часто требуется дальнейший анализ, чтобы понять, допускает ли она эксплуатацию, и если да, то при каких условиях.

Для обеспечения невозможности преднамеренного овладения информацией лицом, распространяющим программное обеспечение, могут применяться методы исследования недеklarированных возможностей программного обеспечения.

В зависимости от функционала не декларированные способности программного обеспечения могут нанести как экономический вред, так и привести к уничтожению информации, ее блокированию, копированию или модификации, что может быть квалифицировано по ч. 1 ст. 272 УК РФ «неправомерный доступ к компьютерной информации» [3]. Также, в зависимости от квалифицирующих признаков (размер нанесенного ущерба, наличие корыстной заинтересованности и т. д.) могут применяться и другие части данной статьи.

Также разработка программного обеспечения, имеющего недеklarированные способности, предусмотрена в ст. 273 УК РФ «создание, использование и распространение вредоносных компьютерных программ», если они имеют признаки вредоносного программного обеспечения, то есть предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Для производства судебной компьютерной экспертизы необходимо само программное обеспечение, а также техническое задание.

Объектом данной экспертизы является программное обеспечение.

При производстве судебной компьютерной экспертизы эксперту могут задаваться такие вопросы:

1. Соответствует ли результат работы (в данном случае результатом работы является программное обеспечение) требованиям технического задания?
2. Может ли результат работ использоваться в соответствии с его целевым назначением с учетом технического задания?
3. Имеет ли программное обеспечение функции, не заявленные в техническом задании? Если имеет, то каково их целевое назначение?

При производстве судебной компьютерной экспертизы могут применяться различные методы, такие как:

- 1) исследование технического задания;
- 2) компиляция и тестирование программного обеспечения;
- 3) определение соответствия программного обеспечения техническому заданию (не соответствует, соответствует или частично соответствует);

4) определение возможности использования программного обеспечения в соответствии с его целевым назначением.

При производстве судебной компьютерной экспертизы могут быть решены следующие задачи:

- 1) установление общих характеристик исследуемого программного обеспечения;
- 2) классификация отдельных программных средств и утилит;
- 3) установление подлинности программного обеспечения и его компонентов;
- 4) установление функционального предназначения программного обеспечения и его компонентов;
- 5) выявление в программном обеспечении отклонений в функционировании;
- 6) выявление скрытых кодов от изначальной версии программного обеспечения;
- 7) определение модификаций программного обеспечения и его компонентов;
- 8) установление возможности выполнения исходного функционала после внесения изменений в программное обеспечение или его компоненты;
- 9) анализ компонентного состава программного обеспечения;
- 10) установление сетевой активности вредоносного программного обеспечения.

В заключении необходимо установить ошибки и несоответствия, допущенные при создании программного обеспечения; определить, может ли программное обеспечение в текущем состоянии использоваться по целевому назначению; определить наличие не декларированных способностей (если такие имеются); определить целевое назначение не декларированных способностей.

Криминалистическая значимость нахождения информации в операционной системе компьютера в общем случае определяется по ценности этой информации. Значимость заключения эксперта заключается в разъяснении сведений, полученных путем производства экспертизы. В конкретных случаях это сведения о наличии не декларированных способностей программного обеспечения, а также об их функциональных возможностях.

Также при проведении расследования необходимо запросить у оператора связи сетевую активность зараженного устройства с целью установки наличия возможности самораспространения вирусного программного обеспечения, взаимодействия с облачными ресурсами (прием с зараженного устройства и передача файлов на него). Значимость такой информации поможет определить лицо, причинившее ущерб и его примерную величину, а также охват сетевых ресурсов, в некоторых случаях поможет определить внешние сетевые ресурсы, которые эксплуатируются вирусным программным обеспечением.

В рамках данной статьи были рассмотрены вопросы и задачи, ставящиеся перед экспертом при исследовании программного обеспечения, позволяющие выявить незаявленные разработчиком возможности программного обеспечения.

Список использованных источников:

1. Гонохова Д. Ю. Вредоносное ПО // Перспективы развития науки и образования : сборник научных трудов по материалам VII международной научно-практической конференции / под общ. ред. А. В. Туголукова. 2016. С. 65–67.

2. Фостер Д. С. Защита от взлома. Сокеты, shell-код, эксплойты : учебное пособие. М. : Пресс, 2006. 783 с.
3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // НПП «Гарант-сервис». URL: <https://base.garant.ru/10108000/>.

Дворянкин О. А.¹,
старший преподаватель кафедры информационной
безопасности учебно-научного
комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук

Рязанова А. М.²,
курсант факультета подготовки
специалистов в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ ПРИ ВЫЯВЛЕНИИ И ПРЕСЕЧЕНИИ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ, СВЯЗАННЫХ С ТОРГОВЛЕЙ ЛЮДЬМИ

Торговля людьми – деятельность, запрещенная Уголовным кодексом Российской Федерации, которая посягает на одну из основных ценностей общества – личную свободу граждан. Деяние является преступлением международного характера, и наносит ущерб интересам государства и людям.

Большинство жертв – женщины и дети, поскольку они представляют собой «легкую добычу» для лиц, причастных к преступной деятельности, т. е. занимающихся торговлей людьми.

Преступления, связанные с торговлей людьми, по данным экспертов, это прибыльный незаконный бизнес и очень сложная сфера правоотношений, приносящая огромные деньги преступникам. Так, согласно данным Организации Объединенных Наций теневой доход данной преступности составляет около 9 млрд \$ в год, а Интерпол оценивают его в 19 млрд \$ [1].

В эпоху интернета, когда всемирная сеть стала так же важна, как и основные потребности человека, торговцам людьми стало довольно легко с помощью информационных технологий интернета заманивать девочек или женщин в свои преступные сети.

С ростом использования социальных сетей среди молодежи, торговцы людьми получили возможность легко связаться с ними или установить с ними связь, а также легко получать доступ к их планам виртуально [2].

Преступления (в том числе торговля людьми), совершаемые через интернет, составляют киберпреступность. Они происходят в киберпространстве и используют интернет в качестве средства для их совершения. Торговля людьми является серьезной проблемой, которая возрастает с каждым днем.

¹ © Дворянкин О. А, 2022.

² © Рязанова А. М, 2022.

Вербовщикам облегчает работу то, что люди сами проявляют интерес к посещению сайтов, социальных сетей, в которых пропагандируется «красивая» жизнь, легкий и доступный заработок и т. д.

Как показывает практика, торговля людьми начинаются с того, что преступник связывается с потенциальными жертвами через социальные сети, такие как Одноклассники, Вконтакте, Тик-Ток, различные сайты знакомств и т. д.

Методы, используемые преступниками для завоевания доверия жертвы, широко варьируются, например, включая выражение любви и восхищения жертвой, обещание сделать жертву «звездой» (поп-дивой) или предложение нового места работы вдали от дома и, как результат, предоставление билета на новое место жительства, где ее ждет рабский труд или если это женщина, то ее часто делают секс-рабыней. На новом месте жертва находится под полным контролем преступника, который используя различные методы ограничивает ее связь с домом, применяет физическое насилие, а если жертва не подчинится его требованиям, то в ход идут дополнительные угрозы, связанные с шантажом членов ее семьи, друзей, родственников или в крайнем случае смерти жертвы.

Так, например, знакомство через интернет чуть не обернулось для 19-летней жительницы Санкт-Петербурга сексуальным рабством в Египте. 20-летний юноша под предлогом религиозного обучения убедил девушку в необходимости уехать с ним за границу и даже успел купить для них авиабилеты на рейс Санкт-Петербург – Стамбул. Сотрудники УФСБ России по Санкт-Петербургу и Ленинградской области своевременно получив оперативную информацию, задержали «обольстителя» и спасли девушку [3]. Подобные истории встречаются нередко.

Сексуальное насилие и другие формы эксплуатации происходят виртуально, а фотографии и видео продаются на разных платформах клиентам по всему миру, что приносит еще больше денег торговцам людьми без каких-либо дополнительных затрат.

Важно отметить, что торговцы людьми быстро адаптируют «актуализированную» преступную бизнес-модель к своим потребностям и увеличивают свою прибыль, поэтому, они пристально следят за новейшими тенденциями и информационными технологиями в интернете.

Так, они применяют технологии: профилирование, вербовку, контроль и информационную эксплуатацию своих жертв, а также используют интернет, особенно темную сеть (Даркнет), для сокрытия от оперативных работников и следователей сведения о своих незаконных действиях [4].

Наряду с этими технологиями они стали использовать криптовалюты, чтобы скрыть перемещение и оборот крупных денежных сумм, чтобы не быть обнаруженными.

Также, используя возможности отсутствия географических ограничений в интернете, т. е. быстрое и доступное соединение с партнерами, которые находятся в разных местах России или стран мира, торговцы людьми стали быстро находить и вербовать потенциальных жертв, посредством создания поддельных веб-сайтов (зеркала) или размещать фейковые объявления на законных порталах о трудоустройстве или любовных отношениях. При этом торговцы людьми стали дистанционно управлять своими жертвами, используя Интернет приложени

и мобильные телефоны по определению местоположения жертвы, а также камеры в смартфонах, применяемые вовремя видео звонков (они видят своих жертв и их окружение), что позволяет не встречаться с ними лично.

Кроме этого, используя, технологии живого общения, т.е. визуализация взаимоотношений, посредством «лжефотографий», появилась возможность непринужденно, на доверии, получать у жертвы личную информацию (персональные данные), как например, паспортные данные, банковские реквизиты и т. д.

Еще одним фактором, который помог торговцам людей активизировать свою деятельность – это пандемия COVID-19.

Она открыла дополнительные возможности в связи с более широким использованием интернета, в частности, социальных сетей и сайтов онлайн-видеоигр.

Меры по сдерживанию распространения вируса привели к тому, что люди проводили гораздо больше времени в интернете, особенно дети, поскольку школы были закрыты, а молодым людям хотелось дополнительного общения и развлечений. Увеличилось количество материалов о сексуальной эксплуатации детей, созданных и распространяемых в интернете во время пандемии.

По данным экспертов в этот период времени (2020–2021 гг.) только в России примерно 40 % жертв секс-торговли стали вербоваться онлайн, что сделало интернет наиболее распространенным местом, где происходит вербовка жертв.

Таким образом можно отметить, что информационные технологии Интернета, страх жертвы перед преступником и перед членами семьи, родственниками и знакомыми (угрозы обнародовать интимные фотографии или видеозаписи) приводит к тому, что жертвы боятся подавать заявления в правоохранительные органы и таким образом значительная часть преступлений становятся латентными, что затрудняет органам внутренних дел осуществлять борьбу с этими преступлениями.

Когда преступление планируется в одной стране, жертвы – в другой, а заказчик – в третьей, правоохранительные органы сталкиваются с практическими проблемами, такими как поиск и сбор доказательств, поскольку любое расследование требует трансграничного сотрудничества и определенного уровня информационных, аналитических и цифровых знаний.

Таким образом, в заключение необходимо отметить, что информационные технологии интернета стали новым вызовом правоохранительным органам, а применяемые преступниками в торговле людьми данных технологий в определенной степени, осложнили деятельность правоохранительных органов, но с другой стороны общественная опасность и защита людей от насилия и произвола, привели к тому что сотрудники органов внутренних дел активизировали свои оперативно-розыскные мероприятия и следственные действия, обмен опытом между силовыми органами и контролирующими органами, гражданскими институтами, что в результате привело к своевременным результатам, но также и заставило сотрудников полиции совершенствовать свои профессиональные навыки в виде самообучения (аналитической работе) и повышения квалификации.

Список использованных источников:

1. Департамент по экономическим и социальным вопросам // Официальный сайт Организации Объединенных Наций. URL: <https://unstats.un.org/UNSDW-ebsite/>.
2. Петросян С., Хачатрян Г. Торговля людьми (траффикинг) : учебное пособие. Ереван : Международная организация по миграции (МОМ), 2013 С. 234.
3. Знакомство в интернете чуть не довело петербуженку до сексуального рабства. Как не стать жертвой онлайн-любви? // Сайт «360». URL: <https://360tv.ru/tekst/obschestvo/zhertva-onlajn-ljubvi/>.
4. Бухоризода Б. Р. Социальные сети и интернет: новая форма совершенствования торговли людьми // Академическая мысль. 2019. № 2. С. 178.

Корнилов А. А.¹,
старший преподаватель кафедры
организации и обеспечения раскрытия
и расследования преступлений
Тверского филиала Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Анализ применения искусственного разума в профессиональной сфере действительно важен, ибо триумф в данной области многократно упрощает деятельность квалифицированных специалистов во всевозможных отраслях.

Включение искусственного мозга благоприятствует существенному росту результативности работы органов внутренних дел. История формирования искусственного интеллекта в России началась зарождаться в 1954 г. Его предназначением служит разработка таких систем, которые смогут реализовывать те функции и различной сложности задачи, как правило присуще только разумным существам.

Процесс перехода к информационным технологиям, который осуществляется уже длительное количество лет, влечет за собой и помощь в оцифровке необходимой различным областям данных о людях, их имуществе, их деятельности и множестве других области. Данный способ хранения информации достаточно удобен и полезен для деятельности многих организаций, в том числе и для деятельности органов внутренних дел.

Цифровое общество следует рассматривать как не какое-либо еще одно нововведение, а как явление, которое будет оказывать огромную помощь в работе органов. Людям следует с пониманием и поддержкой отнестись к подобным тенденциям, поскольку это будет влиять на количество раскрываемости преступлений, тем самым обеспечивая правопорядок в обществе. Ведь создание единой базы с идентификационными элементами упростит и сократит время поиска необходимого человека, поможет в менее сжатые сроки опознать личность и посмотреть историю правонарушений какого-либо гражданина. Интеллектуальные системы содействуют улучшению качества аналитики и прогнозируют криминальную деятельность.

Сегодняшние биометрические системы предлагают обширный спектр путей реализации, которые будут оказывать влияние на процесс распознавания личности по их отпечаткам пальцев. Это будет способствовать увеличению раскрываемости преступлений, примером может быть: распознавание трупов и также быстрый поиск людей, которые могут быть причастны к данному преступлению или же возможность поиска подозреваемого преступника в базе или по истории [2, с. 16–32].

Невероятное значение в таких процессах присуще работе полиции, которая использует систему номерных знаков, которые находятся на каждом автомобиле.

¹ © Корнилов А. А., 2022.

Это выступает как помощь следственным органам в поиске, отслеживании необходимого объекта или же просто предоставляет информацию о владельце транспортного средства, которая может быть полезна органам.

Еще одной областью использования систем в профессиональной деятельности сотрудников Министерства внутренних дел является применение справочно-правовых систем в их работе. В правовой системе находится база информации по законодательству, которая позволяет в положенный срок обновлять данные и выполнять оперативный поиск.

Само собой, данные системы увеличили возможности подразделений Министерства внутренних дел Российской Федерации, предоставив оперативно приобретать из них информацию об интересующих их объектах. Принимая во внимание все положительные факторы этой системы: ее наполнение, использование и получение результатов осуществляется только по желанию пользователей, что считается большим недостатком. Конечно, автоматизация документооборота — это очень хорошо, но без «руки» человека, которая направлена на получение необходимой информации, эти данные остаются данными, которые хранятся в системе.

Известны случаи, когда автоматизированная система дорожных камер, фиксирующих нарушения скорости, ошибочно «выписывала» штраф владельцу транспортного средства только с учетом связки «государственный номерной знак — хозяин автомобиля» и благодаря тому, что данная информация имеется в базе данных, (даже если не совпадают модель авто с номерным знаком), говоря другими словами, алгоритм работы системы не предусматривает возможности проверки обстоятельств происшествия. Обстоятельства могут быть разного рода: от неправильного определения государственного номера, до использования поддельных или специально переделанных номеров:

1. Существуют риски, которые связаны с зарубежным происхождением систем (присутствие устаревших функций, могут содержаться ошибки, так же вероятность несанкционированного доступа, потеря информации).

2. Имеют место быть технологические риски (невозможно держать под контролем скрытые внутренние функции).

3. Опасность фальсификации с данными и махинации с ними.

4. Неквалифицированные специалисты не могут донести до начальника соображения пользы от внедрения интеллектуальных систем.

5. Могут быть риски, связанные с отсутствием нормативных правовых актов, которые определяют ответственность за резолюцию, принимаемые информационными системами [3, с. 55–65].

Тем не менее, при всех особенностях искусственного интеллекта, мы не должны забывать — это не лекарство от всех несчастий, а всего на всего — инструмент. Соответственно, эффективность работы зависит от того, как она будет использоваться. И здесь надо помнить: данная деятельность касается широкого круга проблем экономического, юридического, этического, политического и в некоторой степени демографического характера.

Список использованных источников:

1. Ахтямов М. К. Концепция интеллектуального обеспечения инновационного развития предпринимательства : дис. ... д-ра экон. наук. СПб, 2010. 415 с.
2. Бабаев М. М. Интеллектуальное обеспечение процессов борьбы с преступностью // Ученые труды Российской академии адвокатуры имени Ф.Н. Плевако. 2000. Вып. 1. С. 16–32.
3. Бабаев М. М., Пудовочкин Ю. Е. Криминологическое мышление в контексте интеллектуального обеспечения уголовной политики // Журнал российского права. 2013. № 8. С. 55–65.

Шкинин Д. А.¹,
*научный сотрудник отдела научных
исследований по специальным видам экспертиз
и экспертно-криминалистического обеспечения
противодействия наркопреступности
управления научных исследований
Экспертно-криминалистического центра МВД России*

О НЕГАТИВНОЙ РОЛИ КРИПТОВАЛЮТЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ

Важнейшей отличительной чертой современной экономической ситуации, складывающейся в России, является крайне стремительное развитие цифровых технологий, в связи с чем возрастает как потенциал мощностей различных отраслей промышленности, так и уровень противоправной деятельности, связанной с получением незаконных доходов.

В настоящий момент повсеместно ведутся дискуссии о криптовалютах, созданных на основе технологии блокчейн, и их влиянии на мировую экономику. В частности, в России отношение к такого рода средствам весьма неоднозначно в связи с их неопределенностью. Кроме того, использование нестабильных и неопределенных финансовых инструментов способствует развитию дисбаланса экономической обстановки путем создания теневой конкуренции с государственной валютой. Многочисленные физические и юридические лица уже видят в данном инструменте средство обогащения путем спекуляций на финансовых рынках. Например, по состоянию на 1 октября 2020 г. 1 биткоин – самая популярная криптовалюта – стоил 10,6 тыс. \$, по состоянию на 1 ноября 2021 г. его цена составила 60,9 тыс. \$, а по состоянию на 1 сентября 2022 г. – 20,1 тыс. \$ [1].

В научной литературе отмечается, что обменные курсы криптовалют являются не просто волатильными, они в течение короткого отрезка времени (например, в течение недели) могут вырасти или упасть в несколько раз. Поэтому они не способны выступать мерилom стоимости, следовательно, быть деньгами [2, с. 53].

Важно отметить, что криптовалюты становятся привлекательным инструментом для осуществления разнообразных завуалированных схем, в том числе транснационального характера, связанных с мошенничеством, незаконным оборотом наркотических средств, торговлей людьми, выводом капитала за границу и другими преступлениями. Это обусловлено тем, что отследить маршрут движения средств по криптографическим счетам в настоящее время возможно только при согласии самих участников данной системы расчетов. С целью противодействия преступной деятельности правоохранительными органами в настоящее время разрабатываются системы, позволяющие сделать криптовалюту более «прозрачным» инструментом.

Приоритетными органами надзора за рисками, целесообразностью внедрения и развития криптовалют в России являются Федеральная служба по финансовому мониторингу (далее – Росфинмониторинг) и Центральный Банк Российской

¹ © Шкинин Д. А., 2022.

Федерации (далее – ЦБ РФ), поскольку данный инструмент за счет крайне высокой степени анонимности данных о транзакциях несет прямую угрозу, связанную с легализацией (отмыванием) доходов, полученных преступным путем, финансированием терроризма и финансированием распространения оружия массового уничтожения, что в условиях современной действительности приобрело особую актуальность. Кроме того, следует помнить, что согласно Конституции Российской Федерации, основной функцией Банка России является защита и обеспечение устойчивости рубля с исключительным правом денежной эмиссии.

В Информационном сообщении «Об использовании криптовалют» от 6 февраля 2014 г. Росфинмониторинг указал, что «процесс выпуска и обращения наиболее распространенных криптовалют полностью децентрализован и отсутствует возможность его регулирования, в том числе со стороны государства. Еще одной из ключевых особенностей использования криптовалют является анонимность пользователей таких криптовалют. Также, криптовалюта не требует ведения специальной отчетной документации.

Вышеуказанные обстоятельства, и в первую очередь анонимность платежа, обусловили активное использование криптовалют в торговле наркотиками, оружием, поддельными документами и иной преступной деятельности. Данные факты, а также возможность бесконтрольного трансграничного перевода денежных средств и их последующего обналичивания, служат предпосылками высокого риска потенциального вовлечения криптовалют в схемы, направленные на легализацию (отмывания) доходов, полученных преступным путем, и финансирование терроризма» [3].

Аналогичную позицию обозначил и Центральный Банк Российской Федерации в Информации от 4 сентября 2017 г. «Об использовании частных “виртуальных валют” (криптовалют)», указав, что большинство операций с криптовалютами совершается вне правового регулирования как Российской Федерации, так и большинства других государств. Криптовалюты не гарантируются и не обеспечиваются Банком России.

Криптовалюты выпускаются неограниченным кругом анонимных субъектов. В силу анонимного характера деятельности по выпуску криптовалют граждане и юридические лица могут быть вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.

Операции с криптовалютами несут в себе высокие риски как при проведении обменных операций, в том числе из-за резких колебаний обменного курса, так и в случае привлечения финансирования через ICO (Initial Coin Offering – форма привлечения инвестиций граждан в виде выпуска и продажи инвесторам новых криптовалют/токенов). Существуют также технологические риски при выпуске и обращении криптовалют и риски фиксации прав на «виртуальные валюты». Это может привести к финансовым потерям граждан и к невозможности защиты прав потребителей финансовых услуг в случае их нарушения [4].

На сегодняшний день правовая регламентация криптовалют обеспечена Федеральным законом «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»

от 31 июля 2020 г. № 259-ФЗ (далее – Закон), формулировки которого крайне размыты и абстрактны, во многом не содержат конкретики, что ведет к возникновению судебных и внесудебных споров, а также проблемам толкования норм, в связи с чем вступление в силу данного закона в настоящее время представляется неоправданным и преждевременным как несоответствующего правилам юридической техники. В силу изложенного, остается открытым вопрос о том, каким образом осуществлялась антикоррупционная экспертиза Закона.

Исходя из того, что экономическая ситуация в мире, в частности, в России, нестабильна, внедрение нового финансового инструмента требует всеобъемлющей апробации на государственном уровне, чего проведено не было, а принятие Закона основано лишь на разрозненных данных об использовании цифровых активов.

Стоит особо отметить вопрос эмиссии криптовалют. Технология блокчейн предоставляет возможность создавать виртуальную валюту практически любому пользователю, в распоряжении которого имеется компьютер с выходом в сеть Интернет, а также вычислительные мощности, обеспечиваемые в первую очередь количеством видеокарт компьютера.

Закономерным результатом подобного бесконтрольного выпуска и использования виртуальной валюты физическими лицами является обесценивание государственной валюты и последующая дестабилизация экономики.

Также необходимо обратить внимание на перспективу внедрения криптовалют в оборот в условиях возрастающей цифровизации. Если исходить из того, что подобный финансовый инструмент эмитируется не государством, а любым физическим и (или) юридическим лицом, то со временем неизбежно появление и накопление так называемых «частных средств», используемых вместо национальной валюты при совершении расчетно-платежных операций.

В данном контексте хоть и отдаленно, но прослеживается некая аналогия с имевшими место «вбросами» фальшивых денег в экономику России и других стран во времена наполеоновских войн, а также Второй мировой войны с целью обесценивания государственной валюты и обрушения экономики [5; 6].

Наличие и динамическое развитие цифровых технологий обостряет ситуацию путем попыток создания на их основе денежных суррогатов для обеспечения конкуренции с государственной валютой или ее полного вытеснения. Подобные «эксперименты» ведут, помимо названных, к иным непредсказуемым последствиям, однако сторонники новых финансовых инструментов в своих выступлениях, публикациях и комментариях всячески пытаются обосновать их пользу, возможности и перспективы, не воспринимая иных точек зрения, тем самым создавая впечатление, что продвижение такого рода средств осуществляется не из благих намерений.

Значимым моментом при исследовании вопроса необходимости в криптовалютах является отношение к ним рядового населения страны, которое в большинстве не обладает знаниями, связанными с различными аспектами эмиссионной деятельности государства и экономических наук в целом, благодаря чему

злоумышленники получают новый способ обмана людей путем разработки способов мошенничества на базе криптовалют преимущественно с использованием интернет-технологий с целью обеспечения полной анонимности.

Таким образом, исходя из вышеизложенного и учитывая, что современная экономика характеризуется наличием большого количества лиц, осуществляющих различные финансовые спекуляции, теневые схемы, а также совершающих экономические преступления, полагаем, что внедрение криптовалют в настоящее время является необоснованным в связи с крайне высокими рисками, моментно связанными с преступной деятельностью и отрицательным влиянием на экономическую ситуацию в стране.

Важно также соблюдать осторожность с целью недопущения дальнейшего ухудшения экономической ситуации, в связи с чем необходим более подробный и всесторонний анализ данного инструмента на государственном уровне, так как принятие скоротечных решений в условиях экономической нестабильности закономерно приведет к хаосу, что недопустимо.

Список использованных источников:

1. Инвестиционный ресурс Investing.com // Портал «Investing». URL: <https://ru.investing.com/crypto/bitcoin/historical-data>.
2. Деньги, кредит, банки : учебник и практикум для вузов / ред. В. Ю. Катысонов, В. П. Битков. М. : Юрайт, 2021. С. 53.
3. Информационное сообщение Росфинмониторинга от 6 февраля 2014 г. «Об использовании криптовалют» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
4. Информация Банка России от 4 сентября 2017 г. «Об использовании частных “виртуальных валют” (криптовалют)» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
5. Первый выстрел Наполеона по России был сделан фальшивыми деньгами // Новостной портал «Московский Комсомолец – МК». URL: <https://www.mk.ru/economics/700let/2016/12/10/pervyy-vystrel-napoleona-po-rossii-byi-sdelan-falshivymi-dengami.html>.
6. Как гитлеровцы пытались «свалить» британский фунт // Сетевое издание «Военное обозрение». URL: <https://topwar.ru/36541-kak-gitlerovcy-pytalis-svalit-britanskiy-funt.html>.

Забавин М. В.¹,
 слушатель факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя,

Научный руководитель:
Максимченко А. М.,
 преподаватель кафедры специальных
 информационных технологий
 учебно-научного комплекса
 информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ СЛЕДООБРАЗОВАНИЯ ПРИ РЕАЛИЗАЦИИ УДАЛЕННОГО ДОСТУПА К ПЕРСОНАЛЬНОМУ КОМПЬЮТЕРУ

С начала 1970-х гг. на территории нашего государства происходит довольно прогрессивный технологический прогресс, который связан с распространением и внедрением в повседневную жизнь различного рода информационных технологий для упрощения жизнедеятельности человека. На кардинальные изменения во взаимодействии людей оказала особенное влияние всемирная компьютерная сеть Интернет. Если ранее персональный компьютер (далее – ПК) был изолирован, то 7 апреля 1994 г. был официально зарегистрирован первый домен в зоне Российской Федерации (ru). В наши дни невозможно представить ПК без выхода в глобальную сеть Интернет. Важной характеристикой глобальной сети является то, что она существует как открытая информационная система, к ресурсам которой имеют полный и анонимный доступ люди из любого населенного региона нашей планеты. Ввиду этого глобальная сеть является очень хорошим средством для получения несанкционированного доступа (далее – НСД) к пользовательской информации, находящейся в энергозависимой памяти устройств пользователей.

Информатизация общества предполагает в себе ускоренное овладение знаниями в сфере информационных технологий, к тому же среди молодого поколения. Также, на протяжении всего времени использования ПК, специалистами в области информационных технологий было разработано множество программного обеспечения и специализированной техники для упрощения взаимодействия работы пользователя с устройством. Однако наряду с этим было разработано и не раз успешно применено вредоносное программное обеспечение для НСД. Все эти случаи повлияли на развитие преступности в информационной сфере.

Целью работы является разработка теоретических рекомендаций для выявления и рассмотрения случаев НСД с помощью удаленного воздействия, совершаемых с помощью всемирной компьютерной сети Интернет.

¹ © Забавин М. В., 2022.

Задачей работы является потребность компьютерных экспертов и следователей, которым необходима методика и тактика для решения возникающих практических задач.

Объектом работы информационная сфера, в которой обрабатывается в ходе криминальной деятельности компьютерная информация и технологии для НСД.

Предметом работы являются объективные закономерности криминальной деятельности при НСД к компьютерной информации, хранящейся в энергозависимой памяти устройств пользователей.

Под удаленным несанкционированным доступом к информации устройства следует понимать способ совершения преступления, при котором злоумышленник применяет специальные приемы, средства и методы для получения доступа к данным, хранящимся в памяти устройства жертвы. Совокупность методов и правил, разработанных и применяемых, с помощью которых реализуется доступ к информации, является механизмом взаимодействия злоумышленника с данными, хранящимися на ПК жертвы.

Удаленный доступ является непосредственным способом совершения преступления независимо от того, с помощью какой сети осуществлялся доступ. С точки зрения выявления следов абсолютно неважно находился ли ПК, к которому был осуществлен несанкционированный доступ, в локальной или глобальной сети, белый или серый IP-адрес он имел. Основопологающим и существенным является тот факт, что злоумышленник получает доступ к информации, хранящейся на ПК жертвы, с помощью своих периферийных устройств ввода-вывода при помощи линии связи, а не с устройства, на которое оказано воздействие.

Достижение уголовно наказуемых последствий неправомерного доступа к компьютерной информации (уничтожение, блокирование, модификация и т. д.) возможно только в силу доступа к процессам, позволяющим реализовать эти последствия. Под процессом понимается программное обеспечение, которое может находиться продолжительный промежуток времени в стадии выполнения, т. е. загруженной в энергозависимую память ПК и ожидающую команд пользователя или иных событий.

Некоторые злоумышленники пытаются получить доступ не к файлам ПК жертвы, а к процессам, выполняющимся на устройстве пользователя. Таким образом можно получить доступ к данным, которые хранятся в энергозависимой памяти устройства или передаются по сети. В случае передачи по сети, файлы представляют из себя пакеты данных, расположенных в оперативно-запоминающем устройстве. К данным файлам обращаются только те устройства, программы и файлы которых передают, принимают или просто являются посредниками при передаче информации.

Некоторые специалисты, обладающие специальными познаниями в области информационных технологий, предлагают определять обстановку совершения преступления следующими субъектами:

- 1) аппаратные средства;
- 2) программные средства;
- 3) средства защиты.

Также компьютерными экспертами предлагается ввести такой элемент, как «уязвимость». Суть данного понятия заключается в том, что оно дает представление о качестве защищенности объекта от удаленного воздействия на него злоумышленником.

Взаимодействие пользователя с компьютером осуществляется с помощью периферийных устройств (монитор, клавиатура, мышь), так и с помощью бинарного кода, с помощью которого информация в системе ПК обрабатывается и хранится. Вот и с помощью множества логических и математических операций происходит воздействие на энергозависимую память с устройства злоумышленника на устройство пользователя. В результате чего получается изменение двоичного кода в памяти устройства жертвы.

С точки зрения физики данное воздействие заключается в совокупности измененных электрических сигналов, которые несут в себе бинарный код, а в соответствии с логикой работы ПК происходит и изменение энергозависимой памяти носителя информации. Надо заметить, что не все модификации двоичного кода будут приводить к изменению памяти носителя информации. Все это из-за того, что изменения в устройство вносят только те процессы, которые связаны с алгоритмами конкретной программы.

Компьютерные эксперты отмечают, что существуют два источника, позволяющих получить сведения о событии удаленного воздействия:

- 1) компьютерная информация на информационном носителе ЭВМ (сети), подвергшейся удаленному воздействию;
- 2) лица, обладающие информацией, относимой к событию преступления.

О событии удаленного воздействия могут свидетельствовать различные следы, возникшие в компьютере:

- изменения в работе программных и/или аппаратных средств;
- уничтожение или изменение файлов сетевых журналов;
- изменение содержания Web-страницы;
- уменьшение объема свободного пространства на жестком диске;
- высокая интенсивность работы в сети;
- неразборчивый режим сетевых интерфейсов;
- присутствие новых пользователей в системе;
- использование учетных записей локальных пользователей для доступа к удаленным компьютерам;
- предупреждения других администраторов;
- запуск необычных процессов и необычная работа компьютера;
- изменение конфигурации системы;
- изменение, удаление или создание новых файлов;
- необычная активность в определенный день или определенное время.

Последние двадцать лет во всех высокоразвитых странах мира возникла очень важная проблема – появление преступности, связанной с получением доступа к пользовательской информации с помощью удаленного доступа. В данное время компьютерная криминалистика еще имеет некоторые пробелы и нахо-

дится на этапе становления. Это, в первую очередь, связано с недостаточным количеством практики по данному направлению, а во-вторых, в нехватке научно обоснованных теоретических методик для органов исполнительной власти. На сегодняшний день в данной области отмечается довольно прогрессивный рост преступности. И, к сожалению, наиболее сложным по части раскрытия и расследования преступлений в области высоких технологий являются преступления с использованием информационно-телекоммуникационных технологий.

Список использованных источников:

1. ГОСТ Р ИСО/МЭК 30121-2017 Информационные технологии (ИТ). Концепция управления рисками, связанными с проведением судебной экспертизы свидетельств, представленных в цифровой форме. М. : Стандартиформ, 2017. 12 с.
2. Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 5 (57). С. 31–44.
3. Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе : монография. М. : Норма : Инфра-М, 2018. 576 с
4. Аверьянова Т. В. Судебная экспертиза. Курс общей теории. М. : Норма : Инфра-М, 2014. 479 с.
5. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе : монография. М. : Юрлитинформ, 2012. 152 с.
6. Юбко Ю. М., Скачек Р. В. Производство по материалам о нарушении права интеллектуальной собственности на программный продукт «1С: Предприятие»: организационные и тактические аспекты // Актуальные проблемы уголовного процесса и криминалистики при раскрытии и расследовании преступлений : тезисы докладчиков научно-практической конференции (Минск, 15 ноября 2013 г.). Минск : Академия МВД, 2013. С. 276–278.
7. Ткачев А. В. Исследование компьютерной информации в криминалистике // Эксперт-криминалист. 2012. № 4. С. 5–8.

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

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ ДЛЯ ПОИСКА КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ ИНФОРМАЦИИ

В настоящее время общество уже не может представить свое существование в отрыве от современных технологий. Прогресс происходит повсеместно, затрагивая абсолютно все сферы деятельности человека. Технологический прогресс подарил человечеству такие незаменимые вещи, как интернет, спутниковое телевидение и т. п. Появившиеся возможности открыли новые горизонты для взаимодействия людей по всему миру, позволяя общаться, обмениваться опытом, искать интересующую информацию.

С развитием интернета, человек, находящийся практически в любой точке мира, получил доступ к огромному массиву информации, используя возможности, которые предоставляют различные поисковые системы, форумы, социальные сети и иные виртуальные платформы. При этом можно отметить, что размер аудитории, которая получает информацию посредством сети Интернет, с каждым днем растет. Это связано, прежде всего с доступностью, мобильностью и простотой использования интернет-ресурсов.

Развитие информационных технологий приводит не только к увеличению числа пользователей сети Интернет, но и к бурному росту количества размещенной там информации. В этой связи логично предположить, что с течением времени любой человек, обладающий выходом в интернет, будет способен, буквально не выходя из дома, получить информацию любого характера, набрав нужную комбинацию клавиш в поисковом запросе.

При этом, источником информации в сети становятся не только отдельные физические лица, организации и корпорации, но и органы государственной власти. Уже сейчас государство начало понимать важность использования возможностей, предоставляемых глобальной сетью. И здесь возникает вопрос, какую информацию необходимо и следует размещать в сети. Не секрет, что, проведя анализ открытой, общедоступной информации можно получить данные, которые будут иметь статус ограниченного доступа.

Преимущество использования информационных ресурсов, а также других возможностей сети Интернет оценили не только законопослушные граждане, но и различные преступные группировки. И правоохранительные органы должны это учитывать в своей работе.

¹ © Клочкова Е. Н., 2022.

В настоящее время, правоохранительные органы имеют высокое материально-техническое оснащение. Все структурные подразделения в системе МВД России оснащены специальными закрытыми базами данных, аппаратно-программными комплексами, информационными банками данных и т. п. Любой сотрудник в рамках правового поля имеет доступ к этим системам. Указанные системы значительно упрощают процесс поиска необходимых сведений, что является хорошим подспорьем в решении повседневных задач оперативно-разыскной деятельности.

Но в то же время правоохранительные органы, кроме имеющихся оперативных баз, вынуждены искать дополнительную информацию, осуществляя мониторинг сети и поиск информации по открытым источникам. Огромный массив данных, циркулирующий на просторах сети Интернет, представляет не меньший интерес и полезность для органов правопорядка. Ведомственные информационные системы не могут содержать в себе всю требуемую информацию, они не содержат, например, такой информации, как наличие социальных сетей у лица, представляющего оперативный интерес, круга лиц, поддерживающего с объектом заинтересованности тесный контакт в сети, его интересы, принадлежность к какому-либо сообществу, организации и многое другое, т. е. того, что касается его так называемой «виртуальной» жизни. Такая жизнь может быть значительно активнее, богаче, чем его повседневное общение. Всю эту информацию можно найти на различных веб-форумах, пабликах, видеохостингах, телеграм-каналах и других платформах, т. е. сотрудники правоохранительных органов вынуждены для раскрытия преступлений заниматься OSINT-ом – поиском информации по открытым источникам.

Информация из открытых источников хоть и не является информацией ограниченного доступа, но порой может превосходить их своей ценностью. Общая ценность данных из открытых источников определяется рядом аспектов, среди которых:

1. Оперативность поступления.
2. Объем полученных данных.
3. Качество.
4. Ясность.
5. Легкость дальнейшего использования.
6. Стоимость получения.

Традиционное использование поиска информации с открытым исходным кодом (OSINT) – это, прежде всего, национальная безопасность, расследование преступлений и киберпреступлений. Но в то же время в настоящий момент OSINT начали использовать и специалисты по кибербезопасности обычных компаний, проводящих тестирование на проникновение, а также и простые пользователи (не всегда законопослушные), которым необходима та или иная информация.

К открытым источникам информации относят следующие:

1. Информацию, опубликованную в средствах массовой информации.
2. Данные, циркулирующие в глобальной сети Интернет (социальные сети, видеохостинги, вики-справочники, блоги, веб-форумы и т. д.).

3. Общедоступные отчеты и заявления, данные из официальных ресурсов, материалы пресс-конференций.

4. Наблюдения – радиомониторинг, использование общедоступных данных дистанционного зондирования земли и аэрофотосъемок.

5. Статьи и доклады конференций, профессиональные и академические отчеты.

Наиболее популярные такие типы открытых данных как:

1. Культурные – сведения о раскопках и артефактах, музеях, культурных мероприятиях и пр.

2. Научные – результаты научных исследований, начиная от астрономии и заканчивая зоологией.

3. Финансовые – сведения о состоянии финансовых рынков, о государственных счетах, (доходы и расходы государства).

4. Метеорологические – данные, которые бы позволили следить за изменениями в погоде и климате.

5. Статистические – данные, полученные с помощью статистических управлений, таких как переписи населения и основные социально-экономические показатели.

6. Данные об окружающем пространстве – информация, связанная с окружающей природной средой, например, присутствия и уровень загрязняющих веществ, качество рек и морей.

7. Данные о транспорте – всевозможные сведения о маршрутах, расписания движений и т. д.

Можно предположить, что приведенные данные хоть и представляют в совокупности определенную ценность, для правоохранительных органов больший интерес представляет информация, распространяемая, например, на различных форумах с противоправным умыслом. Для них такого рода данные также будут представлять оперативно-значимый интерес, а информация будет «криминалистически значимой».

Криминалистически значимые данные – это фактические данные, находящиеся в причинно-следственной связи с событием преступления, а также сведения справочного характера, используемые в процессе расследования преступлений.

Существует два вида криминалистически значимой информации:

1. Актуальная криминалистически значимая информация.

2. Потенциальная криминалистически значимая информация.

К первому виду относится информация, характеризующая способ совершения преступления, обстоятельства, лиц, его совершивших, предмет преступного посягательства, орудия преступления, а ко второму информация, характеризующая признаки различных объектов (человека, материалов, веществ, предметов и изделий).

Криминалистически значимые данные ввиду своей специфики в большей своей части располагаются в анонимных сегментах сети Интернет. В этой связи актуальным вопросом на сегодняшний день, стоящим перед правоохранительными органами, является сбор и анализ такой информации, а также разработка

и применение на практике приемов и методов, позволяющих осуществлять своевременный контроль за действиями лиц, возможно причастных к совершению преступления, в целях недопущения распространения материалов криминогенного характера и осуществления преступной деятельности. Но в то же время отсутствие необходимых знаний, умений и навыков у сотрудников оперативных подразделений зачастую не позволяет на плановой основе осуществлять поиск, использование и анализ такой информации. Однако в том случае, если проведения таких исследований становится возможным, это может значительно повысить качество работы оперативных подразделений.

Список использованных источников:

1. Оперативно-розыскная деятельность в цифровом мире : сборник научных трудов / под ред. В. С. Овчинского. М. : Инфра-М, 2021.
2. Павлюков В. В. Компьютерная разведка как оперативно-розыскное мероприятие // Вестник Нижегородской академии МВД России, 2016 № 4. С. 236–240.
3. Поликарпов Е. С. Основы компьютерной разведки. М. : Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя, 2020. 321 с.

Кофтина Ю. Н.¹,

*доцент кафедры психологии, педагогики
и организации работы с кадрами
Академии управления МВД России,
кандидат юридических наук*

Екимов А. Ю.²,

*слушатель факультета подготовки
руководителей (начальников)
территориальных органов МВД России
Академии управления МВД России*

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ИХ ИСПОЛЬЗОВАНИЕ В ОРГАНИЗАЦИИ КАДРОВОГО ОБЕСПЕЧЕНИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Современное общество XXI в. является информационным, основу которого составляет беспрецедентное по объему и скорости передачи информации развитие инновационных технологий. Ставшая столь крылатой фраза «тот, кто владеет информацией, владеет миром», затрагивает проблему огромной роли информации для достижения преимуществ во всех областях жизнедеятельности общества. Актуальность рассматриваемой проблемы заключается в том, что развитие информационных технологий в системе государственной службы является важным условием обеспечения эффективного управления кадровыми ресурсами; в модернизации в сфере кадровой политики в целом, в том числе в органах внутренних дел Российской Федерации.

Современный период развития цивилизации характеризуется переходом человечества от постиндустриального общества к обществу информационному через информатизацию всех сфер и направлений деятельности. Становление глобального информационного пространства обеспечивает эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам и удовлетворение их потребностей в информационных продуктах и услугах. В информационном обществе главными продуктами производства становятся именно информация и знания, а информационно-коммуникационные технологии воздействуют на все сферы человеческой деятельности и общество в целом [5; 7].

Отметим, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и о защите информации» закреплены основные понятия, в том числе: информация – сведения (сообщения, данные) независимо от формы их представления; информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов; информационная система

¹ © Кофтина Ю. Н., 2022.

² © Екимов А. Ю., 2022.

(далее – ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [1].

Вместе с тем, данный нормативный правовой акт определил понятие «документированной информации» – это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель [1]. Таким образом, возможность оперативно получать и эффективно обрабатывать информацию для принятия соответствующих управленческих решений – необходимое условие успеха современной организации. Помочь в решении этой задачи призваны информационные технологии.

В своих выступлениях и посредством подписания конкретных нормативных правовых актов Президент Российской Федерации В. В. Путин неоднократно обосновывал необходимость совершенствования управления государственной службой, преобразований кадровой политики и внедрения новейших технологий. В первую очередь, это Указ Президента Российской Федерации от 9 мая 2017 г. № 203, утверждающий Стратегию развития информационного общества в Российской Федерации на 2017–2030 гг. [3]

В современных условиях широкое использование информационных технологий как действенного инструмента повышения эффективности органа государственной власти осуществляет и МВД России. Для совершенствования системы информационного обеспечения деятельности органов внутренних дел Российской Федерации стали широко использоваться новые информационные технологии, основанные на автоматизации процессов обработки информации.

Подчеркнем, что одним из основных направлений деятельности МВД России является кадровое обеспечение, при этом совершенствование служебной деятельности кадровых подразделений остается приоритетной задачей, решаемой на всех уровнях управления. В современных условиях формирование кадровой политики МВД России невозможно без использования информационных технологий. Вместе с тем, технические и информационные преобразования неизбежны, поэтому законодатель не случайно включил в Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» принцип использования достижений науки и техники, современных технологий и информационных систем как один из основополагающих принципов деятельности правоохранительных органов [2].

Следует отметить, что электронные базы данных, используемые в МВД России, предназначены для систематизации и хранения информации, а также позволяют получить оперативный доступ к необходимым сведениям, облегчают их поиск и предоставление в самом различном формате – в тестовом, цифровом, графическом, фото- и видео. Исходя из широкого перечня используемых в процессе служебной деятельности органов внутренних дел персональных данных следует вывод о том, что информация о сотрудниках наличествует в различных учетах и банков данных, функционирующих в МВД России. Эти банки данных сопоставимы с гигантским хранилищем документальной памяти, как живого организма, обеспечивающего процесс поиска, обработки и анализа информации.

Работа с личным составом неразрывно связана с накоплением, формированием, обработкой и использованием значительных объемов сведений о всех категориях сотрудников органов внутренних дел. В условиях нарастающего темпа развития новых технологий в обществе вопрос необходимости применения информационно-аналитических систем и перехода службы кадровых подразделений ОВД в новый формат приобретает особое значение. Важным шагом в создании единой кадровой системы, покрывающей потребности учета государственных служащих, гибкость системы в плане возможности ее дополнения, функциональных процедур и отчетных форм стал созданный в 2016 г. на базе ИСОД МВД России – Сервис обеспечения кадровой деятельности МВД России (СОКД).

Оптимизация информационных процессов кадровой деятельности, автоматизированный анализ больших массивов информации, а также оперативный доступ сотрудников к распределенным информационным ресурсам способствует эффективному выполнению служебных задач, стоящих перед органами внутренних дел. За счет автоматизации целого ряда информационных процессов сотрудники кадровых подразделений освобождаются от рутинных, трудоемких операций и могут основное время посвятить аналитической работе, повышению профессиональных навыков и дальнейшему совершенствованию своей служебной деятельности. Однако, в настоящее время, можно отметить психологическую и профессиональную неподготовленность руководителей и сотрудников к всестороннему использованию появившиеся технических возможностей. Недостаток специальной профессиональной подготовленности в сфере информационных технологий сотрудников кадровых подразделений, неумение правильно выразить свою информационную потребность, оперативно найти, проанализировать и извлечь необходимую информацию, а также использовать ее рациональным способом существенно замедляет процесс выполнения служебных обязанностей по замещаемой должности.

Подчеркнем, что пандемия новой коронавирусной инфекции наглядно продемонстрировала приоритеты информатизации общества в целом и государственных ведомств в частности, существенно изменила устоявшиеся рабочие процессы. Внедрение цифровых технологий, создание и совершенствование процессов формирования и использования кадровых учетов, основанных на принципах однократности ввода и широкого спектра использования информации, автоматизация и оптимизация работы с данными сотрудников, в настоящее время, позволяют осуществить качественные преобразования в МВД России и выводят кадровую систему органов внутренних дел на новый профессионально качественный уровень.

Так, в управлении по работе с личным составом УМВД России по Тамбовской области в период с 1994 г. разработаны и внедрены в эксплуатацию АИС «Кадры», не входящие в состав ИСОД МВД России.

Данная автоматизированная информационная система (далее – ИС), была создана сотрудниками УРЛС УМВД России по Тамбовской области с целью оптимизации и актуализации учета кадровой работы, а также минимизации исполь-

зования рабочего времени и трудовых ресурсов. На постоянной основе ИС модернизируются с целью соответствия постоянно изменяющимся требованиям действующих нормативных правовых актов и оперативного решения поставленных перед кадровыми подразделениями задач по обеспечению служебной деятельности органов внутренних дел Тамбовской области.

АИС «Кадры» предоставляет возможность ведения учета личного состава в объеме электронного личного дела за исключением частей, составляющих государственную и иную охраняемую законом тайну, что позволяет оперативно получать необходимую отчетную информацию по работе с кадрами, а также осуществлять контроль ее соответствия предъявляемым требованиям действующего законодательства. С помощью разработанных программных продуктов данная АИС имеет ряд неоспоримых преимуществ в анализе и имеет возможность осуществления следующих мероприятий: получение информации о кандидатах на службу в ОВД, стадии оформления и контроля сроков приема на службу; оперативное получение актуальной информации о наличии вакантных должностей всех категорий с датами образования вакансий; разработана и введена в действие подсистема «Кадровый резерв», которая позволяет осуществлять учет сотрудников и контроль удовлетворения «резервистов» установленным требованиям при их включении в кадровые резервы области, формировать списки; на основе подготовленной отчетной информации автоматизировано формирование ведомственной оценки по подразделениям (в соответствии с требованиями распоряжения МВД России от 26 декабря 2018 г. № 1/14868) и др.

Одним из важных разделов программного обеспечения являются функции мониторинга вводимой в базу данных информации на соответствие требованиям нормативных правовых актов, включающих в себя контроль присвоения специальных званий, обоснованность и правильность перемещения по службе, наличие конфликта интересов, связанных с прохождением службы близкими родственниками, назначение на должности сотрудников соответствующей квалификации, своевременности прохождения первоначальной подготовки, информации об имеющемся образовании, выявления перемещения по службе с целью присвоения звания, контроль сдачи нагрудных знаков сотрудника полиции при увольнении и перемещении по службе, наличие дисциплинарных взысканий, контроль приказов по личному составу, контроль наличия судимости, наличие и статистика поощрений и наград, обоснованность и своевременность снижения/лишения квалификационного звания, задержание присвоения очередного специального звания.

Одной из последних разработок является сервис «Пенсионный фонд». В связи с вступлением в силу Федеральных законов Российской Федерации возникла необходимость ежемесячно представлять в Пенсионный фонд Российской Федерации (далее – ПФР) отчет формы СЗВ-ТД, утвержденный Постановлением Правления ПФР от 25 декабря 2019 г. № 730п, в электронном виде. Таким образом, указанный сервис позволяет своевременно и в полном объеме представлять в ПФР сведения о трудовой деятельности работников, государственных гражданских служащих, стажеров и аттестованных сотрудников УМВД России по Тамбовской области.

Следует отметить, что в АИС «Кадры» масса других полезных сервисов, позволяющих ускорить процесс учета кадровой работы, максимально исключать возможность допущения ошибок, так называемого «человеческого фактора», при работе с кадрами и служебной документацией. Каждый разработанный инструмент является уникальным и имеется возможность его модификации с учетом постоянно изменяющихся требований.

Автоматизированная информационная система «Кадры» УМВД России по Тамбовской области находится в постоянном ежедневном совершенствовании, разрабатываются новые учеты, возможности и методы контроля учетной информации с целью повышения эффективности кадровой работы, недопущения ошибок и нарушений. Автоматизированная система ведется длительное время и накопленные за время эксплуатации данные, позволяют оперативно получать необходимую информацию, что является неоспоримым преимуществом перед СОКД ИСОД МВД России, а применение данных информационных технологий кадровыми подразделениями УМВД России по Тамбовской области ежедневно позволяют обеспечить основные функции, такие как: оперативность выполнения служебных задач; упорядоченность потока кадровой информации; своевременность получения учетной и учетно-аналитической информации; освобождение от трудоемкой и однообразной деятельности; перераспределение функций среди сотрудников; повышение культуры служебной деятельности и т. д.

Резюмируя изложенное, подчеркнем, что уровень информационной компетентности определяется состоянием информационной культуры и информационной грамотности сотрудника [4]. Ежедневная работа с информационными системами несомненно повышает уровень информационной компетентности сотрудников кадровых подразделений УМВД России по Тамбовской области, что в свою очередь предполагает их способность эффективно использовать средства информатизации и новые информационные технологии для решения служебных задач, стоящих перед органами внутренних дел Российской Федерации.

Список использованных источников:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.
2. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_11016.
3. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 290.
4. Елистратова Н. Н. Информационная культура как критерий информатизации высшего образования в современных условиях реформирования // Современные научные исследования и инновации. 2012. URL: <http://web.snauka.ru/issues/2012/07/15770>.

5. Сафронов А. Д., Иванов Р. О. Информационное обеспечение кадровых технологий территориальных органов МВД России : учебное пособие. М. : Академия управления МВД России, 2014.

Курбакова Д. О.¹,
 курсант Института-факультета подготовки
 сотрудников для органов
 предварительного расследования
 Московского университета
 МВД России имени В.Я. Кикотя

Задохина Н. В.²,
 доцент кафедры информатики
 и математики
 Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат педагогических наук

ОСОБЕННОСТИ ПСИХОЛОГИЧЕСКОГО ПОРТРЕТА ЖЕРТВЫ КИБЕРПРЕСТУПЛЕНИЙ

Актуальность проблемы научной интерпретации понятия «жертва киберпреступления» обоснована рядом причин, среди которых можно выделить основные:

- 1) особенности развития современного общества в период тотальной цифровизации;
- 2) дефицит нормативно-правовых ориентиров в вопросах кибербезопасности общества и государства;
- 3) недостаточное внимание законодателей к проблеме виктимизации в виртуальной среде.

Кроме того, недостаточно изученным является и «психологический портрет» жертвы киберпреступления.

Очевидно, что цифровые технологии, постепенно проникающие во все сферы жизни современного общества, зачастую используются человеком даже для удовлетворения элементарных потребностей. Однако у всеобщей цифровизации есть и свои минусы, среди которых – риск стать жертвой киберпреступления, является наиболее значимым. Киберпреступность – достаточно широкое понятие. Тем не менее данное понятие изучено довольно глубоко в отличии от понятия «жертва киберпреступления» или «кибержертва».

Среди ученых-правоведов бытует мнение о том, что преступления общеуголовной направленности, которые совершаются с использованием интернет-ресурсов, не всегда корректно признавать киберпреступлениями в «чистом виде». В этой связи и толкование понятия «кибержертва» как потерпевшее лицо, которому был нанесен вред с помощью интернет-ресурсов, является в настоящее время дискуссионным вопросом.

Так, Д. В. Жмуров подчеркивает, что «кибержертва – это потерпевший от любых преступлений, осуществленных в цифровой среде (было ли это оконченное

¹ © Курбакова Д. О., 2022.

² © Задохина Н. В., 2022.

преступление или покушение). Лица, виктимизированные в реальности из-за своего провокационного или неосмотрительного поведения в сети, кибержертвами не являются. Однако таковыми можно признать тех, кто «попался на удочку» многоходовых комбинаций, исполнение которых началось в интернете и окончилось за его пределами. Также под определение кибержертв подпадают и те, кто, не используя сеть лично, пострадал от действий компьютерных злоумышленников» [2, с. 52].

В своих исследованиях Д. В. Жмуров выделяет особенности кибервиктимизации. Автор предлагает следующее определение данному понятию: «Причинение вреда физической личности посредством компрометации ее цифровой идентичности или в ходе негативного взаимодействия с этой идентичностью» [2, с. 50].

Говоря о цифровой идентичности личности – киберличности, автор подчеркивает, что зачастую при совершении киберпреступлений подвергается каким-либо лишениям не столько сама жертва, сколько ее субличность (ее визуализация, информационное поле, образ и репутация, репрезентация в сетевом окружении и др.) [2, с. 50].

Набор качеств киберличности зачастую кардинально расходится с качествами данной личности в реальной жизни. Подобное явление выражается, прежде всего, в:

- 1) активной презентации выдуманного виртуального образа;
- 2) несдержанном поведении в интернет-пространстве;
- 3) ощущении безопасности и уверенности в анонимности.

Иными словами, виртуальное поведение личности зачастую крайне отличается от реального поведения этой же личности. В. М. Жеребин в своих исследованиях выделяет мотивы подобного поведения интернет-пользователей:

- 1) мотив самоутверждения;
- 2) мотив аффилиации;
- 3) мотив самореализации и развития личности и др. [3, с. 119–120].

В основе мотива самоутверждения лежат глубинные психологические явления – самооценка личности, уровень притязаний, мотивация достижения. В своих исследованиях А. С. Перевозчикова говорит о самоутверждении личности, как о «процессе, в ходе которого в условиях собственной активности личность реализует не только социально обусловленную потребность во взаимодействии с себе подобными, но и свою самость» [4, с. 138]. Одна из причин желания человека самоутвердиться заключается в стремлении актуализироваться в социальной деятельности, оказаться полезным в окружающей действительности. Важную роль играет в такой ситуации и ценностная конституция человека, от которой зависят такие составляющие личности, как: черты характера, особенности поведения в определенных ситуациях, закономерные реакции на поведение других людей, потенциал и другие характеристики.

Австрийский психолог, психиатр и мыслитель, создатель системы индивидуальной психологии А. Адлер, вслед за Ф. Ницше, признавал стремление к собственной власти одной из причин психологического стимула человека к самоутверждению. А. Адлер выделил два вида психологического самоутверждения:

- 1) самоутверждение, характерное для людей без психических отклонений;

2) самоутверждение, свойственное невротикам.

В первом случае нормальный человек со здоровой психикой не имеет комплексов по поводу своего превосходства или ничтожества, он стремится совершенствовать свои личностные качества в разумных пределах, исходя из адекватных мотиваций. Такой человек, в первую очередь, стремится преодолевать трудности и решать проблемы внешнего мира, с помощью чего, собственно, и происходит процесс совершенствования его личности. Стоит добавить, что процесс самоутверждения нормальной личности можно охарактеризовать как перманентный, постепенный, умеренный процесс. Такая характеристика обуславливается тем, что для личности с нормальной адекватной самооценкой необходимо определенное время для достижения своих целей, получения успеха от решаемых задач. Его устремления не направлены на скорость, они направлены на результат.

Что касается невротиков, в данном случае у таких людей присутствует комплекс неполноценности, поэтому вся их деятельность направлена на то, чтобы продемонстрировать свое собственное превосходство, даже, если это будет достигнуто путем унижения чужого достоинства. Стоит сказать, что на самом деле, деятельность невротика по самосовершенствованию является фальшью и притворством, от которого он все равно не получает в полной мере удовлетворения по достижении определенных результатов. Такое самоутверждение способно лишь на короткий промежуток времени «заглушить» боль, вызываемую осознанием своей ничтожности, что, кстати, зачастую не является объективной самооценкой, в связи с чем невротик вынужден постоянно доказывать себе и окружающим людям свою личностную ценность.

Следующий выделенный мотив – мотив аффилиации, т. е. мотив стремления быть в обществе других людей, потребность человека в создании теплых, доверительных, эмоционально значимых отношений с другими людьми. Аффилиация проявляет социальную сущность человека. Таким образом, существующее в психологии понятие «потребность в аффилиации» означает потребность в общении, нахождении индивидуума в социуме.

Так, Т. И. Толчинская в своих исследованиях выделяет высокоаффилиативных и низкоаффилиативных людей. Для людей высокоаффилиативных характерно стремление к установлению и поддержанию позитивных отношений с окружающими. Такие люди подвержены сильным переживаниям при ухудшении этих отношений. Чтобы восстановить дружеские связи, высокоаффилиативные люди готовы отказаться от собственных удобств. Для лиц с низкой потребностью в аффилиации общение не является столь значимой потребностью. Но это не означает, что низкоаффилиативные люди не нуждаются в общении совсем, просто данная необходимость у них выражена в меньшей степени [6, с. 39–42].

Мотив самореализации представляет собой побуждение к творческому процессу, носит положительный характер. Многие интернет-пользователи осознают перспективы интернет-пространства для саморазвития и достижения определенных карьерных высот.

В заключение стоит подчеркнуть, что в настоящее время еще не существует стандартизованного определения жертвы киберпреступлений. Эта категория лиц

получает значительно меньше внимания со стороны средств массовой информации, ученых-правоведов, законодателей, чем киберпреступники. Потребность в таком правовом регуляторе назревает и, по всей видимости, это вопрос ближайшего времени. Обращаясь к вышесказанному, хочется отметить, что чаще среди кибержертв встречаются высокоаффилиативные, творческие люди, которым свойственны излишняя доверчивость и невысокая самооценка.

Список использованных источников:

1. Гаврилюк Р. В., Носаненко Г. Ю., Уразов А. А. Аффилированные лица: понятие и признаки // Балтийский гуманитарный журнал. 2020. Т. 9. № 2 (31). С. 347–349.
2. Жмуров Д. В. Кибержертва: решение проблемы терминологической неопределенности // Вестник Восточно-Сибирского института МВД России. 2021. № 2 (97). С. 45–56.
3. Жеребин В. М., Алексеева О. А., Вершинская О. Н. Социально-психологические особенности пользователей Интернета // Народонаселение. 2017. № 1 (75). С. 116–124.
4. Перевозчикова Л. С. Конструктивное самоутверждение личности как философская проблема // Сибирский педагогический журнал. 2007. № 1. С. 138–145.
5. Старцев А. А., Гришанин Н. В., Кириллина Н. В. Идентичность и идентификация личности в социальных сетях // Коммуникология. 2018. № 4. С. 76–87.
6. Толчинская Т. И. Связь потребности в аффилиации с субъективными характеристиками личности // Актуальные вопросы психологии. 2015. № 9. С. 39–45.

Клочкова А. М.¹,
*студент кафедры цифровых технологий
и информационных систем
Московского авиационного института*

Максимов Н. А.²,
*доцент кафедры цифровых технологий
и информационных систем
Московского авиационного института*

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Интернет вещей все больше входит в нашу повседневную жизнь. Сейчас уже очень сложно найти область, в которой бы не использовались возможности, предоставляемые интернетом вещей. Это медицина и здравоохранение, мониторинг окружающей среды, управление городской и сельской инфраструктурой, цифровые системы управления, общественная безопасность и т. д. Рассмотрим, что же такое интернет вещей, и какие проблемы с обеспечением его безопасности существуют на текущий момент.

Необходимо отметить, что единого определения понятия интернета вещей (IoT) не существует, в данной статье мы приведем определение, данное в рекомендациях Сектора стандартизации электросвязи Международного союза электросвязи. Интернет вещей – это глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий. Вся инфраструктура интернета вещей состоит из четырех уровней:

Первый уровень – уровень «вещей». При этом под «вещами» принято понимать некоторые физические или виртуальные объекты, которые можно идентифицировать и интегрировать в коммуникационные сети.

Второй уровень – предназначен для первичного сбора и обработки данных. Данный уровень обеспечивает связь первого уровня с глобальными сетями передачи данных.

Третий уровень – представляет собой непосредственно сети передачи данных. С помощью таких сетей информация передается в облачные хранилища данных. При этом необходимо обратить внимание, что совершенно не обязательно, чтобы это была сеть Интернет, главное, чтобы была возможность передавать данные.

На четвертом уровне уже располагаются облачные платформы, приложения, инструменты, которые предназначены для анализа и обработки массива получаемых данных.

¹ © Клочкова А. М., 2022.

² © Максимов Н. А., 2022.

Бурное развитие интернета вещей приводит к тому, что область его применения постоянно расширяется, количество подключенных устройств стремительно растет. При этом обеспечение безопасности в настоящее время является одной из главных проблем данной сферы. Если для защиты последних двух уровней создано больше количество инструментов, технологий, которые активно внедряются и используются, то с обеспечением безопасности первых двух уровней все значительно сложнее. Среди основных причин можно выделить следующие.

Устройства, используемые при реализации технологии интернета вещей, нельзя рассматривать как совокупность независимых единиц, это всегда разнообразная и широкая экосистема, включающая устройства, коммуникации, интерфейсы и непосредственно людей.

Разработчики устройств в качестве основных критериев при их создании традиционно выбирают минимизацию стоимости и времени разработки, увеличение объемов выпускаемой продукции. Результатом такого подхода, становится то, что окончательные устройства в итоге не имеют необходимых ресурсов для размещения инструментов безопасности, и они становятся инструментами злоумышленников для атак на другие ресурсы. А учитывая то, что современные технологии интернет вещей все больше проникают в критически важную инфраструктуру страны, то это уже может нести угрозу безопасности государству.

В последнее время о безопасности интернета вещей говорят все чаще, но ее обеспечение требует не только создание системы защиты, но и постоянную поддержку в актуальном состоянии. Огромное количество используемых устройств затрудняет обеспечение безопасности при установке обновлений IoT, так как специфика пользовательских интерфейсов не позволяет использовать традиционные механизмы обновления.

В связи с бурным развитием IoT, данная область все больше привлекает к себе различных злоумышленников. Это приводит к тому, что угрозы и риски, связанные с интернетом вещей, становятся все более разнообразными и быстро развиваются. Учитывая их влияние на здоровье, безопасность и конфиденциальность пользователей, их опасность нельзя игнорировать. Пользователи могут не знать, что IoT в значительной степени основывается на и обработке больших объемов данных из различных источников, включая и конфиденциальные данные, и обмене ими.

Еще одна проблема связана с тем, что интернет вещей – это еще очень молодая сфера, и о проблемах защиты данных в данной области начали говорить не так давно, поэтому наблюдается острая нехватка квалифицированных, подготовленных специалистов в области безопасности IoT.

Одним из возможных решение в области защиты IoT от киберугроз может стать создание безопасной операционной системы для сетевых устройств, автоматизированных систем управления и других систем интернета вещей. Такой операционной системой стала российская разработка Лаборатории Касперского – Kaspersky OS.

Данная операционная система позиционируется, как операционная система, архитектурно ориентированная на системное решение проблемы киберзащиты технологических процессов. Если про традиционные операционные системы

можно сказать, что они в той или иной мере уязвимы, так как проектировались они без четкого представления о безопасности, то особенностью Kaspersky OS стало то, что проблемы безопасности выступали в качестве основополагающих при ее создании.

Предполагается, что продукты на основе данной ОС наделяются кибериммунитетом, т. е. можно сказать «врожденной» устойчивостью к рискам информационной безопасности.

Кибериммунитет – новый подход к разработке безопасных IT-решений на базе KasperskyOS. Такие решения по умолчанию защищены от подавляющего числа кибератак (как существующих, так и еще неизвестных) и будут выполнять свои критические функции даже в условиях агрессивной среды.

Подход, на котором основано решение «Лаборатории Касперского» заключается в том, что внимание уделяется не безопасности каждого из огромного количества устройств, а обеспечивается защита от угроз при передаче данных по каналам связи, от атак на шлюз и подключаемые к нему устройства. Создание защищенного шлюза позволяет повысить надежность всей инфраструктуры.

В основе Kaspersky OS лежит легкое микроядро, которое допускает только заранее определенный способ взаимодействия и может работать на разных платформах. Защитный компонент Kaspersky Security System (KSS) контролирует взаимодействие между всеми частями системы, делая эксплуатацию уязвимостей бесполезной для злоумышленников.

В заключении хотелось бы отметить, что интернет вещей – это новая тема, имеющая важное техническое, социальное и экономическое значение. Потребительские товары, автомобили, промышленные и энергетические компоненты, датчики и другие предметы повседневной жизни проектируются с подключением к интернету и с мощными функциями анализа данных. Влияние IoT на интернет и экономику в ближайшем будущем трудно переоценить. Однако в то же время, перед интернетом вещей стоит ряд проблем, которые могут помешать нам воспользоваться его потенциальными преимуществами.

Список использованных источников:

1. Верещагина Е. А., Капецкий И. О., Ярмонов А. С. Проблемы безопасности Интернета вещей : учебное пособие. М. : Мир науки, 2021.
2. Смушкин А. Б. Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // Всероссийский криминологический журнал. 2020. Т. 14. № 3. С. 453–460.
3. Жуков Р. Обзор Kaspersky IoT Secure Gateway, шлюза для построения безопасных систем интернета вещей // Сайт «Anti-malware». URL: <https://www.anti-malware.ru/reviews/Kaspersky-IoT-Secure-Gateway>.

Поликарпов Е. С.¹,
*начальник кафедры специальных
 информационных технологий
 учебно-научного комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат технических наук, доцент*

Мурашев А. Е.²,
*слушатель факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя*

ИСПОЛЬЗОВАНИЕ ЦИФРОВОГО ОТПЕЧАТКА УСТРОЙСТВА В ОПЕРАТИВНО-АНАЛИТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аналитическая деятельность является одним из направлений деятельности органов внутренних дел, являясь при этом многогранным понятием, включающим в себя ряд таких процессов как сбор, обработка, систематизация, анализ и оценка поступающей информации. Являясь по своей сути одной из современных тенденций, аналитика решает множество вопросов, стоящих перед правоохранителями и поддерживает их в принятии тех или иных решений. Так, она может быть прогностической, предлагая возможные способы расстановки сил и средств, основываясь на полученной информации о состоянии криминогенной обстановки определенных районов, позволяет находить нужную информацию в огромном массиве данных, поступающих из различных источников – будь то выборка необходимого лица из видеопотока или сбор информации об объекте оперативного интереса из разных источников. Предметами сравнительного анализа могут быть также различные направления оперативно-служебной деятельности (предупреждение, раскрытие и расследование преступлений, розыск преступников и лиц, пропавших без вести, результаты противодействия преступности и т. д.) и организаторской (управленческой) деятельности руководителя органа или подразделения (стиль и методы работы, эффективность управления силами и средствами и т. п.).

Одним из важнейших направлений оперативной деятельности является выявление общностей, отыскание закономерностей тех или иных процессов с целью поиска связей между событиями, предметами и людьми. Так, понимание этих закономерностей помогает более наглядно представлять взаимосвязь между членами преступных сообществ, подельниками и лицами, невольно попавшими под влияние криминального мира, когда необходимо установить, что два и более лица являлись соисполнителями конкретного преступления.

¹ © Поликарпов Е. С., 2022.

² © Мурашев А. Е., 2022.

Цифровой след, иногда называемый цифровой тенью или электронным следом – это данные, которые пользователь оставляет при использовании интернета. Эти данные включают посещаемые веб-сайты, отправляемые электронные письма и информацию, указываемую в онлайн-формах. Цифровой след можно использовать для отслеживания действий человека и его устройств в интернете. Пользователи интернета активно или пассивно создают собственный цифровой след. Процесс расширения цифрового следа не всегда очевиден, например, веб-сайты могут отслеживать активность, устанавливая файлы cookie на устройство пользователя, а приложения без его ведома могут считывать данные. Применительно к цифровым следам часто используются термины «активный» и «пассивный».

Как известно, персональный компьютер каждого человека также содержит огромное количество как информации относящейся к его владельцу, так и технически данных, создаваемых системой в процессе эксплуатации технического средства. Так, операционная система, являющаяся оболочкой для взаимодействия пользователя с аппаратной частью персонального компьютера, хранит помимо прочего и записи о подключениях к другим устройствам. Данная функция создана в первую очередь для облегчения взаимодействия пользователя со своим устройством и упрощения выполнения некоторых задач, таких как, например, подключение к беспроводной сети, обнаружение и подключение Bluetooth-устройств, USB-устройств и т. д. Пользователю удобно не хранить пароль у себя в памяти, а передать эту функцию компьютеру для облегчения аутентификации и ускорения данного процесса. Так, в памяти сохраняются все сети беспроводной передачи данных, к которым подключалось устройство. Хранится информация об SSID точки доступа, способе ее защиты (например, WPA2-Personal), шифре и содержимом ключа безопасности. Узнать эту информацию можно путем введения в командную строку следующих команд: «netsh wlan show profile» для отображения всех сохраненных SSID и «wlan show profile Имя_сети key=clear» для отображения более подробной информации о конкретном подключении, в том числе и пароля в открытом виде в поле «Содержимое ключа».

Помимо этого, компьютер сохраняет множество другой информации, таких как список используемых USB-накопителей (данные хранятся в реестре в HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\ и HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\), записи DNS, информацию о том, к каким сетям подключался персональный компьютер и многое другое. Во многом, это также объясняется ускорением процесса взаимодействия с ними в будущем, так как использование уже сохраненных конфигураций на порядок быстрее создания новых.

Весь этот массив данных образуют так называемый «слепок устройства», что позволяет использовать его в аналитической деятельности для выявления взаимосвязей нескольких устройств на предмет общности используемого ими периферийного оборудования, подключения к схожим сетям, использования одинаковых USB-носителей, что может говорить о связи их владельцев. Помимо этого, данные извлекаемые из персональных компьютеров могут свидетельствовать об использовании пользователем тех или иных интернет-ресурсов, выступать

в качестве сравнения с тем, какие следы злоумышленник оставил в системе, в процессе его идентификации.

На данный момент существует достаточно большое количество программного обеспечения, позволяющего осуществлять визуализацию связей между объектами, обладающими рядом признаков-маркеров. К таким решениям, например, относится продукт Maltego от компании Paterva, IBM i2 Analyst's Notebook, SpiderFoot и другие, однако их функционал заключается в сборе информации из различных источников об объекте исследования и анализа, являясь при этом интеграторами различных сервисов. При этом есть необходимость в разработке и создании системы, которая бы осуществляла сравнительный анализ таких «слепков», полученных с персональных компьютеров злоумышленников для получения оперативно-значимой информации об их связях между собой, используемых ими носителях, иных сведений, которые могли бы быть полезны в рамках оперативно-розыскной деятельности.

Подводя итог стоит отметить, что создание и ведение базы данных «слепков устройств» позволит открыть отдельное оперативно-аналитическое направление, которое позволит выявить связи разрабатываемых лиц.

Список использованных источников:

1. Кузнецова Л. В., Миронов Е. В., Бояркин А. Б. Аналитическая работа в территориальных органах МВД России на районном уровне. 3 изд. Барнаул : Барнаульский юридический институт Министерства внутренних дел Российской Федерации, 2020. 51 с.
2. Что такое цифровой след? // Сайт «Лаборатория Касперского». URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprin>.
3. Колисниченко Д. Заметаем следы. Как заставить Windows удалить историю, логи, кеши и все забыть // Хакер. 2016. № 20.

Никитин Г. К.¹,
 слушатель факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Поликарпов Е. С.,
 начальник кафедры специальных
 информационных технологий
 учебно-научного комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат технических наук, доцент

АЛГОРИТМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ВЫЯВЛЕНИЮ ФАКТОВ ПРОДАЖИ ТЕХНИЧЕСКИХ СРЕДСТВ С ФУНКЦИЕЙ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Возможности сети Интернет при раскрытии преступлений имеют большой потенциал. Огромные массивы информации, циркулирующие в информационно-телекоммуникационной сети, могут содержать как напрямую нарушение закона, так и представлять большое оперативное значение в раскрытии. По оценкам института статистических исследований и экономики знаний в 2022 г. общий объем фиксированного интернет-трафика достиг 78.1 экзабайт, увеличившись на 26 % по сравнению с 2021 г. и динамика интернет-трафика, а, следовательно, объема информации стремительно набирает обороты. Наиболее рациональное решение по выявлению противозаконных действий в сети, это автоматизация обработки данных.

Цель исследования состоит в изучении факта незаконного оборота специальных технических средств, предназначенных для негласного получения информации посредством использования интернет-сервисов для размещения объявлений о продаже товаров, а также возможных способов автоматизации процесса выявления и раскрытия такого рода преступлений. Продажа и использование устройства «скрытого слежения» запрещены ст. 138.1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации».

Несмотря на то что такие устройства запрещены отдельные граждане даже не в курсе и заказывают на зарубежных сайтах товары для скрытой аудио-, видео-, фотофиксации и определения геолокации для развлечения или пере-

¹ © Никитин Г. К., 2022.

продажи, а по факту оказывается, что это уголовная ответственность и нарушение прав других граждан на неприкосновенность частной жизни согласно ст.ст. 23 и 24 Конституции Российской Федерации.

В России наиболее известными интернет-сервисами по продаже товаров в России являются Avito и Юла. Согласно данным представленных на интернет-платформе Similarweb, которая проводит веб-аналитику, Avito занимает первое место в категории электронная коммерция и шопинг в Российской Федерации и за сентябрь 2022 г. ресурс Avito был посещен более 341 млн раз [1]. Интернет-сервис Юла, в свою очередь, был посещен в сентябре 2022 г. более 15 млн раз [2].

Популярность и простота использования интернет-сервисов по продаже товаров привлекает не только лиц, которые заинтересованы в продаже бывших в использовании собственных товаров, но и лиц, которые занимаются незаконным оборотом различных товаров. Например, к такого рода товарам можно отнести специальных технические средства, предназначенные для негласного получения информации.

Согласно комментариям к ст. 138.1 Уголовного Кодекса Российской Федерации к специальными техническими средствами, предназначенными для негласного получения информации относятся приборы, системы, комплексы, устройства, специальные инструменты для проникновения в помещения и (или) на другие объекты и программное обеспечение для электронных вычислительных машин и других электронных устройств для доступа к информации и (или) получения информации с технических средств ее хранения, обработки и (или) передачи, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя. К важному замечанию относительно СТС НПИ необходимо отнести, что органы управления и индикация об их работе, а также маркировка о типе устройства должны быть скрыты или отсутствовать [3].

Так, например, на *рис. 1* представлен GPS-трекер, найденный на интернет-сервисе по продаже товаров Avito, который не обладает какими-либо органами управления, индикацией и маркировке о полном функционале устройства. Блок GPS скрыт в корпусе автомобильного зарядного устройства [4].

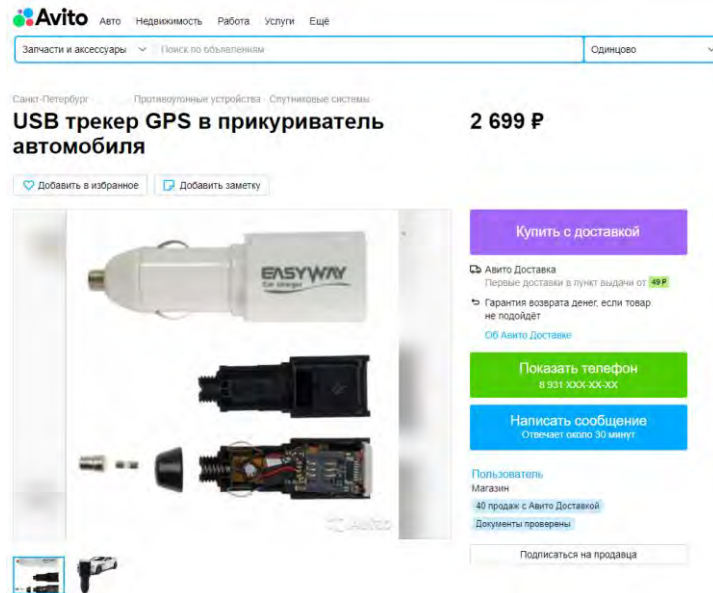


Рис. 1. GPS трекер в автомобиль

Изучив профиль пользователя, можем установить факт того, что лицо на постоянной основе занимается продажей различных устройств слежения на основе системы глобального позиционирования. Профиль продавца представлен на рис. 2.

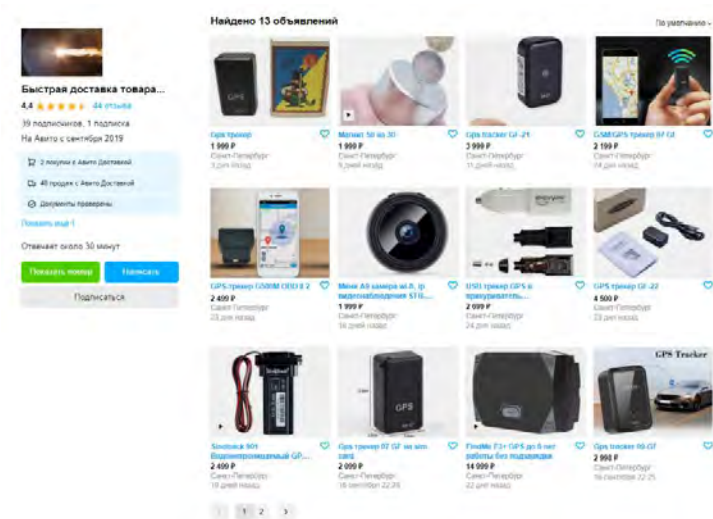


Рис. 2. Профиль продавца GPS-трекера в автомобиль

Исходя из массовости использования людьми таких сервисов как Avito и Юла, а также возможного их использования в противоправной деятельности, считаю целесообразным создание программы с возможностью автоматизированного отслеживания выше указанных площадок для установления факта продажи устройства, подходящего под описание СТС НПИ, последующего изучения профиля пользователя, продающего такого рода устройства, для получения информации о возможном обороте, а не разовой продажи, а также с возможностью дальнейшего отслеживания и регистрации действий такого лица [5].

Алгоритм программного обеспечения по выявлению фактов продажи технических средств с функцией негласного получения информации состоит из семи этапов:

1. Автоматизированный анализ интернет-сервисов по продаже товаров, по ключевым словам, для выявления и сбора объявлений, подходящих под описание специальных технических средств негласного получения информации. Выгрузка собранных объявлений в telegram-чат для более удобного изучения, в случае возникновения вопросов у оператора информационной системы.

2. Автоматизированный анализ отобранных объявлений, а именно изучение фотографии товара по ключевым параметрам СТС НПИ, а также описания к товару.

3. Автоматизированный анализ профиля продавца для установления факта продажи схожих товаров или же отсутствия данного факта.

4. Автоматизированный сбор информации о продавце, представленной на интернет-сервисе по продаже товаров. К такой информации можно отнести: отмеченную локацию места продажи, номер мобильного телефона, адрес электронной почты и отзывы.

5. Получение дополнительных сведений путем разведки по открытым источникам информации.

6. Отправка программы-агента продавцу через возможные каналы связи с ним.

7. Проведение удаленного изучения информации об устройстве злоумышленника, а также имеющейся на нем значимой информации для органов внутренних дел.

В заключении стоит отметить, что на настоящее время необходимо уделить больше внимания на интернет-площадки по продаже товаров, так как проведенное изучение ресурса Avito показало о возможном незаконном обороте специальных технических средств для негласного получения информации, попадающего под действия, указанные в ст. 138.1 УК РФ.

Список использованных источников:

1. Анализ компании avito.ru // Сайт «Similarweb». URL: <https://pro.similarweb.com/#/sales/account-overview/avito.ru/company>.

2. Анализ компании youla.ru // Сайт «Similarweb». URL: <https://pro.similarweb.com/#/sales/account-overview/youla.ru/company>.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 24.09.2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.

4. USB трекер GPS в прикуриватель автомобиля // Сайт «Avito». URL: https://www.avito.ru/sanktpeterburg/zapchasti_i_aksessuary/usb_treker_gps_v_prik.

5. Поликарпов Е. С., Анисимов С. Л., Толстых А. А. О защищенности сайта сети интернет от автоматизированного сбора данных // Вестник Воронежского института МВД России. 2020. № 1. С. 77–84.

Ситникова А. В.¹,
*курсант международно-правового
 факультета Московского университета
 МВД России имени В.Я. Кикотя*

Научный руководитель:
Стащенко С. П.,
*доцент кафедры противодействия преступлениям
 в сфере информационно-телекоммуникационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя*

К ВОПРОСУ О МЕХАНИЗМАХ ОБРАЗОВАНИЯ ЦИФРОВЫХ СЛЕДОВ

На современном этапе все большее распространение приобретают преступления, совершаемые в сфере информационно-телекоммуникационных технологий. В связи с этим, острым становится вопрос расследования данных преступлений, которое является невозможным без рассмотрения следов, а именно цифровых. Правильное определение механизмов образования цифровых следов необходимо для раскрытия преступлений в информационно-телекоммуникационной сфере. В статье рассматриваются механизмы образования цифровых следов, их значение при раскрытии киберпреступлений.

Вместе с развитием экономической и информационной сфер жизни общества, открываются новые возможности для совершенствования способов совершения преступлений в информационно-телекоммуникационной сфере (далее – ИТ). В связи с этим, в 1970-х гг. появилась такая частная криминалистическая теория – «цифровая криминалистика», предметом изучения которой являются: «закономерности обнаружения, фиксации, предварительного исследования, использования компьютерной информации и средства ее обработки в целях выявления, раскрытия, расследования и предупреждения правонарушений...» [1, с. 15]. Закономерности образования цифровых следов изучаются в разделе криминалистического учения о компьютерной информации и является элементом особенной части цифровой криминалистики.

Понятие «цифровой след», по мнению О. В. Гайдаша, подразумевает особый блок деятельности на цифровых устройствах и сети Интернет [2, с. 10], однако в теории цифровой криминалистики применяется понятие цифрового следа, как любая значимая цифровая информация, представленная в виде электрических сигналов [1, с. 20].

Ключевой целью статьи является изучение механизмов образования цифровых следов. Задачи научной статьи можно выделить следующие:

1. Определить основные понятия, а именно: «следообразование», «предварительное расследование», «киберпреступление».
2. Изучить механизмы образования цифровых следов.

¹ © Ситникова А. В., 2022.

3. Выдвинуть предложения по увеличению эффективности расследования и раскрытия преступлений в сфере ИТТ.

4. Цифровой след – значимый элемент, лежащий в основе доказательственной базы при расследовании преступлений в сфере ИТТ.

Понятие «след» зафиксировал в научных трудах С. М. Потапов [3, с. 13] еще в 1945 г., и под данным термином он подразумевал отображение признаков определенных предметов на материальном объекте и причинную связь между ними. Соответственно, из определения понятия «след» можно уяснить термин «следообразование» как процесс отображения признаков предмета на материальном объекте. Но каким образом происходит образование цифровых следов, зная, что информация не является объектом материального мира? Данный вопрос в настоящее время является дискуссионным. Однако с точностью известно, что каждое действие имеет свой след, так и действия, связанные с информацией, оставляют след, только особенностью механизма образования между следообразующим и следовоспринимающим объектами является то, что она происходит в искусственно созданной сфере – информационной, к которой относятся, например, электронные носители информации, информационно-телекоммуникационные сети и информационные сети.

Цифровые следы имеют большое значение при производстве предварительного расследования, которое подразумевает под собой регламентированную уголовно-процессуальным Законом деятельность следователя или дознавателя по собиранию, проверке, оценке доказательств в целях установления значимых обстоятельств по делу [4, раздел 8], в данном случае это касается «киберпреступлений». Научный деятель М. Е. Батухин выдвигает определение «киберпреступление» как «всякое преступное деяние, которое совершено с помощью компьютерных средств, информационной сети в электронной сфере» [5, с. 28]. Другое определение данному понятию дает Организация Объединенных наций: киберпреступление – это преступление, совершенное как с помощью компьютерной системы и сети, так и в ее рамках и направленное против них [6].

В основе механизмов образования цифровых следов лежат электромагнитные взаимодействия, осуществляемые посредством электромагнитных сигналов и фиксируются на материальных носителях информации. Механизм следообразования означает процесс, вследствие которого образуются цифровые следы. Такой механизм основывается на взаимодействии цифровых объектов. Цифровые следы принято делить на три группы: активные цифровые следы, то есть активные действия лиц, например, переписка на электронной почте, оставление публикаций в сети Интернет; пассивные цифровые следы, которые остаются без ведома лица, например, истории поиска в браузере; следы, оставленные злоумышленником. По данному вопросу А. Н. Яковлев в своей научной работе разъяснял, что активные и пассивные следы взаимодействуют по алгоритмам, находящимся в компьютерных программах, которые и определяют степень и характер вносимых изменений [7, с. 129].

Так, наличия цифрового следоотображения свидетельствуют такие признаки:

1) какие-либо изменения компьютерной информации, ее характеристик, формата, либо содержания;

2) изменение алгоритма компьютерных программ;

3) фиксация обработки компьютерной информации программами, работающими автоматически.

Цифровыми следами (предметами) являются любые материальные носители информации, содержащейся в любом формате. К таким носителям относят, например, жесткие диски, USB-накопители, электронно-вычислительные машины и их сети и системы,

Известно, что цифровые следы являются цифровыми доказательствами и, соответственно, имеют значение при расследовании преступлений. Цифровые доказательства представляют собой большой объем значимой для следователя или дознавателя информации, который имеет различные источники формирования, например, А. Ю. Черданцев приводит наиболее часто используемые источники [8, с. 4–5]: записи транзакций, информация, хранящаяся в «облачном хранилище», электронные письма, персональные компьютеры, жесткие диски и флеш-накопители, телефонные записи. Данный список далеко не исчерпывающий, но при этом значимый для наиболее эффективного раскрытия преступлений в сфере ИТТ.

Появление и развитие интеллектуально новых способов совершения преступлений в ИТТ сфере знаменуется все большим усложнением расследования таких преступлений. Стоит отметить, что несмотря на стремительное развитие способов совершения преступлений, законодательство Российской Федерации наращивает темпы усовершенствования нормативно-правовой базы, предусматривающую ответственность за совершение киберпреступлений. Так, Уголовный кодекс Российской Федерации [9, гл. 28] предусматривает целую главу, устанавливающую ответственность за ряд составов преступлений в сфере информационно-телекоммуникационных технологий. Следует сказать, что в Российской Федерации Указом Президента от 5 декабря 2016 г. № 646 утверждена Доктрина национальной безопасности [10], одной из целей которой является закрепление системы официальных взглядов на обеспечение национальной безопасности в информационной сфере. Для улучшения эффективности пресечения, выявления и раскрытия преступлений в сфере ИТТ был создан федеральный проект «Информационная безопасность», а также при Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации существует Департамент обеспечения кибербезопасности. Исходя из вышесказанного, следует сказать о том, что деятельность по минимизации преступлений в сфере ИТТ осуществляется на должном уровне как на государственном уровне, так и на уровне непосредственного осуществления предварительного расследования, в процессе которого следователями и дознавателями на основании законодательства Российской Федерации применяются нормативно-правовые акты и новые информационные технологии.

Искоренение преступности как в общем, так и в сфере ИТТ является невозможным, но к этому всегда нужно стремиться и прикладывать для этого все возможные законные способы. Соответственно, для повышения эффективности расследования и раскрытия киберпреступления можно предложить следующие действия:

1) профилактика, то есть активная пропаганда защищенного использования информационных систем и сетей;

2) усовершенствование технологий и технических возможностей для проведения компьютерных экспертиз и увеличение числа экспертных учреждений для увеличения скорости проведения судебных экспертиз;

3) обеспечение обучения высококвалифицированных кадров для органов следствия и дознания, а также специалистов в сфере ИТТ;

4) повысить уровень мониторинга киберпреступлений.

Высокая цифровизация – это новый этап в развитии современного общества, наряду с очевидными «плюсами» существуют и неизгладимые «минусы», заключающиеся в быстром распространении и совершенствовании киберпреступлений. Однако отечественная наука не отстает и развивается в ногу с появляющимися новшествами.

Огромную роль в расследовании и раскрытии киберпреступлений играют цифровые следы, механизмы образования которых были рассмотрены в данной статье. Следует отметить, что данный вопрос является сложным и спорным в части теоретических основ, так как научные деятели в области криминалистики имеют различное мнение. В статье были рассмотрены наиболее важные аспекты по вопросу механизма образования цифровых следов, а также вынесены предложения по повышению эффективности по расследованию и раскрытию преступлений.

Список использованных источников:

1. Цифровая криминалистика : учебник для вузов / [В. Б. Вехов и др.] ; под ред. В. Б. Вехова, С. В. Зуева. М. : Юрайт, 2021. 417 с.

2. Гайдаш О. В. Феномен цифрового следа в современном обществе // Вестник магистратуры. 2020. № 6 (105).

3. Потапов С. М. Введение в криминалистику : учебное пособие. М. : РИО ВЮА КА, 1946. 24 с.

4. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 24.09.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/.

5. Батухтин М. Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе : материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. 2018.

6. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Официальный сайт Организации Объединенных Наций. URL: <https://www.unodc.org/congress/ru/previous-congresses.html>.

7. Вехов В. Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография. Волгоград : Волгоградская академия МВД России, 2008.

8. Черданцев А. Ю. Понятие цифровых доказательств, современное состояние и их роль в доказательственном процессе // Юридическая наука и практика. 2019. № 15 (4). С. 55–60.

9. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 24.09.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.

10. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины национальной безопасности Российской Федерации» // Российская газета. URL: <https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html>.

Цыцурин С. Л.¹,
*научный сотрудник Центра средств
и систем связи СТус МВД России*

Меликов Э. Э.²,
руководитель направления АО «Крибрум»

ЦИФРОВАЯ БЕЗОПАСНОСТЬ. НЕДАВНЯЯ ПРОБЛЕМА, РЕАЛЬНАЯ УГРОЗА

В статье рассматриваются особенности программного обеспечения для сбора, хранения и обработки информации из сети Интернет, научно обоснованных методик и моделей обработки больших массивов данных, методов интерпретации результатов мониторинга и анализа информации.

Рынок IT-технологий в последнее десятилетие переживает стремительный рост. В обиходе появляется все больше гаджетов с приложениями и интернет-сервисами, позволяющим делать жизнь комфортнее. Люди все более погружаются в информационную паутину, а бумажные носители постепенно уходят в прошлое. Однако, одновременно с этим технологии несут значительные риски, так как если традиционные СМИ функционируют в рамках правового поля, то размещение информации в соцмедиа, блогах, мессенджерах, как правило, не регулируется.

Использование сети Интернет (далее – сети) для распространения деструктивных материалов, экстремистской информации, манипулирования общественным мнением, вовлечения граждан в противоправную деятельность приобретает все более глобальный масштаб. Особую опасность такие действия несут с учетом технической возможности таргетированного (ориентированного на определенную группу) распространения информации.

Сталкиваясь с огромным потоком информации, люди попросту не способны отфильтровать правду от лжи, манипуляцию от достоверного изложения, пропаганду от независимой подачи фактов. Все более очевидно, что для обеспечения безопасности и гарантирования здорового развития общества, необходимо иметь эффективные средства противостояния такого рода информационным нападкам.

Многие страны уже давно обеспокоились влиянием деструктивного контента, разрабатывая эффективные средства борьбы с ним. Основная деятельность в данной области сосредоточена на двух связанных направлениях – разработка программного обеспечения для сбора, хранения и обработки информации из сети, а также создание научно обоснованных методик и моделей обработки больших массивов данных, методов интерпретации результатов мониторинга и анализа информации.

¹ © Цыцурин С. Л., 2022.

² © Меликов Э. Э., 2022.

В Российской Федерации для исследования деструктивных явлений реализованы системы, осуществляющие мониторинг социальных медиа по таким деструктивным направлениям деятельности как скулшутинг, наркотики, анархизм, криминальные субкультуры.

Одной из систем мониторинга, сбора данных из социальных медиа в реальном времени, осуществляющей дальнейшую обработку массивов данных, является уникальная платформа «Крибрум» (далее – система). Так, например, 60 % всего потока собирается за час, а весь поток – не более, чем за 5 часов. Грубо говоря, вы делаете пост в социальной сети, а система об этом уже знает.

Система позволяет выявлять информационные угрозы; информацию о нарушении работы (сбои, утечка данных), факты и схемы мошенничества. Для обеспечения релевантности поиска создано более 400 уникальных лингвистических моделей. Объем информации, который система собирает, обрабатывает и хранит, составляет несколько десятков миллионов сообщений в месяц.

Непрерывный сбор данных ведется с 2014 г. на серверах в России, общий объем хранимой информации составляет порядка 3 петабайт (1 петабайт информации – стопка компакт-дисков высотой 3 км или около 500 млрд страниц стандартного печатного текста). Система поддерживает сбор и анализ данных на 23 языках, включая английский, арабский, китайский. Ежедневно система собирает, обрабатывает и хранит порядка 1 млрд единиц информации (500 млн действий аккаунтов социальных сетей, 140 млн текстовых сообщений, 40 млн изображений и т. п.).

В системе реализованы: интеллектуальный поиск, средства ретроспективного анализа, инструменты количественного и качественного анализа данных. Другими словами, ее ресурсы, например, позволяют проследить, что писал человек десять лет назад, что пишет сейчас, несет ли его активность риски как ему самому, так и окружающим.

Отличительными особенностями системы являются:

- работа, как с текстом, так и графикой, она может определять тональность текста, распознавать текст на изображении, а в перспективе – определять лица на изображениях;
- наличие экспертных функций – изучение поведения отдельных пользователей и целых сообществ в сети (лайки, репосты, участие в группах, выявление неявных связей между пользователями);
- поиск аккаунтов в социальных медиа по заданному паттерну активности с целью формирования индивидуальных и групповых портретов пользователей; прогнозирование поведения, включая противоправные действия;
- анализ распространения информации, классификация информационных поводов (кампаний, информационных волн) и определение их происхождения (организованное или органическое), выявление первоисточников распространяемой информации;
- возможность развертывания в закрытом контуре заказчика (банковская сфера и т. п.), что обеспечивает дополнительный уровень информационной защищенности.

Система успешно применяется для анализа ситуации с коронавирусом. По результатам мониторинга готовятся ежедневные и еженедельные отчеты, в которых отражается влияние пандемии на различные сферы жизни общества (экономика, политика), изучаются изменение показателей тревожности и агрессивности аудитории, динамика отношения пользователей к политикам и результатам деятельности органов власти.

На основе полученных данных проводится постоянное изучение общественно-политической ситуации и протестной активности в других странах в сравнении с информационной повесткой российских социальных медиа.

Система используется при аналитическом сопровождении работы ситуационных центров федерального уровня в период выборов. Настройка специализированного интерфейса, содержащего информацию о текущей ситуации в социальных медиа позволяла оперативно выявлять инциденты на избирательных участках и контролировать информационное поле вокруг выборов.

Сейчас активно ведутся работы над собственными алгоритмами машинного обучения для распознавания лиц и объектов (в основном символики запрещенных на территории Российской Федерации организаций). В перспективе это должно помочь оперативно выявлять потенциальных экстремистов и террористов. Кроме того, разработка поможет искать по фото аккаунтов социальных сетей лица людей, находящихся в розыске.

Система и ее отдельные компоненты успешно эксплуатируются в государственном и корпоративном секторах. В состав системы входят зарегистрированные в Едином реестре российских программ для электронных вычислительных машин и баз данных: «Крибрум. Объекты», «Крибрум. Зеркало», «Крибрум. Сигнал», «Крибрум. Публичный поиск».

Оборудование (аппаратное обеспечение) установлено в специальном помещении, имеет резерв на случай выхода из строя одного или нескольких элементов, а также основной и резервный источники электропитания.

Процесс эксплуатации системы предусматривает резервное копирование не реже раза в сутки хранимых и обрабатываемых данных на независимые носители информации.

В МГУ благодаря системе проведена модернизация существующих программ, а также разработаны рабочие программы для новых направлений обучения, Инструменты системы знакомят студентов с возможностями и средой анализа, позволяют применять их для получения и обработки данных.

Таким образом, применение систем, осуществляющих мониторинг, сбор, обработку информационного поля социальных сетей для выявления и анализа распространения деструктивного контента становится все более важным для нужд государственного управления.

Список использованных источников:

1. Искусственный интеллект и принятие решений. 2020. Т. 5. № 3.

Шутов О. Н.¹,
*преподаватель кафедры специальных
информационных технологий
учебно-научного комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя*

ОБ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ BIG DATA В ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Под термином «Big data» (или иначе – большие данные) часто понимают огромное количество информации, хранящейся на любом носителе. В то же время, объем настолько велик, что нежелательно пытаться обрабатывать его с помощью обычного программного или аппаратного обеспечения. В отдельных случаях обработка такой информации с помощью программного или аппаратного обеспечения не представляется возможной.

Характеристики, описывающие большие данные, определяются следующим образом: «V» – volume (в переводе с англ. – объем), velocity (в переводе с англ. – скорость), variety (в переводе с англ. – разнообразие). Это основные принципы, на которых строится работа с Big data. По мере совершенствования технологии к указанным принципам стало применительно еще одно понятие – value, которое подразумевает под собой характеристику ценности информации.

Говоря иными словами, понятие «информация» должно приносить необходимую пользу, в теории и на практике. Это необходимо для того, чтобы стоимость ее хранения и обработки была бы оправдана.

Поэтому среди направлений, которые имеют значительную доказательную ценность в исследовании преступности, стоит отметить применение термина «большие данные».

Актуальность использования технологий Big data связана, в частности, с принятием Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 гг. и на перспективу до 2025 г. (распоряжение Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 – 2020 гг. и на перспективу до 2025 г.») (далее – Стратегия). Стратегия включает следующие приоритеты:

- новые системы поиска и разведки, подразумевающие установление новых решений для поиска и идентификации информации в аудио- и видеофайлах;
- анализ больших данных, которые также подразумевают использование новых методов и алгоритмов с целью сбора, хранения и проведения анализа больших объемов информации;
- новые методы хранения, обработки и передачи информации;
- развитие коммуникационных и навигационных технологий.

¹ © Шутов О. Н., 2022.

Методы обработки и анализа информации с помощью технологии Big data являются доказательством потенциала ее применения в настоящее время.

К примеру, для следователя результаты анализа являются различные данные для поиска закономерностей, подтверждающих или опровергающих его версию. Стратегия решения, основанная на получении данных оперативным путем, и получения информации, извлеченной из открытых источников, является наиболее целесообразной.

Анализ необработанных и неподготовленных данных значительно снижает качество полученных результатов.

Под влиянием цифровизации преступления в сфере компьютерной информации, в том числе формы преступлений и стратегии их организации, постоянно развиваются, что привело к появлению новых типов преступлений и методов сокрытия следов преступной деятельности.

Смещение направления деятельности от традиционных методов организованной преступности к преступлениям в сфере компьютерной информации говорит о том, что традиционные формы организованной преступности и формы киберпреступности сливаются в более опасную категорию организованной преступности, где частично подготовленный и уже интегрированный арсенал сил, средств и методов преступной деятельности вынуждает правоохранительные органы бороться с преступностью совершенно новыми способами, методами и средствами. В сегодняшних быстро меняющихся условиях этого можно достичь только путем совершенствования существующих инструментов; расширения источников оперативной информации; адаптации теоретического и практического уровня деятельности органов внутренних дел по отношению к научному и техническому мышлению; пересмотра методов организации оперативно-разыскной деятельности.

Разумеется, что реализация указанных требований по обновлению и совершенствованию оперативной деятельности неизбежно столкнется с рядом проблем и различных недостатков.

Технологические достижения, разработки и технологические решения в области информационной безопасности и телекоммуникаций являются неотъемлемым фактором, влияющим на развитие и совершенствование оперативно-разыскной деятельности в существующих реалиях. Формирование соответствующей инфраструктуры, а также предоставление высококвалифицированных экспертов, одинаково важно.

Благодаря использованию технологий Big data стало возможным прогнозирование и контроль за поведением преступной деятельности в различных сферах, которая представляет оперативный интерес. Современная аналитическая деятельность включает в себя преобразование больших данных – цифровой информации из различных источников в «оперативно значимую информацию». Используя эти данные, можно с разной степенью вероятности предсказать наступление того или иного события.

Значительно повысить эффективность борьбы с преступностью в сфере компьютерной информации в условиях массовой цифровизации во всех сферах общественной жизни может модель организации ОРД, обеспечивающая аналитическую обработку всей имеющейся и оперативно значимой информации с целью

подготовки необходимого материала для принятия решений по реализации превентивных мер в оперативно-разыскной деятельности, что позволяет повысить эффективность борьбы с преступностью в указанной сфере.

Отечественная модель системы организации оперативно-разыскной деятельности невозможна без согласованности действий, без соответствующей платформы и без необходимой инфраструктуры. По этой причине на сегодняшний день есть необходимость в изменении существующих технических ресурсов.

Очевидно, что одной из основных проблем, которая препятствует формированию новой организационной модели оперативно-разыскной деятельности, является неурегулированность правовых положений, касающихся применения технологий Big data, что приводит к наличию правовой основы для использования указанных технологий.

Применение технологий Big data в рамках любого анализа подразумевают обработку информации, содержащей персональные данные людей и граждан. Наличие этого факта подразумевает вопрос о правовом регулировании при обращении с указанной информацией.

В связи с этим важно сосредоточиться на разработке и принятии нормативно-правовых актов, направленных на «обезличивание» информации, полученной с помощью технологий Big data.

Необходимость внесения изменений в российское законодательство является серьезным фактором, влияющим на эффективность борьбы с преступностью в сфере компьютерной информации в условиях массовой цифровизации.

Развитие информационных технологий является одним из важнейших факторов, способствующих решению ключевых вопросов государственной политики в области обеспечения правопорядка, общественного порядка и общественной безопасности.

В последнее время государство приняло ряд стратегий по прогнозированию, мониторингу, предотвращению и устранению потенциальных угроз, а также контроля и устранения последствий преступности.

Список использованных источников:

1. Распоряжение Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р (ред. от 18.10.2018) «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_154161/.

2. Осипенко А. Л. Перспективы использования информационно-аналитических технологий в оперативно-розыскной деятельности // Общество и право. 2018. № 4 (66). С. 80–87.

3. Овчинский В. С. Технологии будущего против криминала. М. : Книжный мир. 2017.

4. Волеводз А. Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 17–25.

5. Прогноз научно-технологического развития Российской Федерации на период до 2030 года // Официальный сайт Правительства Российской Федерации.
URL: <http://government.ru/>

Гершкович М. А.¹,
 слушатель факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Минаев В. А.,
 профессор кафедры специальных
 информационных технологий учебно-научного
 комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,
 доктор технических наук, профессор

ОПТИМАЛЬНОЕ РАСПРЕДЕЛЕНИЕ ПОЛИЦЕЙСКИХ ПАТРУЛЬНЫХ НАРЯДОВ С УЧЕТОМ ИНФОРМАЦИИ ИЗ АНОНИМНОГО СЕГМЕНТА СЕТИ ИНТЕРНЕТ

Современные преступники все больше применяют интернет-возможности, усиленно прибегая к анонимному сектору всемирной сети. Распространение наркотиков, оружия, поддельных денежных средств, документов, практически полностью перешло в так называемый Даркнет (от англ. Darknet).

Анонимная сеть представляет возможности передачи информации через систему виртуальных туннелей, в том числе – в зашифрованном виде. В Darknet файлообмен происходит анонимно, поскольку IP-адреса недоступны в публичном пространстве. Следовательно, пользователи могут общаться, особо не опасаясь вмешательства государственных органов. Это и стало причиной того, что Даркнет сегодня воспринимается как инструмент для осуществления коммуникаций при различных подпольных отношениях и незаконной деятельности.

Очевидно, что недостаток необходимых теоретических знаний и слабая аналитическая работа могут негативно влиять на планирование и разработку методов борьбы с преступностью в данной сфере. Поэтому современные сотрудники органов внутренних дел (ОВД) все активнее прибегают к современному инструментарию, связанному с применением информационных технологий и математического моделирования [1–3].

Самым распространенным способом проникновения в теневой сегмент сети является программное обеспечение (ПО) TOR. Это инструмент для обеспечения приватности и анонимности в интернет-пространстве. Данное программное обеспечение не просто браузер, который запускается на компьютере пользователя. TOR – это огромная сеть, состоящая из тысячи компьютеров, распределенных по всему миру, которые используют одинаковое программное обеспечение

¹ © Гершкович М. А., 2022.

и подключены друг к другу. Некоторые из этих компьютеров являются узлами TOR, которые обеспечивают передачу информации внутри сети.

Данное ПО затрагивает три типа участников цепи продажи наркотиков и прочих товаров, оборот которых запрещен или ограничен. Этими лицами являются продавец, покупатель и агрегатор магазинов. Существуют также и другие звенья данной цепи, но они, как правило, используют другие программные продукты.

Покупатели получают доступ к данной торговой площадке через браузер TOR. Они приобретают любой товар только за криптовалюту, получая координаты товара. Товар может как находится в «закладке» к моменту оплаты, так и быть помещенным туда после.

Еще одним известным инструментом распространения запрещенной продукции является мессенджер Telegram, имеющий, как и TOR, удобные механизмы анонимизации. Как правило, в Telegram преобладает продажа наркотических веществ.

Первое, что нужно знать о Telegram: в используемых «облачных» чатах не применяется сквозное шифрование, когда сообщения шифруются на своем устройстве, а расшифровываются только на устройстве собеседника, т. е. весь путь от отправителя до получателя сообщение преодолевает в зашифрованном виде.

Данный тип защиты активно используются в специальных «секретных» чатах Telegram, в которых можно передавать и текстовую информацию, и мультимедиа, но ключи шифрования имеют только собеседники. При этом все данные, передаваемые в чатах, хранятся на устройствах пользователей, а не на серверах Telegram.

Именно такой метод общения используется для взаимодействия продавцов наркотических средств, наркокурьеров и «спортиков». Принцип работы данных субъектов наркобизнеса достаточно прост. Продавцы запрашивают личные данные потенциального курьера. Обычно это фото с паспортом и высылают координаты «закладки» с небольшим объемом запрещенных наркотических веществ. Задача «кладмена» заключается в распределении товара на более мелкие дозы по различным районам города. С увеличением доверия растет и объем товара, доверенного курьеру. Если данная цепочка перестает функционировать из-за невыполнения своих обязанностей «закладчиком», в работу включается третий элемент цепи – «спорттики» (спортсмены). Их функции заключаются в поиске обманувшего магазин и нанесении ему различного рода ущерба, а также взыскания компенсации за потерянную прибыль.

Современные методы борьбы с распространением запрещенных товаров путем «закладок».

Неотъемлемый атрибут «кладмена» – мобильный телефон. Даже при отключенном GPS-модуле или использовании старого телефона, правоохранительные органы могут применить метод триангуляции, в соответствии с которым возможные координаты закладок сопоставляются с данными нескольких базовых станций мобильной связи. Это позволяет вычислять закладчиков даже при включении «самолетного режима» или полном отключении гаджета

Если включены данные о местоположении («закладчик» отправляет координаты заказчику, применяя GPS-модуль), тогда его поиск и поимка – дело техники. Пока такие методы используются лишь при интенсивной наркоторговле в определенных районах.

Нужно также учитывать, что магазины специально «сливают» своих работников, чтобы не выплачивать им «заработанные» средства. При этом нехватки в новых «кадрах» они не испытывают, когда у наркокурьера накапливается серьезная сумма, его попросту «сдают» оперативникам.

Существуют и иные способы поиска наркокурьеров. Одним из распространенных способов пресечения их деятельности является патрулирование территорий полицейскими нарядами, а также рейды подразделений МВД по «зачным местам» и каждодневная работа оперативников.

К сожалению, наряду с совершенствованием технологий борьбы с преступностью, развиваются и методы противодействия правоохранителям. Один характерный пример. На запрещенных маркетплейсах уже продаются специальные методические рекомендации для работы анонимных курьеров (рис. 1) [4].

В указанных рекомендациях учат удалять метаданные с отправляемых фотографий, правильно подбирать одежду, чтобы не попадаться в записи камер видеонаблюдения, а также другим методам сокрытия своей преступной деятельности.

В настоящей статье рассмотрим в качестве перспективного метода разработку оптимальных маршрутов полицейских патрульных нарядов с целью максимизации эффекта их деятельности в борьбе с распространением запрещенных товаров. Улучшение таких методов борьбы с преступностью требуют детальных знаний об анонимном сегменте интернета, а также достаточно высокого уровня аналитической работы с получаемой оттуда информацией.

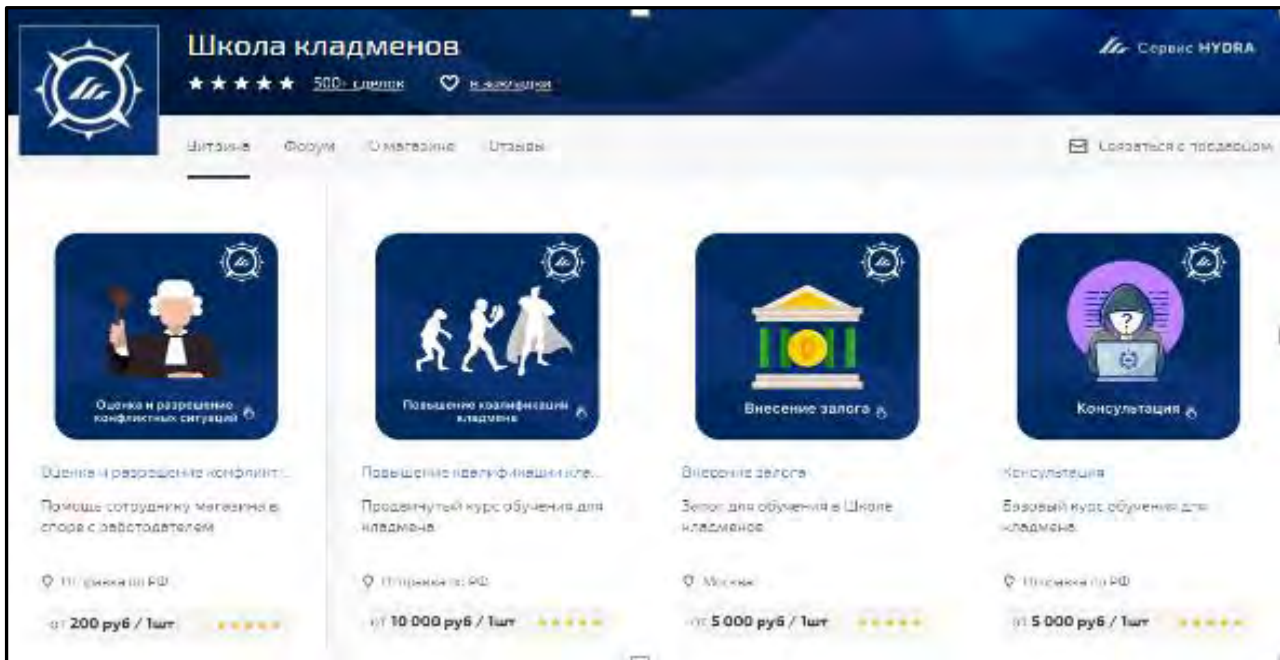


Рис. 1. Фрагмент из методички «Школа кладменов»

Моделирование маршрутов полицейских патрульных нарядов. Работа по моделированию маршрутов патрульных полицейских нарядов должна базироваться

на сборе актуальной информации о распространении запрещенных товаров по районам города, проведении аналитической работы по выявлению наиболее уязвимых в этом отношении мест и применению современных методов анализа данных.

Для выявления наиболее «зараженных» мест исследуемого района города получена информация с портала открытых данных г. Москвы [5], предоставляющего возможность получить координаты расположения камер видеонаблюдения на домах и подъездах, а также данные о расположении подразделений органов внутренних дел. Необходимо отметить, что более лучшее обеспечение процесса моделирования может быть реализовано с применением данных о камерах АПК «Безопасный город».

Конечно, важным ресурсом для сбора информации является анонимный сегмент сети Интернет. В частности, сайт safeklad.com, а также торговые площадки, доступные в TOR.

Safeklad.com является географической картой, на которой делаются отметки о расположениях патрульных нарядов полиции, камерах видеонаблюдения и полицейских рейдах. Это позволяет курьерам запрещенных веществ во многих случаях избегать сотрудников полиции при осуществлении своей преступной деятельности. Однако данную информацию можно использовать и для корректировки маршрутов патрульных полицейских нарядов.

Торговые площадки в сети TOR, как правило, позволяют покупателям получать информацию о количестве запрещенных предметов и веществ в конкретном районе города. Такие данные позволяют составить актуальную аналитическую картину об интенсивности торговли запрещенными товарами в конкретном районе.

Для сбора данных, их фильтрации и последующего расчета маршрутов использовались инструменты QGIS [6] и Яндекс.Конструктор [7]. QGIS – это географическая информационная система с открытым кодом, позволяющая визуализировать данные с портала открытых данных, а также производить сортировку геометок в нужном районе. При необходимости можно использовать встраиваемую карту с помощью сервиса OpenStreetMap. Это веб-картографический проект по созданию подробной географической карты. Данный сервис легко подключается в QGIS (рис. 2).

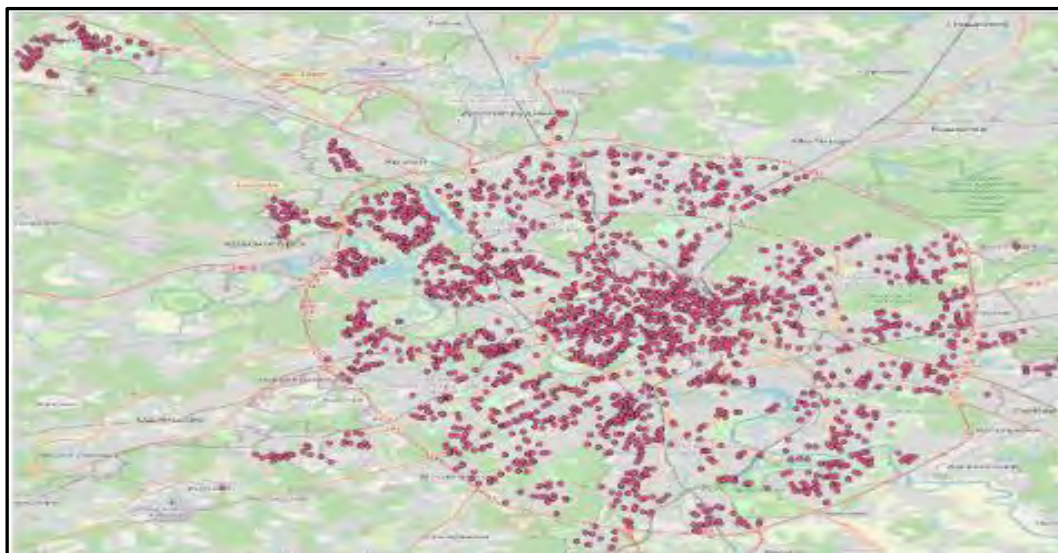


Рис. 2. Демонстрация выгруженных данных в QGIS с OpenStreetMap

Далее отфильтровывались нужные данные по нужному району со всеми геометками (рис. 3).



Рис. 3. Карта после фильтрации

Отметим, что в данной программе карта недостаточно хорошо отрисована. Среди инструментов программы нет алгоритма, позволяющего строить оптимальные маршруты на территории обслуживания.

Решением указанных проблем может выступить конструктор карт от компании Яндекс. Конструктор позволяет создать карту онлайн без навыков программирования. На ней можно отметить нужные объекты, нарисовать схему проезда. Готовую карту можно использовать оффлайн, обезопасив данные от утечки.

После выгрузки геоданных с QGIS по нужному району, необходимо перенести геометки с сайта safeclad.com на подготовленную карту для анализа мест района, где наиболее часто производятся закладки запрещенных объектов (рис. 5).

Следующий этап заключается в поиске основных мест для закладывания наркотических средств [8]. Для этого можно воспользоваться инструментом выделения областей на карте. Как правило, наиболее уязвимыми являются зеленые

зоны и дворы. Большие проезжие части и огражденные территории не являются территориями для закладок (рис. 6).

Заключительным этапом является построение оптимальных маршрутов патрулирования, охватывающих уязвимые зоны. Количество маршрутов зависит от наличных сил и средств подразделений ОВД.

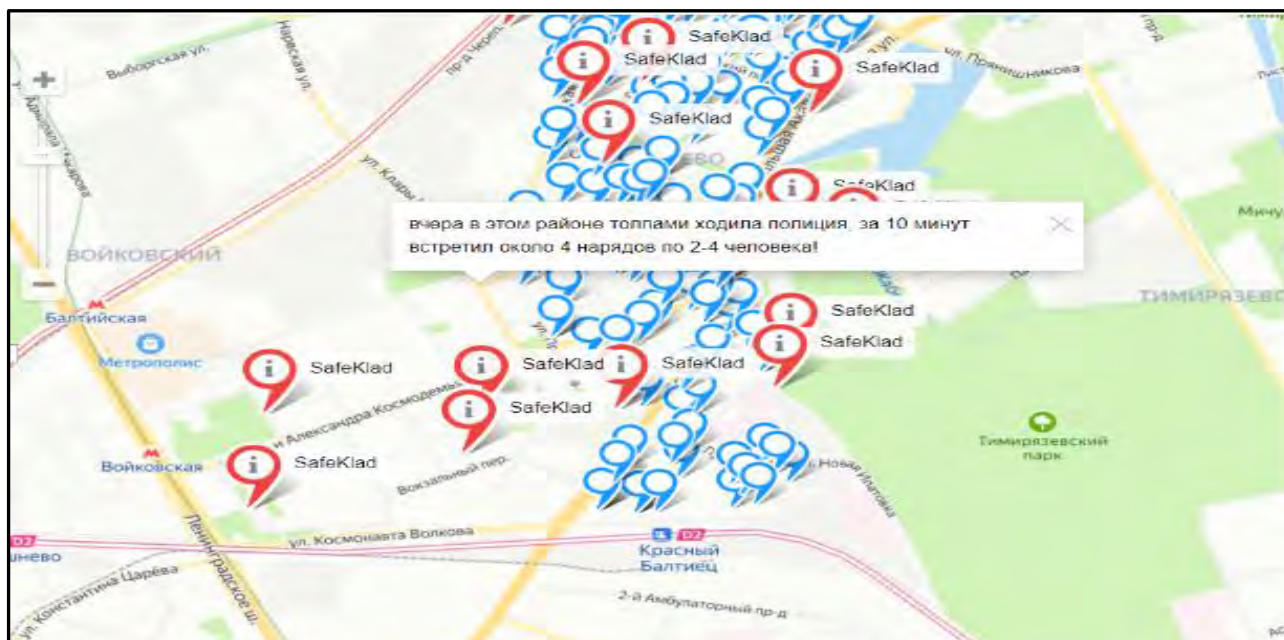


Рис. 5. Готовая карта с геометками



Рис. 6. Уязвимые места района

Используя встроенную функцию оптимизации, сокращены пути патрулирования и время прибытия в нужные точки маршрута без потери качества работы патрульных. Данный алгоритм учитывает загруженность маршрута и различные дорожно-транспортные происшествия на дорогах в реальном времени, что позволяет

добиться эффективной оптимизации в любой период времени. В данной статье оптимизация привела к снижению проезда по ненужным маршрутам на 23 %.

В заключении отметим, что современная модель противодействия преступности связана с использованием высокотехнологичных инструментов анализа, прогнозирования, управления ресурсами полицейских подразделений. Необходимость в них связана с появлением специальных школ обучения криминальному ремеслу, методических материалов, упрощающих криминальную деятельность, незаконных торговых площадок по продаже наркотиков и других запрещенных товаров. Более того, крупные криминальные структуры уже имеют собственные силы и средства обеспечения кибербезопасности.

Данная ситуация делает комплексный научный подход важнейшим средством при организации борьбы с новыми видами преступной деятельности, связанными с использованием современных информационных технологий и математических методов. В частности, выявление и картографирование на их основе криминальных зон на территории обслуживания дает возможность установить за ними особый контроль и построить оптимальные маршруты патрулирования.

Список использованных источников:

1. Пьянков О. В., Романов М. С. Оптимизация процессов принятия решений в ситуационных центрах органов внутренних дел // Вестник Воронежского института МВД России. 2014. № 1. С. 120–129.
2. Котиков Ю. Г. Геоинформационные системы : учебное пособие. СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2016. 224 с.
3. Yamuna S., Bhuvaneswari N. S. Datamining Techniques to Analyze and Predict Crimes // The International Journal of Engineering and Science. 2012. Vol. 1. Issue 2. P. 243–247.
4. Библия кладмена // Сайт «Telegra.ph». URL: <https://telegra.ph/BIBLIYA-KLADMENA-06-30-6>.
5. Портал открытых данных Правительства Москвы // Официальный сайт Правительства Москвы. URL: <https://www.data.mos.ru/>
6. Свободная географическая информационная система с открытым кодом // Сайт «QGIS». URL: <https://qgis.org/en/site/>.
7. Конструктор карт Яндекса // Сайт «Yandex». URL: <https://yandex.ru/map-constructor/>.
8. Кладмен не пройдет. Как защитить парадные от вторжения // Сайт «Fontanka». URL: <https://www.fontanka.ru/2021/05/07/69904373/>.

Осипова А. А.¹,
 слушатель факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя,

Научный руководитель:
Шутов О. Н.,
 преподаватель кафедры специальных
 информационных технологий
 учебно-научного комплекса информационных
 технологий Московского университета
 МВД России имени В.Я. Кикотя

СПЕЦИФИКА РАСПОЗНАВАНИЯ НЕДОСТОВЕРНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Наблюдая за собой, другими людьми и обществом в целом, можно заметить одно сходство – это использование социальных сетей в повседневной жизни. По статистике агентства «We Are Social» и платформы для SMM «Hootsuite» население России на 2022 г. составляет около 145,9 млн человек, из которых 106,0 млн человек пользуются социальными сетями, что составляет 72,7 %.

Социальные сети – это онлайн-платформы, созданные для объединения людей для общения, обмена идеями и интересами или завести новых друзей. Так как социальных сетей очень много, их можно разделить на следующие группы:

- 1) общение (ВКонтакте, Facebook (принадлежит компании Meta, признанной экстремистской в Российской Федерации), Одноклассники, LinkedIn и др.);
- 2) отзывы и рецензии (TripAdvisor, Foursquare, Отзовик и др.);
- 3) коллективные обсуждения (Quora, 4PDA, Ответы Mail.ru и др.);
- 4) обмен контентом (TikTok, YouTube, Instagram (принадлежит компании Meta, признанной экстремистской в Российской Федерации) и др.);
- 5) мессенджеры (Telegram, WhatsApp, Viber и др.);
- 6) авторские записей (Blogger, Tumblr и др.) [1].

Однако в настоящее время в социальных сетях и за их пределами критически важной проблемой является недостоверная информация (дезинформация или фейк), обычно определяемая как «преднамеренное создание и распространение ложной и/или искаженной информации, которая предназначена для обмана и введения аудитории в заблуждение либо с целью причинения вреда, либо для политической, личной или финансовой выгоды». А дезинформация в сфере политики характеризуется как значительная угроза демократии, являясь частью более широкого спектра информационных операций, проводимых правительствами и другими организациями. Предполагаемые последствия включают политическое влияние, усиление групповой поляризации, снижение доверия

¹ © Осипова А. А., 2022.

и в целом подрыв гражданского общества. Последствия не ограничиваются онлайн-процессами. Они регулярно распространяются на другие сферы повседневной жизни.

Недостоверная информация в социальных сетях очень широко используется в качестве инструмента влияния: компьютерная пропаганда была описана как всепроникающая и повсеместная часть современной повседневной жизни. Есть множество реальных примеров, показывающие как ее воздействие может привести к общественному резонансу:

Пример № 1: Президент Украины, приказывающий сдаться войскам. В марте в социальных сетях начали появляться видео, на котором Владимир Зеленский приказывает властям сдаться. Хакеры взломали телеканал «Украина 24» и выложили такой же видеоролик туда, но фейк быстро был разоблачен, когда Зеленский выложил опровержение на странице социальной сети Facebook (принадлежит компании Meta, признанной экстремистской в Российской Федерации).

Пример № 2: Президент Габона и военный переворот. В Габоне дипфейк с речью Президента вызвал военный переворот. Переворот предотвратили. Видеоролику предшествовали слухи о болезни президента. Следует отметить, что на дипфейке президент выглядел неестественно, тем самым могло послужить слухам о его плохом самочувствии.

Пример № 3: Сбор гуманитарной помощи в соцсетях. Первыми с этим столкнулись в Курской области, где в местных сообществах социальной сети Instagram (принадлежит компании Meta, признанной экстремистской в Российской Федерации) появились посты сбора материальной помощи российским солдатам. Однако Дом Советов опроверг данную информацию и добавил, что военнослужащие обеспечены всем необходимым.

После того, как дезинформация изначально была посеяна в интернете ее создателями, одним из способов распространения являются действия отдельных пользователей социальных сетей. Например, пользователь поставил «лайк» на запись, прокомментировал и/или поделился ею, срабатывают алгоритмы платформ социальных сетей для отображения его другим пользователям. И как видно из приведенных примеров, последствия могут обернуться в борьбу, которая могла не произойти. Из этого следует, что для предотвращения нежелательных конфликтов, необходимо распознавать недостоверную информацию.

Рассмотрим несколько способов распознавания фейковой информации, размещенных в социальных сетях:

1. Социальные сети в помощь. Одни сообщества и каналы созданы для распространения фейков, другие же для их разоблачения. Так, например, в мессенджере Telegram есть каналы, направленные на разоблачение фейков как в интернете, так и в социальных сетях. Например, телекомпания «Первый канал» создал телеграмм-канал «Война с фейками», который направлен на разоблачение дезинформации и доведение до пользователей объективных публикаций.

Также популярностью пользуются телеграмм-каналы «АнтиФейк Основа» (@antifakeosnova) и «АнтиФейк» (@anti_fake_channel).

Следующими примерами являются сообщества телекомпаний «РЕН ТВ» и «Пятый канал» социальной сети «ВКонтакте», которые публикуют информацию о распространении ложных сведений с целью предотвращения обмана людей.

Список сообществ намного больше («РИА Новости», «Новости Первого канала», «Рамблер Новости» и т. д.) и не только в приведенных социальных сетях. Все официальные компании в сфере средств массовой информации (далее – СМИ) усиленно занимаются предотвращением ложной информации и доведением до общества достоверных данных в эфирах, своих сайтах и онлайн-платформах.

2. Изучение и следование рекомендациям профильных компаний. В данном случае, можно рассмотреть статью Лабораторию Касперского, в которой дается подробное описание фейковой информации, а также приводится алгоритм для их распознавания. Алгоритм включает в себя проверку источника и сравнение с иными источниками, критическое мышление, оценку своих убеждений и комментариев других людей, проверку других фактических данных и подлинности фотографий и/или видео.

3. Проведение научных исследований и разработки, направленные не только на выявление источников дезинформации, но и борьбы с ними. К примеру, ученые М. Aldwairi и А. Alwahedi из Южной Каролины предлагают использование инструмента [7], который может идентифицировать и удалить поддельные сайты из результатов, предоставляемых пользователю поисковой системой или новостной лентой социальных сетей. Инструмент может загружаться пользователем и впоследствии добавляется в браузер или приложение, используемое для получения электронных новостных лент.

Следующим примером является разработка ученых Национального исследовательского университета «Высшей школы экономики» О. Кольцовой, Я. Синявской, и М. А. Терпиловского – эксперимент по выявлению фейковых новостей пользователями социальных сетей, где при проведении исследования выделяются факторы, по которым можно их распознать [4].

Последним примером будет исследования нескольких ученых, а именно: М. Goksu, N. Cavus [5], K. Shu, A. Sliva, S. Wang, J. Tang, H. Liu [8], О. Соколова, А.В. [9] Власенко, П.С. Киселев, Е.А. Склярова [6] и др., которые изучали способ распознавания недостоверных данных с помощью инструментария искусственного интеллекта.

Наличие недостоверной информации в социальных сетях является большой проблемой, так как несет за собой неприятные последствия. С их помощью распространители обманывают и «вертят» людьми для достижения своих целей. Однако в настоящее время уже существуют и разрабатываются новые способы их выявления и борьбы с дезинформацией и их источниками.

Список использованных источников:

1. Огнева А. С. Социальные сети: понятие, виды, технологические возможности продвижения // Молодой ученый. 2021. № 9 (351). С. 75–79.
2. Buchanan T. Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation // Plos One. 2020. № 15 (10). С. 1–33.
3. Демичева К. А. Понятие и классификация социальных сетей в контексте взаимодействия в сети Интернет // International scientific review. 2015. №3 (4).
4. Кольцова О., Синявская Я., Терпиловский М. Разработка эксперимента по распознаванию пользователями социальных сетей политических фейковых новостей: факторы отсева // Международная конференция по взаимодействию человека и компьютера. НСИ 2020: Социальные вычисления и социальные медиа. Дизайн, этика, поведение пользователей и анализ социальных сетей. СПб. : Springer, 2020. С. 261–277.
5. Goksu M., Cavus N. Fake News Detection on Social Networks with Artificial Intelligence Tools: Systematic Literature Review // 10th International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions. ICSCCW-2019. Springer, 2019. С. 47–53.
6. Василькова В. В., Садчиков Д. И. Фейки и боты как механизмы информационных искажений в социальных сетях // Казанский социально-гуманитарный вестник. 2019. № 2 (37). С. 24–30.
7. Aldwairi M., Alwahedi A. Detecting Fake News in Social Media Networks // The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2018). Abu Dhabi : ScienceDirect, 2018. С. 215–222.
8. Fake News Detection on Social Media: A Data Mining Perspective // Site «ArXiv». URL: <https://arxiv.org/abs/1708.01967>.
9. ИИ vs тролли: нейроаудит соцсетей, SERM-системы и распознавание фейков // Сайт «Хайтек». URL: <https://hightech.fm/2021/04/20/ai-negative-social-media>.
10. The global state of digital // Сайт «We Are Social». URL: <https://wearesocial.com/uk/blog/2022/07/the-global-state-of-digital-in-july-2022/>.
11. Как распознать фейковые новости // Сайт «Kaspersky». URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/how-to-identify-fake-news>.
12. Подробный каталог социальных сетей // Сайт «Selection». URL: <https://infoselection.ru/infokatalog/obshchenie-i-znakomstva/sotsialnye-seti/item/54-podrobnyj-katalog-sotsialnykh-setej#s1>.

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

Пименова О. В.²,
*доцент кафедры информационной
безопасности учебно-научного
комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук*

ИННОВАЦИОННЫЕ ИНСТРУМЕНТЫ ФРОД-МОНИТОРИНГА В ПРАКТИКЕ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

В статье рассматривается необходимость применения фрод-мониторинга в информационных системах МВД России с целью повышения уровня их защищенности. Антифрод-системы давно и достаточно успешно используются в банковской сфере для противодействия мошенничеству и краже конфиденциальной информации. При определенных настройках антифрод-система позволила бы оперативно выявлять факты незаконных выгрузок данных из информационных систем и использования сотрудниками чужих учетных данных для доступа к информационным ресурсам.

В современном мире, когда цифровизация прочно вошла в нашу повседневную жизнь, наиболее актуальным вопросом становится противодействие преступным посягательствам, совершаемым с использованием современных информационных технологий. Наиболее уязвимой стала система банковского обслуживания. Именно операции с банковскими картами больше всего подвержены риску мошенничества, так как эти операции осуществляются дистанционно, а в некоторых ситуациях даже при отсутствии карты владельца можно совершить любую транзакцию. В целях борьбы с мошенничеством кредитными организациями активно внедряются и антифрод-системы. Инструмент фрод-мониторинга является важнейшим способом для выявления мошенничества в сфере банковской деятельности. Важно обратить внимание, что инструменты фрод-мониторинга в режиме реального времени помогают своевременно реагировать и предотвращать преступность.

Обратимся к определению фрод-мониторинга. Антифрод или фрод-мониторинг – система, предназначенная для проверки операций, связанных с финансами или не финансами, по определенным критериям на подозрительность

¹ © Соколова Я. С., 2022.

² © Пименова О. В., 2022.

с точки зрения мошенничества и предотвращающая их. Также эта система предлагает рекомендации по дальнейшей обработке подозрительной операции. В 2011–2012 гг. антифрод системы стали активно применяться российскими банками. Это произошло вследствие первых крупномасштабных кибератак на системы дистанционного банковского обслуживания. Система фрод-мониторинга и их механизмы нашли свое применение и в других сферах.

Принцип работы этой системы заключается в следующем. При не соответствии какой-либо банковской или онлайн операции критериям осуществляется более тщательная проверка, вследствие чего принимается решение о разрешении или блокировке транзакции.

Существуют два типа антифрод систем: транзакционный, связанный с банковскими или онлайн операциями, и сессионный. Сессионный фрод-мониторинг обеспечивает отслеживание определенных параметров сессии пользователя и определяет подозрительную деятельность мошенников на сервисе. Сессионная антифрод система собирает общие данные о пользователе, его устройстве, окружении, поведении с цифровых каналов в рамках сессии и формирует индивидуальный профиль каждого пользователя на основе искусственного интеллекта, т. е. машинного обучения. Анализ основывается на детальном разборе данных, которые изменялись в рамках конкретного временного интервала, а именно в прошлых сессиях пользователя. Главная задача сессионной антифрод системы – выявить нетипичное, аномальное, подозрительное поведение пользователя на протяжении сессии, основываясь на различных признаках.

Данная система, благодаря машинному обучению, способна в режиме реального времени, для выявления мошенничества, анализировать большое количество параметров. Для повышения показателей точности и полноты обнаружения аномалий антифрод формирует глобальные профили пользователей. Сессионный антифрод используется в следующих направлениях:

1. Для предотвращения краж аккаунтов пользователей: система отслеживает неправомерные попытки входа по определенным факторам, которые присущи мошеннической авторизации, или отклонения от типичного поведения клиентов.
2. Для обнаружения учетных записей, принадлежащих мошенникам: выявляет использование большого количества аккаунтов с одного устройства, а также различные авторизации, которые осуществляются через устройства с плохой репутацией.
3. Для улучшения UX: упрощает осуществление законной авторизации пользователей с помощью технологии RBA.
4. Для защиты от бот-атак: система позволяет выявлять ботов и блокировать их активность.

За кажущейся простотой понимания процесса системы фрод-мониторинга стоит сложнейшая работа, которая связана с разработкой точечных индикаторов и сигналов, дающих возможность предвидеть наступление рисков.

Вместе с тем фрод-мониторинг возможно использовать и в других сферах. Например, в целях исключения фактов неправомерного доступа пользователей к данным, содержащимся в информационной системе.

Так, применение фрод-мониторинга в информационных системах МВД России, в которых содержится огромное количество персональных данных, позволило бы повысить уровень их защищенности. При определенных настройках антифрод-система оповещала администратора безопасности системы или даже блокировала действия пользователей, которые носят нетипичный для повседневной деятельности характер. Применение фрод-мониторинга позволило бы оперативно выявлять факты незаконных выгрузок данных из информационных систем, использования сотрудниками чужих учетных данных для доступа к информационным ресурсам, неправомерного доступа к информации.

Список использованных источников:

1. Разина О. М., Костерина Т. М. Инновационные инструменты фрод-мониторинга в практике внутреннего аудита банка // Вопросы инновационной экономики. 2015. № 5 (4). С. 253–266.
2. Божор Ю. А. Необходимость создания в России федеральной системы фрод-мониторинга // Расчеты и операционная работа в коммерческом банке. 2013. № 6. С. 80–87.
3. Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response // KPMG International, 2006.

Булгаков В. Г.¹,
заместитель начальника кафедры
естественнонаучных дисциплин
учебно-научного комплекса информационных
технологий Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук, доцент

ИСПОЛЬЗОВАНИЕ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

В качестве одного из действенных инструментов повышения эффективности деятельности правоохранительных органов можно рассматривать современные информационные системы, содержащие биометрическую информацию, средства видеонаблюдения и видеофиксации правонарушений, совмещенные с системами видеоаналитики и биометрического розыска.

Биометрическая информация содержится в биометрических персональных данных, ряд которых уже давно собирается, хранится и используется в криминалистических регистрационных системах (например, дактилоскопическая информация, фотоизображения лиц), а для некоторых, еще только создаются информационные системы (изображение радужной оболочки глаза, походка и др.).

Под биометрическими персональными данными понимают сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (ст. 11 Федерального закона «О персональных данных») [1].

В настоящее время правоохранительный сегмент аппаратно-программного комплекса «Безопасный город» установлен практически во всех крупных городах России и активно развивается. Данный АПК представляет собой комплекс средств видеонаблюдения, фото- и видеофиксации нарушений правил дорожного движения, преступлений, административных правонарушений и происшествий, а также технических средств для обеспечения экстренной связи граждан с дежурными частями территориальных органов МВД России [2].

Активное использование биометрической информации создает новые уникальные возможности для правоохранительных органов в решении задач выявления, раскрытия и расследования преступлений. В частности, использование видеоаналитики [3] в интеллектуальных системах видеонаблюдения позволяет осуществлять автоматическое обнаружение, распознавание, подсчет и отслеживание объектов на видеоизображении [4].

Накопление значительных по объему информации баз данных, содержащих биометрические данные людей, создает условия для более эффективного использования их для розыска лиц. Системы распознавания лиц уже используются правоохранительными органами на протяжении несколько лет. Кроме распознава-

¹ © Булгаков В. Г., 2022.

ния человека по лицу, сегодня уже имеются технологии бесконтактной идентификации человека по биометрическим параметрам в движении, что очень важно для приложения в сфере правоохранительной деятельности. Разработаны методические основы решения диагностических и идентификационных задач при криминалистическом исследовании динамических признаков человека (походки, артикуляции, мимики, жестикуляции человека) [5].

Следует обратиться к положительному опыту КНДР в направлении использования ситуационных центров и системы распознавания лиц «SkyNet» для розыска пропавших без вести лиц и преступников в условиях мегаполисов с разветвленной системой видеонаблюдения. «SkyNet» может сканировать лица и сравнивать их с базой подозреваемых в совершении преступлений со скоростью 3 млрд человек в секунду [6].

Безусловно, создание и использование подобных систем при решении задач раскрытия и расследования преступлений будет возможным только на базе современных информационно-коммуникационных технологий, использующих надежные сети передачи информации, обеспечивая высокую степень ее защиты от несанкционированного доступа и взлома [7].

Внедрение в практическую деятельность органов внутренних дел России информационных и управленческих технологий: телекоммуникационных технологий, коллективного отображения информации, информационно-аналитических систем и расширения практики использования коллективных форм управления на основе ситуационных центров [8], будет также способствовать более рациональному распределению сил и средств при решении практических задач в ходе раскрытия и расследования преступлений.

Дальнейшая адаптация таких систем к решению практических задач в рамках правоохранительной деятельности потребует:

- создания единой биометрической системы криминалистической регистрации в интересах всех правоохранительных органов, в которой будет содержаться интегрированная информация о всех биометрических параметрах подучетных лиц [9]; При этом необходимо отметить, что данная информационная система должна интегрировать все значимые биометрические характеристики подучетных лиц, доступные для получения. В настоящее время стало возможным на основе технологий больших данных получить корреляционные связи между различными биометрическими характеристиками человека. Хотя и ранее высказывались учеными такие идеи, но реализация их была не возможна без цифровизации соответствующих сфер деятельности человека. Аналогично и с криминалистической характеристикой, которая сейчас может быть более эффективным инструментом раскрытия и расследования преступлений, при использовании технологий анализа больших данных [10];

- разработки теоретических и методических основ использования видеоаналитики для решения идентификационных задач как по статическим биометрическим параметрам, так и по динамическим. Использование интеллектуальной функции отслеживания (треккинга) передвижения человека по изображению

лица и другим биометрическим параметрам, в том числе, создание мультибиометрических систем, использующих комплекс из нескольких биометрических характеристик;

– разработки теоретических и методических основ использования видеоаналитики для решения диагностических задач по распознавание подозрительной деятельности (активности) человека.

Внедрение в практику органов внутренних дел современных информационных технологий, основанных на использовании биометрии человека, видеоаналитики, технологий обработки больших данных позволит значительно повысить эффективность деятельности по раскрытию и расследованию преступлений.

Список использованных источников:

1. Распоряжение Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р (ред. от 05.04.2019) «Об утверждении Концепции построения и развития аппаратно-программного комплекса «Безопасный город» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_172077/4ff-ea2b90b5bab278aea41a0808edb7fb67f43c9/.
2. «Безопасный город»: силовой сегмент // Сайт «RuБез». URL: <https://ru-bezh.ru/journal-23/18522-bezopasnyij-gorod-silovoj-segment>.
3. Пескин А. Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации. М. : Горячая линия – Телеком, 2017. С. 82–85.
4. Аппаратно-программная технология видеоаналитики // Сайт «Взор-центр». URL: <https://vzor.center/articles/videoanalitika>.
5. Булгаков В. Г. Методические основы криминалистической идентификации и диагностики человека по его динамическим признакам : монография / под ред. А. М. Зинина. М. : Юрлитинформ, 2014. 144 с.
6. Китай запустил систему распознавания «Skynet», которая может сравнивать 3 млрд лиц в секунду // Сайт «Inosmi». URL: <https://inosmi.by/2018/04/10/kitaj-zapuskaet-sistemu-raspoznavaniya-lic-skynet-kotoraya-mozhet-sravniyat-3-milliarda-lic-v-sekundu/>.
7. Колотушкин С. М., Лосева С. Н. Информационно-коммуникационные основы формирования баз данных личности человека по его биометрическим параметрам // Материалы межвузовской научно-практической конференции, посвященной памяти заслуженного деятеля науки РСФСР доктора юридических наук, профессора А. И. Зубкова и Дню российской науки : Организационно-правовое регулирование деятельности уголовно-исполнительной системы: теоретические и прикладные аспекты. Рязань : Академия права и управления ФСИН России. 2018. С. 113–117.
8. Лукашов Н. В. Инновационные технологии оперативного управления в органах внутренних дел России // Труды академии управления МВД России. 2015. № 3 (35). С. 129–135.
9. Булгаков В. Г., Барковская Е. Г. Отражение концепции биометрии человека в системе криминалистической регистрации // Вестник Волгоградской академии МВД России. 2009. № 1(8). С. 32–37.

10. Big data in investigating and preventing crimes / [E. V. Bulgakova and other] // Studies in Systems, Decision and Control. 2019. T. 181. P. 61–69.

Григорькин А. А.¹,
старший преподаватель кафедры
естественнонаучных дисциплин
учебно-научного комплекса
информационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат физико-математических наук

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ЯДЕРНОГО МАГНИТНОГО РЕЗОНАНСА ДЛЯ ХИМИЧЕСКОГО И ФИЗИЧЕСКОГО АНАЛИЗА ВЕЩЕСТВ

1. Физические основы метода ЯМР.

Методы ЯМР спектроскопии уже более полувека активно применяются в физических, химических и биологических исследованиях. Суть метода можно понять из классической аналогии - поведения стрелки компаса в магнитном поле. Как известно, стрелка стремится ориентироваться вдоль поля. При попытке вывести стрелку из этого устойчивого положения, она начинает колебаться с частотой, пропорциональной величине поля и собственному магнитному моменту. Как известно, почти все элементарные частицы обладают собственными механическими моментами (спинами) s и связанными с ними магнитными моментами m . Соответственно, в магнитном поле их поведение оказывается схожим с классическим магнитом, т. е. в магнитном поле с индукцией B они совершают колебания (прецессируют) с частотой $\omega = \gamma B$ (1), где γ – гиромагнитное отношение частицы. Собственно, наблюдение ЯМР основано на том, что ускоренно движущиеся с частотой (1) элементарные магнитные моменты ядер излучают электромагнитные волны, которые детектируются катушкой индуктивности.

Первым необходимым условием для наблюдения ЯМР является само существование ядерного магнитного момента. Хотя все ядра состоят из протонов и нейтронов, имеющих спины $s=1/2$, магнитными свойствами обладают не все элементы. В так называемых четно-четных ядрах, состоящих из четного числа протонов и нейтронов (например, ^{12}C , ^{16}O , ^{32}S), спины их внутриядерными силами ориентированы так, что суммарный момент ядра равен нулю. Такие ядра для ЯМР непригодны. Удобнее всего получать ЯМР отклик от ядер, основные изотопы которых являются нечетными (^1H , ^{19}F).

Вторым условием наблюдения является согласованность сигналов ЯМР от разных частей образца. Обычно, в веществе ядерные моменты разупорядочены (рис. 1). Соответственно, излучаемые ими волны со случайными начальными фазами в сумме дадут величину, близкую к нулю. Для получения четкого детектируемого сигнала необходимо произвести поляризацию вещества, в ходе которой магнитные моменты упорядочиваются,

¹ © Григорькин А. А., 2022.

складываясь в намагниченность вещества M . Обычно для этого используют сильное внешнее магнитное поле (рис. 1).

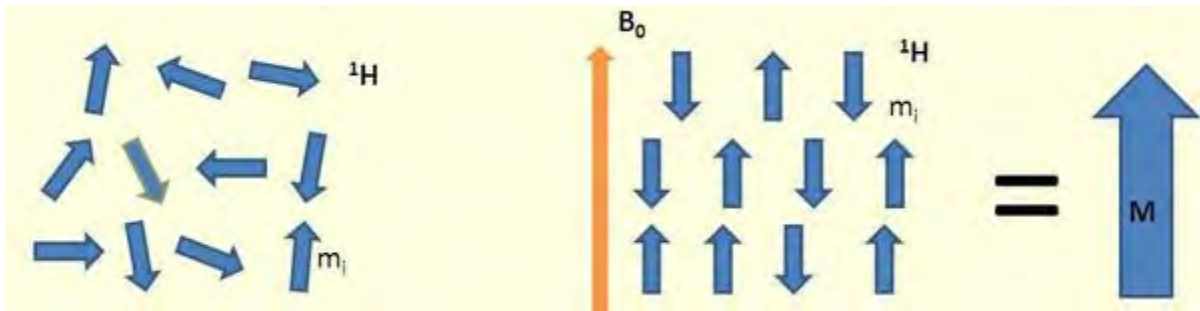


Рис. 1. Поляризация ядерных спинов внешним магнитным полем B_0

Расположенный вдоль поля вектор M не прецессирует. Для получения сигнала используют катушку индуктивности, радиочастотный импульс которой разворачивает M на 90° относительно внешнего поля (рис. 2). Повернутая намагниченность будет прецессировать вокруг поля, излучая электромагнитные волны с частотой (1) (рис. 2).

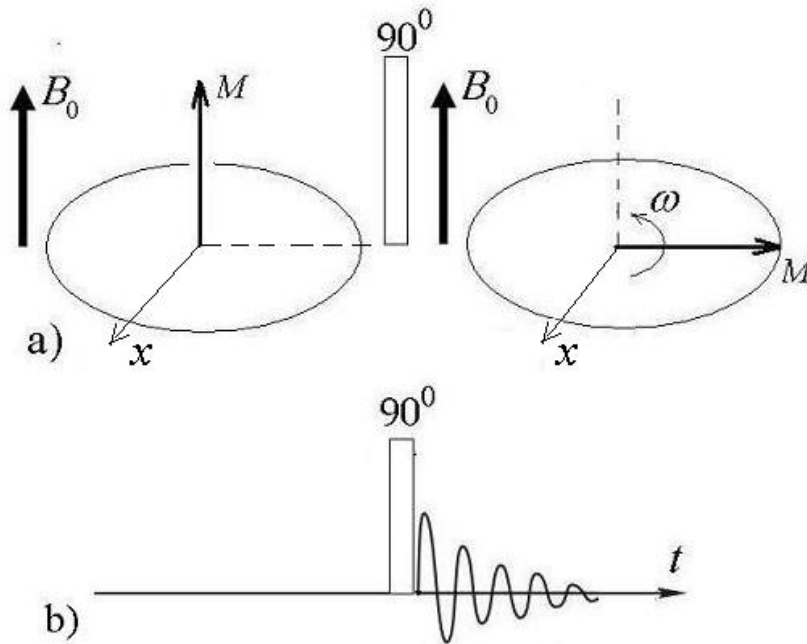


Рис. 2. а) предварительная поляризация ядерных спинов внешним магнитным полем B_0 и поворот намагниченности M вокруг оси x радиочастотным 90° импульсом; б) сигнал свободной прецессии намагниченности вокруг B_0

Регистрируемый сигнал прецессии постепенно экспоненциально затухает со временем из-за спин-спиновых и спин-решеточных взаимодействий. Характерное время разрушения поперечной намагниченности называют временем релаксации T_2 , а время прихода продольной относительно поля компоненты намагниченности в равновесное состояние – T_1 . Для максимизации сигнала исследуемый образец обычно помещают непосредственно внутрь катушки индуктивности (рис. 3) и регистрируют индуцированный в ней ток.

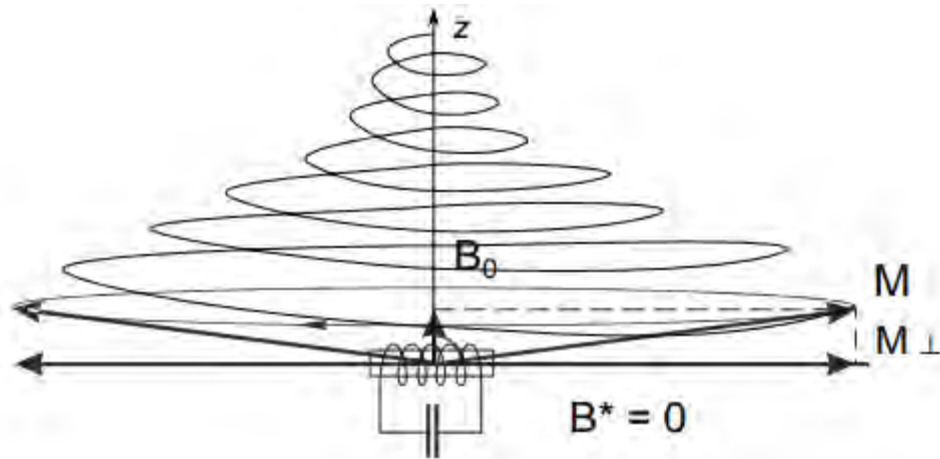


Рис. 3. Изменения продольной и поперечной намагниченностей образца в ходе свободной прецессии вокруг B_0

Кроме регистрации сигналов свободной прецессии существует большое число различных типов ЯМР экспериментов, основанных на последовательностях нескольких радиочастотных импульсов. Особенную роль играет явление, известного как спиновое эхо. Явление это основано на том, что согласно (1), в пространственно-неоднородном магнитном поле в разных частях образца спины будут прецессировать с разными скоростями. Это приведет к расплыванию единого вектора намагниченности M в веер, где спины, имеющие меньшую ω , будут отстающими, а большую – опережающими (рис. 4).

После воздействия импульса, вращающего M на 180° вокруг оси x , отстающие и опережающие спины меняются местами и веер намагниченности начинает сжиматься. Полное схлопывание произойдет через промежуток времени t , равный промежутку времени между импульсами. Затем M снова начнет расплываться. Спиновое эхо является удобным методом в некоторых видах ЯМР исследований и может служить базой для создания линий задержки в радиотехнических устройствах [1].

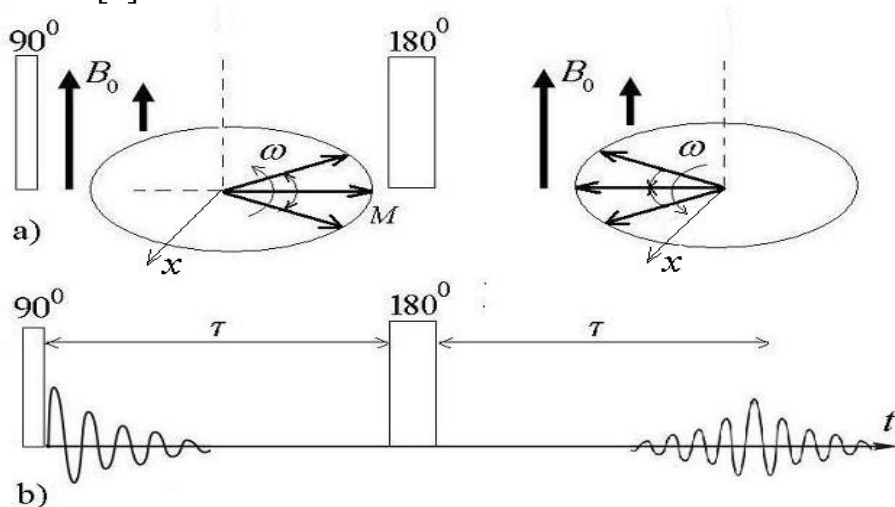


Рис. 4. а) в неоднородном магнитном поле в разных частях образца спины прецессируют с разными скоростями. После поворота M вокруг оси x радиочастотным 180° импульсом происходит последующее сфазирование спинов; б) сигнал свободной прецессии и спинового эха

Широкое применение в практических приложениях методы ЯМР обрели после того, как вычислительная техника дошла до уровня, позволяющего производить быстрые Фурье-преобразования сигналов (*рис. 5*), что позволило получать спектральные портреты различных веществ.

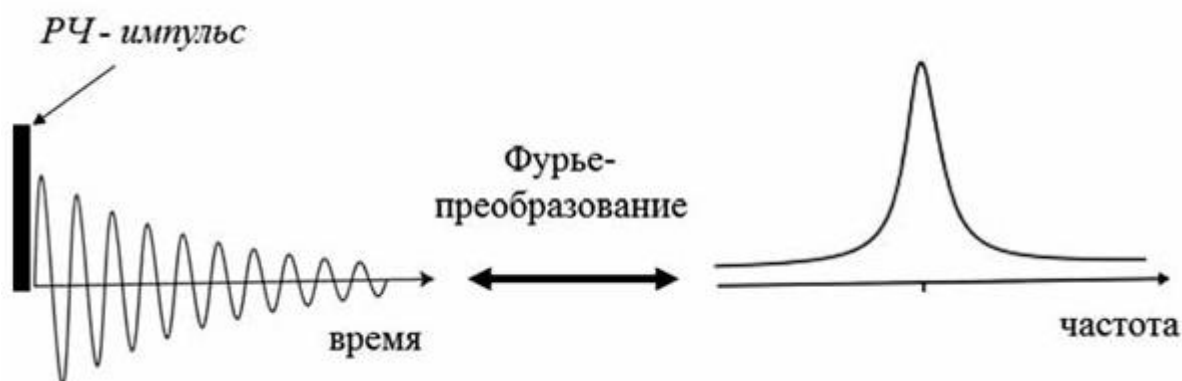


Рис. 5. Преобразование сигнала свободной прецессии в спектр при помощи Фурье-преобразования

2. Применение ЯМР в химическом анализе.

Ядра водорода ^1H – протоны, являются самыми популярными объектами в ЯМР исследованиях. Все протоны имеют одинаковые магнитные моменты и, казалось бы, должны давать отклик на одной и той же частоте. Но, в реальности, частота резонанса протона в различных молекулах будет несколько отличаться. Более того, она может отличаться в одной и той же молекуле, если позиции протона в ней химически неэквивалентны (*рис. 6*). Таким образом, из рассмотрения ЯМР спектров можно получить важную информацию о химической структуре вещества, а имея базу данных спектров известных веществ, можно проводить их быстрое опознание. Причем, общий эффект химического окружения для данного протона можно при анализе разбить на две части, одна из которых связана с окружающими электронами, а другая – с соседними магнитными ядрами. Это позволяет при помощи ЯМР различать между собой вещества с одинаковой химической структурой, но разным изотопным составом.

Пики, соответствующие каждой из частот спектра, имеют определенную ширину и в слабых полях могут сливаться, не позволяя производить точный анализ (*рис. 6*). В свою очередь, необходимость создания магнитных полей высокой напряженности приводит к использованию весьма дорогих магнитов, что негативно влияет на цену ЯМР-спектрометров.

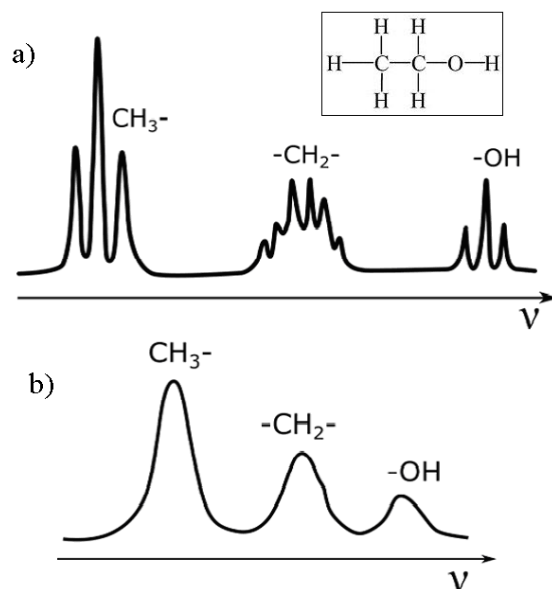


Рис. 6. а) ЯМР спектр этилового спирта, полученный в сильном магнитном поле; б) ЯМР спектр этилового спирта, полученный в слабом (земном) магнитном поле

3. ЯМР в земном магнитном поле и его практические приложения.

Напряженность магнитного поля Земли довольно мала (10^{-4} – 10^{-5} Тл) и не позволяет производить тонкий химический анализ. В то же время труднодостижимая для «искусственных» полей однородность земного поля сделала возможным применение квантовых магнитометров как инструментов поиска различных объектов как в воде, так и в грунте. Принцип действия большинства современных магнитометров основан на регистрации сигналов свободной прецессии в земном поле. Искомые объекты искажают земное поле, меняя частоту резонанса, что регистрируется прибором. В отличие от металлоискателей, магнитометры являются пассивными приборами, не облучающими объект электромагнитными полями, что в некоторых случаях может быть весьма важным качеством.

Современные магнитометры обладают очень высокой чувствительностью к изменениям магнитного поля. Портативные сравнительно дешевые протонные магнитометры обнаруживают вариации поля величиной около 1 нТл, а магнитометр с динамической накачкой (магнитометр Оверхаузера) на практике обеспечивает 0,01 нТл [2]. Для сравнения, пистолет, закопанный на глубине 1,5–2 м, создает магнитную аномалию величиной 10–20 нТл.

Хотя прецессия в датчике магнитометров идет в земном поле, для предварительной поляризации вещества датчика требуется мощный магнит, что делает квантовые магнитометры довольно дорогими приборами в сравнении с металлоискателями [3].

Обратной стороной чувствительности магнитометров является их подверженность помехам со стороны промышленных объектов и бытовых приборов. В современных магнитометрах и других приборах ЯМР земного поля реализованы методы отстройки от помех за счет некоторого уменьшения их чувствительности.

Применение ЯМР в земном поле для химического анализа веществ кажется бессмысленным лишь на первый взгляд. Малая чувствительность к химическим

сдвигам частот, все же позволяет даже по грубым спектрам уверенно различать между собой различные химические соединения (рис. 7), что может быть актуальным для систем досмотра.

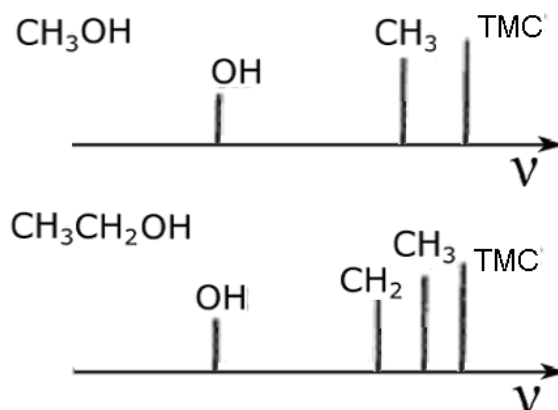


Рис. 7. ЯМР спектры метилового и этилового спиртов

Малая частота сигналов прецессии протонов в земном поле (1,5–2,5 кГц) обеспечивает хорошую проникаемость электромагнитных волн в том числе и через металл. В настоящее время реализована лабораторная установка, обеспечивающая уверенную регистрацию ЯМР от жидкости в закрытом диамагнитном металлическом контейнере с толщиной стенок до 0,5 мм [4].

Спиновое эхо в однородном магнитном поле кажется явлением принципиально невозможным, однако в движущейся жидкости при некоторых условиях оно наблюдается [5]. Данное явление принципиально позволяет создать прибор для магнитной регистрации движения жидкости, что может быть актуальным, например, для неразрушающего контроля за трубопроводами и в системах контроля подводной обстановки.

Причиной спинового эха в настоящее время считается сочетание неоднородности поляризующего поля в большом датчике и турбулентного движения жидкости [5]. Наши результаты, однако, показывают, что определяющую роль в эффекте играет прецессия Томаса спина, движущегося по криволинейной траектории во внешнем поле [6]. Эффект спинового эха, таким образом родственен эффекту, приводящему к модификации спин-орбитального взаимодействия в электронных оболочках атомов.

Результаты подтверждаются качественной компьютерной моделью датчика ЯМР. Движение жидкости в модели считается заданным. Моделируются однородное и неоднородное вращение вязкой жидкости, вихри Хилла и Ламба.

Список использованных источников:

1. Померанцев Н. М. Явление спинового эхо и его применение // УФН. 1958. № 1. Т. 65. С. 87–110.
2. Смекалова Т. Н., Восс О., Мельников А. В. Магнитная разведка в археологии. 12 лет применения Оверхаузеровского градиентометра GSM-19WG. Спб. : Санкт-Петербургский государственный университет, 2007. 73 с.

3. Звежинский С. С., Парфенцев И. В., Метод магнитометрического обнаружения взрывоопасных предметов // Специальная Техника. 2008, № 2. С. 8–17.
4. Куприянов П., Чижик В., Вечерухин Н. Получение ЯМР сигнала в магнитном поле Земли от образца в металлическом контейнере // Вестник Санкт-Петербургского государственного университета. 2013. № 2. С. 20–24.
5. Мельников А. В., Вечерухин Н. М., Бородин П. М. Альтернативный метод наблюдения спинового эха в движущейся жидкости // Вестник Санкт-Петербургского государственного университета. 2000. № 3. С. 139–142.
6. Малыкин Г. Б. Прецессия Томаса: корректные и некорректные решения // УФН. 2006. Т. 176. С. 865–882.

Булгакова Е. В.¹,

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

Лузганов Д. В.²,

*слушатель факультета подготовки
специалистов в области
информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя*

ОЦЕНКА СТЕПЕНИ ЗНАЧИМОСТИ И УСТОЙЧИВОСТИ ДАННЫХ ЦИФРОВОГО ПРОФИЛЯ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ, НЕОБХОДИМЫХ И ДОСТАТОЧНЫХ ДЛЯ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

Актуальность темы обуславливается тем, что в настоящее время ежедневно приходится сталкиваться с большим количеством данных, представленных в цифровом виде, которые обладают персонифицирующим свойством. Вместе с тем, по-прежнему, отсутствует унифицированный перечень сведений, который позволял бы отнести ту или иную информацию к данной категории данных.

Цифровой профиль – это совокупность достоверных и юридически значимых сведений о гражданах и юридических лицах, получаемых напрямую из информационных систем федеральных органов исполнительной власти осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации.

С технологической точки зрения цифровой профиль можно разделить на три больших подсистемы. Первая подсистема – это непосредственно профиль гражданина, то есть это данные, которые собираются из государственных информационных систем и объединяются в некоторую единую сущность, которая является профилем. Вторая подсистема – это платформа согласий, которая отвечает за регулированием доступа коммерческих организаций к данным физических лиц. Третья подсистема – это сервисы, которые обеспечивают возможность доступа к данным, возможность управления согласием через различные интерфейсы, возможность актуализации данных и быстрого доступа к ним.

Требования к цифровизации процессов:

- постоянная доступность данных, на основе которых предоставляются услуги;
- актуальность и достоверность получаемых сведений;

¹ © Булгакова Е. В., 2022.

² © Лузганов Д. В., 2022.

- идентификация и аутентификация;
- возможность граждан распоряжаться доступом к сведениям о себе;
- юридическая значимость.

На сегодняшний день не разработан четкий алгоритм идентификации цифрового профиля пользователей различных интернет ресурсов, таких как «ВКонтакте», «Одноклассники», «Телеграмм» и др. Для того, чтобы идентифицировать аккаунт, надо определить перечень критериев, на основе которых будет производиться идентификация, таких как достоверность, актуальность и полнота. Для каждого критерия должен быть определен свой процент соответствия, чтобы в дальнейшем можно было произвести корреляционный анализ цифрового профиля конкретного пользователя интернет ресурса к примеру, с его имеющимся подтвержденным аккаунтом на портале Государственных услуг Российской Федерации (далее – Госуслуги РФ), так как этот портал располагает проверенными, достоверными, актуальными и полными сведениями об документах, удостоверяющих личность граждан, необходимых для идентификации лиц. Если же вместо портала Госуслуг РФ брать какие-либо другие официальные или неофициальные источники сведений, то тут следует определять коэффициент доверия к данному ресурсу. Все же основу идентификации цифрового профиля составляют информационные системы федеральных органов исполнительной власти таких как Росреестр, ФНС, Пенсионный фонд и МВД России.

На данный момент компания, владеющая мессенджером «ВКонтакте», начинает запускать проект по интеграции портала Госуслуг РФ в свой мессенджер, но на раннем этапе развития будет доступно только два пункта – это «здоровье» и «авто», как говорится в анонсе.

Перечень сведений, доступных через цифровой профиль на портале Госуслуг Российской Федерации:

1. Фамилия, имя и отчество гражданина Российской Федерации, указанные в паспорте гражданина Российской Федерации.
2. Пол гражданина Российской Федерации, указанный в паспорте гражданина Российской Федерации.
3. Дата рождения гражданина Российской Федерации, указанная в паспорте гражданина Российской Федерации.
4. Серия и номер паспорта гражданина Российской Федерации, указанные в паспорте гражданина Российской Федерации.
5. Дата выдачи паспорта гражданина Российской Федерации, указанная в паспорте гражданина Российской Федерации.
6. Орган, выдавший паспорт гражданина Российской Федерации, указанный в паспорте гражданина Российской Федерации.
7. Код подразделения, указанный в паспорте гражданина Российской Федерации.
8. Место рождения, указанное в паспорте гражданина Российской Федерации, в том числе сведения о стране, регионе, населенном пункте рождения, указанные в паспорте гражданина Российской Федерации.
9. Сведения о гражданстве гражданина Российской Федерации, в том числе наличии двойного гражданства.

10. Сведения о регистрации гражданина Российской Федерации по месту жительства или месту пребывания (снятии с регистрационного учета) [1].

Предоставление гражданам возможности цифровой идентификации имеет много преимуществ – например, это эффективный инструмент для облегчения и оптимизации доступа к данным, необходимым государственным органам, для осуществления информационного взаимодействия с гражданами, а также укрепления и ускорения социальной и финансовой интеграции.

Криминалистическое значение цифрового профиля состоит в реализации таких функций, как идентификация без необходимости предоставления бумажных документов и развитие цифровых услуг – предоставление необходимой информации операторами связи, провайдерами в целях расследования и раскрытия преступлений. Данное направление модернизации процесса собирания доказательственной информации имеет огромный потенциал и является особо актуальным в современное время при стремительном развитии информационных технологий [4]. Это может иметь большое практическое значение при установлении лица, совершившего преступление (непосредственно идентификации), мотивов, определении связей между участниками предварительного расследования, розыска лиц по определенным параметрам, создании цифрового профиля таких лиц и др. Кроме того, одну из первостепенных ролей играет и возможность облегчения процесса получения необходимой информации от других органов без затрат дополнительных ресурсов и времени. Также ядром такой системы, усиливающим скорость поиска и эффективность расследования, станут биометрические персональные данные (изображение лица человека, данные голоса и др.) [5].

Федеральная государственная информационная система «Единая система идентификации и аутентификации» должна обеспечивать санкционированный доступ участников информационного взаимодействия в единой системе идентификации и аутентификации к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах [6]. Это дает возможность пользователям входить на Интернет ресурсы (каких-либо государственных или коммерческих организаций) без прохождения регистрации на данном сайте, что является более удобным и практичным способом авторизации.

Существуют также риски, связанные с различными утечками и коммерческим использованием личной информации. В связи с этим возникает вопрос об определении уровня безопасности данных, хранящихся в системе цифрового профиля граждан. Ряд крупных корпораций таких, например, как «Яндекс» отказываются от работы с персональными данными, опасаясь возможности утечки такой информации.

По нашему мнению, для решения данной проблемы необходимо создать алгоритм, который бы считывал всю информацию цифрового профиля интернет-ресурса, проверял полученные сведения на соответствие требованиям, таким как актуальность, достоверность, полнота и коэффициент доверия, и производил корреляционный анализ, сравнивая информацию цифрового профиля из источника, обладающего подтвержденными и достоверными сведениями.

Список использованных источников:

1. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // Сайт «Киберленинка». URL: <https://cyberleninka.ru/article/n/tsifrovoy-profil-ponyatie-mehanizmy-regulirovaniya-i-problemy-realizatsii>.
2. Цифровой профиль гражданина: перспективы внедрения систем удаленной идентификации // Сайт «VC». URL: <https://vc.ru/u/619012-digital-rights-center/169277-cifrovoy-profil-grazhdanina-perspektivy-vnedreniya-sistem-udalennoy-identifikacii>.
3. Цифровой профиль гражданина: криминалистическое значение и вопросы безопасности // Сайт «Интернет-конференции Сибирского юридического университета». URL: <https://conf.siblu.ru/cifrovoy-profil-grazhdanina-kriminalisticheskoe-znachenie-i-voprosy-bezopasnosti>.
4. Булгакова Е. В., Булгаков В. Г. Организационно-правовые аспекты использования биометрических персональных данных в раскрытии и расследовании преступлений // Сборник тезисов докладов в 4-х частях : Московский юридический форум онлайн. М., 2020. С. 193–195.
5. Булгаков В. Г., Булгакова Е. В. Использование информационных технологий для установления лиц, причастных к совершению преступлений // Материалы Международной научно-практической конференции : Следственная деятельность: настоящее и будущее. 2018. С. 51–54.
6. Единая система идентификации и аутентификации (ЕСИА) // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: <https://digital.gov.ru/ru/activity/govservices/infosystems/21/>.

Тукаева Ф. А.¹,
*доцент кафедры управления в органах
внутренних дел Уфимского
юридического института МВД России,
кандидат экономических наук, доцент*

ОПАСНОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ

Наш век характеризуется необычайным развитием цифровых технологий. Сегодня то, что еще лет 20–25 считалось фантастикой, стало обыденностью. Диджитал-технологии проникли в каждую отрасль, каждую область экономики и повседневной жизни. Не стали исключением и бизнес-отношения, и правовые аспекты их осуществления.

Привычные нашему поколению бумажные документы теперь не только имеют копии на электронных носителях; все чаще бизнес и государственные структуры обращаются к электронному документообороту.

Вначале под электронным документооборотом понималась передача документации, сформированной на бумажном носителе и затем отсканированной. В настоящее время, кроме таких электронных документов, широкое распространение получили и документы, изначально создаваемые только в электронном виде. Юридическую силу таким документам придает электронная подпись.

Любой документ, в том числе и электронный, действителен только при наличии подписи. Электронная подпись – это «информация в электронной форме, присоединенная к электронному документу или иным образом связанная с ним и позволяющая идентифицировать лицо, подписавшее электронный документ» [5, с. 3]. Она считается более безопасной, чем подпись на бумажном носителе, так как ее не только невозможно подделать, но, кроме того, при ее использовании изменения информации в документе, возникшие после проставления подписи, будут обязательно обнаружены. Это определяется процедурой формирования и подтверждения подлинности электронной подписи. Такая подпись ставится и проверяется при помощи специальных ключей, представляющих собой уникальную последовательность символов. Для того, чтобы подтвердить, что последний исходит именно от него, владелец подписи должен получить в удостоверяющем центре специальный сертификат. Функции удостоверяющего центра могут выполнять государственные органы, органы местного самоуправления, юридические лица и даже индивидуальные предприниматели.

Законодательно в нашей стране различают три вида электронных подписей, отличающихся разным уровнем защиты.

Практически каждый из нас знает простую электронную подпись. Мы используем ее, когда входим в электронную почту, личные кабинеты на различных сайтах, подтверждаем свое участие в электронном анкетировании и т. д.

Для создания усиленной неквалифицированной подписи необходимо криптографическое преобразование информации. Поэтому именно ее можно считать

¹ © Тукаева Ф. А., 2022.

подписью, имеющей все необходимые для электронной подписи признаки: установление лица – владельца подписи и нахождение изменений в электронном документе, если таковые возникли уже после его подписания.

Конечно же, наиболее высокий уровень защиты демонстрирует усиленная квалифицированная подпись. Во-первых, выдать ее может только аккредитованный удостоверяющий центр; во-вторых, для ее создания и верификации применяются средства электронной подписи, соответствующие требованиям Закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Такой уровень защиты позволяет приравнять электронные документы с квалифицированной подписью к бумажным документам, подписанным собственноручно [1, с. 3].

Электронная подпись позволяет ускорить документооборот и заключение сделок даже при условии удаленности сторон и контрагентов друг от друга. Одновременно это экономия средств: для государственных структур – за счет сокращения штата сотрудников, ведущих прием документации; для коммерческих организаций – за счет сокращения трудозатрат и административных расходов, ускорения обработки заказов и сокращения времени на их исполнение.

Электронная подпись стала обычным явлением в межведомственном документообороте и в корпоративных системах. Однако физические лица прибегают к использованию электронной подписи не так часто. Это обусловлено как техническими сложностями при получении и использовании электронной подписи, недостаточной информированностью и неграмотностью части населения в области возможностей цифровых технологий, а также опасениями использования подписи мошенниками.

Технически использование электронной подписи надежно, так как лица, решившие воспользоваться чужой подписью, должны будут решить довольно сложные задачи. Например, подделать ее, то есть найти значение подписи; или же подделать (модифицировать) документ с уже проставленной подписью. Возможны также варианты подмены электронного документа (подбор двух разных документов с одинаковыми значениями подписи, но не зная секретного ключа) и генерации подписанного документа [4, с. 75].

В то же время собственноручная подпись лучше электронной в плане простоты проставления (не нужны дополнительные механизмы), она не имеет срока давности.

Определенные проблемы использования электронных подписей могут возникнуть при длительном хранении документов: ограниченный срок действия электронных подписей может поставить под сомнение архивной информации, зафиксированной в цифровом виде [2, с. 79].

Несмотря на законодательные и технические меры по защите электронных подписей, не редки случаи незаконного применения электронной подписи мошенниками. В частности, известны подобные случаи при заключении сделок купли-продажи квартир, когда злоумышленники, получив электронную подпись гражданина через сотрудника удостоверяющего центра, продают квартиру этого лица третьим лицам. При этом гражданин может быть в полном неведении, что на него оформлена электронная подпись.

Во избежание таких ситуаций гражданам рекомендуют оформить заявление об обязательном личном присутствии при оформлении подобного рода сделок.

В качестве технического ограничения предлагают ведение фото- и видеосъемки процесса получения электронной подписи, а также подтверждать электронную подпись биометрическими параметрами, например, отпечатком пальца [3, с. 191].

Таким образом, электронная подпись сегодня стала неотъемлемым атрибутом повседневной деловой жизни. Цифровые технологии развиваются и, возможно, появятся новые, более совершенные технические средства защиты электронных подписей от несанкционированного использования третьими лицами. Однако криминальный мир также активно использует новейшие достижения. В этой связи, на наш взгляд, предстоит работа по дальнейшему совершенствованию законодательного регулирования применения электронной подписи, идентификации участников электронного документооборота.

Список использованных источников:

1. Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_112701/.
2. Ермолаева А. В. Электронный документ и электронная подпись: проблемы регламентации и практики применения // Региональная власть, местное самоуправление и гражданское общество: механизмы взаимодействия : сборник научных трудов. Саратов : Поволжский институт управления имени П.А. Столыпина, 2017. С. 77–80.
3. Ефремова А. В. Правовое регулирование порядка использования электронного документа и электронной подписи // Вестник студенческого научного общества Донецкого национального университета. 2021. Т. 4. № 13. С. 187–192.
4. Сабанов А. Г. Роль аутентификации и электронной подписи в обеспечении юридической силы электронным документам для систем М2М // ГЛОНАСС – Регионам : материалы 4-ой Всероссийской научно-практической конференции / под общ. ред. А. Н. Новикова. Орел : Государственный университет – учебно-научно-производственный комплекс», 2014. С. 73–78.
5. Соловяненко Н. И. Юридическое значение электронной подписи в правовых отношениях электронного бизнеса // Colloquium-Journal. 2020. № 8-7 (60). С. 55–58.

*Альховская А. В.¹,
курсант международно-правового
факультета Московского университета
МВД России имени В.Я. Кикотя*

*Худяков В. В.²,
доцент кафедры информатики
и математики Московского университета
МВД имени В.Я. Кикотя*

ЦИФРОВОЙ ПРОФИЛЬ ЧЕЛОВЕКА – ОБЪЕКТ АТАКИ ЗЛОУМЫШЛЕННИКОВ

В статье рассматривается данный вопрос и с точки зрения уполномоченных ведомств, в сферу ответственности которых включено рассмотрение данного вопроса, и с точки зрения рядового гражданина, который передает свой цифровой профиль для обработки и хранения.

Создание цифровой экономики является одной из приоритетных государственных задач России на период с 2019 по 2024 гг. в рамках реализации национального проекта «Цифровая экономика» в соответствии с указом Президента Российской Федерации «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [3]. В связи с этим происходит активное развитие и внедрение инновационных технологий, в том числе цифровых, во все сферы деятельности человека.

На сегодняшний день с целью повышения безопасности и качества жизни граждан, а также конкурентоспособности государства в сфере международных информационных технологий, разрабатывается система обеспечения функционирования цифровой среды, включающая в себя правовое регулирование, кадровый потенциал, информационную безопасность и инфраструктуру. Одной из инициатив в рамках национального проекта является создание цифрового профиля человека, который станет шагом на пути к достижению конечной цели – созданию платформы цифрового государственного управления.

На замену прежним методам установления личности приходят инновационные по своей сути цифровые технологии, что приводит к снижению роли в повседневной деятельности личных идентификационных документов. Одним из таких новшеств является цифровой профиль человека. Появление цифрового профиля человека, как альтернативы физическим носителям данных о лице, позволило существенно изменить подход к осуществлению своей деятельности государственных структур, органов, учреждений, служб, частных предприятий и по праву является передовым достижением эпохи цифровизации в сфере оказания услуг. И хотя, не во всех сферах жизнедеятельности человека представля-

¹ © Альховская А. В., 2022.

² © Худяков В. В., 2022.

ется возможным произвести замену личных документов, существующих на физических носителях, электронными, ежедневно содержание цифрового профиля и, как следствие, функционал расширяются.

Цифровой профиль человека – совокупность сведений о физическом лице, хранящаяся в виртуальном пространстве, представляющая собой пакет анкетных данных, персональных документов, электронных записей государственных и негосударственных информационных систем. Цифровой профиль человека также подразумевает наличие технических средств, приемов и способов, непосредственно с помощью которых осуществляется хранение, изменение, преобразование таких сведений субъектами цифровой деятельности, в том числе владельцем.

Остается открытым вопрос законодательного закрепления термина «цифровой профиль человека», поскольку в настоящее время правовое регулирование данной отрасли осуществляется в соответствии с положениями Конституции Российской Федерации о неприкосновенности частной жизни и запрете распространения сведений о лице без его согласия, а также на основе Федерального закона «О персональных данных» [1; 2].

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры) неоднократно поднимало вопрос о целесообразности внедрения цифрового профиля человека в повседневную деятельность. Под сомнение ставился вопрос о безопасности включения в данный персональный аккаунт электронной подписи, поскольку этот шаг, наряду с очевидными достоинствами использования, несет в себе и дополнительные угрозы. Однако на данный момент обсуждается возможность ее замены на биометрические данные, что может спровоцировать новые по своей природе более скрытные, точечные кибератаки на цифровой профиль человека.

Несмотря на все преимущества, цифровой профиль человека представляет собой угрозу для персональных данных лица ввиду атак злоумышленников, конечной целью которых является получение охраняемых законом сведений о человеке. Масштаб и содержание таких противоправных действий не ограничивается DDoS-атаками на отдельные устройства в традиционном понимании, а включают в себя поражение целых информационных систем посредством компьютерных вирусов и целевых атак. Крупнейшая цифровая платформа, содержащая цифровой профиль человека – Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг (функций)» (далее – Госуслуги) нередко подвергается кибератакам.

Минцифры 26 февраля 2022 г. сообщило о крупных кибератаках, совершенных на портал Госуслуг, со скоростью файлообмена злоумышленников более 1 Тбайт в секунду или 8 млн Мбит в с. Оценивая данный показатель отметим, средняя скорость беспроводной передачи данных современных смартфонов составляет 25–50 Мбит/с. Помимо DDoS – атак применялись и профессиональные атаки на отдельные информационные элементы государственной платформы. Результатом такой активности злоумышленников стало кратковременное прекращение работы сервисов. Ведомство сообщило о запуске специалистами дополнительных средств защиты с целью пресечения противоправного доступа к персональной информации [9].

Исходя из содержания цифрового профиля человека следует вывод, что он, по сути, представляет собой личность конкретного физического лица, существующую в виртуальном пространстве и в связи с чем, выступает самостоятельным объектом атак злоумышленников. Цифровой профиль, дополненный биометрическими данными о владельце, является наиболее желанной целью, поскольку совершенствующиеся современные технологии позволяют преступникам в буквальном смысле «украсть лицо» другого человека.

Ввиду отсутствия единого цифрового профиля человека различают цифровой профиль гражданина, налогоплательщика, лица, осуществляющего индивидуальную предпринимательскую деятельность и ряд других. В частности, цифровой профиль человека, дополненный биометрическими данными, приобрел широкое распространение в банковской сфере. Крупнейшим держателем подобного рода сведений является Публичное акционерное общество «Сбербанк», которое намерено создать собственную биометрическую базу данных.

Самая крупная в истории Сбербанка кибератака на системы и сервисы произошла 6 мая 2022 г., о чем сообщил руководитель кибербезопасности банка на пленарном заседании международного форума в данной области. Специалисты акционерного общества оценивают мощность ее трафика более чем в 450 Гб в с., при том, что общее число пораженных устройств составило 27 тыс. единиц [8]. Особое внимание уделяется и общей численности киберпреступников, действующих против Сбербанка, которая составляет, по оценкам экспертов организации, более 100 тыс. человек. С каждой новой атакой технические устройства и средства ее осуществления совершенствуются, а значит, под угрозой оказываются и персональные данные, цифровые профили, биометрические сведения всех клиентов банка.

Хищение персональных данных в финансовой сфере сопряжено с кражей денежных средств с банковских счетов в следствие недостаточной защищенности платежной инфраструктуры от кибератак злоумышленников [5]. Организациям-операторам необходимо уделить внимание совершенствованию способов защиты обслуживаемых платежных систем.

Специалисты лаборатории Касперского отмечают значительное увеличение спроса и предложения в Даркнете на сведения, составляющие цифровой профиль человека [11]. Данный факт свидетельствует о том, что злоумышленники совершают целевые атаки на отдельные виртуальные аккаунты, содержащие персональные данные о физическом лице. Помимо этого, расширяется так называемый спектр противоправной деятельности – если ранее под угрозой оказывались преимущественно банковские счета, данные документов, удостоверяющих личность, электронные подписи, то на сегодняшний момент кибератаки совершаются в том числе в сфере здравоохранения и страхования – на цифровые медицинские карты и данные о страховании соответственно.

Так, ПАО «Ростелеком», определенная Правительством Российской Федерации в качестве компании-исполнителя мероприятий по обеспечению цифровой инфраструктуры Госуслуг сообщало о проводимых 23 июня 2022 г. кибератаках

на указанную платформу. В результате массовой атаки пострадали информационные системы отдельных регионов России, включая базы данных медицинских учреждений, содержащие в том числе персональные сведения граждан [10].

В российском законодательстве предусмотрена уголовная ответственность за преступные посягательства на персональные сведения, в число которых входят и кибератаки правонарушителей на цифровые профили граждан. Однако заместитель начальника кафедры Нижегородской академии МВД России кандидат юридических наук Н. Н. Потапова в своей работе «Некоторые особенности выявления и раскрытия бесконтактного мошенничества» полагает, что «преступления, совершенные бесконтактным способом наиболее трудоемки в плане расследования и зачастую, злоумышленники остаются безнаказанными» [7].

Для успешного функционирования цифровых технологий необходимо обеспечить их безопасность на материально-техническом, программном, теоретическом уровнях. Качество функционирования указанных уровней в совокупности есть оценка деятельности всей системы, т. е. ее надежность и безопасность. Такое направление совершенствования цифрового профиля человека как защита от цифровых информационных атак злоумышленников, предполагается поручить оператору единой системы персональных данных. Так, в соответствии с указом Президента Российской Федерации, АО «Центр Биометрических Технологий» назначено оператором данной системы организацией, обеспечивающей развитие современных цифровых технологий в части совершенствования методов и способов идентификации личности, в том числе посредством использования биометрических сведений [4].

По мнению доцента кафедры Петербургского государственного университета путей сообщения имени императора Александра I кандидата технических наук О. А. Гуляевой, для минимизации риска получения несанкционированного доступа к персональным сведениям, включая биометрические данные, специалисты в области кибербезопасности должны действовать упреждающе, то есть оценивать потенциальные риски и возможные сценарии поведения злоумышленников [7].

Особое внимание следует уделить подготовке высококлассных квалифицированных специалистов, компетентных в сфере цифровых технологий, которые бы реализовывали устойчивое функционирование системы не только на организационно-правовом уровне, но и обеспечивали бы защиту от кибератак и преступных посягательств.

Таким образом, цифровой профиль человека является не только перспективным направлением развития цифровой экономики в следствие реализации национального проекта Российской Федерации, но и потенциальной угрозой информационной безопасности государства в целом и персональных данных отдельного человека в частности, поскольку выступает объектом атаки злоумышленников.

Список использованных источников:

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных законами о поправках к Конституции Российской Федерации от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ,

от 14.03.2020 № 1-ФКЗ, с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_28399/.

2. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ (ред.14.07.2022) // СПС КонсультантПлюс. URL: <http://www.consultant.ru>.

3. Указ Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СПС КонсультантПлюс. URL: <http://www.consultant.ru>.

4. Указ Президента Российской Федерации от 30 сентября 2022 г. № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации» // СПС КонсультантПлюс.

5. Постановление Московского городского суда от 16 марта 2018 г. по делу № 4у-1053/2018 // НПП «Гарант-сервис». URL: <https://www.garant.ru/>.

6. Абышов Д. З., Потапова Н. Н. Некоторые особенности выявления и раскрытия бесконтактного мошенничества // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40).

7. Гуляева О. А., Андреев А. В., Мардас Д. А. Роль кибергигиены, биометрии в обеспечении цифрового суверенитета компаний в современных экономических условиях // Инновации и инвестиции. 2021. № 11.

8. Руководитель кибербезопасности Сбербанка рассказал о DDoS-атаках небывалой мощности и новых тактиках киберпреступников // Официальный сайт Сбербанка. URL: <https://www.sberbank.com/ru/news-and-media/press-releases/article>

9. Минцифры фиксирует атаки на портал Госуслуг // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций. URL: <https://digital.gov.ru/ru/events/41440>.

10. Портал Госуслуг подвергся кибератакам // Сайт «Интерфакс». URL: <https://www.interfax.ru/digital/847561>.

11. Мне нужны твое лицо, отпечаток пальца и радужная оболочка // Сайт «Kaspersky». URL: <https://www.kaspersky.ru/blog/stealing-digital-identity/9535/>.

Чапля Д. Я.¹,
 курсант факультета подготовки
 специалистов в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Аветисян К. Р.,
 старший преподаватель кафедры
 информационной безопасности
 учебно-научного комплекса
 информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,

ЦИФРОВАЯ ВАЛЮТА КАК СПОСОБ ПРЕСТУПЛЕНИЯ

Как показывает практика, большинство ресурсов, связанных с платежными системами или транзакциями денежных средств уличаются в неспособности грамотно и надежно защитить своих пользователей. Это проявляется не сразу, по началу все до безумия восхищаются новым сервисом и его услугами, затем наступает череда разочарования со стороны пользователей, что их транзакции можно отследить или их кошелек уже принадлежит как минимум трем разным лицам. Немного о сути вопроса и процессах, без которых невозможно понять сути вопроса.

Криптовалюта – виртуальное средство обмена, может стать реальной альтернативой деньгам, выпущенным правительством, но только в том случае, если он выдержит напор спекулянтов.

Когда в январе 2009 г. была выпущена виртуальная валюта биткойн, она оказалась интересным способом для людей торговать между собой безопасным, недорогим и частным образом. Тут стоит подчеркнуть, что речь шла в первую очередь о безопасности и децентрализации транзакций валюты, что на сегодняшний момент уже не так правдоподобно. Сеть Биткойн, разработанная неизвестным программистом с ником «Сатоши Накамото», использовала децентрализованную одноранговую систему для проверки транзакций, что означало, что люди могли обмениваться товарами и услугами в электронном виде и анонимно, без необходимости полагаться на третьи стороны, такие как банки.

Новые цифровые валюты создаются пользователями, запускающими криптоклиент на своих компьютерах. Клиент «добывает» крипту, запуская программу, которая решает сложную математическую задачу в файле под названием «блок», получаемом всеми пользователями сети Ethereum; Zcash; Monero; Bitcoin; Litecoin. Сложность задачи подобрана таким образом, что, независимо от того, сколько людей добывает криптовалюту, проблема решается, в среднем, шесть раз в час. Когда

¹ © Чапля Д. Я., 2022.

пользователь решает проблему в блоке, этот пользователь получает определенное количество криптовалюты. Тщательно продуманная процедура добычи криптовалюты гарантирует, что их предложение ограничено и растет с неуклонно снижающейся скоростью. Примерно каждые четыре года количество биткоина в блоке, которое начиналось с 50, уменьшается вдвое, а количество максимально допустимых биткоинов составляет чуть меньше 21 млн. По состоянию на 2021 г. насчитывалось более 18,6 млн биткоинов, и, по оценкам, максимальное количество будет достигнуто примерно в 2140 г.

Поскольку алгоритм, который производит криптовалюты, производит их с почти постоянной скоростью, ранние майнеры биткойнов получали их чаще, чем более поздние майнеры, потому что сеть была небольшой. Премия, которую получили первые пользователи, и молчание Накамото после 2011 г. привели к критике Биткоина как схемы Понци, причем Накамото получил выгоду как один из первых пользователей. (Анализ первых 36,3 тыс. добытых блоков показал, что один майнер, предположительно Накамото, накопил более 1 млн криптовалюты. Однако по состоянию на 2022 г. эти биткойны, которые тогда оценивались в 50 млрд \$, оставались неизрасходованными). Защитники цифровых валют утверждают, что ранние пользователи должны получать некоторую отдачу за инвестиции в непроверенную технологию.

В каждой прикладной сфере всего вышеперечисленного есть ряд нюансов, которые позволяют мошенникам вести незаконную деятельность.

Вот ряд самых популярных мошенничеств в данной сфере:

- торговые боты;
- сигналы / пампы;
- инвестиционные криптофонды.

Все, что перечислено выше очень трудно доказуемо, как факт преступления.

Про все по-порядку, торговые боты-сама стратегия предполагает лишь малых вложений на старте и далее лишь поддержание системы в нормальном режиме работы, но на практике в 9 из 10 случаев мы получаем схему Понци. Схема Понци – это форма мошенничества, которая заманивает инвесторов и выплачивает прибыль более ранним инвесторам за счет средств более поздних инвесторов. Суть максимально проста и понятна для мошенников.

Второе, сигналы или дампы – это могут быть специализированные телеграм-каналы с уже конкретной аудиторией, созданные для получения прибыли с криптовалюты. Люди намеренно прогревают какие-то сервисы для заработка с цифровых валют, а потом, когда пользователи видят активность и счета, тоже вкладывают средства и через некоторое время основатели «прогрева», коим могут быть медийные личности сети Интернет, выводят свои средства, а сам продукт остается «пустышкой», в который много доверчивых пользователей вложили свои цифровые средства.

И третье, это инвестиционные криптофонды или криптовклады, организации, зачастую даже оформленные официально для предоставления документов в качестве доказательства о законной деятельности. Но как показывает практика – это скорее похоже на пирамиду, если вы являетесь основателем или быть в пер-

вых рядах, тогда можно получить какую-либо прибыль, но опять же, с точки зрения закона все в рамках правового поля, реальная компания заявляет о своем банкротстве и не обязана возвращать вам денежные средства, что прописано в Федеральном законе «О несостоятельности (банкротстве)» от 26 октября 2002 г. № 127-ФЗ.

Как итог, можно сказать, что для полной безопасности в криптовалютной сфере нет, и вряд ли будет, потому что с развитием новых технологий, систем, сервисы предоставляющие услуги, идет развитие и теневого бизнеса, сфера деятельности которого, не чуть не хуже высокотехнологичных систем, как отечественных, так и зарубежных. Чем больше система, тем больше «дыр».

Список использованных источников:

1. Вермеенко Я. С. Современное состояние и перспективы развития ИСОД МВД России // Академическая мысль. 2021. № 3 (16). С. 75–78.
2. Воронов М. В., Пименов В. И., Небаев И. А. Системы искусственного интеллекта : учебник и прак-тикум для вузов. М. : Юрайт, 2022. 256 с.
3. Советов Б. Я., Цехановский В. В. Информационные технологии : учебник для вузов. 7-е изд., перераб. и доп. М. : Юрайт, 2022. 327 с.

Шитов П. М.¹,
 курсант факультета подготовки
 сотрудников в области
 информационной безопасности
 Московского университета
 МВД России имени В.Я. Кикотя

Научный руководитель:
Дворянкин О. А.,
 старший преподаватель кафедры информационной
 безопасности учебно-научного
 комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат юридических наук

ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ИСТОЧНИКОВ ПРИ ВЫЯВЛЕНИИ И ПРЕСЕЧЕНИИ МОШЕННИЧЕСТВА В СФЕРЕ СПОРТИВНЫХ СТАВОК

В современном мире обычный человек все чаще сталкивается с рекламой легкого и быстрого заработка без вложений. Рекламодатель часто обещает своим клиентам возможность быстро получить автомобиль мечты или огромное количество денег. Подобная информация не имеет ничего общего с действительностью.

Одним из способов быстрого заработка является беттинг – вид азартной игры, основывающейся на спортивных ставках. Название происходит от английского слова «bet» – пари или ставка, следовательно, «betting» – процесс заключения ставки или спора. Основным посредником таких азартных игр является букмекер. Суть беттинга проста – игрок заключает пари с букмекерской конторой. Букмекер распределяет коэффициенты на исход спортивного события. При составлении коэффициентов букмекер руководствуется различными статистическими данными – процент побед, процент точных передач или ударов, также существуют косвенные факторы – физическая форма игроков или социальная напряженность в команде.

Исходя из представленных коэффициентов на возможные исходы спортивного события, игрок выбирает стратегию и делает ставку. Если игрок угадал результат события – букмекерская контора умножает его ставку на предложенный коэффициент и выплачивает деньги игроку, если игрок не угадал верный исход – его деньги переходят букмекерской конторе. Результатом пари может быть, как исход одного события, так и исход нескольких событий, при этом заданный коэффициент возрастает. Беттинг имеет существенные отличия от казино – в беттинге игрок полагается на свои аналитические способности, а не на удачу. Стоит отметить, что беттинг это не полноценный способ заработка, а лишь развлечение,

¹ © Шитов П. М., 2022.

многие игроки в процессе игры забывают об этом и поддаются собственному азарту проигрывая внушительные средства и попадая в финансовую яму.

В букмекерском бизнесе важную роль играют капперы – опытные спортивные аналитики, продающие свои прогнозы и анализы другим игрокам с целью заработка. Обычно беттор хорошо разбирается в каком-либо виде спорта и благодаря своим глубоким познаниям может с уверенностью заключать пари против букмекера, выходя из них победителем.

Игроки, которые не могут самостоятельно и качественно проанализировать событие и угадать верный исход, нередко обращаются к капперам, продающим прогнозы и готовые анализы спортивных событий. Профессиональный каппер делает выборку ставок исходя из собственного анализа событий и заключает пари перед началом спортивного события. Зарекомендовав себя в сообществах любителей спортивных пари, специалист может начать продавать свои прогнозы на различных форумах, специальных сервисах или социальных сетях. Подобные сервисы обычно формируют рейтинг капперов, что дает условную гарантию честной игры. На данный момент особенно популярна торговля прогнозами в различных Telegram-каналах.

Первостепенной целью каппера является реальный заработок посредством выигрышей пари. Современная беттинг-индустрия предоставляет капперам широкий выбор спортивных событий и разнообразные условия заключения пари. Вторая категория игроков делают ставки из интереса, они заключают пари только для более интересного просмотра состязания. Самая опасная и нестабильная категория игроков – лудоманы. Лудоманы не могут контролировать свой азарт, что приводит к огромным материальным потерям.

Среди массы профессиональных аналитиков встречаются и недобросовестные люди, занимающиеся мошенничеством в интернете. Отличить мошенника нетрудно: в рекламе мошенников обычно указывается стопроцентная гарантия выигрыша, которая ничем не аргументирована. Мошенник буквально навязывает свои услуги игрокам.

У профессионального каппера есть чистая статистика и доказательство его благих намерений. Большинство уважающих себя гандикапперов пользуются верификаторами – сервисами по фиксации ставок в отдельный сетевой рейтинг, поправить который невозможно вручную (своеобразный капперский патент ставок).

Существует несколько моделей продажи прогнозов, условно можно выделить так называемую подписку – услуги начинающего каппера могут стоить от 1 тыс. рублей, опытные бетторы продают прогнозы за 7 тыс.–10 тыс. рублей. Некоторые прогнозисты обретают широкую популярность, например, американский каппер Vegas Dave имеет 7 млн подписчиков на своем аккаунте в Instagram (принадлежит компании Meta, признана в Российской Федерации экстремистской).

Профессиональные бетторы отлично показывают себя на дистанции, зарабатывают огромное количество денег, однако иногда подписчики остаются без обещанного выигрыша. Есть несколько причин:

1. Рассылка от каппера приходит в неподходящее время. Представим ситуацию: беттор присылает удачный прогноз на матч Бундеслиги, а клиент в это

время уже спит. Итог: каппер заработал деньги, а банк подписчика остался прежним. Другой случай: беттор отправил прогноз, но клиент был занят на работе, но когда увидел ставку, коэффициент уже снизился. Если он заключает пари на менее скромную котировку, то и заработает меньше.

2. Букмекер не принимает ставку. Роспись у разных букмекерских контор может отличаться. Игроку мог прийти прогноз на редкое событие, но не всегда удастся заключить пари у своего букмекера. Маржа в БК тоже отличается: котировки в букмекерской конторе могут быть ниже коэффициентов компании, в которой прогнозист делает ставки.

3. Беттор обманывает. Профессиональные игроки нередко обманывают своих подписчиков. Реальный случай: каппер сайта BetOnSuccess с ником bskok.B.L запустил две платные рассылки прогнозов и все проигравшие ставки отправлял во вторую рассылку. Первая была идеально выигрышной, но сотрудники обнаружили мошенничество со стороны беттора и заблокировали его профиль.

Среди капперов нередко можно встретить мошенников, продающих заведомо ложные прогнозы. Как капперы обманывают игроков? Мошенники часто прибегают к социальной инженерии. Капперы могут продавать договорные матчи. Напомним, что договорные матчи запрещены на законодательном уровне (ст. 184 УК РФ).

Обычно мошенник продает стопроцентную гарантию заработка на исходе какого-либо спортивного события. Стоимость такого прогноза начинается от двух тысяч рублей, для простого человека это довольно большая сумма денег, поэтому он рассчитывает, что такой дорогой прогноз принесет ему большое количество дивидендов.

Другой вариант исхода событий – человек зарабатывает гораздо больше денег и 2 тыс. рублей для него – небольшая сумма, которую он может позволить потратить на развлечение в виде спортивного пари. Игрок хочет попробовать разбогатеть посредством выигрыша на договорном событии и делает относительно небольшую ставку суммой в 2 тыс. рублей. Если игроку повезет, он проиграет и поймет, что его обманули. Если же игрок случайно угадает исход спортивного события, он рискует потерять в разы больше денег, чем в первом случае. После такой мнимой победы формируется механизм доверия капперу: первая игра была своеобразной проверкой – игрок поставил небольшую сумму денег и победил, следовательно, капперу можно доверять, его прогноз надежен. В последующие разы воодушевленный игрок будет делать в разы более дорогие ставки, рассчитывая заработать внушительную сумму денег и рискуя попасть в финансовую яму. Опасность таких азартных игр в том, что в процессе игры у человека может развиваться полноценная зависимость в виде лудомании. Человек, страдающий лудоманией (лудоман) не может остановиться после очередного проигрыша и продолжает заключать пари, не оставляя денег на существование.

Исходя из вышесказанного можно сделать следующие выводы: договорные матчи действительно существуют, но получить доступ к информации о таких видах спортивных событий почти невозможно. Договорные матчи обычно стоят

половину суммы, которую можно на них поставить. Размер максимальной ставки зависит от популярности события. Приведем простой пример: на финал Лиги Чемпионов можно поставить миллионы долларов, а на матчи Российской Премьер Лиги не более нескольких десятков тысяч долларов. Утечка информации о договорном матче вредит в первую очередь лицу, которое разгласило информацию – другой игрок поставит максимальное количество денег на верный исход, что может привлечь внимание правоохранительных органов и непосредственно букмекера, который может снизить коэффициент на исход события или снять его из своей линии.

Список использованных источников:

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 24.09.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34661/.

*Анашкин Ю. Н.¹,
исполнительный директор БлокТехнологии,
группы алгоритмы кибербезопасности*

НЕКОТОРЫЕ ПРОБЛЕМЫ ВЫЯВЛЕНИЯ ВНУТРЕННЕГО ПРАВОНАРУШИТЕЛЯ (ИНСАЙДЕРА)

Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации путем уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты указанной информации может осуществляется сотрудником эксплуатирующей организации, т.е. инсайдером.

Крупные индустриальные компании, действующие в сегменте критической инфраструктуры, как правило встроили в свою инфраструктуру достаточно много технических средств защиты. Технические средства защищают от атак, исходящих из-за периметра организации (внешние атаки) – DDOS-атаки, подбор паролей, обход сетевых экранов, заражение вирусами, эксплуатацию уязвимостей операционной системы – достаточно хорошо изучены.

Именно по причине наличия стабильных средств защиты, крупные организации относительно хорошо защищены от внешних атак. Внешние атаки весьма дорогостоящие и гораздо менее экономически выгодны, по сравнению с использованием внутреннего злоумышленника (инсайдера), которого можно купить или принудить шантажом. Инсайдер может, например, своими руками или руками коллег выгрузить конфиденциальные данные на флэш-носитель, переслать через электронную почту, изъять зашифрованный жесткий диск из рабочей станции или сервера, заразить систему вирусом, сделать настройки, снижающие уровень защиты или даже дающие доступ злоумышленникам извне, удалить защищаемую информацию, и т. д., т. е. негласно, пользуясь своими служебными полномочиями и сетевыми привилегиями создать условия для похищения данных или причинения вреда компьютерной сети, или иными словами своеобразной «диверсии». При этом инсайдер может провести ряд легальных процедур, не вызывающих прямых подозрений, но в конечном итоге которые создадут выше названные условия.

В хорошо защищенных системах инсайдерские атаки становится не только более экономически выгодным способом неправомерного воздействия, а часто единственно возможным.

Инсайдерские угрозы можно определить как вредоносные для организации активности, которые исходят от сотрудников внутри организации (периметра защиты), в частности – от действующих работников, бывших работников, подрядчиков, деловых партнеров и даже завербованных работников или работников, специально внедренных в организацию, которые обладают доступом к конфиденциальной информации по своим должностным обязанностям и которые имеют представление о системе управления информационной безопасностью организации.

¹ © Анашкин Ю. Н., 2022.

Получение оперативно значимой информации в целях выявления противоправной деятельности из журналов аудита (логов) действий сотрудников является весьма непростой задачей. Журналы аудита (логи) в крупных организациях, эксплуатирующих мощные компьютерные системы, столь разнообразны, что их следует отнести к Big Data. Поэтому для поиска признаков инсайдерской активности, то есть вкраплений таких признаков в данные о взаимодействиях большого количества пользователей и автоматизированных систем, необходимо научиться оперировать большими объемами текущей информации, анализируя ее и выделяя из нее оперативно значимую информацию [1, с. 26].

Именно этим обусловлено использование в подобном анализе систем с элементами «искусственного интеллекта», с помощью которых обеспечивается выявление искомых признаков в больших данных в режиме требуемых ограничений по времени.

Инсайдер обычно достаточно умен, профессионален, и именно поэтому ему доверен доступ к обработке ценной информации, следовательно, он знает способы, позволяющие обойти основные системы контроля. Таким образом, анализ инсайдерской активности нужно проводить по всему спектру сведений – как из эксплуатируемых технических систем и систем аудита (логов), так и с учетом информации из реальной жизни персонала – данных HR-служб, оперативной информации служб собственной безопасности или детективных агентств, баз данных различного назначения (разного рода справочных систем, в том числе баз правоохранительных и других гос. органов, социальных сетей, данных кадровых агентств и т. д.). Чем разнообразнее исходные данные – тем точнее работа моделей, и тем более тонкие, малозаметные отклонения можно проанализировать (чем «дальше» по своей природе порождения данные друг от друга, тем ценнее их взаимосвязанный анализ).

Поиск основан на том, что инсайдеры порождают аномалии, по которым удастся выявлять признаки их активности. При этом необходимо, чтобы сформированные в процессе такого анализа данные были объясняемы и понятны экспертам по противодействию инсайдерским активностям – работникам оперативных служб безопасности и сотрудникам органов дознания, ведь именно на них в конечном итоге ложится ответственность за принятые решения и их последствия. Например, могут ли выявленные признаки проявиться случайно, за счет больших отклонений при обработке огромного объема собираемых данных. Так существует проблема борьбы с «ложными тревогами», нет ответа на вопрос – можно ли не пропустить вредоносные признаки инсайдера в условиях больших гетерогенных данных, не ясно, как создать техническую систему обработки больших данных, которая реально решает задачи поиска признаков деятельности инсайдеров [2, с. 89].

Другой, юридической проблемой является представление полученных технических данных в таком виде, в котором они являются интерпретируемыми как оперативно значимая информация и допустимая для использования в качестве доказательств.

Таким образом, в настоящее время можно констатировать появление новой важной задачи при выявлении и раскрытии данного вида преступлений – решение научно-технической проблемы поиска признаков действий инсайдеров в Big Data в условиях, больших обновляемых данных при ограничениях на время поиска.

Для решения поставленной научно-технической и научно-юридической проблемы необходимо разработать методы и программные «инструменты» анализа BigData о действиях большого числа пользователей, которые позволяют – выделять признаки вредоносных или деструктивных взаимодействий и событий, а также решить методологическую задачу представления этой информации в виде, позволяющем использовать ее в оперативно-розыскной и процессуальной деятельности и квалифицировать как определенное правонарушение или преступление.

Список использованных источников:

1. Гончар В. В., Орлова А. А. Особенности расследования преступлений, совершаемых в сфере информационных технологий // Безопасность бизнеса. 2021. С. 25–29
2. Смирнов Д. В. Методы поиска признаков инсайдера в BIG DATA : дис. ... канд. тех. наук. М., 2021.

Чурин Р. А.¹,

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

Ращупкина В. А.²,

*научный сотрудник отдела научных исследований
по специальным видам экспертиз
и экспертно-криминалистического обеспечения
противодействия наркопреступности
управления научных исследований
ЭКЦ МВД России*

НЕКОТОРЫЕ ПРОБЛЕМЫ ИССЛЕДОВАНИЯ ЛЕНТОЧНЫХ НАКОПИТЕЛЕЙ ИНФОРМАЦИИ В РАМКАХ СУДЕБНОЙ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ

Одним из принципов обеспечения отказоустойчивости компьютерной системы является архивирование и резервное копирование данных. Резервирование предполагает формирование отказоустойчивости компьютерных систем хранения и обработки информации, при этом полезный объем резервных копий данных может в несколько раз превышать исходный [1].

Основным носителем информации в системах хранения данных является накопитель на жестких магнитных дисках, ввиду чего для таких систем характерны высокая стоимость и затратное энергопотребление. Наиболее подходящей альтернативой для организации резервного копирования и архивирования данных являются ленточные накопители информации (далее по тексту – ЛНИ) как наименее затратные и достаточно надежные, обеспечивающие непрерывную запись больших объемов данных и доступ к ним.

Ленточный накопитель информации – это запоминающее устройство, в котором принцип хранения информации основан на свойстве магнитной ленты сохранять намагниченность. Принцип действия заключается в последовательном доступе к информации. При использовании такого метода записи данные записываются на ленту в виде нескольких параллельных дорожек. Лента, как правило, может двигаться в двух направлениях [2].

Ленточные накопители информации делятся на три типа:

1. Linear Tape-Open (LTO) (открытая линейная лента) – стандарт открытого формата. Ленты совместимы с накопителями разных производителей. LTO использует линейную, многоканальную, змеевидную (возвратно-поступательную)

¹ © Чурин Р. А., 2022.

² © Ращупкина В. А., 2022.

запись на ленту с магнитным сервоприводом для исправления ошибок и аппаратного сжатия данных. Встроенный электронный модуль может хранить и извлекать информацию об использовании и другую информацию о картридже.

2. Digital Linear Tape (DLT) – цифровая линейная лента. Представляет собой адаптацию записи на двухкатушечное базовое вычислительное устройство (reel-to-reel mainframe) [2], где на съемном носителе используется одна катушка ленты, а накопитель обрабатывает приемный конец.

3. Advanced Intelligent Tape (AIT) – усовершенствованная интеллектуальная лента. Использует запись со спиральной разверткой на ленту. Благодаря более высокой плотности битов и более узкой ленте AIT имеют меньшие размеры, чем другие ленточные накопители, что позволяет создавать ленточные библиотеки, которые содержат больше данных, но занимают меньше места. Накопители AIT включают в себя микросхему памяти внутри картриджа для записи и хранения информации о формате и местоположении файла. Это позволяет лентам загружаться быстрее и сокращает время поисков файлов вдвое.

ЛНИ обладают следующими преимуществами:

- большая емкость;
- низкая стоимость;
- удобство хранения;
- стабильность работы;
- низкое энергопотребление.

К недостаткам относятся:

- низкая скорость доступа к данным;
- высокая стоимость устройства записи;
- отсутствие практического опыта работы с устройством и др.

Существование различных по технологии ЛНИ обусловило создание специальных устройств для чтения и записи информации – стримеров. Стример – это запоминающее устройство на принципе магнитной записи на ленточном накопителе, основным назначением которого является запись и воспроизведение информации, архивация и резервное копирование данных [3].

Стримеры классифицируются по технологии (формату картриджей), форм-фактору, интерфейсу, комплектации и производителю. Разнообразие данных устройств может послужить материалом для дальнейшего отдельного научного исследования.

При исследовании ЛНИ эксперты могут столкнуться с существенными сложностями. Например, с отсутствием возможности получения прямого доступа, недостаточным инструментальным оснащением, отсутствием методических рекомендаций, нетиповым построением дисков и др.

Кроме того, ЛНИ могут содержать дифференциальные резервные копии. Технология такого вида резервного копирования предполагает, что полная копия создается единожды в начале, а все последующие содержат не все данные, а лишь произошедшие изменения с момента создания первичной полной копии.

Изъятые ЛНИ до начала и по окончании компьютерного исследования должны храниться с соблюдением температурного режима, условий влажности,

освещения, вне зоны досягаемости магнитных полей. Ввиду того, что ленты хранятся в негерметичной упаковке, они чувствительны к факторам окружающей среды, таким как: влажность, пыль, дым и т. д. Физическое хранение доказательств на магнитной ленте имеет решающее значение. Поскольку каждое физическое считывание ленты (особенно старых или поврежденных лент) может привести к повреждению доказательств, следует предпринять попытки получить данные с как можно меньшим количеством проходов чтения. Если возможно, получение всей информации должно выполняться за один проход чтения.

В некоторых случаях инструменты анализа криминалистического программного обеспечения могут работать непосредственно с извлеченными данными. При отсутствии такой возможности применяются инструменты, использованные для создания архива, они позволяют восстановить архивные данные из файлов. Также могут быть доступны специальные инструменты преобразования или извлечения.

Отдельные производители ЛНИ (например, компания StorageTek, IBM, Dell, Sony и др.) могут предоставлять дополнительные инструменты для решения криминалистических задач, например, могут быть полезны для извлечения информации о конкретном производителе из ленточного журнала.

Существуют многофункциональные коммерческие инструменты, которые собирают и анализируют файлы на магнитной ленте и имеют поддержку поставщиков. Однако зарубежный опыт показал целесообразность использования в работе с ЛНИ средств, встроенных в операционную систему «Linux», располагающую набором бесплатных инструментов, в том числе для извлечения и анализа данных ленточных файлов. Команды операционной системы «Linux» позволяют перемещать ленту, изменять параметры, стирать и извлекать ленту, копировать блоки с ленты на диск. При копировании блоков следует использовать лентопротяжное устройство без перемотки (вследствие этого каждая операция копирования будет помещать головку ленты в файл, готовый к следующей команде). Также работа с этим устройством гарантирует, что лента не будет автоматически перематываться при выполнении каждой операции с ней. Устройство без перемотки позволит скопировать все файлы ленты за один проход чтения.

Отсутствие в экспертно-криминалистических подразделениях системы МВД России специалистов, владеющих Linux-системами, и их востребованность в ИТ-отрасли создают трудности для качественного исследования ЛНИ в рамках судебной компьютерной экспертизы, проводимой в экспертных учреждениях правоохранительных органов Российской Федерации.

Учитывая изложенное, при производстве компьютерных судебных экспертиз, в которых объектом является ЛНИ, необходимо следовать следующим рекомендациям:

- 1) использовать для исследования стример, обеспечивающий полный доступ к информации;
- 2) соблюдать условия хранения изъятых ЛНИ;
- 3) в первую очередь использовать специализированное программное обеспечение от производителя стримера;

4) применять в исследовании средства, встроенные в операционную систему «Linux».

В связи с увеличением количества случаев применения ЛНИ необходимо изучить вопрос оснащения экспертно-криминалистических подразделений системы МВД России стримерами и другим соответствующим оборудованием. Также необходима разработка методических рекомендаций по исследованию ЛНИ для использования при производстве компьютерных экспертиз и исследований, обучении экспертов по программам дополнительного профессионального образования сотрудников МВД России и подготовке учебно-методических материалов по направлению компьютерных экспертиз.

Список использованных источников:

1. Анализ технических решений по организации современных центров обработки данных / [В. А. Докучаев и др.] // Т-Comm, 2017. № 6.
2. Толковый словарь по вычислительным системам / под ред. Е. К. Масловского. М. : Машиностроение, 1989.
3. Большой толковый словарь русского языка // сост., гл. ред. С. А. Кузнецов. СПб. : Норинт, 1998.

Филимонова Ю. В.¹,
курсант факультета подготовки
специалистов в области
информационно безопасности
Московского университета
МВД России имени В.Я. Кикотя

Научный руководитель:
Галиев Д. В.,
преподаватель кафедры информационной
безопасности учебно-научного
комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

ИСПОЛЬЗОВАНИЕ СЕТЕВЫХ УЯЗВИМОСТЕЙ ДЛЯ ПОЛУЧЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ

За последние десятилетия информатизация и информационные технологии проникли во все сферы жизни общества и области человеческой деятельности. Параллельно с масштабным ростом информационных систем в XXI в., растет и необходимость обеспечения новой формы безопасности общества, информационной. Появляются новые формы преступлений, которые связаны с высокими технологиями, получением несанкционированного доступа к удаленным хостам и информации, хранящейся на них. Целостность систем информационной безопасности может быть нарушена по ряду причин: ошибки в разграничении доступа и политике безопасности, неправильная настройка систем выявления факторов неавторизованного доступа в компьютерную сеть или несанкционированное управления ими, уязвимости установленных сервисов или операционной системы, открытые порты, публичные данные о версии операционной системы, пакетах обновлений и запущенных сервисах, которые могут быть подвергнуты атакам эксплойтов. Также устаревшие системы обнаружения вторжений, антивирусы, другие средства защиты и многое другое.

Открывается возможность осуществления определенных атак, используя подобные уязвимости системы. Например, получить доступ к администрированию системы, управлять разграничением прав других пользователей и политикой безопасности системы в целом, получить доступ к информации ограниченного доступа, внедрить вредоносный код и другие, в зависимости от целей и заготовленных сценариев. Вследствие этого возникает необходимость на этапах проектирования, реализации, тестирования, внедрения и сопровождения, администратору системы проводить мониторинг уровня безопасности и защищенности системы, предъявленный к ней.

Для более детального и углубленного рассмотрения тематики данного вопроса обратимся к ГОСТ Р 56546-2015, который трактует информационную систему как

¹ © Филимонова Ю. В., 2022.

совокупность содержащейся в базах данных информации и обеспечивающие ее обработку информационные технологии и технические средства, а ее уязвимость как свойство предоставляющее возможность реализации угроз безопасности такой системы. Она может возникать вследствие ряда причин: ошибка при создании программного обеспечения, недочет инженера, проектировавшего систему, отсутствие постоянной поддержки и предоставления компанией-поставщиком обновлений. Существует официальный структурированный список уязвимостей CVE (англ. Common Vulnerabilities and Exposures), включающий в себя перечень самых распространенных уязвимостей информационной безопасности, где каждой присвоен идентификационный номер вида CVE-год-номер, а также описание и ряд общедоступных ссылок. Как только новая уязвимость и ее описание появляется в открытом доступе, ей может воспользоваться как злоумышленник и производители программного обеспечения для ее закрытия, так и сотрудники правоохранительных органов с целью получения оперативно-значимой информации для расследования преступлений, совершенных с применением информационных технологий.

С целью реализации установленной уязвимости необходим эксплойт, который представляет из себя полноценную программу, обычный скрипт, то есть некую последовательность исполняемых команд, использующую уязвимости программного обеспечения для проведения атаки на компьютерную систему или же словесное описание того, как должна быть реализована та или иная уязвимость. Целью такой атаки будет получение несанкционированного доступа, нарушение целостности и функционирования системы и т. п. Для защиты от подобных программ используются разнообразные антивирусы, системы обнаружения и предотвращения вторжений и межсетевые экраны. Для того, чтобы работа этих программ соответствовала требованиям, предоставляемым к ним, необходима их детальная настройка специалистом по пентестингу.

Деятельность пентестера напрямую направлена на оценку безопасности компьютеров и сетей по средствам моделирования атак злоумышленника. Он использует активный анализ системы на наличие возможных уязвимостей, которые могут стать причиной несанкционированного доступа или изменения конфигурации системы. Реализуется такая деятельность путем проведения совокупности тестом на проникновение. Используя специализированное программное обеспечение, базы данных уязвимостей и эксплойтов, специалист пытается заполучить доступ к компьютерному серверу или целевой системе.

Одним из самых уязвимых мест компьютерной системы являются сетевые порты, поскольку, как только пользователи собираются обмениваться информацией по сети, именно они в первую очередь открывают информационные порталы для обмена. Вообще говоря, порт – это некое виртуальное расширение, дополнение к сетевому адресу. Информация дойдет до вашего компьютера по уникальному адресу узла в компьютерной сети, построенном на основе стека протоколов TCP/IP, но без определенного номера порта, он просто не поймет, как обработать ее и с помощью какого программного обеспечения. Сетевые порты компьютера – это связи между сервисами, которые запущены в операционной системе и дублирующими процессами на компьютерах-хостах, которые

могут находиться на удаленности многих километров. Например, порты с номерами до 1023 в операционных системах считаются наиболее важными для сетевой деятельности, поэтому для доступа к ним и службам, с ними связанными часто требуется наличие самой высокой степени привилегий в изменении системы, например, root в Unix, то есть специального аккаунта, владелец которого имеет право на выполнение всех без исключения операций.

В рамках оперативно-розыскных мероприятий данный метод сбора доказательств относится к такому мероприятию как снятие информации с технических каналов связи.

Снятие информации с технических каналов связи – оперативно-розыскное мероприятие, заключающееся в негласном съеме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям, путем контроля специальными техническими средствами работы соответствующих систем и устройств, в том числе излучаемых ими электромагнитных и других полей [1].

Данное мероприятие может быть осуществлено путем:

- внедрения программных, аппаратных устройств для перехвата информации;
- непосредственного перехвата информации в компьютерных сетях и на линиях связи, расшифровки этой информации;
- внедрением программного обеспечения, нарушающего функционирование систем защиты, воздействующего на паролевые системы защиты, компрометации ключей в целях получения доступа к защищаемой информации.

Лицами уполномоченными на проведение данного оперативно-розыскного мероприятия выступают оперативные сотрудники, осуществляющие оперативно-розыскную деятельность, с использованием оперативно-технических сил и средств органов федеральной службы безопасности, органов по контролю за оборотом наркотических средств и органов внутренних дел. В ряде случаев возможно привлечение организаций, осуществляющих предоставление услуг связи и сообщений (интернет провайдер, компания – владелец линии связи и др.)

Однако стоит принимать во внимание тот факт, что приобщение доказательств к материалам уголовного дела, полученных проведением рассматриваемого ОРМ, нередко может вызывать ряд трудностей, вызванных в первую очередь недостаточной разработанностью нормативно правовой базы, а также правоприменительной практики.

Так, получение доступа к информации лица наказывается уголовным законодательством – ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Подобное получение информации, ее искажение, блокирование, перехват нарушает конституционные права гражданина, закрепленные в ч. 2 ст. 23 Конституции Российской Федерации, в которой говорится, что каждый человек имеет право на тайну переписки, телефонных переговоров, почтовых и иных сообщений, и ограничение данного права возможно только лишь по решению суда.

В данном случае необходимым будет применение данного программного средства в рамках оперативно-розыскной деятельности. В Федеральном законе от 12 августа 1995 г. № 144-ФЗ (ред. от 29.06.2015) «Об оперативно-розыскной

деятельности», в ст. 7 содержатся основания для проведения оперативно-разыскных мероприятий.

Однако приобщение подобных материалов к уголовному делу весьма трудоемкий процесс. Существует межотраслевая инструкция, которая регламентирует порядок предоставления результатов ОРМ в суде: приказ МВД России № 776, Министерства обороны Российской Федерации № 703, ФСБ России № 509, Федеральной службы охраны России № 507, Федеральной таможенной службы № 1820, Службы внешней разведки Российской Федерации № 42, Федеральной службы исполнения наказаний № 535, Федеральной службы России по контролю за оборотом наркотиков № 398, Следственного комитета Российской Федерации № 68 от 27 сентября 2013 г. «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд».

В настоящее время использование сетевых технологий является одним из приоритетных направлений в развитии, как правовой, так и технической базы. Существует ряд задач, которые необходимо выполнить в ближайшее время, для успешного противодействия преступности:

- совершенствование правовой базы, позволяющей использовать сетевые технологии для получения доказательной базы при расследовании преступлений;
- обучение оперативных сотрудников новым сетевым технологиям, применяющимся в настоящее время;
- совершенствовать техническое оснащение оперативных сотрудников.

Таким образом существенное повышение раскрываемости, а также повышение качества материалов, получаемых в рамках расследования преступлений различной направленности, можно получить путем привлечения в оперативную работу кадров, обладающих специальными знаниями в области науки и техники.

Список использованных источников:

1. Кушнир И. В. Оперативно-розыскная деятельность. М., 2010.
2. Информационные технологии в аналитической разведке : учебное пособие / сост. Е. С. Поликарпов. Краснодар : Краснодарский университет МВД России, 2016. 237 с.

Плотников Г. Г.¹,
*профессор кафедры информационной
безопасности учебно-научного
комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук*

О НАДЕЖНОСТИ СИСТЕМ ПЕРЕДАЧИ ИЗВЕЩЕНИЙ

Среди технических средств охраны в настоящее время значительное место занимают системы, использующие проводные каналы связи. Но, проблема зависимости систем централизованной охраны с передачей информации по существующим абонентским телефонным линиям от операторов телефонной связи, является наиболее острой для технического перевооружения вневедомственной охраны.

Несмотря на применение новых цифровых технологий передачи информации о состоянии объектов устройств, наличие сертификатов Минсвязи России, проведение всесторонних эксплуатационных испытаний системы передачи извещений (СПИ) нового поколения не могут гарантированно обеспечить требуемую на сегодняшний день надежность централизованной охраны объектов и квартир граждан. Основной причиной этого является крайняя нестабильность параметров абонентских телефонных линий. Случайно возникающие затухания, изменение волнового сопротивления пары проводов, значительная емкость достаточно протяженных проводов, зависимость сопротивления утечки от погодных условий, доступность проводных коммуникаций вандализму, а также аварийные ситуации в канализационной сети, создают возможность самопроизвольных ложных срабатываний комплексов технических средств охраны (ТСО), как бы сложны и надежны по протоколам передачи данных и восстановлению обнаруженных ошибок они ни были.

Произведенный анализ причин ложных срабатываний систем централизованной охраны показывает, что в последние годы из-за массового применения приборов приемно-контрольных (с встроенными источниками вторичного электропитания, доля ложных срабатываний по вине операторов связи в настоящее время составляет до 60 процентов от общего количества.

Операторы связи, привыкшие не обращать внимание на сопротивление, емкость линии и прочие параметры технических условий (ТУ), на соответствие которым выдавался Сертификат Минсвязи России, крайне часто игнорируют заявки на приведение параметров к паспортным. К тому же настойчивость сотрудников в достижении требуемых параметров абонентской линии на практике приводит к отказу ГТС в последующих кроссировках со ссылкой на причину несоответствия абонентской линии ТУ. Монопольная политика в определении тарифов на услуги электросвязи, к которым относится и предоставление або-

¹ © Плотников Г. Г., 2022.

нентской телефонной линии для услуг централизованной охраны (кроссирование и абонентская плата), также отрицательно сказывается на снижении себестоимости услуг централизованной охраны.

Осложняют складывающуюся ситуацию внедрение новых цифровых технологий в межстанционных соединениях и различные виды уплотнений абонентских телефонных линий для обслуживания большего количества абонентов. Юридические препоны региональных операторов телефонной связи сдерживают использование абонентских линий клиентов ГТС для охраны нетелефонизированных объектов и квартир граждан методами частотного уплотнения. Разработанные способы организации каналов тональной частоты на волоконно-оптических линиях связи не учитывают роста затрат на оплату таких услуг, значительно превышающих затраты на аренду выделенных линий.

Внедрение радиоканальных систем передачи извещений позволяет:

- расширить сферу деятельности как подразделений вневедомственной охраны, так и частных мониторинговых компаний путем организации охраны объектов, не имеющих надежных каналов связи, обеспечивающих оперативную передачу информации;
- повысить надежность систем охраны особо важных объектов за счет дублирования проводных каналов связи;
- обеспечить при необходимости оперативную установку оборудования на объекте, нуждающемся в охране.

Действительно, РСПИ уже заняли свое место в охранной индустрии и эффективно используются как подразделениями вневедомственной охраны, так и частными охранными предприятиями. Но как же выбрать систему, способную наиболее эффективно работать в конкретных условиях. Современная РСПИ – это большой комплекс программных и аппаратных средств, куда относятся не только оборудование пункта централизованной охраны (ПЦО), но и комплекты разнообразных объектовых систем. Очевидно, что организациям, которые эксплуатируют или хотят развернуть РСПИ, приходится сталкиваться со множеством разнообразных и достаточно сложных вопросов.

Объективная реальность показывает, что полноценный мониторинг объектов различных типов не может быть эффективно организован каким-то одним типом РСПИ. Это происходит из-за различных критериев эффективности в подходе к оценке мониторинга состояний различных объектов. Зачастую предлагаются услуги мониторинга исходя прежде всего из-за одного критерия – стоимости, при этом достаточно очевидно, что, например, такие важные показатели как надежность и достоверность будут весьма ущербны, что в конечном итоге скажется и на эффективности системы безопасности объекта.

Считается, что современные беспроводные системы, обладающие гибкой архитектурой и имеющие в своем составе дополнительные подсистемы, имеют высокую стоимость, а их обслуживание является делом чрезвычайно сложным. Однако практика применения современных коммуникационных технологий показывает, что стоимость объектовых комплектов таких систем приближается к стоимости проводных объектовых приборов, а стоимость базовых станций, ретрансляторов и ПЦН вообще мало отличается от стоимости проводных аналогов.

При этом обслуживание таких систем даже проще, в первую очередь за счет отсутствия необходимости взаимодействия с компаниями-операторами проводных сетей.

Список использованных источников:

1. Плотников Г. Г., Родин С. В., Солодуха Р. А. Вероятностная модель передачи сообщений в условиях воздействия помех в радиосистемах передачи извещений // Вестник Воронежского института МВД России. 2006. № 1 (26). С. 99–104.

Бондарь К. М.¹,
*профессор кафедры информационного
и технического обеспечения ОВД
Дальневосточного юридического
института МВД России,
кандидат технических наук, доцент,*

ИНФОРМАЦИОННОЕ МОДЕЛИРОВАНИЕ КРИМИНОГЕННОЙ ОБСТАНОВКИ

Организационная и управленческая деятельность органов внутренних дел России базируется на аналитических исследованиях криминогенной обстановки и применении эффективных методов управления силами и средствами. Действенную помощь при этом способно оказать информационное моделирование. Научно-практическим направлением, которое перспективно для указанных целей и предоставляет требуемый уровень возможностей, является имитационное моделирование. Оно обладает разнообразными вычислительными возможностями, реализуемыми на современных программных платформах. В результате оно способно удовлетворить субъектов аналитической работы в исследовании криминогенной обстановки и подготовке обоснованных решений по управлению силами и средствами органов внутренних дел.

Глубокие аналитические исследования криминогенной обстановки и принимаемые на их основе решения по управлению имеющимися силами и средствами являются важнейшими направлениями деятельности органов внутренних дел (ОВД) России. Выполнение при этом трудоемких расчетных задач еще на рубеже 70–80-х гг. XX в. обусловило необходимость обращения к методам информационного моделирования [1].

Под информационной моделью объекта будем понимать его *представление в виде информации, отражающей существенные для него параметры и переменные, а также связи между ними, входо-выходные характеристики объекта, позволяющее путем подачи на модель изменений входных величин имитировать возможные состояния объекта*. Сегодня аналитика базируется на приоритетности модельных описаний, выполняемых именно с применением перспективных имитационных платформ.

Понятием «криминогенная обстановка», имеющем прикладной характер, обозначается совокупность взаимодействующих явлений, процессов, факторов, значимых для принятия решений по борьбе с преступностью и охране общественного порядка. Именно криминогенная обстановка выступает основным объектом практического анализа, включая в себя многообразие различных сторон объективной реальности, которые оцениваются в процессе организации деятельности ОВД.

В числе основных направлений информационного моделирования выступают аналитические и имитационные модели. Аналитическое моделирование стало исторически первым и довольно распространенным подходом в управленческой

¹ © Бондарь К. М., 2022.

деятельности ОВД. Внедрение же в практику их аналитической работы компьютерной техники привело к быстрому развитию имитационного моделирования, которое обеспечило реализацию разнообразных моделей развития криминогенной обстановки, управления силами и средствами ОВД.

Охарактеризуем имеющийся опыт информационного моделирования, проблемные вопросы и пути их разрешения.

Опыт и перспективы информационного моделирования. Работу в данном научно-практическом направлении достаточно активно проводили ведущие учреждения системы МВД, свои достижения внедряли в практику крупные ученые. Важной особенностью модельных исследований стала интеграция развитых математических методов и информационных технологий, а также переход от аналитической к имитационной методологии. В результате сформировались многие концептуальные понятия криминогенной обстановки, созданы и апробированы перспективные математические модели управления ресурсами ОВД, развивались научные школы в области информационного моделирования, совершенствовалось методическое обеспечение аналитической деятельности в ОВД.

Из всего многообразия выполненных в то время исследований стоит обратить внимание на работу по долгосрочному прогнозированию развития криминальной ситуации в Российской Федерации [2]. В состав коллектива, выполнившего данную фундаментальную задачу, вошли М. А. Алексеева, М. М. Бабаев, Н. Я. Заблоцкис, Г. Ф. Коимшиди, Е. А. Коновалова, В. И. Кононенко, Н. В. Кузнецова, С. В. Максимов, В. А. Минаев, В. И. Селиверстов, Г. К. Синилов, А. Д. Шестак, О. В. Яковлев.

Работа осуществлялась по решению Правительства Российской Федерации [3] на основе статистических данных о ведущих показателях криминогенной обстановки в стране за прошедший период в 25 лет. В ней сконцентрированы передовые по тому времени методы долгосрочного прогнозирования и, следовательно, реализован стратегический уровень поддержки решений в области управления силами и средствами ОВД.

Результаты прогнозирования были представлены по разным видам и группам статистических показателей на периоды от 5 (с 1996 по 2000 гг.) до 10 лет (с 1996 по 2005 гг.). Примененный в работе многомерный кластерный анализ позволил выделить на территории страны однородные группы регионов по состоянию криминогенной обстановки. Это позволило провести сравнительный анализ полученных территориальных кластеров по ее различным показателям.

Успешное выполнение указанной работы уже на тот период подтвердило наличие развитых математических и информационных технологий, способных обосновать стратегические решения развития ОВД. Последующее развитие криминальной ситуации в стране показало адекватность прогнозов.

Однако сегодня приходится констатировать, что подобные исследования больше не проводилось по ряду организационных, информационно-технологических и иных причин. С точки зрения теории и практики управления, отсутствие результатов более современного стратегического прогнозирования снизило качество обоснования и принятия решений в сфере оценки криминогенной обстановки и реализации требуемого управления ресурсами ОВД.

Необходимо отметить, что текущее состояние модельных и прогностических исследований, характеризуемое отставанием отечественных разработок от зарубежных аналогов в указанной области, требует новых шагов в развитии и масштабном внедрения в аналитическую деятельность ОВД современных моделей, методов и технологий.

Конечно, работа в направлении использования и развития, ставших уже классическими аналитических подходов, безусловно, продолжается [4–6]. Проводимые процедуры при этом ориентируются на типовые алгоритмические шаги, но в концептуальном плане ограниченные возможностями исследования внутренней структуры криминогенной обстановки как объекта. Данный подход, позволяет более качественно обосновывать принимаемые решения, однако без получения новой информации о состоянии и динамике криминогенной ситуации. Такие возможности призваны предоставлять, например, развитые имитационные модели.

Поэтому интерпретация полученных результатов проходит без глубокого модельного обоснования происходящих криминологических процессов и отсутствия реальной возможности «проигрывания» различных сценариев, вариантов развития криминогенных процессов и альтернатив управления ОВД. В результате сложно описать возможный ход событий, оценить их значимость для деятельности ОВД и обосновать выбор ресурсных затрат для достижения нужного прогнозного развития криминогенной обстановки на определенную перспективу.

Особым потенциалом при этом обладает развиваемая система информационно-аналитического обеспечения деятельности МВД России – ИСОД МВД России. Она предполагает реализацию большинства перспективных технологий – поддержку обработки больших данных, расширение интеллектуальной составляющей при аналитических исследованиях, а также имитационного моделирования. Развитию названной системы может способствовать создание имитационных компьютерных платформ отечественного производства типа *Anylogic*. Они обладают перспективным набором исследовательских характеристик и, кроме всего, могут обеспечить качественное обучение сотрудников ОВД информационно-аналитической деятельности современного уровня применительно к самым различным задачам, возникающим в деятельности их подразделений.

Продemonстрируем реальность этого утверждения на результатах двух авторских исследований рассматриваемой предметной сферы.

Обратимся к примеру моделирования динамики преступности, в быстроразвивающемся регионе при разной эффективности использования кадровых ресурсов ОВД.

Не вдаваясь в содержательное описание примененной модели, детально представленной в [7], приведем базовую модель динамики региональной преступности. Исходя из криминологических концепций относительно «воспроизводства» преступности, построена модель, в которой выделено шесть состояний индивидов:

– *состояние 1* формируют законопослушные индивиды, не нарушающие уголовно-правовых запретов. Сюда же относится категория индивидов, отбывших наказания за ранее совершенные преступления и прекративших преступную деятельность. Обозначим их совокупность переменной $N(t)$;

– в *состояние 2* входят лица, совершившие преступления, но не выявленные в этой связи правоохранительными органами, т.е. так называемые латентные преступники. Их совокупность – переменная $X(t)$;

– в *состоянии 3* сгруппированы индивиды, совершившие преступления, в отношении которых осуществляются судебные-следственные мероприятия – переменная $Y(t)$;

– *состояние 4* формируют осужденные к наказанию, связанному с лишением свободы, а также осужденные условно – переменная $Z(t)$;

– *состояние 5* формируется из неустойчивой категории лиц, ранее судимых, при определенных обстоятельствах способных совершить новые преступления или при некотором сочетании факторов полностью порывать с преступным прошлым – переменная $S(t)$;

– в *состояние 6* входят ранее судимые, имеющие после освобождения установку на совершение преступлений и активно ищущие условия для реализации криминального акта, – переменная $R(t)$.

Модель устанавливает статистическую зависимость между числом индивидов, которые будут находиться в указанных состояниях в тот или иной момент времени, параметрами, отражающими переходы между состояниями, а также потоки индивидов, поступающих в систему и выходящих из нее.

Выделенные состояния связаны переходов, показанных на *рис. 1*.

Адекватность формализованного описания соответствующей информационной модели зависит от используемых при этом положений и гипотез, выбор и принятие которых представляют достаточно трудную и нестандартную задачу. Эти положения и гипотезы, образующие концептуальное основание модели, отражают уровень соответствующих теоретических представлений о преступности, а также результаты специальных эмпирических исследований преступности.

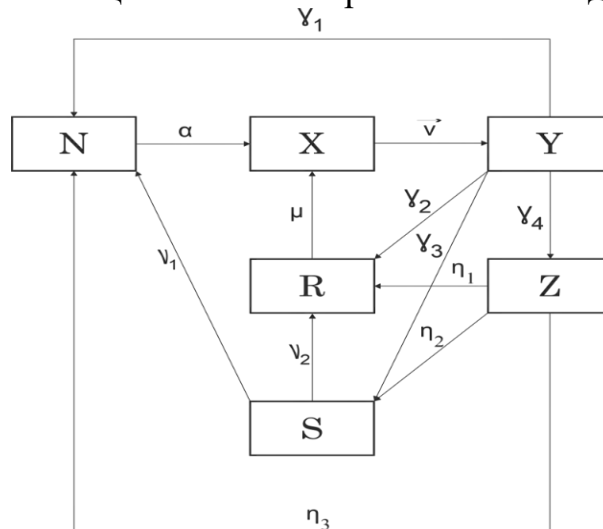


Рис. 1. Блок-схема модели динамики региональной преступности

В основу динамической модели преступности положены следующее предположения.

Во-первых, считалось, что поток, отражающий воспроизводство новых преступников среди ранее несудимых – $W_1(t)$, зависит от общей численности невыявленных преступников и пропорционален ей (коэффициент пропорциональности – α), т. е.:

$$W_1(t) = \alpha \cdot X(t). \quad (1)$$

Во-вторых, предположено, что поток преступников среди ранее судимых (рецидивисты) пропорционален произведению числа ранее судимых, имеющих установку на совершение преступлений, и числа невыявленных преступников (коэффициент пропорциональности – μ):

$$W_2(t) = \mu \cdot X(t) \cdot R(t). \quad (2)$$

В-третьих, описание процесса выявления преступников осуществлялось, исходя из предположения, что численность преступников, выявляемых в единицу времени, зависит от двух факторов:

- а) реальной численности преступников в регионе;
- б) ресурсной обеспеченности ОВД людскими силами и материально-техническими средствами.

Конкретное функциональное представление зависимости числа выявленных преступников от числа невыявленных преступников и ресурсной обеспеченности ОВД сделано с учетом следующих предположений:

– увеличение реальной численности преступников при фиксированных ресурсах приводит к увеличению численности выявленных. Однако вследствие ограниченной «пропускной способности» ОВД, определяемой конкретной ресурсной обеспеченностью, зависимость числа выявленных преступников от количества латентных непропорциональна (несмотря на увеличение количества выявленных преступников, их доля в общей массе лиц, совершивших преступления, уменьшается);

– в связи с ростом ресурсной обеспеченности увеличиваются абсолютное количество выявленных преступников и их доля по отношению ко всем преступникам. Но все более полное выявление лиц, совершающих преступления, требует непропорционального роста трудозатрат. Отсюда по мере увеличения ресурсной обеспеченности ОВД количество выявленных преступников, приходящееся в среднем на одного работника, должно снижаться. Это связано с необходимостью применения все более совершенных методов оперативно-розыскной деятельности при раскрытии все более замаскированных преступлений.

Здесь уместно провести аналогию с освоением природных ресурсов, где также наблюдается непропорциональный рост трудовых затрат по мере все более полного освоения. Это определяется необходимостью разработки более глубоко залегающих и труднодоступных месторождений, внедрения более современной и дорогостоящей технологии и т. д. Применительно к деятельности зарубежной полиции отмечается нелинейная зависимость результатов ее деятельности

от размера вложенных ресурсов: при увеличении штатов на 1 % раскрываемость преступлений возрастает лишь на 0,5 %.

Хорошо интерпретируемым представлением зависимости числа выявленных преступников от ресурсной обеспеченности и реального числа преступников является следующее:

$$V(t) = a_0 \cdot F(t) \cdot (1 - \exp(-a_1 \cdot X(t)/F(t))), \quad (3)$$

где a_0 и a_1 – некоторые постоянные положительные параметры; $F(t)$ – некоторый обобщенный ресурс, в интегральном виде учитывающий ресурсную обеспеченность (во всех ее разновидностях) ОВД.

С учетом высказанных предположений базовая модель динамики преступности приобретает вид:

$$\begin{aligned} N(t) &= M(t) - X(t) - Y(t) - R(t) - Z(t) - S(t); \\ X(t+1) &= X(t) + \alpha \cdot X(t) + \mu R(t) \cdot X(t) - V(t); \\ Y(t+1) &= Y(t) + V(t) - \sum_{i=1}^{i=4} \Upsilon_i \cdot Y(t); \\ Z(t+1) &= Z(t) + \Upsilon_4 \cdot Y(t) - \sum_{i=1}^{i=3} \eta_i \cdot Z(t); \\ S(t+1) &= S(t) + \Upsilon_3 \cdot Y(t) + \eta_2 \cdot Z(t) - (v_1 + v_2) \cdot S(t); \\ R(t+1) &= R(t) + \Upsilon_2 \cdot Y(t) + \eta_1 \cdot Z(t) + v_2 \cdot S(t) - \mu \cdot R(t) \cdot X(t); \\ V_1(t) &= a_{01} \cdot F_1(t) \cdot [1 - \exp(-a_{11} \cdot X(t)/F_1(t))]; \\ V_2(t) &= a_{02} \cdot F_2(t) \cdot [1 - \exp(-a_{12} \cdot X(t)/F_2(t))]; \\ V_3(t) &= \beta_3 \cdot X(t), \end{aligned} \quad (4)$$

где $M(t)$ – численность криминологически активного населения (лица в возрасте 14–60 лет); $V_1(t)$, $V_2(t)$, $V_3(t)$ – соответственно, число преступников, выявленных в связи с правонарушениями, регистрируемых по линии уголовного розыска, экономических преступлений, иных служб; $F_1(t)$ и $F_2(t)$ – обеспеченность кадрами аппаратов уголовного розыска и борьбы с экономическими преступлениями.

Одним из практических применений базовой модели (4) стало исследование взаимосвязи показателей динамики зарегистрированной преступности и кадрового обеспечения ОВД в быстро развивающемся регионе.

На *рис. 2* показана динамика зарегистрированной преступности на прогнозный период в зависимости от значения параметра a_0 , характеризующего эффективность использования кадровых ресурсов. Как показывают расчеты, увеличение параметра a_0 сказывается в снижении реальной и зарегистрированной преступности к концу прогнозного периода.

Другие примеры использования информационного моделирования в деятельности ОВД приведены для исследования противодействия терроризму и экстремизму в работах [8–9].

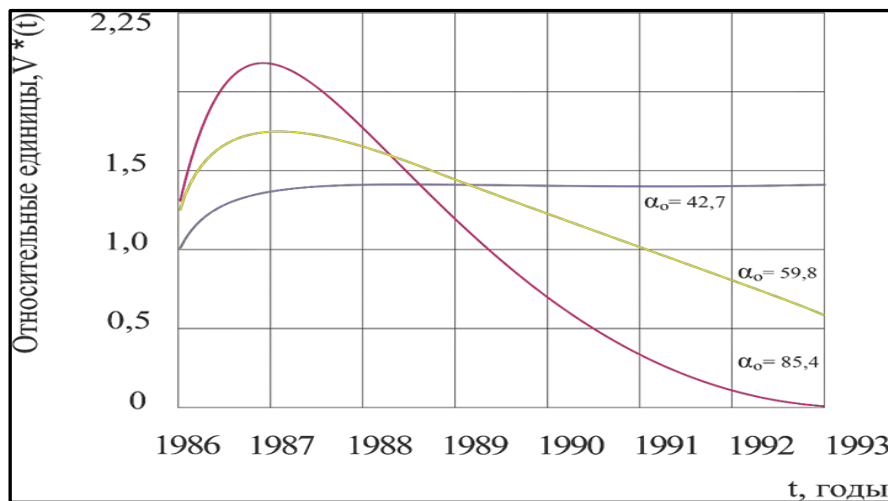


Рис. 2. Динамика зарегистрированной преступности при различных значениях параметра α_0 – эффективности кадровых ресурсов

Обсуждение и выводы. Приведенные результаты применения математического моделирования в решении задач анализа, оценки и прогнозирования криминогенной обстановки, совершенствования на этой основе информационно-аналитической деятельности ОВД по обоснованию решений по управлению силами и средствами ОВД, убедительно показывают актуальность, перспективность и научно-практическую значимость рассматриваемой методологии.

Вместе с тем, последние два десятилетия показали существенное снижение в развитии методологии математического моделирования как эффективного инструментария в управлении ОВД, раскрывающего принципиально новые возможности обработки больших объемов информации, приближающего реализацию концепций искусственного интеллекта при поддержке управленческих решений.

В то же время, более рациональная и целенаправленная загрузка ИСОД МВД России задачами, базирующимися на концепциях системного математического моделирования, для реализации которых она и создавалась, пока мало используемый ресурс.

А ведь имеющиеся теоретические и практические достижения в имитационном подходе к «проигрыванию» вариантов развития криминогенной обстановки, управления ресурсами ОВД России сегодня подкреплены не только возросшим уровнем современного компьютерного парка, но и наличием развитых программных платформ для информационного имитационного моделирования.

Список использованных источников:

1. Распоряжение Правительства Российской Федерации от 31 декабря 2020 г. № 3684-р «Программа фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021–2030 гг.)» // СПС «Консультант Плюс». URL: <http://www.consultant.ru/>.
2. Долгосрочный прогноз развития криминальной ситуации в Российской Федерации / [Алексеева М. А. и др.]. М. : Академия МВД России, ВНИИ МВД России, 1996. 66 с.

3. Постановление Правительства Российской Федерации от 27 ноября 1995 г. № 1170 «О разработке прогноза и программы социально-экономического развития Российской Федерации на 1996–2000 гг., прогноза и концепции социально-экономического развития Российской Федерации на 1996–2005 гг.» // СПС «Консультант Плюс». URL: <http://www.consultant.ru/>.
4. Федорова О. Б., Хейло Л. Г. Статистические методы анализа, оценки и прогнозирования оперативной обстановки : учебно-методическое пособие. М. : ОАД МВД России, 2018. 85 с.
5. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналитический обзор / [Ю. М. Антонян и др.]. М. : ВНИИ МВД России, 2018. 86 с.
6. Ульянов А. Д., Захватов И. Ю., Болдырев У. К. Оперативная обстановка: понятие, анализ, прогноз : учебное пособие. М. : Академия управления МВД России, 2020. 104 с.
7. Минаев В. А. Кадровые ресурсы органов внутренних дел: современные подходы к управлению. М. : Академия МВД СССР, 1991. 163 с.
8. Андреев А. А., Бондарь К. М., Минаев В. А. Терроризм и экстремизм: моделирование информационного противодействия : монография. Хабаровск : Дальневосточный юридический институт МВД России, 2020. 248 с.
9. Киракосян А. Э., Минаев В. А., Сычев М. П. Моделирование информационного противоборства в социальных медиа : монография / под общ. ред. В. А. Минаева. М. : Наука, 2020. 152 с.

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

ВЫБОР НАИЛУЧШЕЙ МОДЕЛИ ИДЕНТИФИКАЦИИ ДЕСТРУКТИВНОГО КОНТЕНТА В СОЦИАЛЬНЫХ МЕДИА

Эффективными моделями классификации контента деструктивного характера в социальных медиа являются модели искусственного интеллекта. Формальная постановка задач заключалась в том, чтобы с достаточным уровнем точности отделить текст деструктивного характера от допустимого контента, похожего синтаксически, но отличающегося семантически (шумового контента). Анализировался смешанный контент, состоящий из текстов Федерального списка экстремистских материалов и из материалов социальных медиа, включая социальные сети ВКонтакте, Одноклассники и др., а также системы обмена мгновенными сообщениями Telegram, WhatsApp и т. п. Корпуса исследуемых деструктивных текстов включали материалы антисемитской направленности, прославляющие нацизм, продвигающих идеологию радикального ислама. Все реализованные модели искусственного интеллекта показали высокое качество выявления экстремистского контента при учете шумовых эффектов (не менее 82 %). При этом наиболее результативной является модель BERT (97 %). Сделан вывод, что в статье предложена и практически реализована эффективная методика выявления и идентификации контента экстремистской направленности в социальных медиа, базирующаяся на применении нейронных сетей как перспективного направления искусственного интеллекта.

На современном этапе развития российского общества наблюдается существенное возрастание угроз кибербезопасности, в числе ключевых из которых в Доктрине информационной безопасности Российской Федерации названы информационно-психологические воздействия (ИПВ) на индивидуальное, групповое и общественное сознание.

Отмечается рост распространения контента экстремистского характера, к которому относятся материалы с прославлением нацизма, содержащие призывы радикальных исламистов, обращения, направленные на развитие расизма и криминальной культуры в обществе, насильственный захват власти и активизацию противоправной деятельности. Особенно опасно, что такой контент, в первую очередь, направлен на подростков и молодежь, которые активно используют современные информационные системы и коммуникационные сети, заражаясь через них экстремистскими идеями.

В связи с широким охватом различных социальных групп аудитории, а также не всегда эффективным контролем со стороны противодействующих структур,

¹ © Минаев В. А., 2022.

манипуляторы в социальных медиа (СМ) совершенствуют механизмы образования и распространения контента деструктивного характера.

Государственные органы Российской Федерации активно противодействуют распространению деструктивных материалов. Так, современный этап развития правоохранительной системы России характеризуется ускоряющимся использованием информационно-аналитических систем в управлении социальными процессами, включая перспективные технологии искусственного интеллекта. Для целей выявления и идентификации контента экстремистского характера в СМ эффективно используются математические методы анализа, имеющие высокий уровень устойчивости к шумовым эффектам при классификации текстового материала. Такие работы активно ведутся как российскими [1–4], так и зарубежными [5–7] учеными.

Целью исследований, приводящихся в Московском университете МВД России имени В. Я. Кикотя, является оценка и поиск классификаторов, имеющих высокий уровень устойчивости к шумовым эффектам при выявлении манипулятивного текстового контента в СМ на примере информационных сообщений экстремистского характера.

Автоматизация – как основное направление противодействия. Социальные медиа включают не только известные социальные сети ВКонтакте, Одноклассники и другие, но и системы обмена мгновенными сообщениями – Telegram, WhatsApp и т. п. В СМ осуществляется рабочее взаимодействие между сотрудниками учреждений, общение с друзьями и близкими, публикация и обсуждение новостей, а также реализация развлекательного контента. Основным форматом контента для распространения был и остается текстовый, как наиболее удобный в распространении, передаче и изменчивости.

Выявление деструктивного контента в СМ осуществляют как с использованием автоматизированных систем (АС), так и в результате экспертных процедур. Поскольку ежемесячно создается более миллиарда новых текстовых публикаций – основные направления поиска социально опасного контента в СМ связываются с автоматизированными системами, так как проводить качественный анализ такого объема новых публикаций с привлечением человека-эксперта просто невозможно.

В этой связи при разработке и модификации такого рода АС необходимо учитывать точность их работы, связанную с шумостойкостью. Под термином «шумостойкость» определим способность АС с необходимой вероятностью отделять контент деструктивного характера от допустимого контента, похожего синтаксически, но отличного семантически, далее называемом шумовым.

Настоящая статья посвящена оценке шумостойкости различных моделей обнаружения деструктивного контента.

Модели классификации. Для проведения экспериментальных исследований шумостойкости различных моделей выбраны следующие корпуса текстов: СМК – корпус контентов из социальных медиа, в который вошли русскоязычные публикации в «Twitter» и новости интернет-издания «Lenta.ru», моделирующие основное наполнение СМ; РК – радикальный корпус, состоящий из запрещенных к рас-

пространению в России текстов по теме радикального ислама; ШК – шумовой корпус, включающий религиозную литературу, одобренную муфтиями России.

Автором осуществлен анализ не менее десятка моделей интеллектуальной классификации применительно к деструктивному контенту. Среди них выбраны три наиболее перспективные: алгоритм машинного обучения – метод опорных векторов (SVM – Support Vector Machines) [8], классификатор на основе рекуррентной нейронной сети (GRU – Gated Recurrent Units) [9], а также классификатор текста на основе искусственных нейронных сетей (трансформер BERT – Bidirectional Encoder Representations from Transformers) [10].

SVM – один из распространенных методов обучения, основная идея которого заключается в построении гиперплоскости, разделяющей исследуемые объекты оптимальным образом.

GRU – рекуррентная нейронная сеть с памятью, при решении целого ряда задач показывающая аналогичные или более высокие результаты.

BERT – известный трансформер для классификации текста, состоящий примерно из двух десятков искусственных нейронных сетей.

Оценены их свойства и влияние шумовых факторов на качество классификации экстремистского контента.

Обработка текстов из CM до подачи на вход классификатора различается для моделей SVM, GRU и BERT. Так, для SVM и GRU в целях получения качественных результатов, в первую очередь, необходимо провести процедуру лемматизации – замену формы слова ее основой. После этого, в частности, для классификатора SVM производится операция векторизации по методу TF-IDF.

Так как классификатор на основе BERT учитывает информацию, хранящуюся в суффиксах и окончаниях – проведение процедуры лемматизации для BERT нецелесообразно.

Далее для GRU и BERT следует процедура токенизации – преобразования составляющих текстового контента в числовую последовательность. После этого числовая последовательность подается на вход указанных классификаторов.

Для оценки работы классификаторов использовалась F -мера:

$$F = (P_{rec} \cdot R_{ec}) / (P_{rec} + R_{ec}),$$

где P_{rec} – определенность работы классификатора, рассчитываемая как:

$$P_{rec} = TP / (TP + FP)$$

R_{ec} – полнота работы классификатора, рассчитываемая по формуле:

$$R_{ec} = TP / (TP + FN),$$

где TP – истинно-положительное решение классификатора;

TN – истинно-отрицательное решение классификатора;

FP – ложноположительное решение классификатора;

FN – ложноотрицательное решение классификатора.

F -мера учитывает как полноту, так и определенность классификации, что позволяет более объективно оценивать качество модели.

Для оценки шумостойкости указанных трех моделей проведена первая серия

из 5 экспериментов:

Эксперимент № 1 – моделирование ситуации, при которой отсутствуют шумовые текстовые корпуса, а присутствует только СМ-контент и радикальные тексты.

Эксперимент № 2 – моделирование ситуации, в которой применяется классификатор, обученный на выборке из эксперимента № 1, то есть только на СМ и радикальном корпусах, но классифицирует в том числе и тексты из шумового корпуса, добавленные в СМ класс. Целью эксперимента является оценка того, насколько снижаются результаты классификатора, если при его обучении не учитывать шумовые составляющие.

Эксперимент № 3 – расширение классификатора текстов путем добавления шумового класса. В данном случае применяется F -мера по трем рассматриваемым классам с целью учета влияния шумового корпуса на радикальный.

Эксперимент № 4 – применение бинарной классификации, когда тексты разделяются на 2 класса – нерадикальный и радикальный. Причем в нерадикальном корпусе смешиваются корпус СМ с шумовым корпусом.

Эксперимент № 5 – создание сложной модели, состоящей из двух последовательных классификаций. Первая отделяет СМ от совместного класса шумового и радикального корпуса, а вторая – разделяет шумовой и радикальный класс. Тем самым проверяется гипотеза снижения ошибок первого рода за счет двойной классификации.

Сравнение шумостойкости моделей. На *рис. 1* представлены измерения F -меры всех классификаторов, используемых в экспериментах.

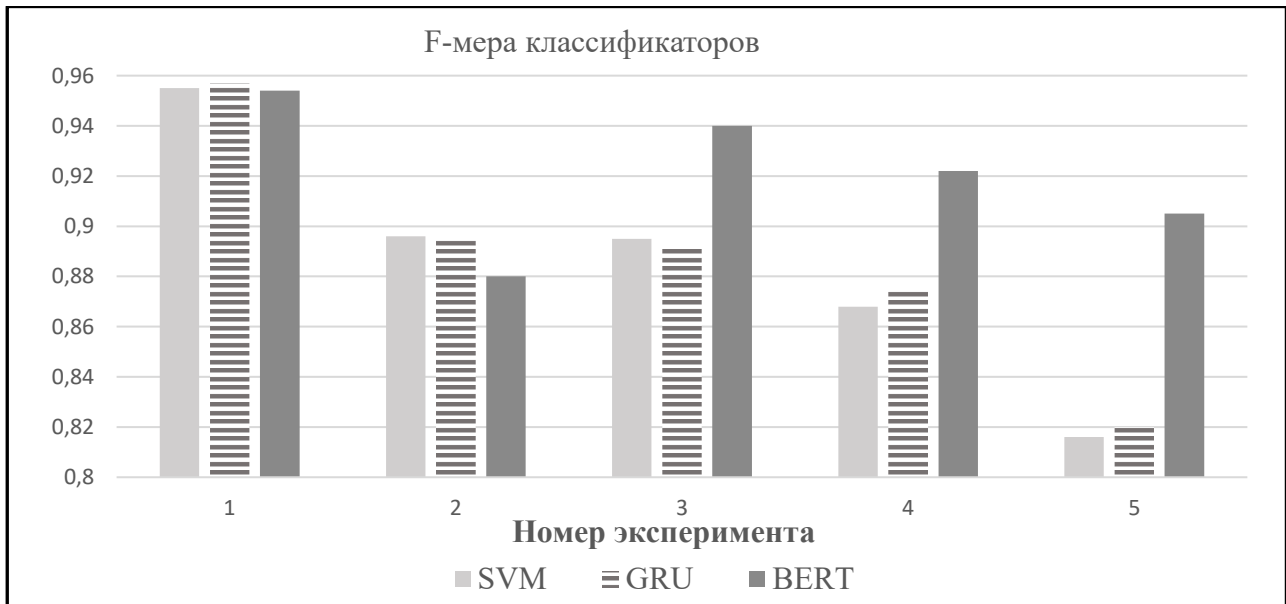


Рис. 1. Значения F -меры классификаторов, используемых в экспериментах

Как следует из *рис. 1*, все три классификатора при отсутствии шумовых факторов показывают одинаковое качество работы. Однако при добавлении шумового контента наиболее шумостойким является классификатор на основе BERT (эксперименты 3–5). При этом наиболее результативным является модель BERT с бинарной классификацией (эксперимент № 3).

Сравнение точности моделей по идентификации контента. Во второй серии проведены компьютерные эксперименты по выявлению наиболее точной модели искусственного интеллекта по идентификации экстремистского контента по его различным направлениям (антисемитизм, реабилитация нацизма, радикальный ислам).

При этом анализировался смешанный контент, состоящий из двух примерно равных частей – из текстов Федерального списка экстремистских материалов [11] и из материалов СМ, включая известные социальные сети ВКонтакте, Одноклассники и др., а также системы обмена мгновенными сообщениями Telegram, WhatsApp и т. п. Корпуса текстовых массивов состояли каждый примерно из трехсот тысяч предложений экстремистской направленности со средним количеством слов в них, равном 14, а также шумового корпуса из СМ (материалы, не являющиеся экстремистскими). Характеристики корпусов экстремистского характера приведены в *табл. 1*.

Таблица 1

Объем исследованных текстовых массивов экстремистской направленности

Характер текстового деструктивного массива	Количество предложений, тыс.
Антисемитизм	268
Реабилитация нацизма	284
Радикальный ислам	310

Проведены компьютерные эксперименты с указанным выше объемом текстового материала для поиска наиболее точной модели искусственного интеллекта по идентификации контента экстремистского характера. При этом для обучения нейронных сетей выявлению экстремистского контента использовался Федеральный список экстремистских материалов [11].

Основные этапы выявления контента экстремистской направленности в СМ:

1. Формирование текстовых массивов, содержащих экстремистскую идеологию.
2. Нахождение наилучшей модели выявления контента экстремистской направленности.
3. Распознавание контента экстремистской направленности наилучшей модели.

Как видно из *табл. 2*, все упомянутые в статье модели искусственного интеллекта показывают достаточно высокое качество выявления экстремистского контента (не менее 82 %) при учете шумовых эффектов. При этом наиболее результативной также выступает модель BERT (92 %). В итоговом варианте модель RuBERT-base показала результат 97 %.

Таблица 2

**Точность методов искусственного интеллекта по выявлению контента
экстремистской направленности**

Модель искусственного интеллекта	Точность выявления, %
Модель опорных векторов (SVM)	82
Рекуррентная нейронная сеть (GRU)	82
Трансформер BERT	95

Из *табл. 3* очевидна очень высокая точность распознавания текстовых массивов экстремистской направленности, если использовать автоматизированную систему анализа контента.

Таблица 3

**Точность распознавания текстовых массивов
экстремистской направленности**

Характер текстового деструктивного массива	Точность распознавания, %
Антисемитизм	91
Реабилитация нацизма	93
Радикальный ислам	95

Итоговые результаты классификации по моделям RuBERT-base и RuBERT-tiny2 после процедуры доменной адаптации

Таблица 4

Точность распознавания текстовых массивов с прославлением нацизма

Модель BERT	<i>F</i>-мера
RuBERT-base	0,97
Rubert-tiny2	0,96

Как видно из *табл. 4*, доменная адаптация позволила повысить *F*-меру классификации модели ruBERT-base до 97 %, однако для модели Rubert-tiny2 доменная адаптация не принесла какого-либо значительного роста результатов.

Отметим, что в сложных случаях, когда с помощью АС не удастся идентифицировать деструктивность текстов, составляющих 5–9 %, как это следует из *табл. 3*, следует привлекать профессионалов-экспертов (*рис. 3*).

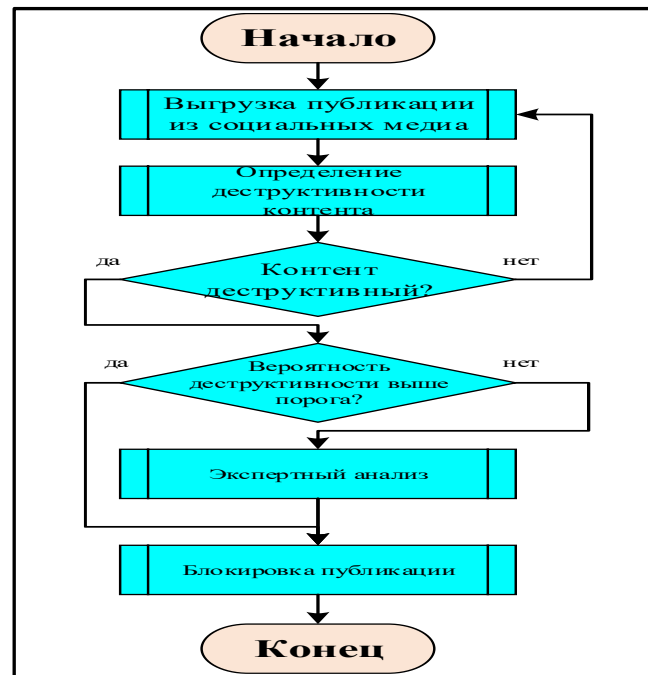


Рис. 3. Алгоритм автоматизированного распознавания и блокировки контента деструктивной направленности с привлечением экспертов

Обсуждение и выводы. В заключение подчеркнем, что на современном этапе развития российское общество характеризуется ускоряющейся цифровизацией, и новые разработки в области анализа и прогнозирования деструктивных информационно- психологических воздействий могут стать серьезным вкладом в борьбу с криминальными проявлениями в обществе, особенно с терроризмом и экстремизмом, информационно все активнее и заметнее проявляющихся в социальных медиа. Нужно также учитывать и огромный манипулятивный потенциал иных воздействий в социальных медиа, направленных на отдельные группы населения, в частности, подростков и молодежь, воинские контингенты, правоохранительные структуры.

Учитывая многоплановость, обширный спектр информационно-психологических аспектов проблемы кибербезопасности, ее серьезный научный и практический объем и потенциал, исследования в этом направлении предполагают решение многих новых задач анализа, оценки и прогнозирования распространения деструктивной информации в информационных сетях.

Для практики ценность полученных при этом научных результатов заключается в новых возможностях методологического и методического обеспечения аналитической деятельности, связанной с обработкой и анализом больших данных (Big Data), зашумленных искусственно и естественно генерируемыми «текстовками». Поэтому задача отделения деструктивного контента, результаты решения которой необходимы для принятия своевременных и эффективных мер по противодействию ИПВ в социальных медиа, от шумовых эффектов, весьма актуальна.

В настоящем докладе исследовались свойства шумостойкости наиболее известных текстовых классификаторов – SVM, GRU, BERT.

В целях выявления свойств шумостойкости классификаторов сформированы большие корпуса текстов, моделирующих основное наполнение социальных медиа, целевой радикальный корпус, а также шумовой корпус (материалы, не являющиеся экстремистскими).

Показано, что наибольшую точность определения шумового контента при выявлении текстов деструктивной составляющей в СМ имеет архитектура классификатора на основе трансформера BERT. Результаты работы данного классификатора при моделировании шумовых воздействий превосходят аналогичные архитектуры классификаторов моделей SVM и GRU.

Полученные результаты исследования целесообразно учитывать при разработке и модернизации автоматизированных систем правоохранительных и иных структур, в частности – МВД России, для автоматизации поиска в социальных медиа контента деструктивной направленности.

Отметим, что, если существуют ограничения на вычислительные ресурсы, целесообразно использование классификатора SVM, как наиболее быстрого способа нахождения опасного деструктивного текстового контента.

Таким образом, предлагается методика выявления и идентификации в социальных медиа манипулятивных воздействий, в том числе – контента экстремистской направленности, базирующаяся на применении нейронных сетей как перспективного направления искусственного интеллекта.

Достигнутая в исследованиях высокая точность распознавания деструктивности текстов позволяет использовать полученные результаты для практического совершенствования работы по противодействию распространению идеологии терроризма и экстремизма в социальных медиа. Эта точность также необходима для принятия своевременных и эффективных мер по противодействию и иным деструктивным воздействиям в социальных медиа. Так, полученные результаты целесообразно учитывать при выявлении информационных воздействий на молодое поколение при склонении к суицидальному поведению, вовлечении в различные опасные сообщества.

Список использованных источников:

1. Минаев В. А., Поликарпов Е. С., Симонов А. В. Применение глубинных нейронных сетей для выявления деструктивного контента в социальных медиа // Информация и безопасность. 2021. Т. 24. № 3. С. 361–372.
2. Минаев В. А., Симонов А. В. Количественная оценка деструктивности больших текстовых массивов в социальных медиа // Информация и безопасность. 2021 Т. 24. Вып. 2. С. 267–280.
3. Минаев В. А., Реброва А. Д., Симонов А. В. Выявление деструктивного контента в социальных медиа на основе моделей машинного обучения // Информация и безопасность. 2021. № 1. Т. 24. С. 7–20.
4. Kuratov Y., Arkhipov M. Adaptation of deep bidirectional multilingual transformers for Russian language // arXiv preprint arXiv:1905.07213. – 2019. – С 1-7.
5. Van Aken B. et al. Challenges for toxic comment classification: An in-depth error analysis // Proceedings of the 2nd Workshop on Abusive Language Online (ALW2). 2018. С. 33–42.

6. Wang X. et al. Drifted Twitter spam classification using multiscale detection test on KL divergence // IEEE Access. 2019. Т. 7. С. 108384–108394.
7. Vaswani A. et al. Attention is all you need // Advances in neural information processing systems. 2017. Т. 30. С. 1–15.
8. Scheinberg K. An efficient implementation of an active set method for svms // J. Mach. Learn. Res. 2006. Vol. 7. P. 2237–2257.
9. Будыльский Д. В. GRU и LSTM: современные рекуррентные нейронные сети // Молодой ученый. 2015. № 15 (95). С. 51–54.
10. Sun C. et al. How to fine-tune BERT for text classification? // China National Conference on Chinese Computational Linguistics. Springer, Cham, 2019. С. 194–206.
11. Экстремистские материалы: Министерство юстиции Российской Федерации // Официальный сайт Министерства юстиции Российской Федерации. URL: <https://minjust.gov.ru/>.

Степанов Р. О.¹,

директор Дирекции Арктических программ Московского государственного технического университета имени Н.Э. Баумана, кандидат технических наук, доцент

Фаддеев А. О.²,

главный научный сотрудник Дирекции Арктических программ Московского государственного технического университета имени Н.Э. Баумана, доктор технических наук, доцент

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ОПЕРАТИВНЫХ СЛУЖБ ПРИ ВЕТРОВОМ ПЕРЕНОСЕ ОПАСНЫХ ВЕЩЕСТВ

В рамках разработки и реализации метода оценки техногенного риска в целях совершенствования информационного обеспечения оперативных служб (МЧС, МВД, медицинская служба) решались три ключевые задачи – построение траектории движения облака, насыщенного парами опасного химического вещества; моделирование диссипации этого облака; оценка техногенного риска вдоль траектории движения облака. Построен новый численный метод оценки техногенного риска в результате ветрового переноса и диссипации опасных химических веществ. Показаны этапы реализации алгоритма расчета риска. Произведена имитация пространственного распространения опасных последствий условного техногенного события. Делается вывод, что предложенный подход может быть адаптирован к модельному описанию выбросов в атмосферу радиоактивных веществ, экологическому загрязнению местности в результате масштабных промышленных и геологических разработок, геодинамических катастроф.

В статье смоделирован условный сценарий – при заходе на посадку потерпел катастрофу транспортный самолет, перевозящий опасное химическое вещество, которое в разогретом состоянии было выброшено в атмосферу. Под действием ветра образовавшееся опасное облако начало перемещаться по территории района, формируя по пути следования зону техногенного риска.

В рамках разработки и реализации нового метода оценки техногенного риска, решались три ключевые задачи – построение траектории движения облака, насыщенного парами опасного химического вещества; моделирование диссипации этого облака; собственно, оценка техногенного риска вдоль траектории движения облака.

Описание модели. Рассмотрим задачу построения траектории движения облака. Пусть в начальный период времени некоторая фиксированная точка характеризует центр облака в пространстве с начальными координатами $M_0(\lambda_0, \phi_0)$, где λ_0 – долгота, ϕ_0 – широта. Координаты центра облака вдоль траектории своего движения при этом задаются в соответствии с выражениями:

¹ © Степанов Р. О., 2022.

² © Фаддеев А. О., 2022.

$$\begin{cases} \lambda_i = \lambda_{i-1} + \Delta\lambda_i, \\ \varphi_i = \varphi_{i-1} + \Delta\varphi_i, \end{cases} \quad (1)$$

где $\Delta\lambda_i$ и $\Delta\varphi_i$ – изменения координат центра облака вдоль траектории его движения под действием ветровых потоков; $i = 1; \dots; n$.

Для определения новых координат центра облака, спустя некоторый промежуток времени Δt , необходимо знать его предыдущие координаты и изменения координат за тот же промежуток. При практической реализации модели принято, что направление и скорость ветра за промежуток Δt не должны изменяться более, чем на 5 %. Шаг сетки по долготе и широте принимается равным $0,01^\circ$. В таком случае координаты центра облака в некоторый момент времени t_i будут определяться в градусной мере в соответствии с соотношениями:

$$\begin{cases} \lambda_i(t_i) = \lambda_{i-1}(t_{i-1}) + \frac{0,01 \cdot V_\lambda^{(i-1)}(t_{i-1}) \cdot \Delta t}{\Delta\varphi \cdot \cos\varphi_{i-1}}, \\ \phi_i(t_i) = \phi_{i-1}(t_{i-1}) + \frac{0,01 \cdot V_\phi^{(i-1)}(t_{i-1}) \cdot \Delta t}{\Delta\varphi}, \end{cases} \quad (2)$$

где $V_\lambda^{(i)}(t_i)$ и $V_\phi^{(i)}(t_i)$ – скорости ветра в некоторый момент времени t_i в долготном и широтном направлениях, соответственно; $\Delta\varphi = 1111,11$ метров.

Рассмотрим теперь задачу о диссипации облака.

В работах, посвященных исследованиям опасных техногенных явлений и их последствий, приводятся соотношения, позволяющие оценить размеры облаков, например, в [4]:

$$L(t) = 0,011 \left(\frac{Q_0 \cdot g(\rho_r - \rho_a)}{\rho_a} \right)^{0.25} \cdot t^{0.5}, \quad (3)$$

где Q_0 – начальный объем облака, вычисляемый по соотношению $Q_0 = \pi L_0^3 / 8$ (L_0 – первоначальный радиус облака); g – ускорение свободного падения; ρ_r – плотность облака; ρ_a – плотность атмосферы; t – время.

Вследствие процессов конвекции и диффузии облачные массы начинают диссипировать, облако «расползается» в пространстве [1; 4]. При этом оно еще и подчиняется воздействиям ветровых потоков. Поэтому необходимо рассчитывать техногенные риски не только непосредственно вдоль траектории движения центра облака, но и на его границе.

Расчет координат точек границы облака выполняется по формулам, аналогичным соотношениям системы (1), а вот для вычисления приращений долгот $\Delta\lambda_i^{(k)}$ и широт $\Delta\varphi_i^{(k)}$ необходимо вычислить величины проекций перемещения облака на оси $X - u_i^{(k)}$ и $Y - w_i^{(k)}$ в системе координат, связанной с траекторией его движения (рис. 1):

$$\begin{cases} u_i^{(k)}(t_i) = \delta_i(t_i) \cdot \cos\theta_k, \\ w_i^{(k)}(t_i) = \delta_i(t_i) \cdot \sin\theta_k, \end{cases} \quad (4)$$

где δ_i – истинный радиус облака в некоторый момент времени t_i , определяемый в соответствии с выражениями $\delta_i(t_i) = S_i(t_i) + L_i(t_i)$; $S_i(t_i) = V_i(t_i)\Delta t$.

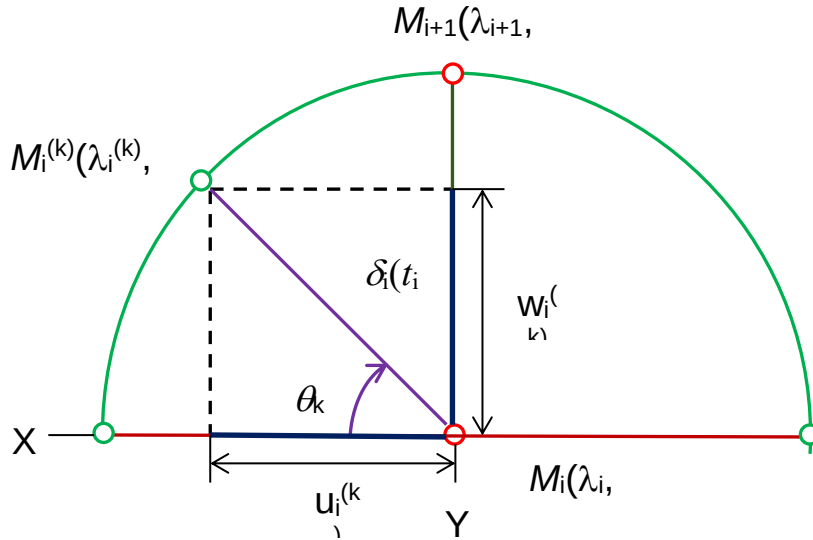


Рис. 1. Схема вычисления перемещений $u_i^{(k)}$ и $w_i^{(k)}$

Переходя от системы координат XY , связанной с траекторией движения облака, к системе координат долгота – широта $(\lambda-\phi)$, учитываем величины проекций скорости ветра на ось долготы $V_{\lambda}^{(i)}$ и ось широты $V_{\phi}^{(i)}$ посредством расчета величины угла поворота α (для i -ой точки):

$$\alpha_i(t_i) = \arctg \left| \frac{V_{\lambda}^{(i)}(t_i)}{V_{\phi}^{(i)}(t_i)} \right|. \quad (5)$$

Тогда в системе координат долгота – широта в момент времени t_i проекции смещений $\tilde{u}_i^{(k)}$ на ось долгот и $\tilde{w}_i^{(k)}$ на ось широт находятся из выражений:

$$\begin{cases} \tilde{u}_i^{(k)}(t_i) = u_i^{(k)}(t_i) \cdot \cos \alpha_i(t_i) + w_i^{(k)}(t_i) \cdot \sin \alpha_i(t_i), \\ \tilde{w}_i^{(k)}(t_i) = -u_i^{(k)}(t_i) \cdot \sin \alpha_i(t_i) + w_i^{(k)}(t_i) \cdot \cos \alpha_i(t_i). \end{cases} \quad (6)$$

Учитывая приращения по долготу $\Delta \lambda_i^{(k)}$ и широте $\Delta \phi_i^{(k)}$ для момента времени t_i и диссипацию облака, получены окончательные выражения для координат центра облака:

$$\begin{cases} \lambda_i(t_i) = \lambda_{i-1}(t_{i-1}) + \frac{0,01 \cdot [V_{i-1}(t_{i-1}) \Delta t + L_{i-1}(t_{i-1})]}{\Delta \phi \cdot \cos \phi_{i-1}} \cdot \cos \left[\frac{\pi}{2} - \arctg \left| \frac{V_{\lambda}^{(i-1)}(t_{i-1})}{V_{\phi}^{(i-1)}(t_{i-1})} \right| \right] \\ \phi_i(t_i) = \phi_{i-1}(t_{i-1}) + \frac{0,01 \cdot [V_{i-1}(t_{i-1}) \Delta t + L_{i-1}(t_{i-1})]}{\Delta \phi} \cdot \sin \left[\frac{\pi}{2} - \arctg \left| \frac{V_{\lambda}^{(i-1)}(t_{i-1})}{V_{\phi}^{(i-1)}(t_{i-1})} \right| \right] \end{cases} \quad (7)$$

Задача оценки техногенного риска вдоль траектории движения облака. В основу оценки изменения величины техногенного риска положено время существования облака η :

$$\eta = \frac{100 \cdot L_0}{\sqrt{g h_0 \cdot (\rho_r - \rho_a) / \rho_r}}, \quad (8)$$

где L_0 – первоначальный радиус облака; g – ускорение свободного падения; h_0 – высота начального облака; ρ_r – плотность облака; ρ_a – плотность атмосферы [1; 4].

Формула для расчета величины техногенного риска R_{T_i} (для его положительных значений) в момент времени t_i в точке с координатами (λ_i, φ_i) будет иметь вид:

$$R_{T_i}(t_i) = R_{T_0} \cdot \left(1 - \frac{t_i}{\eta}\right), \quad (9)$$

где R_{T_0} – величина техногенного риска в начальный момент времени t_0 , соответствующий началу движения облака, образовавшего при опасном техногенном событии.

Моделирование поля скорости ветра. Для моделирования поля скорости ветра использована следующая система уравнений:

$$\begin{cases} \frac{dV_x}{dt} = \ell \cdot V_y - R_\mu \cdot T'_x, \\ \frac{dV_y}{dt} = -\ell \cdot V_x - R_\mu \cdot T'_y, \end{cases} \quad (10)$$

где $T'_x = \frac{\partial T}{\partial x}$; $T'_y = \frac{\partial T}{\partial y}$; $R_\mu = \frac{R}{m_\mu}$; m – молярная масса; R – универсальная газовая

постоянная; T – температура атмосферного воздуха; V_x, V_y – проекции скорости ветра на координатные оси X, Y , соответственно; ℓ – параметр Кориолиса, определяемый из соотношения $\ell = 2\omega \cdot \sin\varphi$; $\omega = 7,3 \cdot 10^{-5} \text{ с}^{-1}$ – угловая скорость вращения Земли; φ – широта местности.

Запишем уравнения этой системы для некоторой точки (x, y) применительно к фиксированному моменту времени t_0 в виде малых приращений:

$$\begin{cases} \frac{\Delta V_x(t_0)}{\Delta t} + R_\mu T'_x(t_0) - \ell V_y(t_0) = \varepsilon_x(t), \\ \frac{\Delta V_y(t_0)}{\Delta t} + R_\mu T'_y(t_0) + \ell V_x(t_0) = \varepsilon_y(t), \end{cases} \quad (11)$$

где $\varepsilon_x(t)$ и $\varepsilon_y(t)$ – некоторые бесконечно малые величины.

Преобразовывая систему уравнений (11) и обозначая через $O_x(t) = \varepsilon_x(t) \cdot \Delta t$ и $O_y(t) = \varepsilon_y(t) \cdot \Delta t$, получим:

$$\begin{cases} V_x(t_0 + \Delta t) = V_x(t_0) + [\ell V_y(t_0) - R_\mu T'_x(t_0)] \cdot \Delta t + O_x(t), \\ V_y(t_0 + \Delta t) = V_y(t_0) - [\ell V_x(t_0) + R_\mu T'_y(t_0)] \cdot \Delta t + O_y(t). \end{cases} \quad (12)$$

Согласно (12), если имеется информация о значениях скорости ветра и градиенте температур в некоторой точке (x, y) в начальный момент времени t_0 , то можно вычислить значение скорости ветра в момент времени $t = t_0 + \Delta t$.

Система уравнений, представляющая собой реализацию численного метода Эйлера [2–3], является математической моделью поля скоростей ветра.

Пример оценки техногенного риска. Для имитации пространственного распространения опасных последствий техногенного события использована реальная метеорологическая информация о скорости и направлении ветра в районе аэропорта Тикси для условного начального момента времени – 00 ч. 00 мин 15.04.21.

Для расчета проекций скорости ветра на оси долгот и широт применена следующая система уравнений:

$$\begin{cases} V_{\lambda}(\lambda_i, \phi_i, t_{i+1}) = V_{\lambda}(\lambda_i, \phi_i, t_i) + [\ell V_{\phi}(\lambda_i, \phi_i, t_i) - R_{\mu} T'_{\lambda}(\lambda_i, \phi_i, t_i)] \cdot \Delta t + O_{\lambda}(t), \\ V_{\phi}(\lambda_i, \phi_i, t_{i+1}) = V_{\phi}(\lambda_i, \phi_i, t_i) - [\ell V_{\lambda}(\lambda_i, \phi_i, t_i) + R_{\mu} T'_{\phi}(\lambda_i, \phi_i, t_i)] \cdot \Delta t + O_{\phi}(t). \end{cases} \quad (13)$$

Численные оценки показали, что общее время существования опасного облака η составляет около 17 ч. 30 мин. Кроме того, оценки, выполненные для всех трехчасовых временных интервалов в течение суток 15.04.21, привели к выводу, что за величину длительности промежуточных временных отсчетов следует принять $\delta t = 10$ мин. На (рис. 2) представлены результаты оценки техногенного риска, возникающего из-за движения (в результате ветровых и диссипационных воздействий) над исследованной территории облака, насыщенного опасными химическими веществами.

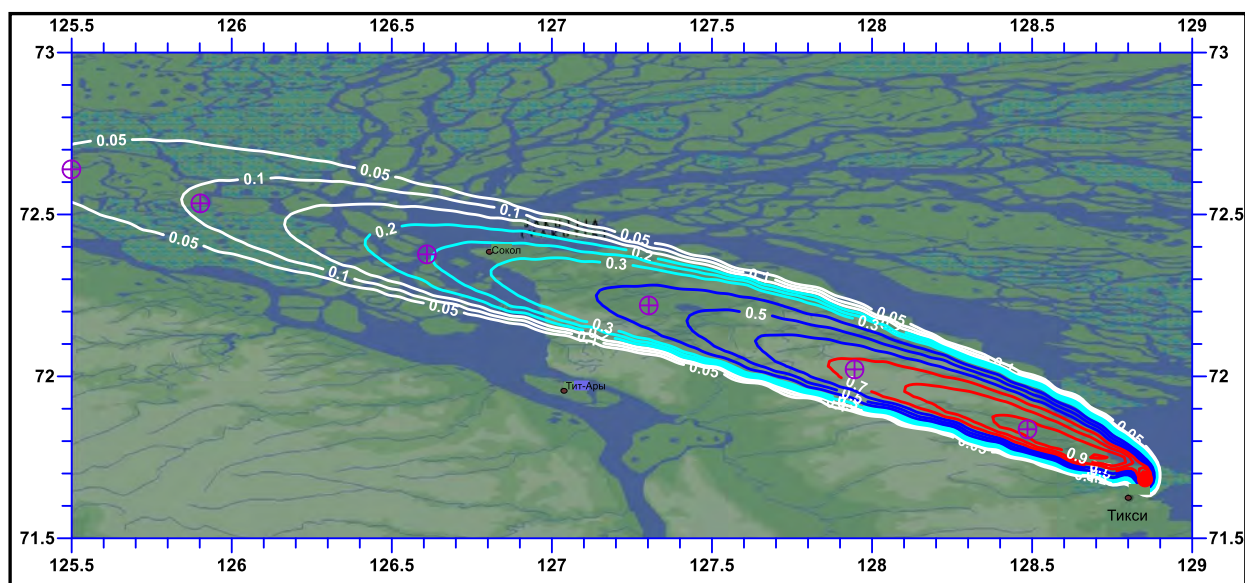


Рис. 2. Результаты реализации численного метода оценки техногенного риска для участка исследуемой территории

Из рис. 2 следует, что ядовитое химическое облако, образовавшееся в результате произошедшего опасного техногенного события, в процессе своего движения под действием ветра и диссипации, оставляет след из выпадающих ядовитых осадков, протянувшийся в северо-западном направлении, формируя зону техногенного риска.

Фиолетовыми окружностями с перекрестием обозначены положения центра облака с интервалами в 3 часа от момента формирования опасного облака, т. е. через 3 часа и 6 часов, прошедших с момента формирования зараженного облака, техногенный риск вдоль траектории движения облака очень велик (зоне, ооконтуренной красными линиями, характерен риск 0,7–0,9). Через 9 часов величина риска вдоль траектории движения спадает до величины примерно 0,45, через 12 часов от момента формирования облака техногенный риск уменьшается до величины 0,25 вдоль траектории его движения. Соответственно, через 15 часов от момента реализации опасного техногенного события риск составляет величину всего 0,1, а еще через 2 часа 20 минут и вовсе спадает до минимальных значений.

Очевидно, что информация об оценке техногенного риска, представленная на Рисунке 2, крайне необходима для своевременного развертывания сил и средств МЧС России, полицейских подразделений и медицинских служб в целях адекватного формирования территориально-временных заградительных мероприятий, оповещения населения о грозящей опасности, принятия эвакуационных мер и при необходимости – мер спасения.

Заключение. В статье рассмотрено построение нового численного метода оценки техногенного риска, возникающего в результате ветрового переноса и диссипации опасных химических веществ. Показаны этапы реализации алгоритма расчета риска и результаты имитационного моделирования пространственного распространения риска для ограниченной территории. Предложенный подход может быть достаточно легко адаптирован и к модельному описанию выбросов в атмосферу радиоактивных веществ, экологическому загрязнению местности любого региона в результате масштабных промышленных и геологических разработок, геодинамических катастроф, террористических действий [5].

Список использованных источников:

1. Газовая динамика. Избранное. Издание второе, исправленное / редактор-составитель А. Н. Крайко. М. : Физматлит, 2005. Т1. 720 с.
2. Калиткин Н. Н. Численные методы. М. : Наука, 1978. 512 с.
3. Математическое моделирование / под ред. А. Н. Тихонова, В. А. Садовниченко. М. : Физматлит, 2005. 316 с.
4. Britter R. E. Atmospheric dispersion of dense gases // Annual Review of Fluid Mechanics. 1989. Vol. 21. P. 317–344.
5. Минаев В. А., Степанов Р. О., Фаддеев А. О. Арктические риски: моделирование, комплексная оценка, управление : монография. М. : МГТУ имени Н. Э. Баумана, 2022. 538 с.