

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
(20 апреля 2023 г.)**

Сборник научных статей

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

Научное электронное издание

Москва
Московский университет
МВД России имени В.Я. Кикотя
2023

© Московский университет МВД России
имени В.Я. Кикотя, 2023
ISBN 978-5-9694-1408-2

УДК 004.9
ББК 16.3
И74

Рецензенты:
заместитель начальника отдела БСТМ ГУ МВД России
по г. Москве **Е. А. Буланцев**;
начальник 9-го отдела ЦИТСиЗИ ГУ МВД России
по г. Москве **А. С. Топилин**

Составитель *И. С. Мельцева*

И74 Информационные технологии в деятельности органов внутренних дел : Всероссийская научно-практическая конференция, 20 апреля 2023 г. : сборник научных трудов / [сост. И. С. Мельцева]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2023. – 297 с. – 1 электронный оптический диск (CD-R). – Системные требования : CPU 1,5 ГГц ; RAM 512 Мб ; Windows XP SP3 ; 1 Гб свободного места на жестком диске.
ISBN 978-5-9694-1408-2

В сборнике представлены статьи авторов, принявших участие во Всероссийской научно-практической конференции «Информационные технологии в деятельности органов внутренних дел», прошедшей 20 апреля 2023 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 органов внутренних дел.

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, 2023

Издание подготовлено
с помощью программного обеспечения InDesign

Корректор *Чеботарева С. О.*
Компьютерная верстка *Киселева М. Е.*

Подписано к изданию 19.09.2023
Объем издания: 3,81 Мб
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-1408-2



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

СОДЕРЖАНИЕ

Скворцов П. В.

Описание решения по анализу информационных ресурсов
на предмет выявления запрещенной информации..... 12

Росляков А. В.

Обеспечение антикриминальной безопасности
как одно из направлений национальной безопасности 14

Овчинский А. С.

Угрозы ментально-когнитивных смысловых войн 17

Андреев И. В.

Угрозы информационной безопасности, связанные
с технологиями виртуальной реальности 20

Борзунов К. К.

Противодействие распространению
деструктивных идеологий в России..... 22

Халимбеков Хасанбек Иброхим угли

Искусственный интеллект..... 26

Хотамов Мухаммадали Маликбой угли

Сравнительный анализ BIOS и UEFI..... 29

Казаков М. Б.

MITM-атаки и их предотвращение 32

Лузганов Д. В.

Корреляционный анализ данных цифрового профиля
гражданина Российской Федерации в целях идентификации лиц 34

Лиманская А. Р.

Алгоритм криминалистического исследования
по установлению общего источника происхождения
наркотических средств 37

Баринова А. К.

Анализ эффективности программ, предназначенных
для восстановления компьютерной информации 40

Андреева Е. Н.

Возможности использования агрегаторов сбора данных
для поиска информации по открытым источникам 43

<i>Артамонов И. В.</i> Значение дезинформации и методы ее использования.....	45
<i>Болдырев М. А.</i> Отдельные подходы к определению видов социальной инженерии и пути противодействия им.....	47
<i>Бороздина В. Н.</i> Анализ социальных сетей на выявление субъектов, представляющих интерес для подразделений органов внутренних дел	49
<i>Чурин Р. А.</i> Особенности исследования беспилотных летательных аппаратов	51
<i>Братищева В. В.</i> Применение OSINT в правоохранительной деятельности	55
<i>Гончар В. В.</i> Проблемы противодействия мошенничествам с использованием средств мобильной связи и отдельные пути их решения.....	60
<i>Кияева Е. Ю.</i> Основные направления применения информационных технологий в деятельности экспертно-криминалистических подразделений.....	63
<i>Гребнева А. С., Ромашенко О. Л.</i> О некоторых особенностях технологии экспертного исследования в области информационных технологий	68
<i>Егоров Д. А.</i> Применение квантовых технологий в области обеспечения системы информационной безопасности.....	72
<i>Коняхин Д. И., Дворянkin О. А.</i> Роль человеческого фактора в кибербезопасности с учетом использования искусственного интеллекта	74
<i>Завьялова А. А., Завьялов В. В.</i> Использование информационных технологий в ходе криминалистического исследования наркотических средств по установлению общего источника происхождения.....	77
<i>Шилов М. А.</i> Использование нейросети для обнаружения подозрительной сетевой активности	81

Калашикова А. А., Соболев А. О.

Анализ создания компьютерно-мозговых
интерфейсов для киборгов 84

Катионов Д. С.

К вопросу изучения методов взлома информационных систем
органов внутренних дел и разработке мер по их защите 87

Савоськин Р. А.

Основные виды киберпреступлений и первоначальные действия
сотрудников правоохранительных органов по противодействию им 90

Назаров А. К.

Кибербезопасность: проблемы и угрозы 96

Куриленко Ю. А., Михайлова В. Д.

Кибершпионаж – угроза информационной безопасности 98

Лустин В. И.

Защита информации. Виброакустический канал 101

Климова Е. К.

Инновационный подход в определении дефектов матриц
в съемочных устройствах 104

Миляев Г. А.

Компьютерная экспертиза
при расследовании преступлений,
совершенных с использованием информационных технологий 108

Кубасов И. А.

Развитие и внедрение информационных технологий
в деятельности органов внутренних дел 110

Макеев В. А.

Математические методы и средства распознавания человека
по радужной оболочке 115

Маликов С. А.

Некоторые проблемные вопросы
в сфере развития искусственного интеллекта 118

Васильев Р. А.

Математические методы и программные средства
для распознавания мимики человека 120

Медведев В. А.

Современное состояние раскрытия
и расследования преступлений, совершаемых
с использованием информационных технологий 125

Мирзахмедов Д. М.

О практическом применении последовательности Фибоначчи 128

Миронов В. Л.

Дипфейк как вероятный инструмент
совершения преступлений 130

Козаева К. И.

Индустрия телефонного мошенничества
на современном этапе 134

Перепелица Е. А.

Основные способы установления личности
с помощью информационно-поисковых систем 138

Руденко М. П.

О вопросах разработки собственных систем
предотвращения утечек конфиденциальной информации (DLP)
для обеспечения деятельности ОВД 141

Филимонова Ю. В.

Особенности получения компьютерной информации
при реализации атак типа MITM 144

Панков Е. С.

Отдельные направления
использования открытых источников информации
в противодействии киберпреступности 147

Полякова О. С.

Анализ данных из открытых источников
в раскрытии и расследовании преступлений 149

Смолянинов В. А., Севастьянов Д. С., Котова Н. А.

Проблемы исследования памяти квантового компьютера 152

Филимонов А. А.

Создание персональных экспертных
инструментов исследования цифровых данных
в среде разработки Jupyter Notebook на языке Python 155

Пучков Г. Ю.

Особенности создания сервисов ИСОД МВД России
в интересах оперативных служб
органов внутренних дел Российской Федерации..... 162

Ромашкин Т. Р., Атласов И. В.

Исследование возможности внедрения
стеганографических методов
при организации современных компьютерных атак 166

Рахмонбердиев Б. Б.

Спуфинг/сниффинг HTTPS 169

Гуков А. А., Фареник Д. С., Холодков К. И., Гуков А. А.

Современные технологии в проведении осмотра
места происшествия при дорожно-транспортном происшествии 172

Худяков В. В., Владимирова В. Э.

Социальная инженерия как один из методов
несанкционированного доступа к компьютерной информации 178

Кучина А. М.

Математические методы автоматизированного
распознавания динамических признаков человека..... 183

Каримов А. К.

Отдельные проблемы противодействия внутренним нарушителям
на предприятиях 186

Поташов М. Р.

О возможностях использования линейки
программных продуктов «АИПСИН»
в экспертно-криминалистической деятельности 192

Баранова А. А.

Фейковые сообщения
как угроза информационной безопасности 195

Батоев В. Б.

Использование аппаратно-программного комплекса «Безопасный город»
при раскрытии преступлений 197

Данилова Е. А.

Эволюция вредоносных программ
и их влияние на современные модели безопасности..... 200

Клочкова Е. Н.

Уязвимости систем искусственного интеллекта,
основанных на использовании нейронных сетей 202

Клочкова А. М., Максимов Н. А.

Возможности использования защищенной,
киберимунной операционной системы Kaspersky OS
для дистанционного управления
мобильным роботом..... 205

Кондрашечкин Р. В.

Искусственный интеллект в правоохранительной деятельности..... 209

Лопухов В. В.

Информационно-аналитическое обеспечение
как неотъемлемая часть процесса
раскрытия преступлений на примере организации работы
подразделений ГУ МВД России по г. Москве 215

Меняйло Д. В., Барсова Е. Р.

Применение информационных технологий
в сфере противодействия коррупции 222

Папуша Е. Ю.

Проблемы голосовых помощников
по распознаванию deepfake и как защитить себя
от несанкционированного доступа к вашим данным 227

Коломина А. С., Полякова О. С.

Дипфейки: поддельное прошлое, настоящее и будущее 230

Лащенков П. М.

Развитие и характеристики искусственного интеллекта
в сфере кибербезопасности 233

Боровиков В. Б., Боровикова В. В.

О проблемах преподавания разделов курса уголовного права
об ответственности за преступления,
совершенные с использованием
информационно-телекоммуникационных технологий 236

Баранов В. М., Жукова П. Н., Прокопенко А. Н.

Единая биометрическая система персональных данных:
правовое регулирование и особенности функционирования
в инфраструктуре электронного правительства..... 240

Рамаева К. В.

Позитивный результат от внедрения
в деятельность органов внутренних дел
информационно-телекоммуникационных технологий 246

Ситников А. А.

Интеллектуальная система автоматизированного поиска
оперативно значимой информации
в системах мгновенного обмена сообщениями 250

Фролкина А. М.

Модель цифровой платформы профилактики преступлений 252

Цыцурин С. Л.

Автоматизация поиска сведений в открытых источниках –
эффективное средство проведения оперативных мероприятий 255

Шайдаев М. Ш.

Возможности технологий Интернета вещей
в обеспечении правоохранительной деятельности 258

Черкесова Д. А.

Использование больших данных в информационно-аналитическом
обеспечении оперативно-разыскной деятельности 264

Осипова А. А.

Отдельные аспекты использования специальных знаний
по распознаванию дипфейков 267

Пименова О. В.

Комплекс первоочередных организационных
и технических мер по обеспечению защиты
внешних информационных ресурсов МВД России
в современных условиях активизации
зарубежных хакерских группировок 270

Гавриленко А. А., Котов И. Д.

Анализ защищенности IoT-устройств с голосовыми помощниками
на предмет вмешательства злоумышленников
в управление с использованием аудиодипфейков 275

Рудковская Е. Р.

Анализ рисков и угроз информационной безопасности
при использовании мобильных устройств
в органах внутренних дел 279

Акинъшин И. С.

Особенности изучения некоторых видов
электронных носителей информации 281

Толстых М. Ю.

Обеспечение информационной безопасности цифровых продуктов
на всех этапах их жизненного цикла..... 285

Турсунов У. Н., Галиев Д. В.

Идентификация пользователя при помощи browser fingerprint 288

Шикалова В. М.

Компьютерная преступность как социологическая категория 291

Шикалова В. М.

Проблема организации защиты личной информации сотрудников ОВД..... 293

Шульга Д. С.

Понятие и виды дистанционных мошенничеств 295

Скворцов П. В.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОПИСАНИЕ РЕШЕНИЯ ПО АНАЛИЗУ ИНФОРМАЦИОННЫХ РЕСУРСОВ НА ПРЕДМЕТ ВЫЯВЛЕНИЯ ЗАПРЕЩЕННОЙ ИНФОРМАЦИИ

Глобальные разработки в области компьютерных технологий охватили все области человеческой и национальной деятельности, начиная от общения между людьми и заканчивая национальной безопасностью.

Существует множество программных решений по анализу информации по ключевым словам в сети Интернет, но каждый из них обладает рядом минусов и не позволяет в полной мере осуществлять поставленные перед ОВД задачи. Именно поэтому принято решение разработать собственный программный комплекс Flipper.

Для начала работы с программой с сайта Минюста России был загружен список экстремистских материалов и организаций в формате «.docx». После загрузки списка материалов данный документ был открыт и проанализирован. В качестве основы для обработки данных был выбран текст для оценки тональности и обучения нейронной сети.

Вкладка «Тональность» позволяет выполнить оценку тональности выбранного текста с помощью нейронной сети, выявить негативные, позитивные и нейтральные слова и выражения на основе обученной языковой модели. За основу данных для обучения была выбрана фраза, указанная на вкладке «Тональность» и имеющая негативную языковую оценку тональности текста. На вкладке «Генерация данных» произведено обучение модели и сгенерирована фраза для поиска по ключевым словам.

Вкладка «Поиск по форумам» позволяет выполнить поиск ключевых слов на введенной пользователем ссылке форума. Для работы программного обеспечения необходимо в поле «Ключевые слова» указать список ключевых слов через пробел. После этого необходимо указать ссылку на рассматриваемый форум и нажать кнопку «Поиск». В результате выполнения скрипта в окне выполнения программы появится результат поиска в виде ссылок на публикации форума, содержащие указанные ключевые слова.

¹ © Скворцов П. В., 2023.

С помощью вкладки «Поиск по vk.com» у пользователя есть возможность осуществить поиск по ключевым словам в постах и комментариях к ним в сообществах «vk.com». Необходимо перейти на вкладку «Поиск по vk.com», указать ключевые слова через пробел в поле «Ключевые слова», добавить ссылку на сообщество в поле «Ссылка на сообщество» и нажать кнопку «Поиск».

Вкладка «Аналитика» представляет возможность выполнить поиск по имени пользователя аккаунты сразу в нескольких социальных сетях и мессенджерах. Для работы с этим модулем необходимо переключиться на вкладку «Аналитика», в поле «Введите никнеймы» указать никнеймы пользователей через запятую, ввести с использованием запятой список ресурсов, на которых необходимо выполнить поиск в поле «Введите список ресурсов». Если необходимо выполнить поиск по запрещенным на территории Российской Федерации ресурсам, то необходимо в поле «Введите прокси» указать параметры прокси для выполнения поиска, указать предполагаемый пол объекта поиска и нажать кнопку «Поиск». Результат также сохранится в файле.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993, действующая редакция) // СПС «КонсультантПлюс».
2. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс».
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».
4. Закон от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ Кодекс Российской Федерации об административных правонарушениях // СПС «КонсультантПлюс».
6. Федеральный закон от 13 июня 1996 г. № 63-ФЗ Уголовный кодекс Российской Федерации // СПС «КонсультантПлюс».
7. Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // СПС «КонсультантПлюс».
8. Хургин В. Об определении понятия «информация» // Информационные ресурсы России. 2007. № 3.
9. Чекунов И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9–22.
10. Галеева И. С. Достоверность информации в Сети: как определить? // Вестник Библиотечной Ассамблеи Евразии. 2014. № 2. С. 50–52.
11. Евдокимов К. Н. Проблемы квалификации и предупреждения компьютерных преступлений. Иркутск : Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2009.
12. Прохоренок Н. А., Дронов В. А. «Python 3. Самое необходимое». СПб. : БХВ-Петербург, 2016. 464 с.

Росляков А. В.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Борзунов К. К.,

доцент кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук, старший научный сотрудник

ОБЕСПЕЧЕНИЕ АНТИКРИМИНАЛЬНОЙ БЕЗОПАСНОСТИ КАК ОДНО ИЗ НАПРАВЛЕНИЙ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В современных условиях, когда укрепление связей между странами играет все более важную роль, национальная безопасность становится неотъемлемой частью личности, общества и государства. Важную роль в эффективности обеспечения национальной безопасности государства выполняет психологическая безопасность как составляющая национальной безопасности страны [2]. Сфера безопасности активно влияет на состояние политической, экономической, духовной и других составляющих национальной безопасности страны.

В совокупности многие компоненты создают общую психологическую безопасность нации, в том числе индивидуально-психологические, социально-психологические, религиозно-психологические, политико-психологические, нравственно-психологические, этнопсихологические, профессионально-психологические и другие факторы, что влияет на общественное сознание. Данные компоненты формируют национальное понимание, а также цели, методы и поведение общества. Это влияет на формирование общественного сознания нации, а также на психические состояния и социологический статус ее граждан.

Индивидуально-психологическая составляющая отражает психологию отдельной личности – гражданина, его готовность к общественно полезной деятельности, отношение к власти, соотношение собственного и общественного и т. п., а также его психическое здоровье. Социально-психологическая составляющая проявляется в характере общения и взаимодействия различных социальных групп, а также таких явлениях, как наличие работы или безработица, справедливость или несправедливость, социальный оптимизм или пессимизм и др. Элитнопсихологическая составляющая характеризуется деятельностью политической и экономической элиты, ее близостью или отдаленностью от своего народа, отношением к национальным ценностям и стремлениям, жизни граждан и т. д. Профессионально-психологическая составляющая отражает степень подготовки к профессиональной деятельности граждан, а также подготовленность руководителей всех звеньев при-

¹ © Росляков А. В., 2023.

нимать профессиональные решения, касающиеся их сфер деятельности. Религиозно-психологические феномены возникают в результате межконфессионального сотрудничества населения.

В мирное время реализуются комплексы информационно-психологических операций. Специализированные подразделения или отдельные специалисты осуществляют целенаправленные действия, оказывающие психологическое воздействие. Негативным психологическим воздействиям внешних противников противопоставляются позитивные меры, такие как искусство или образование. Также осуществляется специальная пропаганда, нацеленная на снижение лояльности данным психологическим воздействиям.

Во время ведения боевых действий для воздействия на военнослужащих и гражданское население противника используются различные психологические приемы и стратегии. К таким действиям относятся экономические и политические санкции, демонстрации военной силы, угрозы применения военной силы, поддержка оппозиции внутри страны, расовые, разжигание этнических и религиозных конфликтов и иные методы, оказывающие психологическое воздействие на противника. Подобные деяния могут нанести значительный психологический вред противнику, что выражается в подавлении воли к сопротивлению и отступлении от национальных целей. В период ведения боевых действий информационно-психологические операции также проводятся с целью воздействия на международное общественное мнение, на граждан государства и на личный состав противника в его вооруженных силах, что создает благоприятные условия для подрыва боевого духа или потенциального нанесения превентивного удара. Цель состоит в том, чтобы снизить боеспособность, уменьшить волю к борьбе, подтолкнуть к дезертирству, игнорированию приказов руководителей и сдачи в плен.

Психологические операции в основном осуществляются через средства массовой информации, радио- и телепередачи или с помощью информационно-коммуникационной сети Интернет. Результатом проведения информационно-психологических операций также могут являться ослабление действующей власти и создание дисбаланса сил в политике, экономике.

Таким образом, национальная безопасность отражает совокупность явлений, которые влияют на жизнедеятельность и развитие общества, формирует духовный, социальный, экономический и политический фундамент, обеспечивает деятельность государственных органов, политических и общественных организаций, а также самого государства. При этом можно сделать вывод о важности психологических аспектов в системе национальной безопасности Российской Федерации.

По мнению исследователей Г. Г. Горшенкова и Г. Н. Горшенкова, под антикриминальной безопасностью понимается состояние, при котором личность не подвергается возможной или реальной угрозе со стороны криминальных элементов [11].

Анализируя определения терминов «национальная безопасность» и «антикриминальная безопасность», в которых объектом обеспечения антикриминальной безопасности выступает личность, можно прийти к выводу, что безопасность личности также входит в структуру национальной безопасности и в этом смысле антикриминальная безопасность является обязательным условием обеспечения национальной безопасности России.

Список литературы

1. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
2. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «Консультант плюс». URL: <http://www.consultant.ru/>.
3. Стратегия национальной безопасности США» от 12 октября 2022 г. URL: <https://vvesti.com/politika/strategia-nacionalnoj-bezopasnosti-ssa-ot-12-oktabra-2022-goda-nelza-terat-vrema>.
4. Стратегия национальной безопасности Великобритании. URL: <http://www.zapiski-ieran.ru/images/analitika/2021/an235.pdf>.
5. Стратегия национальной безопасности Франции. URL: <http://www.publishing-vak.ru/file/archive-law-2021-2/6b-samogin-galanova.pdf>.
6. Стратегия национальной безопасности Германии. Вооружиться, чтобы пережить бурю: новая стратегия безопасности Германии. URL: <https://globalaffairs.ru/articles/strategiya-bezopasnosti-germanii/>.
7. Стратегия национальной безопасности Германии. Берлин разработает национальную стратегию безопасности // Редакция Германия. URL: <https://www.rg-rb.de/berlin-razrabotaet-naczionalnuyu-strategiyu-bezopasnosti/>.
8. Стратегия национальной безопасности Китая. Концепция национальной безопасности Китая в «новую эпоху»: предварительные итоги XX Всекитайского съезда Коммунистической партии Китая. URL: <https://docs.yandex.ru/docs/view?tm=1681396413&tld=ru&lang=ru&name=10AED699-D34C-4CFD-B64D-0225424C15A0.pdf>.
9. Китай представил шесть принципов для обеспечения глобальной безопасности // Forbes.ru. URL: <https://www.forbes.ru/society/485215-kitaj-predstavil-sest-principov-dla-obespecenia-global-noj-bezopasnosti/>.
10. Горшенков Г. Г., Горшенков Г. Н. Антикриминальная безопасность личности в уголовно-процессуальной сфере // Серия «Право». Вестник Нижегородского университета имени Н.И. Лобачевского. 2015. № 2. С. 97–101.

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, Академик РАЕН*

УГРОЗЫ МЕНТАЛЬНО-КОГНИТИВНЫХ СМЫСЛОВЫХ ВОЙН

Трансформация представлений об информационной безопасности. Осознание угроз информационной безопасности происходит в контексте развития технологий, их криминального использования и войны, в которую уже втянута наша страна.

На этапе автоматизации угрозы связывались с необходимостью защиты информации. Это нашло отражение в первых американских стандартах, перешло в наши документы и до сих пор многих дезориентирует.

На фоне цифровизации в Доктрине, утвержденной указом Президента Российской Федерации, информационная безопасность предстала состоянием защищенности личности общества и государства от угроз в информационной сфере [1]. При этом среди основных угроз выделяются деструктивные воздействия на сознание людей, сообществ, народов.

Сегодня в условиях неудержимой цифровой трансформации практически всех сторон жизни и деятельности возникает задача обеспечения безопасности, в первую очередь социальных, да и многих других сфер жизни общества, которые объективно становятся информационными в силу:

- новых промышленной и технологической революций;
- провозглашения информационного общества и вступления в цифровой мир;
- использования больших данных и развития систем искусственного интеллекта;
- расширяющегося применения роботов и достижений геномной инженерии;
- внедрения распределенных реестров и цифровых валют;
- технологий виртуальной реальности и перспектив квантовых вычислений.

Вместе с новыми возможностями открывается и «ящик Пандоры» как криминального, так и военного применения технологий. И это происходит как раз на фоне информационных войн с нарастающей интенсивностью деструктивных акций, направленных на самые разнообразные сферы общественных отношений.

Можно выделить технологические аспекты информационных войн, борьбу в киберпространстве, угрозы системам управления критически важных объектов... Мы же сосредоточим внимание на том, что несет непосредственно угрозы существованию самой российской цивилизации.

О реальности таких угроз свидетельствует наша история, в которой не раз возникали смутные времена, когда в результате гражданских конфликтов, преда-

¹ © Овчинский А. С., 2023.

тельства управляющих элит и, главное, мощных воздействий внешних сил страна оказывалась на пороге распада.

Сегодня наши противники не скрывают своих намерений провести так называемую «деколонизацию» народов России, а точнее, расчленить страну на отдельные анклавы. Так, нашей цивилизации грозит возвращение в XII век. Также, как 30 лет назад, советские граждане оказались в разных государствах, некоторые из которых уже воевали и воюют с Россией, живущие в нашей большой стране люди могут «проснуться» кто в Московии, кто в Уралии, кто в Сибири...

Информация как инструмент информационной войны. Можно встретить результаты огромного количества рассекреченных исследований, имеются тысячи открытых публикаций об информационных войнах и непосредственно о воздействиях на сознание людей. Но представления об информации как инструменте информационной войны остаются в глубокой тени.

Западные философы, социологи и разнообразные эксперты после многочисленных дискуссий пришли к весьма консолидированному мнению о том, что в условиях всеобщей цифровизации «информация не нуждается в том, чтобы ее воспринимали, не нуждается в том, чтобы ее понимали, она не требует умственных усилий для своей интерпретации, ей не требуется иметь смысл, чтобы существовать» [3].

В такой позиции сфокусирована практически вся ложь современной западной цивилизации. Из этой лжи вырастают двойные стандарты в политике, праве, морали. В ней же и корни ментальных, когнитивных и смысловых войн.

На самом деле информация в ее функциональном значении – это то, что позволяет адекватно реагировать на воздействия на всех уровнях организации живой природы (реактивная проекция информации). Она возникает в сознании человека как функция целевой интерпретации получаемых сообщений. Именно реактивная информация позволяет понимать смысл происходящих событий, оценивать прошлое, заглядывать в будущее.

Важно то, что информация может фиксироваться, накапливаться и передаваться как на естественных, так и на искусственных носителях (ресурсная проекция информации). В таком качестве информация (биологическая, генетическая) является необходимым ресурсом эволюции природы и основным (социальная, духовная) ресурсом развития цивилизации.

Наконец, информация – это и то, что непосредственно отражает окружающую реальность (фоновая проекция информации). Именно отражение (в философском осмыслении) представляет атрибутивное проявление информации, ставит ее в один ряд с материей и энергией. В то же время фоновая информация может оказывать воздействия, которые обходят защитные функции сознания.

В силу того, что жизнь общества и деятельность людей построены на информационных взаимодействиях, используя представления о реактивной, ресурсной и фоновой проекциях информации, мы получаем трехмерную систему координат, в которой раскрываются самые разнообразные процессы, явления, понятия [4]. Так, в глубинной, пролонгированной информационной войне, которая ведется годами, десятилетиями и даже веками, выделяются ментальные, когнитивные и смысловые компоненты воздействий на сознание людей и народов.

Ментальная война – это, о чем будет думать человек, каким будет его мировоззрение, главное, каким будет его отношение к своей стране, как к родной, которую любишь и защищаешь, или как к чужой, которую бросаешь в поисках «лучшей жизни» и предаешь (ресурсный – мировоззренческий вектор пролонгированной информационной войны).

Когнитивная война – это, как будет думать человек, в какой парадигме будет формироваться его сознание, главное, какое он получит образование, освоит фундаментальные знания, научится мыслить или лишь овладеет теми или иными компетенциями, чтобы быть способным зарабатывать и потреблять (реактивный – образовательный вектор пролонгированной информационной войны).

Смысловая война – это, чем должна наполняться жизнь человека: высокими идеалами, творчеством, любовью, духовными стремлениями или, скажем, потребительством, получением удовольствий, уходом в мир иллюзий, наркотиков, игр, виртуальной реальности (фоновый – идеологический вектор глубинной информационной войны).

Теоретические основы информационных войн уже весьма детально разработаны нашими противниками. Данные теории прошли апробацию в многочисленных цветных революциях, государственных переворотах, обеспечении вооруженных вторжений, политических и экономических акциях, в культурных и образовательных интервенциях, в создании аттракторов социального хаоса в разных странах и регионах мира.

В информационном противоборстве, направленном на обеспечение безопасности социальных сфер, важно различать информационно-психологические операции по дестабилизации общественных отношений здесь и сейчас и акции глубинной многоэтапной ментально-когнитивной смысловой войны.

В то же время наибольшие угрозы безопасности личности, обществу и государству таятся в глубинной многоплановой информационной войне, в ходе которой осуществляются более скрытые, замаскированные воздействия на сознание народов, сообществ, представителей элиты и лиц, принимающих решения.

Удары этой ментально-когнитивной смысловой войны происходят по исторической памяти народов, напрямую затрагивают проблемы демографии, а основным полем боя здесь была и остается идеология.

Список литературы

1. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: <https://www.garant.ru/products/ipo/prime/doc/71456224/?ysclid=lh6buiifsvn209551170>.
2. Веллер М. Киев – Москва. Расхождение. М. : АСТ, 2023.
3. Уэбстер Ф. Теория информационного общества / пер. с англ. М. : Аспект Пресс, 2004.
4. Овчинский А. С., Борзунов К. К., Чеботарева С. О. Информационные координаты. Управление. Противоборство. Безопасность. М. : Горячая линия – Телеком, 2018.

Андреев И. В.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Овчинский А. С.,

профессор кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

доктор технических наук, профессор, Академик РАЕН

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С ТЕХНОЛОГИЯМИ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

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

Общепринятое определение виртуальной реальности – 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. Технология виртуальной реальности может быть полезна в самых разных сферах жизни человека.

Военная сфера. Технология виртуальной реальности используется в военных целях, чтобы улучшить подготовку военнослужащих и увеличить их эффективность в боевых действиях. Например, специалисты могут создавать целые сценарии боевых действий, которые военнослужащие могут разыгрывать в виртуальной среде. Это позволяет устранить риски, которые могут возникнуть во время реальных учений, и снизить расходы на их проведение.

Криминальная сфера. Преступники могут использовать технологию виртуальной реальности для тренировки перед совершением преступлений. Например, они могут создавать виртуальные сцены грабежей, ограблений и других противоправных действий, чтобы подготовиться к их выполнению. Также технология виртуальной реальности может использоваться в расследовании преступлений для восстановления сцен происшествий и идентификации подозреваемых.

¹ © Андреев И. В., 2023.

Общебытовое использование. Технология виртуальной реальности может быть полезна в самых разных сферах жизни человека. Например, она может использоваться для образовательных целей, имитируя экспериментальные ситуации или виртуальные лекции.

Потенциальные угрозы. Рассмотрим некоторые из них.

Физическая безопасность: Носители VR могут потерять чувство реальности и не заметить опасности в реальном мире, в котором они находятся. Например, они могут не заметить, что подошли к обрыву или к огню, что может привести к травме или пожару.

Зависимость: Некоторые пользователи могут стать зависимыми от VR. Это может привести к заболеваниям и угрожать здоровью их производительности на работе [3].

Опасность злоупотребления: Некоторые люди могут использовать виртуальную реальность в качестве эскапизма, чтобы избегать реальности и жизненных проблем. Они могут стать зависимыми от виртуального мира и начать игнорировать свои обязанности и личные отношения [4].

Социальные нормы и этика: Многие виртуальные миры могут создавать свои собственные культуры и социальные нормы, которые не соответствуют традиционным. Это может привести к недопониманию и конфликтам в реальной жизни.

Воздействие на психическое здоровье: Некоторые исследования показывают, что долгое использование VR может иметь влияние на психическое здоровье пользователя, такое как увеличение уровня тревожности и депрессии.

Положительное воздействие виртуальной реальности. В первую очередь оно заключается в возможности использования воздействия виртуальной реальности в медицинских целях для лечения различных психических расстройств. Так, например, виртуальная реальность может использоваться для лечения посттравматического стрессового расстройства, фобий, депрессии и других состояний. Виртуальная реальность позволяет пациентам находиться в контролируемой среде симуляции, что помогает им постепенно привыкнуть к стимулам, вызывающим страх или тревогу. Например, если у пациента есть фобия перед высотой, то виртуальная реальность может помочь ему справиться с этим страхом, предоставив ему возможность постепенно привыкнуть к высоте.

Список литературы

1. URL: <https://habr.com/ru/companies/droider/articles/538748/>.
2. URL: https://www.kaspersky.ru/resource-center/threats/security-and-privacy-risks-of-ar-and-vr?referer2=tcid_admitad_e09780ea6401b0cda28c0fa575cab41c_442763_x4&tagtag_uid=e09780ea6401b0cda28c0fa575cab41c.
3. URL: <https://habr.com/ru/companies/trendmicro/articles/481954/>.
4. URL: <https://virtre.ru/articles/virtual-reality/vred-virtualnoj-realnosti-dlya-zdorovya-i-psixiki.html>.

Борзунов К. К.¹,

доцент кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук, старший научный сотрудник

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ ДЕСТРУКТИВНЫХ ИДЕОЛОГИЙ В РОССИИ

1. Актуальность борьбы с деструктивными идеологиями. Определяется на современном этапе, прежде всего, стремлением Запада, внешне проявляя некое позитивное «миссионерство», навязать России собственные мировоззрение, идеалы, традиции, политическое и государственное устройство, считая ее страной, нуждающейся в некоем «попечении».

Запад, используя внедрение деструктивных идеологий, по факту осуществляет эгоистическую политику, направленную на полное подчинение жизни населения России в целях удовлетворения исключительно западных нужд и потребностей, на перевод страны в состояние внешнего управления и безропотного послушания интересам Запада, перевода России в состояние сырьевого придатка.

2. Представления о деструктивных идеологиях. В процессе становления личности (в ходе воспитания, социализации, образования...) формируется жизненная позиция отдельно взятого индивидуума. Естественно взрослея, человек при этом придерживается определенной идеологии [1] – некой системы политических, правовых, нравственных, религиозных, эстетических и философских взглядов и идей, в которых осознаются и оцениваются отношения людей к действительности.

Воздействие деструктивной идеологии (последствие) всегда связывалось с таким понятием, как «деструктивное поведение». И в этом контексте развивались, в свою очередь, представления о деструкции (ее видах и симптомах); деструктивном поведении (его причинах и признаках, особенностях) и, как итог, о деструктивных отношениях, критике и общении, конфликте, чувствах и эмоциях, мыслях и разговорах, характерах, личностях, влияниях, видах деятельности...

3. Деструктивные идеологии как угроза национальной безопасности государства. В общем уже давно (несколько десятилетий) внедрение Западом деструктивных идеологий на территории России направлено на потерю традиционного воспитания подрастающего поколения, образования населения, формирования самостоятельного мировоззрения, морали и этики, дестабилизацию государственного и социального управления в стране.

«Глобалистами» приветствовались тенденции воспитания населения в духе отсутствия каких бы то ни было традиционных ценностей, приверженности к неким глобальным идеалам – без границ, без Родины – и, прежде всего, потребительского отношения к жизни.

¹ © Борзунов К. К., 2023.

Текущая ситуация в России такова, что дальнейшее появление и распространение деструктивных идеологий влекут за собой следующие риски [2]:

1. Внедрение антиобщественных стереотипов поведения, распространение аморального образа жизни, вседозволенности и насилия, рост употребления алкоголя и наркотиков.

2. Причинение вреда нравственному здоровью людей, навязывание представлений, предполагающих отрицание человеческого достоинства и ценности человеческой жизни.

3. Создание условий для саморазрушения общества, ослабление семейных, дружеских и иных социальных связей.

4. Формирование общества, пренебрегающего духовно-нравственными ценностями.

5. Усиление социокультурного расслоения общества, снижение роли социального партнерства, обесценивание идей созидательного труда и взаимопомощи.

6. Искажение исторической правды, разрушение исторической памяти.

7. Отрицание российской самобытности, ослабление общероссийской гражданской идентичности и единства многонационального народа России, создание условий для межнациональных и межрелигиозных конфликтов.

8. Подрыв доверия к институтам государства, дискредитация идеи служения Отечеству, формирование негативного отношения к воинской службе и государственной службе в целом.

4. Противодействие деструктивным идеологиям. В условиях тотального решения задач коллективным Западом – «выключить Россию из мирового сообщества» и «окончательно решить русский вопрос» – приходится принимать, в частности, меры по противодействию деструктивным идеологиям.

Предварительно следует отметить, что решение проблемы находится и в сфере правоохранительной деятельности, и в сфере государственного управления, и в рамках социального партнерства государственных структур с общественными организациями, избравшими направление деятельности, связанное с противодействием распространению деструктивных идеологий и борьбе с ними.

Объектами контроля и защиты от проникновения и распространения деструктивных идеологий могут быть: общеобразовательные организации, осуществляющие основную деятельность по программам начального общего, основного общего и среднего общего образования; профессиональные образовательные организации, осуществляющие основную деятельность по образовательным программам среднего профессионального образования и по программам профессионального обучения; образовательные организации высшего образования, осуществляющие основную деятельность по образовательным программам высшего образования и научную деятельность.

Следует отметить, что среди зарегистрированных на территории России многочисленных и различных некоммерческих общественных организаций практически не реализуется активная координация мероприятий, направленная на противодействие деструктивным идеологиям.

Объектами контроля процессов проникновения и распространения деструктивных идеологий могут быть также и научно-исследовательские организации, высокотехнологичные и передовые производства, прежде всего, и многочисленные трудовые коллективы в промышленности и сельском хозяйстве. Определенные трудности возникают в связи с тем, что требуется устанавливать и подтверждать приверженность определенной именно деструктивной идеологии, поскольку в Российской Федерации признается идеологическое многообразие и никакая идеология не может устанавливаться в качестве государственной или обязательной [10; пп. 1 и 2 ст. 13].

Стратегия противодействия экстремизму в Российской Федерации до 2025 года [9] и по отношению к этим рассмотренным объектам является универсальным правовым средством их защиты.

Уважительное и трепетное в определенной мере отношение к чувствам верующей части населения усложняет осуществление противодействия деструктивным идеологиям, их появлению и распространению.

Особыми объектами контроля процессов проникновения и распространения деструктивных идеологий могут быть многочисленные и разнообразные сайты, блоги, чаты... в виртуальном пространстве социальных сетей – паутин. Основные уязвимости и сложности противодействия появлению и распространению деструктивных идеологий в виртуальном пространстве связаны с анонимностью пользователей сети; с применением динамических IP-адресов узлов, серверов, компьютеров и гаджетов, включенных в сеть, и их возможной мобильностью; с нахождением некоторых объектов за пределами территории Российской Федерации... Однако и в этой ситуации Стратегия противодействия экстремизму в Российской Федерации до 2025 года [9] используется как универсальное правовое средство защиты от появления и распространения деструктивных идеологий. А в отношении защиты детей применяется как универсальное правовое средство – Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» [8].

5. Выводы. Перспективные направления противодействия распространению деструктивных идеологий в России связаны с различными сферами.

Традиционной сферой является законотворческая деятельность. И в ней уже обозначаются предложения по ужесточению наказания преступлений экстремистской и террористической направленности. В условиях проведения специальной военной операции (СВО) на Украине рассматриваются поправки в УК и КоАП об ответственности за дискредитацию участников СВО [11]. В сфере правоохранительной деятельности наблюдается активизация аналитических исследований, направленных на выявление: реальных угроз появления и распространения деструктивных идеологий в России; конкретных лиц, непосредственно причастных к культивированию деструктивных идеологий, участвующих в дестабилизации социальной обстановки на территории России, дискредитирующих участников СВО, создающих и распространяющих дипфейки и т. д.

В духовно-нравственной, политической и идеологической сферах общественные организации и объединения, в сферах культуры и искусства средства массовой информации, телевидение и кинопрокат определенно очищают сознание

от деструкции и пропагандируют традиционный уклад жизни народов и народностей, патриотическое поведение граждан и отношение к событиям, происходящим в стране, укрепляют веру и надежду, дух населения.

В социальной сфере Правительство России предпринимает всевозможные меры, направленные на стабилизацию экономики страны, поддержку граждан в условиях международных санкций коллективного Запада и проведения СВО.

Список литературы

1. Энциклопедический словарь. 2009. URL: <http://niv.ru/doc/dictionary/encyclopedic/fc/slovar-200-6.htm#zag-45735>.
2. Указ Президента Российской Федерации от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». URL: <https://www.garant.ru>.
3. Минобрнауки объявило, что все российские вузы исключили из Болонского процесса. URL: <https://habr.com/ru/news/t/669866>.
4. Цитата по ТАСС. URL: <https://www.kommersant.ru/doc/5392347>.
5. Послание Президента Федеральному Собранию. 21 февраля 2023 г. URL: <http://www.kremlin.ru/events/president/transcripts/statements/70565>.
6. Основные направления деятельности Совета Безопасности РФ. URL: <http://www.scrf.gov.ru/about/history>.
7. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (ред. от 17.02.2023) (с изм. и доп., вступ. в силу с 28.02.2023). URL: <https://www.garant.ru>.
8. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (последняя редакция). URL: <https://www.garant.ru>.
9. Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года». URL: <https://www.garant.ru>.
10. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г. URL: <https://www.garant.ru>.
11. Что считается дискредитацией СВО: новости, примеры. URL: <https://iz.ru/1477314/shaipova-mariia/sem-let-za-feiki-nakazanie-za-diskreditaciiu-svo-uzhestochat>.

*Халимбеков Хасанбек Иброхим угли¹,
слушатель факультета подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

*Борзунов К. К.,
доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, старший научный сотрудник*

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Сфера ИИ. Искусственный интеллект (ИИ) – это область науки, которая изучает, как компьютеры могут выполнять задачи, которые раньше требовали наличия человеческого интеллекта для их выполнения. В основе ИИ лежат алгоритмы машинного обучения и нейронные сети, которые позволяют компьютерам извлекать знания из больших объемов данных и использовать их для решения задач. ИИ имеет широкий спектр применений, от автоматизации производственных процессов и управления логистикой до медицинской диагностики и развлечений.

История искусственного интеллекта начинается с появления первых идей о создании машин, способных думать, в 1950-х годах. В 1956 году в Дартмутском колледже (США) состоялась первая конференция по искусственному интеллекту, где был сформулирован термин «искусственный интеллект». В это время многие ученые считали, что создание машин, способных мыслить, как люди, было вполне реальным. Однако к середине 1970-х годов начало распространяться разочарование в области искусственного интеллекта. Развитие технологий шло не так, как ожидалось, и проблемы обработки больших объемов данных и сложных алгоритмов машинного обучения оставались нерешенными. В 1980-х годах, в связи с появлением более мощных компьютеров и новых методов обработки данных, искусственный интеллект снова стал актуальной темой.

Искусственный интеллект имеет огромное значение в современном мире, так как он является ключевой технологией для решения многих современных проблем. Ниже приведены некоторые области, где ИИ имеет большое значение.

Медицина: Искусственный интеллект может использоваться для обработки медицинских данных, анализа снимков. ИИ может помочь в диагностике заболеваний и повысить ее точность, в разработке индивидуальных планов лечения на основе анализа медицинских данных и ускорить процесс лечения.

Производство: Искусственный интеллект может автоматизировать производственные процессы и повысить качество продукции.

Логистика: Искусственный интеллект может оптимизировать логистические процессы и уменьшить время доставки товаров.

¹ © Халимбеков Хасанбек Иброхим угли, 2023.

Бизнес: Искусственный интеллект может автоматизировать и оптимизировать бизнес-процессы.

Финансы и банки: Искусственный интеллект может помочь в анализе финансовых рынков и в принятии решений по инвестиционной деятельности банков.

Транспорт: Искусственный интеллект может управлять автономными автомобилями и улучшить безопасность дорожного движения.

Образование: Искусственный интеллект может помочь в персонализации образования и разработке индивидуальных планов обучения.

Правоохранительная деятельность: Искусственный интеллект может контролировать дорожное движение и соблюдение общественного порядка в публичных местах, распознавать лица граждан, находящихся в розыске, и анализировать большие объемы данных.

Развлечения: Искусственный интеллект может создавать интерактивные игры и развлекательные приложения.

Технологии искусственного интеллекта включают в себя различные методы и алгоритмы, которые позволяют компьютерным системам обрабатывать информацию и использовать ее для решения задач. Ниже представлены некоторые из основных технологий ИИ.

Машинное обучение – это технология, которая позволяет компьютерным системам «учиться» на основе данных и алгоритмов. Машинное обучение используется для создания систем распознавания образов, систем рекомендаций, анализа текстов и многого другого.

Нейронные сети – это технология, которая моделирует работу мозга для обработки информации. Нейронные сети используются для распознавания образов, анализа текстов и данных, а также для создания автономных систем, таких как роботы и автомобили.

Обработка естественного языка – это технология, которая позволяет компьютерным системам понимать и генерировать естественный язык. Обработка естественного языка используется для создания систем автоматического перевода, голосовых помощников и анализа текстов.

Робототехника – это технология, создающая автономные системы, которые могут выполнять физические задачи. Робототехника используется в производстве, медицине, науке и многих других областях.

Обработка изображений – это технология, которая позволяет компьютерным системам анализировать и распознавать изображения. Обработка изображений используется для создания систем видеонаблюдения, распознавания лиц, транспортных средств, критических ситуаций и многого другого.

Риски ИИ. С развитием искусственного интеллекта возникает ряд вопросов [1], связанных с безопасностью и приватностью данных, которые обрабатываются моделями ИИ. В частности, существует риск утечки конфиденциальной информации, а также возможность использования ИИ для злоумышленных целей. Одной из основных угроз для безопасности данных в ИИ является атака на модели машинного обучения, которая может привести к искажению данных и введению ложных результатов. Это может быть особенно опасно в случае при-

менения ИИ в критических отраслях, таких как медицина или авиация, контроль общественного порядка и дорожного движения. Регулирование обработки данных становится все более строгим, поэтому компании должны обеспечить соблюдение соответствующих правил и нормативных актов. Для обеспечения безопасности и конфиденциальности данных в ИИ существуют различные методы, такие как шифрование данных, контроль доступа, аутентификация и авторизация пользователей, а также мониторинг защиты данных и применение соответствующих методов борьбы с атаками.

Достижения ИИ. Развитие искусственного интеллекта привело к возникновению множества новых рабочих мест и профессий, а также к изменению требований, которые уже существуют. В этом контексте занятость в области ИИ представляет собой перспективную возможность для специалистов в различных областях. Одной из основных областей работы в ИИ являются разработка и создание моделей машинного обучения, которые могут быть применены в различных сферах. Еще одной областью работы в ИИ являются инженерия данных, которая включает в себя работу с базами данных и инфраструктурой хранения и обработки данных. Кроме того, важным направлением в ИИ являются исследование и разработка новых методов машинного обучения и анализа данных.

Перспективы и будущее ИИ. С развитием технологий искусственного интеллекта возникает вопрос о том, кто несет ответственность за принятие решений, принимаемых системами ИИ. Важно понимать, что системы ИИ не являются субъектами права и не могут нести ответственность за свои действия.

Применение систем ИИ не должно нарушать права и свободы человека, приватность; безопасность людей, наносить вред людям; проявлять предвзятость, дискриминировать отдельных лиц или групп людей.

Развитие ИИ вызывает оправданные опасения по поводу безопасности и недопустимости автономных систем, которые могут принимать решения без контроля и могут наносить вред людям. Важно учитывать эти аспекты при разработке и применении систем ИИ.

В заключение следует отметить, что искусственный интеллект представляет собой одно из самых перспективных направлений в современной технологии и его развитие будет продолжаться в будущем. Возможности технологий ИИ уже сегодня ощутимо изменяют многие области жизни.

Список литературы

1. Стратегическая технология: перспективы и риски генеративного ИИ. URL: <https://trends.rbc.ru/trends/industry/64380a4d9a7947a90164ccfe>.
2. Фомина А. Н. Проблемы и перспективы развития рынка искусственного интеллекта в России. URL: <https://1economic.ru/lib/114607>.
3. Будущее искусственного интеллекта. URL: <https://invlab.ru/tehnologii/budushhee-iskusstvennogo-intellekta/>.

*Хотамов Мухаммадали Маликбой угли¹,
слушатель факультета подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

*Борзунов К. К.,
доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук, старший научный сотрудник*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ BIOS И UEFI

С созданием первых персональных компьютеров стало очевидно, что требуется создание оперативного системного устройства для ввода и вывода. Базовая система ввода-вывода (basic input and output system, в дальнейшем BIOS) запускается при загрузке компьютера, контролирует и отвечает за подключение комплектующих элементов вычислительной системы, устанавливает порядок их взаимодействия. BIOS является посредником между операционной системой и комплектующими элементами вычислительной системы и без него операционная система, в частности семейства Windows, просто не будет загружаться [1].

Понятие, история создания, особенности и виды BIOSa. Итак, BIOS – базовая система ввода и вывода. В целом BIOS отвечает за запуск и за настройку комплектующих элементов компьютера. BIOS можно рассматривать и как набор микропрограмм, реализующих низкоуровневые наборы компонентов, с помощью которых можно использовать аппаратное обеспечение компьютера, а также создающих необходимую программную среду для запуска операционной системы у IBM PC-совместимых компьютеров. BIOS относится к системному программному обеспечению [2].

Сразу после включения питания компьютера процессор читает код BIOS из ПЗУ, записывает его в ОЗУ (оперативную память) и передает управление коду BIOS. Прежде всего, код BIOS запускает программу тестирования – POST (от англ. power-on self-test), которая начинает проверку аппаратного обеспечения компьютера. В ходе этого тестирования код BIOS проверяет работоспособность контроллеров, расположенных на материнской (системной) плате, задает низкоуровневые параметры их работы (в частности, частоту шины и параметры центрального микропроцессора, контроллера оперативной памяти, контроллеров FSB, AGP, PCI, USB).

BIOS реализует API – набор компонентов, с помощью которых какая-либо программа может использовать другую программу для работы с внутренними и внешними устройствами компьютера. Загрузчик и сама ОС используют этот API для работы с оборудованием до тех пор, пока не загрузятся собственные драйверы оборудования.

¹ © Хотамов Мухаммадали Маликбой угли, 2023.

Однако, используя BIOS, можно создавать лишь MBR-диски с соответствующей организацией до четырех разделов (трех основных и одного дополнительного по максимуму) и нельзя загрузить операционную систему с жесткого диска объемом больше 2 Тбайт. А при попытке использовать GPT-диск, BIOS не «понимает» соответствующую организацию разделов, пытается ее «исправить» и тем самым полностью нарушает организацию хранения данных на диске, который для дальнейшего применения не пригоден и требует по-новому создавать разделы – структуру хранения данных.

Итак, с одной стороны, BIOS представляет собой набор микропрограммных чипов, установленных на материнской плате. С другой стороны, BIOS записывается только на энергонезависимых устройствах (памяти). На материнской (системной) плате BIOS выглядит в виде микросхемы рядом с батареей.

Существует несколько видов микросхем, на которых можно установить (записать) BIOS.

Стираемое перепрограммируемое Постоянно Запоминающее Устройство (далее – *стираемое перепрограммируемое ПЗУ*). ПЗУ – это устройство, которое запоминает информацию даже, если отключено полностью электропитание. Содержание стираемого перепрограммируемого ПЗУ может быть стерто при воздействии ультрафиолета (это форма электромагнитного излучения с длиной волны от 10 нм до 400 нм). Этот вид микросхемы считается устаревшим и в настоящее время практически не используются.

Электрически стираемое перепрограммируемое ПЗУ – является современным видом микросхемы для записи BIOS и перепрограммировать такие микросхемы легче, так как данные можно стереть посредством электрических сигналов, даже не вынимая чип из материнской платы при обновлении BIOSa.

Особенность BIOSa заключается в том, что без нее компьютер не может запускаться после подачи электропитания. Компьютер является программно-управляемым устройством, а микросхема BIOSa как раз и содержит набор микропрограмм – инструкции работы персонального компьютера в период первичной инициализации.

Понятие, история создания, особенности и виды UEFI. История развития UEFI берет свое начало с середины 1990-х гг. [4]. В те годы уже BIOS не был достаточным для работы мощных серверов. Поэтому для первых систем Intel-HP Itanium была разработана новая технология, которая получила название Intel Boot Initiative. Немного позже название было сменено на EFI или Extensible Firmware Interface. Первой официальной спецификацией UEFI является EFI 1.02, которая была создана в 12 декабря 2000 г. В 2005 г. была сформирована компания под названием Unified EFI Forum или UEFI Forum, а микросхема сменила название от EFI на UEFI.

Extensible Firmware Interface (в дальнейшем – UEFI) можно рассматривать одновременно, и как это унифицированный расширяемый интерфейс прошивки – обновленный набор микропрограмм BIOS, и как вид микросхем, который пришел на замену устаревшему BIOS.

Сравнение BIOS и UEFI. В частности, UEFI или, как его иногда обозначают UEFI BIOS, имеет новые возможности по сравнению с устаревшим BIOS:

- не зависит от архитектуры процессора и может использоваться как с x86 процессорами, так и с процессорами на базе архитектуры ARM;
- графический интерфейс для настройки оборудования с поддержкой мышки, который намного удобней аскетичного интерфейса BIOS;
- позволяет выполнять многие задачи, круг которых приближает прошивку к сильно ограниченному состоянию операционной системы;
- встроенный менеджер загрузки, который позволяет выполнять загрузку операционной системы как с MBR-дисков объемом до 2 Тбайт, так и GPT-дисков.

Следует отметить также, что UEFI за счет параллельного тестирования компонентов компьютера сокращает время, которое проходит от момента включения компьютера до момента начала работы операционной системы, как минимум на две секунды.

Современные операционные системы используют BIOS только на этапе начальной загрузки (так называемый bootstrapping). После этого к BIOS не обращаются, а все функции операционной системы по управлению устройствами переходят к драйверам устройств. Процедуры BIOS выполняются только в реальном режиме работы процессора, когда ядро операционной системы работает в защищенном режиме. MBR содержит небольшие по объему таблицу разделов и загрузчик. Раздел, на котором установлена операционная система, выбирается с помощью флага активного раздела, указанного в ячейке таблицы разделов. Таким образом, можно загружать только те операционные системы, ядро которых находится на активном разделе.

Для сохранения информации BIOS использует MBR (от англ. Master Boot Records – основную загрузочную запись), а UEFI использует GUID (от англ. Globally Unique Identifier – глобальный уникальный идентификатор) или, как говорят, расширенную таблицу разделов GUID (GPT).

Список литературы

1. БИОС (BIOS) – что это такое и зачем нужен простыми словами БИОС. URL: <https://dzen.ru/a/YNDYJlmKpwvUtux2>.
2. Что такое БИОС простыми словами. Как зайти на ноутбуке и компьютере. URL: <https://itspectr.ru/chto-takoe-bios-prostymi-slovami-kak-zajti-na-noutbuke-i-kompyutere/>.
3. Адриан Вонг Оптимизация BIOS. Полный справочник по всем параметрам BIOS и их настройкам. 3-е изд. : «ДМК Пресс», 2005. 350 с.
4. Что такое UEFI. URL: <https://wiki.osdev.org/UEFI>.
5. UEFI vs BIOS: в чем разница? Что такое <https://dzen.ru/a/Y6IELXXn1QretU7k>.

Казаков М. 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*

MITM-АТАКИ И ИХ ПРЕДОТВРАЩЕНИЕ

В последнее время в современном обществе участились атаки, нацеленные на конфиденциальные данные пользователей и владельцев кредитных карт, одна из них носит название: «MITM – Man in the middle» атака или же в переводе «Человек посередине».

Данное понятие гласит, когда преступник обозначает себя в диалоге между клиентом и приложением – или же для прослушивания, либо для того, чтобы выдать себя за оператора, создавая впечатление, что совершается обычный обмен информацией.

Как правило, такие атаки нацелены на пользователей финансовых, курьерских и иных приложений, в которых требуется ввод номера дебетовой карты или же виртуального кошелька.

Данные, полученные во время атаки, используются для различных целей, как правило, это несанкционированные переводы средств.

Самым простым примером такой атаки является, когда почтальон открывает вашу банковскую выписку, записывает данные вашего счета, а затем запечатывает конверт и доставляет его к вашей двери.

Успешное выполнение атаки выполняется через перехват и дешифрование. Примером может служить общественная сеть отеля, злоумышленник называет ее достаточно просто, чтобы отвести все подозрение, например, Moskva Hotel Wi-Fi Free. Как только жертва подключается к такой точке доступа, злоумышленник получает полный доступ к любому онлайн-обмену информации.

Злоумышленники, стремящиеся применить более активный подход к перехвату, могут совершить одну из следующих атак.

ARP-подмена – это процесс связывания MAC-адреса злоумышленника с IP-адресом законного пользователя в локальной сети с использованием поддельных сообщений ARP. В результате данные, отправленные пользователем на IP-адрес хоста, вместо этого передаются злоумышленнику.

Подмена DNS, также известная как отравление кэша DNS, включает в себя проникновение на DNS-сервер и изменение адресной записи веб-сайта. В резуль-

¹ © Казаков М. Б., 2023

тате пользователи, пытающиеся получить доступ к сайту, отправляются измененной записью DNS на сайт злоумышленника.

После перехвата любой двусторонний SSL-трафик должен быть расшифрован без предупреждения пользователя или приложения. Для достижения этой цели существует ряд методов:

Подмена HTTPS отправляет поддельный сертификат в браузер жертвы после выполнения первоначального запроса на подключение к защищенному сайту. Он содержит цифровой отпечаток большого пальца, связанный со скомпрометированным приложением, которое браузер проверяет в соответствии с существующим списком надежных сайтов. Затем злоумышленник может получить доступ к любым данным, введенным жертвой, до того, как они будут переданы приложению.

Блокирование атак MITM требует нескольких практических шагов со стороны пользователей, а также сочетания методов шифрования и проверки приложений.

1. Избегайте подключений Wi-Fi, которые не защищены паролем.
2. Обращая внимание на уведомления браузера, сообщающие о том, что веб-сайт является незащищенным.
3. Немедленный выход из защищенного приложения, когда оно не используется.
4. Не использовать общедоступные сети (например, кафе, отели) при проведении конфиденциальных транзакций.

Обычному обывателю интернета стоит в первую очередь защитить свой компьютер и браузер, а также воздержаться от подключения к бесплатным Wi-Fi сетям.

Лузганов Д. В.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

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

КОРРЕЛЯЦИОННЫЙ АНАЛИЗ ДАННЫХ ЦИФРОВОГО ПРОФИЛЯ ГРАЖДАНИНА РОССИЙСКОЙ ФЕДЕРАЦИИ В ЦЕЛЯХ ИДЕНТИФИКАЦИИ ЛИЦ

Анализ данных цифрового профиля гражданина РФ в целях идентификации лиц является важной темой, которая становится все более актуальной в современном мире. Рассмотрим, что такое цифровой профиль гражданина, какие данные в него входят, а также, какие методы и инструменты используются для анализа данных цифрового профиля гражданина РФ в целях идентификации лиц.

Что такое цифровой профиль гражданина?

Цифровой профиль гражданина – это совокупность информации, которая относится к конкретному человеку и хранится в различных базах данных. В цифровой профиль могут входить данные о личности гражданина (Ф.И.О., дата рождения, место жительства), информация о его документах (паспорт, водительское удостоверение), данные о работе и доходах, а также информация об использовании различных сервисов и социальных сетей.

Анализ данных цифрового профиля гражданина Российской Федерации в целях идентификации лиц может быть необходимым в различных ситуациях. Например, при проведении расследования в рамках уголовного дела, при идентификации мошенников, при проверке соответствия кандидата на выборных должностях требованиям закона. В этих случаях необходимо определить, кто является владельцем конкретного цифрового профиля и какие данные в него входят.

Анализ данных цифрового профиля гражданина Российской Федерации в целях идентификации лиц может проводиться с использованием различных методов и инструментов. Рассмотрим некоторые из них:

Кросс-проверка данных. Этот метод заключается в сравнении информации, которая содержится в различных базах данных. Например, данные о паспорте можно сравнить с информацией, которая содержится в базах ФНС и ПФР. Если в данных есть расхождения, то это может свидетельствовать о том, что цифровой профиль может использоваться несанкционированными лицами.

¹ © Лузганов Д. В., 2023.

Анализ поведения в интернете. С помощью специальных программ можно проанализировать активность пользователя в интернете, например, какие сайты он посещает, какие запросы отправляет в поисковых системах, какие приложения использует, и т. д. Это позволяет составить цифровой портрет пользователя и выявить несоответствия между реальной личностью и данными в цифровом профиле.

Машинное обучение и анализ больших данных. С помощью методов машинного обучения можно обрабатывать большие объемы данных и автоматически выделять из них признаки, которые свидетельствуют о том, что цифровой профиль принадлежит конкретному человеку. Например, на основе анализа поведения в интернете можно выделить характеристики, которые свойственны именно этому человеку.

Социальная инженерия. Этот метод заключается в использовании психологических приемов для получения доступа к информации о цифровом профиле. Например, мошенники могут обратиться к пользователю с просьбой подтвердить свою личность или передать конфиденциальную информацию.

Корреляционный анализ – это статистический метод, используемый для изучения отношений между двумя или более переменными. В контексте цифрового профиля гражданина Российской Федерации корреляционный анализ может быть использован для идентификации лиц на основе данных, собранных из различных источников.

Цифровой профиль гражданина Российской Федерации включает в себя различные данные, такие как персональную информацию, биометрические данные, местоположение и историю действий в интернете. Эти данные могут быть использованы для идентификации личности гражданина РФ. Однако такие данные могут быть представлены в разных форматах и храниться в разных системах, что усложняет их сбор и анализ.

Важным аспектом корреляционного анализа является коэффициент корреляции. Коэффициент корреляции – это числовое значение, которое показывает степень взаимосвязи между двумя переменными. Коэффициент корреляции может быть положительным, если значения двух переменных растут вместе, отрицательным, если одна переменная растет, а другая убывает, или равным нулю, если между переменными нет взаимосвязи.

При использовании корреляционного анализа в цифровом профиле гражданина Российской Федерации можно использовать различные методы для сбора и анализа данных. Например, можно использовать методы машинного обучения для автоматического извлечения данных из различных источников и определения связей между ними. Кроме того, можно использовать методы визуализации данных, такие как диаграммы рассеяния, для представления связей между переменными в наглядной форме.

Однако при использовании корреляционного анализа в анализе данных цифрового профиля гражданина Российской Федерации в целях идентификации лиц следует учитывать некоторые важные аспекты.

Во-первых, необходимо убедиться в правомерности сбора и использования данных цифрового профиля гражданина Российской Федерации. Сбор и исполь-

зование личных данных регулируется законодательством Российской Федерации, и нарушение правил может привести к серьезным последствиям.

Во-вторых, следует учитывать возможные ошибки и неточности в данных, которые могут исказить результаты корреляционного анализа. Например, необходимо учитывать возможные ошибки при сборе биометрических данных или неточности в персональной информации.

В-третьих, необходимо учитывать ограничения корреляционного анализа, который может показать только наличие или отсутствие взаимосвязи между переменными, но не дает причинно-следственных связей между ними. Для получения полной картины необходимо использовать дополнительные методы анализа данных.

Наконец, следует учитывать этические аспекты при использовании корреляционного анализа в целях идентификации лиц. Например, необходимо убедиться в том, что анализ данных не будет использоваться для дискриминации, преследования или нарушения прав граждан.

В целом корреляционный анализ является полезным инструментом для анализа данных цифрового профиля гражданина Российской Федерации в целях идентификации лиц. Однако его использование должно быть осуществлено в соответствии с правилами и законодательством Российской Федерации, с учетом ограничений и ошибок в данных, а также с учетом этических аспектов.

В заключение анализ данных цифрового профиля гражданина Российской Федерации в целях идентификации лиц – это сложный и многогранный процесс, который требует специальных знаний и навыков. Правильное использование методов и инструментов позволяет обеспечить безопасность и защиту персональных данных граждан, а также повысить эффективность работы правоохранительных органов и других государственных учреждений.

Список литературы

1. Виноградов Е. В. Цифровой профиль: понятие, механизмы регулирования и проблемы реализации // URL: <https://cyberleninka.ru/article/n/tsifrovoy-profil-ponyatie-mehanizmy-regulirovaniya-i-problemy-realizatsii/viewer>.
2. Наумов В. Б. Информационно-правовые вопросы идентификации при использовании цифрового профиля // URL: <https://cyberleninka.ru/article/n/informatsionno-pravovye-voprosy-identifikatsii-pri-ispolzovanii-tsifrovogo-profilya/viewer>.
3. Цифровой профиль гражданина Российской Федерации // URL: https://www.tadviser.ru/index.php/Статья:Цифровой_профиль_гражданина_РФ.
4. Кондаков А. М., Костылева А. А. Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы // Вестник Российского университета дружбы народов. Серия : Информатизация образования. 2019. Т. 16. № 3. С. 207–218.
5. Сценарии использования инфраструктуры Цифрового профиля // URL: https://digital.gov.ru/uploaded/presentations/stsenariiispolzovaniyatspv10-2.pdf?utm_referrer=https%3a%2f%2fyandex.ru%2f.

Лиманская А. Р.¹,

слушатель Института судебной экспертизы

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Завьялова А. А.,

*доцент кафедры технико-криминалистического обеспечения
экспертных исследований*

Московского университета МВД России имени В.Я. Кикотя,

кандидат химических наук

АЛГОРИТМ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ ПО УСТАНОВЛЕНИЮ ОБЩЕГО ИСТОЧНИКА ПРОИСХОЖДЕНИЯ НАРКОТИЧЕСКИХ СРЕДСТВ

В последние несколько лет наибольшее распространение получили преступления, направленные против жизни и здоровья населения граждан Российской Федерации, а также против государственной и общественной безопасности. Такими преступлениями являются правонарушения, связанные, в частности, с незаконным оборотом наркотических средств, психотропных веществ, их прекурсоров, сильнодействующих и ядовитых веществ (далее также – наркотические средства, наркотики). Данные законодательно контролируемые вещества вызывают сильную психическую зависимость и привыкание к постоянному употреблению, получая широкое распространение среди молодежи. Наибольшее количество наркотических средств являются психомоторными стимуляторами, вызывающими психическое состояние, характеризующееся обострением чувств и повышенной эмоциональной свободой. Некоторые наркотические средства в определенных дозах могут оказывать галлюциногенное и психотропное воздействие на человека. Следовательно, у потребителей наркотиков присутствует высокая склонность, с одной стороны, к агрессии, зачастую ничем не мотивированной, а с другой – к суициду. Нередко данные склонности могут чередоваться, сменяя друг друга даже в течение одних суток. Основные причины возникновения наркомании среди общества являются: моральная деградация, неудовлетворенность жизнью, доступность приобретения наркотиков, излишняя свобода действий, отсутствие организованного досуга.

В настоящее время при расследовании преступлений, связанных с незаконным оборотом наркотиков, одной из главных задач является усиленная концентрация правоохранительных органов на противодействие организованной наркопреступности, выявление всей организованной группы, а также ликвидация наркопроизводства и сетевых схем нелегального сбыта законодательно контролируемых веществ. Решению этой задачи в рамках экспертно-криминалистического сопровождения оперативно-разыскной и процессуальной деятельности, направленной на борьбу с наркотрафиком, осуществляется в ходе сравнительного

¹ © Лиманская А. Р., 2023.

исследования различных образцов наркотических средств с целью установления общности источника их происхождения, в том числе принадлежности исследуемых объектов к единой массе.

Главную роль в формулировании выводов при установлении общего источника происхождения наркотиков до сих пор играют физико-химические методы анализа, но при этом существенную помощь может оказать трасологическое исследование упаковок и таблетированных форм наркотиков [1; 2]. Не существует универсальной методики такого исследования по причине чрезвычайно широкого многообразия как самих законодательно контролируемых веществ, так и способов их производства, в том числе нелегального, а также придания им внешнего «товарного вида», в котором они попадают в незаконный оборот – таблетирования и упаковки. Но возможно сформулировать определенный алгоритм проведения сравнительного трасологического исследования упаковок и таблетированных форм наркотиков в рассматриваемых целях. Данный алгоритм предусматривает целесообразность проведения указанного исследования в следующей последовательности:

1. Разделение объектов исследования на группы по признакам группового значения:

- наличие или отсутствие упаковки / таблетированной формы;
- вид упаковки / таблетированной формы;
- цвет упаковки / вещества таблетированной формы;
- материал упаковки;
- размеры упаковки / таблетированной формы;
- способ упаковки / таблетирования;
- наличие линий разделения упаковки / таблетированной формы;
- способ разделения упаковки / таблетированной формы;
- консистенция вещества таблетированной формы.

2. Формирование групп объектов по комплексам признаков индивидуализирующего значения:

- по характерному способу упаковки / таблетирования;
- по характерным следам, в которых отображены индивидуализирующие признаки оборудования, использовавшегося при упаковке / таблетировании;
- по наличию общей линии разделения поверхностей.

3. На основании установления совпадения или различия признаков группового значения и комплекса признаков индивидуализирующего значения, проведение сравнения полученных групп объектов и формулирование выводов.

При исследовании упаковок и таблетированных форм наркотических средств методами трасологического исследования эксперт-криминалист может оказать значительную помощь сотрудникам уголовного розыска в выявлении составных звеньев цепочек нелегального распространения наркотиков и установлении принадлежности различных реализаторов к определенным организованным преступным сообществам, специализирующимся на данном виде преступной деятельности.

В настоящее время установление общего источника происхождения наркотических средств, изымаемых из незаконного оборота, имеет большое значение,

поскольку позволяет пресечь деятельность не только отдельных распространителей наркотиков, но и криминальных организаций, специализирующихся на данном виде преступной деятельности. Поэтому совершенствование методических основ сравнительного трасологического и упаковок, и таблетированных форм как важной составляющей комплексного исследования наркотиков, несомненно, актуально и отвечает современным задачам развития экспертно-криминалистических подразделений органов внутренних дел Российской Федерации [3].

Список литературы

1. Завьялова А. А., Завьялов В. В. Комплексный методический подход к реализации технико-криминалистического обеспечения выявления возможных путей наркотрафика. Техничко-криминалистическое обеспечение раскрытия и расследования преступлений // Сборник статей по итогам международной научно-практической конференции, проводимой в рамках деловой программы Международной выставки «Интерполитех-2019», 22–23 октября 2019 г. М. : Московский университет МВД России имени В.Я. Кикотя, 2020. С. 157–161.
2. Завьялова А. А., Завьялов В. В. Комплексный подход к экспертному установлению общего источника происхождения наркотиков. Бутлеровские сообщения, № 12. Т. 64. Казань : 2020. С. 98–103.
3. Криминалистическое исследование упаковок и таблетированных форм наркотических средств и психотропных веществ в целях установления общего источника происхождения : методические рекомендации / [В. В. Завьялов и др.]. М. : ЭКЦ МВД России.

Баринаова А. К.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель

Чурин Р. А.,

преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

АНАЛИЗ ЭФФЕКТИВНОСТИ ПРОГРАММ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ВОССТАНОВЛЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Эффективность компьютерного экспертного исследования напрямую зависит от обеспечения доступа к анализируемой, в том числе удаленной информации. Для повышения вероятности успешного восстановления данных рекомендуется максимально сократить использование исходного объекта. При обычном удалении файлов операционная система не перезаписывает содержимое секторов на диске. Содержимое записи о файле в файловой системе также не удаляется, но подвергается модификации: система помечает запись как принадлежащую удаленному файлу. Таким образом, все сектора диска, соответствующие вышеупомянутой файловой записи, становятся доступными для использования операционной системой в качестве свободного места для хранения другого файла.

Современные программы для восстановления – это продвинутые средства, которые знакомы с логической структурой файловых систем. Программы восстановления данных обычно следуют единому алгоритму, состоящему из следующих основных действий:

1. Сканирование жестких дисков для определения конфигурации логических дисков;
2. Сканирование указанного раздела для поиска удаленных или поврежденных элементов данных.
3. Запись выбранных данных на новый адрес.

Для анализа эффективности программ, предназначенных для восстановления компьютерной информации, проводились эксперименты с восстановлением данных с различных электронных накопителей информации (в большинстве случаев, построенных с применением NAND-памяти) и посекторные образы их содержимого. Рассмотрено 10 популярных программ, позволяющих восстанавливать информацию. Для исследования были отобраны программы, включая отечественный софт: WinHex 20.3; R-Studio 9.2; MiniTool Power Data Recovery 11.4; Hetman Partition Recovery 4.2; Wondershare

¹ © Баринаова А. К., 2023.

Recoverit Data Recovery 11.5.1; Recuva 1.53; ФЕНИКС 1.31; EaseUS Data Recovery Wizard 15.6.0.0; R.saver 9.5; DM Disk Editor and Data Recovery 4.0.0 (далее – DMDE).

Для построения демонстрационных материалов использовались образ диска расширения dd (образ содержимого накопителя информации на жестких магнитных дисках с системой FAT32) и USB-флеш-карта с файловой системой ExFAT.

С задачей общего восстановления файлов наилучший результат показали программные средства: WinHex, Wondershare Recoverit Data Recovery, MiniTool Power Data Recovery, EaseUS Data Recovery Wizard, DMDE. Но как упоминалось ранее, что для компьютерного эксперта имеет значение не общее количество восстановленных файлов, а их рабочее состояние и возможность получения значимой информации.

Эффективней всего с поставленной задачей справились программы: WinHex, Hetman Partition Recovery, MiniTool Power Data Recovery, DMDE.

WinHex (производитель (Германия, Software AG) – это универсальный HEX-редактор, который предназначается для работы с операционной системой Windows. Эта утилита демонстрирует коды различных программных файлов и контрольные суммы, которые просто невозможно отобразить с помощью обычных текстовых редакторов. Программное обеспечение является всеобъемлющим и может эффективно использоваться не только программистами или различными экспертами в области информационных технологий, но и обычными пользователями, стремящимися найти утерянную информацию.

MiniTool Power Data Recovery (производитель (Канада, MiniTool Solution Ltd) – средство для восстановления утерянных данных с жестких и SD дисков, Flash-карт, CD/DVD, USB-дисков, Memory Stick и других накопителей информации для пользователей Windows. Программа использует специально разработанные алгоритмы сканирования носителей информации, выявляя малейшие следы и остатки данных, с помощью которых и удастся восстанавливать файлы с максимальной точностью. Работать с ней достаточно легко и удобно благодаря интуитивно понятному интерфейсу и пошаговому мастеру.

Hetman Partition Recovery (производитель (США, Hetman Software) – это программный инструмент, который поддерживает восстановление данных из файловых систем FAT и NTFS и совместим с современными версиями Windows. Он имеет низкие системные требования, что делает возможным его использование даже на самых простых компьютерах. Это эффективно не только при восстановлении удаленных файлов, но и при восстановлении структуры носителя данных.

DMDE (разработчик Дмитрий Сидоров) – это приложение для восстановления данных, удаленных и потерянных разделов на различных устройствах хранения данных, включая диски, флэш-накопители и карты памяти. Программа является кроссплатформенной, совместимая, в частности, с такими операционными системами, как Windows OS, Mac OS и Linux.

В заключение компьютерным специалистам крайне важно использовать множество программных средств в своей деятельности по восстановлению данных. Полагаться только на один программный инструмент может оказаться недоста-

точным, поскольку каждый инструмент разработан с уникальными преимуществами при восстановлении определенных форматов данных. Поэтому необходимо интегрировать различные инструменты восстановления данных, чтобы добиться более высокого уровня успеха в восстановлении потерянных или поврежденных данных.

Список литературы

1. Иванов В. Ю. Специальные информационные технологии в правоохранительной деятельности [Комплект] : учебное пособие / В. Ю. Иванов. М. : Московский университет МВД России имени В.Я. Кикотя, 2016. С. 132.
2. Альтерман А. Д. Способ восстановления удаленных данных / А. Д. Альтерман, Н. Д. Лушников, М. С. Ключек. Уфа, 2019. С. 87–90.
3. Дутикова А. А. Восстановление информации с USB-накопителей в целях проведения судебно-компьютерной экспертизы. М. : Московский университет МВД России имени В.Я. Кикотя, 2019. С. 448–451.

Андреева Е. Н.¹,

*командир отделения 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*

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ АГРЕГАТОРОВ СБОРА ДАННЫХ ДЛЯ ПОИСКА ИНФОРМАЦИИ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

Информация всегда играла чрезвычайно важную роль в жизни человека. В наше время она является ключевым ресурсом и одним из важнейших элементов экономического, политического и культурного развития общества. Ее роль в современном мире определяется способностью к быстрому реагированию на происходящие события и процессы, а также созданию и транслированию в обществе идей, ценностей и представлений. Увеличение объемов информации и потребности в ее обработке и хранении, совершенствование методов анализа данных повлекло создание эффективных систем информационного обеспечения.

Новейшие технологии обработки информации позволяют управлять информационным потоком, фильтруя и анализируя его с помощью встроенных алгоритмов. Данный процесс подразумевает под собой агрегирование данных. Агрегация может проводиться с целью получения общей картины описываемой области или явлений, а также для обнаружения закономерностей в данных и построения взаимосвязей в виде графов [1].

Агрегаторы сбора данных широко применяются в различных областях деятельности. В органах внутренних дел агрегаторы сбора данных занимают особое место в процессе поиска информации по открытым источникам. Они позволяют собирать, хранить и анализировать информацию, необходимую для принятия оперативных решений по предотвращению совершения преступлений, а также их раскрытия и расследования [2].

Одним из наиболее известных агрегаторов сбора данных является Maltego. Это общедоступное программное обеспечение, которое производит интеллектуальный анализ данных и отображает полученные результаты в виде направленных графов. Агрегатор используется для поиска взаимосвязей между фрагментами информации из различных источников сети Интернет. Преимуществом данного инструмента является комбинированный подход к осуществлению поиска, который заключается в предоставлении сервисом возможности добавлять сторонние пользовательские данные в автоматически сформированные графы [3].

¹ Андреева Е. Н., 2023.

Еще один инструмент, заслуживающий внимание – это Maigret, который позволяет производить сбор сведений по никнейму. Самый простой вариант эксплуатации подразумевает ввод имени пользователя и последующий запуск с параметром сохранения результатов файл или без него. Модуль не только находит совпадения по никнейму, но и собирает информацию о личных данных человека, которому он принадлежит.

В настоящее время существует огромное множество агрегаторов сбора данных, которые позволяют производить автоматизированный поиск информации о различных объектах. Образуя слаженную систему, они оказывают значительное влияние на процесс сбора и анализа данных в сфере информационной безопасности.

Список литературы

1. Linda Westfall, Dave Meadows // Data aggregators: A smart approach to collecting and analyzing large amounts of information. 2019. С. 18–21.
2. Энциклопедия «Касперского» – Глоссарий (Deep web). URL: <https://encyclopedia.kaspersky.ru/glossary/deep-web/>.
3. Официальный сайт Maltego. URL: <https://www.maltego.com/>.
4. Официальный сайт OSINT SAN. URL: <https://osintsan.ru/>.

Артамонов И. В.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*

ЗНАЧЕНИЕ ДЕЗИНФОРМАЦИИ И МЕТОДЫ ЕЕ ИСПОЛЬЗОВАНИЯ

Каждый человек ежедневно сталкивается с различной информацией, которая распространяется как в СМИ, так и в глобальной сети Интернет. Одной из актуальных проблем является достоверность получаемых сведений из таких источников. Рассматривая данный вопрос, мы сталкиваемся с понятием дезинформация.

Развитие информационных ресурсов в современном обществе позволяет государству распространять сведения, необходимые для укрепления на мировой арене. *Большинство крупных держав стремятся распространить свой суверенитет и на сетевое пространство, которое все чаще превращается в арену для столкновения национальных интересов определенных государств и политического процесса.* Значимость коммуникативных процессов в обществе усиливается, это позволяет определять погруженность государства в информационно-коммуникационную среду политической системы. Благодаря этому оно может эффективно реагировать на возникающие экономические, социально-политические и иные вопросы.

Активное участие постиндустриальных держав в процесс отслеживания интернет-контента в определенной степени минимизировало распространение «фейков». Это было достигнуто за счет наложения на авторитетные источники определенных обязательства по проверке публикуемых сведений (Фильтрация контента зависит от государственной модели регулирования) [1].

Финансовая составляющая информационно-коммуникационных процессов также имеет значение при создании «фейковой» информации. Преднамеренное искажение информации может являться средством получения прибыли. Недостоверная информация часто выражается в качестве «кликбэйтов, вбросов» и других способов привлечения внимания пользователей сети Интернет. Данный метод позволяет достичь более широкого охвата аудитории. Часто можно столкнуться с множеством видеоматериалов и статей, связанных с громким и резонансным, а главное, актуальным событием. Информация в них не всегда является достоверной и правдивой, так как задача автора заключается в привлечении большого количества аудитории, а, как следствие, получение большого заработка. Нельзя не отметить использование черного пиара в целях популяризации среди поль-

¹ © Артамонов И. В., 2023.

зователей цифровой среды. Это является одним из методов недобросовестной конкуренции, для которого создается целая «pr-кампания» [2].

Проблема распространения дискредитирующей информации является наиболее актуальной на данный момент. Многие интернет-площадки внедряют технологии по отслеживанию и фильтрации недостоверных сведений, в частности дискредитирующих политику нашего государства. Стоит отметить факт безразличия многих пользователей сети к такой информации. Многие мессенджеры и социальные сети предоставляют возможность пожаловаться на любой контент, публикуемый в их пространстве, после чего производится проверка содержимой в нем информации. Мониторингом социальных сетей занимаются государственные органы исполнительной власти Российской Федерации, это помогает ограничить распространение недостоверной информации [3].

Парсер – это программа, часто представленная в виде бота или сервиса, который собирает, анализирует и выдает в нужном формате данные с определенного веб-ресурса. Все перечисленные действия он осуществляет систематически и без отклонения от заданных ему параметров поиска. К параметрам относят ключевые слова, которые связаны с тематикой информации, которую нам надо найти. Также мы можем обозначить определенные информационные пространства. Тип требуемого информационного ресурса определяется характером искомой информации. Парсер умеет анализировать активность пользователей для оценки участия пользователя в создании и распространении дискредитирующей информации. На основании полученных данных формируется отчет о проделанной работе. В нем указываются источники информации сети Интернет, а также фрагменты текста, которые отвечают заданным параметрам. Данным методом выявляются обычные лица, распространяющие «фейки» непреднамеренно либо целенаправленно.

В заключение хотелось бы отметить, что проблема выявления дискредитирующей информации является наиболее актуальной. Для борьбы с этим вопросом необходимо постоянное обновление знаний и средств.

Список литературы

1. Дезинформация. – Текст: электронный // Википедия: [сайт]. URL: <https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D0%B7%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F>.
2. Дезинформация vs Мисинформация. – Текст: электронный // ЦЕНТР ПОДДЕРЖКИ СМИ: [сайт]. URL: <http://msc.kg/ru/2020/%D0%B4disinformation-vs-misinformation/>.
3. Самошкин Е. А. Институты борьбы с дезинформацией и мисинформацией в СМИ // Вестник Московского университета. Серия 10 : Журналистика. 2017. № 6. С. 176–190.

Болдырев М. А.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОТДЕЛЬНЫЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ ВИДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ПУТИ ПРОТИВОДЕЙСТВИЯ ИМ

Социальная инженерия – это манипулирование человеческим поведением, путем использования психологических приемов, которые помогают достичь цели, которую преследует социальный инженер.

Ниже перечислены некоторые из наиболее распространенных методов социальной инженерии:

1. *Фишинг*: это один из наиболее распространенных методов социальной инженерии.

2. *Инженерия доверия*: это метод, при котором злоумышленники используют недостаток мер безопасности в компании или организации, чтобы взаимодействовать с ее сотрудниками.

3. *Подделка личности*: это метод, при котором злоумышленник представляет себя другим человеком или организацией, чтобы получить доступ к конфиденциальной информации.

4. *Доступ через вредоносное ПО*: это метод, при котором злоумышленники создают вредоносное ПО, которое может быть установлено на компьютеры жертвы.

5. *Социальный инжиниринг в социальных сетях*: это метод, при котором злоумышленники используют социальные сети, чтобы получить доступ к конфиденциальной информации или убедить пользователей совершить определенные действия.

6. *Инженерия внешнего вида*: это метод, при котором злоумышленники создают впечатление, что они имеют официальный статус или имеют право на доступ к конфиденциальной информации.

7. *Инженерия манипуляции*: это метод, при котором злоумышленники манипулируют психологическим состоянием жертвы, чтобы получить доступ к конфиденциальной информации.

8. *Внутренняя инженерия*: это метод, при котором злоумышленники получают доступ к конфиденциальной информации, используя внутренних работников компании.

¹ © Болдырев М. А., 2023.

Ниже приведены отдельные способы противодействия социальной инженерии:

1. Повышение осведомленности.

Одним из способов борьбы с преступлениями, связанными с социальной инженерией, является повышение осведомленности общественности.

2. Обучение персонала.

Кроме того, необходимо обучить персонал, работающий в организациях, которые могут стать целью социальной инженерии.

3. Использование технологических средств.

Технологические средства могут быть эффективным способом защиты от социальной инженерии.

4. Создание культуры безопасности.

В конечном счете, необходимо создать культуру безопасности, которая будет учитывать потенциальные угрозы социальной инженерии.

Также важно проводить регулярные проверки безопасности, чтобы убедиться, что текущие системы и процедуры остаются актуальными и эффективными. При необходимости политики и процедуры должны быть обновлены, чтобы отразить изменения в технологиях или угрозах социальной инженерии.

Социальная инженерия может быть опасным инструментом в руках киберпреступников. Она может привести к получению конфиденциальной информации, мошенничеству или даже к разрушению компьютерных систем.

Важно осознавать, что социальная инженерия – это не только техническая проблема, но и проблема культуры. Необходимо создавать культуру безопасности, которая будет повышать осведомленность сотрудников о потенциальных угрозах и обучать их обнаруживать и сообщать о подозрительной деятельности. Технические средства могут уменьшить риск социальной инженерии, но только при правильном использовании и при условии, что существует культура безопасности, которая поддерживает их использование.

Использование приведенных методов защиты должно стать обязательным для всех организаций, которые работают с конфиденциальной информацией.

Список литературы

1. Искусство обмана. К. Д. Митник, Вильям Л. Саймон // <https://server.obuka.org/>.

2. Социальная инженерия – как не стать жертвой // <https://efsol.ru/articles/social-engineering.html>.

3. Как избежать атаки с использованием социальной инженерии // <https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks>.

4. Осторожно, это ловушка: что такое социальная инженерия // https://www.reg.ru/blog/chto-takoe-sotsialnaya-inzheneriya/?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com.

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

АНАЛИЗ СОЦИАЛЬНЫХ СЕТЕЙ НА ВЫЯВЛЕНИЕ СУБЪЕКТОВ, ПРЕДСТАВЛЯЮЩИХ ИНТЕРЕС ДЛЯ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В настоящее время представить жизнь современного общества без социальных сетей практически невозможно. Здесь люди знакомятся, общаются, играют, развлекаются. Но помимо этого, сегодня социальные сети начинают использовать и в противоправных целях, с их помощью может происходить мобилизация общественного мнения, организация протестов различными активистами.

Особенностью любых современных сетей является то, что попадающий сюда контент очень быстро расходуется между группами пользователей, охватывая огромную аудиторию. Правоохранительные органы, понимая опасность распространения запрещенного контента, предпринимает активные усилия по выявлению и блокированию информационных ресурсов, а также поиску лиц, причастных к их созданию, осуществляя мониторинг сети.

Анализ социальных сетей – метод, используемый для анализа данных и выявления моделей поведения пользователей. Он предполагает сбор данных с платформ социальных сетей, таких как ВКонтакте, Facebook, Одноклассники и даже YouTube. Полученная информация становится основой для применения специальных алгоритмов, направленных на выявление групп пользователей, разделяющих общие интересы, убеждения или привязанности. И после выявления таких групп правоохранительные органы уже используют различные методы для сбора оперативной информации об их деятельности.

На текущий момент пользователями сети Интернет является огромное число людей, многие из которых состоят в различных социальных сетях и сообществах, зачастую не в одном. Поэтому одна из основных задач, стоящих перед правоохранительными органами, заключается в том, чтобы определить, какие сегменты социальных сетей могут представлять оперативный интерес.

Одним из методов, используемых правоохранительными органами, является поиск по ключевым словам на платформах социальных сетей. Метод предпола-

¹ © Бороздина В. Н., 2023.

гает поиск конкретных слов или фраз, которые ассоциируются с преступной или экстремистской деятельностью.

Еще одна используемая техника – это анализ связей. Она предполагает анализ связей между различными пользователями на платформах социальных сетей. В данном случае поиск идет от обратного, заключается в выявлении связанных со злоумышленниками пользователей сети на предмет их связи. Таким образом, могут быть выявлены потенциальные сообщники, через которых также может быть получена интересующая сотрудников органов внутренних дел информация.

При мониторинге социальных сетей сотрудники оперативных подразделений проводят также анализ «настроений» пользователей, выявляя пользователей, публикующих посты, содержащие поддержку террористическим организациям, агрессивно настроенные высказывания про политику страны и чьи действия могут привести к негативным последствиям в реальной жизни.

Компьютеризация общества, переход общения в виртуальное пространство заставляет правоохранительные органы по-новому подходить к поиску информации о правонарушителях. Сегодня одних только специализированных информационных баз недостаточно. Сотрудникам органов внутренних дел необходимо не только расследовать уже совершенные преступления, но и предотвращать их совершение. Для этого необходимо уходить в виртуальное пространство, где, как показывает имеющаяся статистика, чаще всего и происходят планирование и разработка различного рода противоправных деяний, а также вербовка их исполнителей.

Список литературы

1. Направления деятельности правоохранительных органов по выявлению экстремистского контента в социальных сетях / сост. Т. М. Тхазеплов, А. Н. Пахомов. Журнал прикладных исследований, 2022. С. 70–73 с.
2. Возможности современных социальных сетей в поисковой деятельности правоохранительных органов / сост. А. М. Юрин, С. В. Цемина. Белгородские криминалистические чтения, 2021. С. 175–178.
3. Социальные сети как инструмент, помогающий правоохранительным органам в раскрытии преступлений / сост. А. Д. Пополитов. Академическая публицистика, 2022. С. 289–293.
4. Деструктивность контента, его классификаторы и сканеры для риск-анализа социальных сетей / сост. Е. Ю. Чапурин, А. Е. Гуслянников, К. А. Разинкин, И. Л. Батаронов. Информационная безопасность, 2020. С. 371–374.
5. Социальные сети как основной вид коммуникативных практик современной молодежи : социологический анализ / сост. Н. В. Розенберг. Наука. Общество. Государство, 2022. С. 87–89.

Чурин Р. А.¹,

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

ОСОБЕННОСТИ ИССЛЕДОВАНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Автоматизация – один из важных факторов научно-технического прогресса. Современный мир уже невозможно представить без средств и технологий, исключающих человека из трудоемких или опасных операций. Безусловно, эти тенденции распространяются и на авиастроение.

Внедрение современных технологий в конструкцию летательных аппаратов направлено на увеличение их дальности, автономности, минимизацию ошибок, которые могут привести к летным аварийным происшествиям, а также на частичное или полное исключение человека из управления полетом.

Воздушное судно без экипажа на борту принято называть беспилотным летательным аппаратом [3, с. 136]. Сокращенно БПЛА или БЛА. Реже встречается БВС – беспилотное воздушное судно. Также в разговорной речи закрепились термины «беспилотник» или «дрон». Благодаря применению беспилотной компоновки появляется возможность упростить конструкцию летательного аппарата, сделать ее более компактной, расширить сферу применения, существенно удешевить стоимость затрат на приобретение, обслуживание и применение летательных аппаратов [4, с. 3].

«Беспилотники» нашли широкое применение в таких сферах, как аэрофото-съемка, охрана, разведка, агрохимическая обработка, логистика и другие.

Специальная военная операция, начавшаяся в 2022 году, продемонстрировала всему миру актуальность беспилотных технологий в военном деле. Сегодня можно выделить семь сфер применения БПЛА вооруженными силами: разведка, корректировка огня, создание ложных целей, ретрансляция связи, радиоэлектронная борьба, «беспилотники-мишени» и нанесение непосредственного удара (ударные БПЛА).

Гибридный формат военных действий сделал БПЛА объектом криминалистического исследования, при этом, помимо случаев назначения экспертиз по фактам их целевого применения, они стали часто фигурировать при отработке материалов проверки [5, с. 184]. Например, правоохранительные органы одного из приграничных к зоне СВО регионов ориентированы на изъятие всех «дронов», вне зависимости от их размера, типа и места обнаружения. Чаще всего в этом регионе происходят изъятия гражданских квадрокоптеров при осмотре транспортных средств сотрудниками ГИБДД. В экспертно-криминалистическом подразделении МВД России, отвечающем за рассматриваемую территорию, в прошлом году выполнено более 20 экспертных исследований, при этом ни в одном из случаев не установлено фактов их боевого применения.

Чаще всего БПЛА представляют из себя специальный аппарат, отдельные элементы которого или сам корпус создают подъемную силу, присутствует сило-

¹ © Чурин Р. А., 2023.

вая установка (электрическая, поршневая (роторно-поршневая), воздушно-реактивная, газотурбинная (турбореактивные, турбовинтовые, турбовальные, турбовентиляторные), жидкостные или твердотопливные ракетные двигатели), а также электронная начинка, отвечающая за получение информации, управление полетом и бортовыми системами [6, с. 53].

Бортовая электроника БПЛА может быть как централизованной, когда за управление всех систем отвечает один контроллер, так и децентрализованной, когда имеется несколько самостоятельных бортовых систем (например, система управления полетом и силовой установкой не зависит от системы управления огнем или системы получения информации).

В электронных системах БПЛА может содержаться следующая информация:

1. Данные транспондера или радиолокационного ответчика (в некоторых случаях передают в эфир бортовой номер, заводской номер транспондера, высоту полета, скорость и географические координаты).
2. Полетная карта (запрограммированный маршрут летательного аппарата).
3. Журнал управления (логирование полученных управляющих команд).
4. Географические координаты (цель, точка запуска, расположение оператора).
5. Информация, полученная в ходе полета (видео, фото, термография, спектрограмма радиообстановки, полетная информация и др.).

Информация, формируемая электронными блоками силовой установки (серийные и заводские номера, комплектация, дата сборки или программирования, периоды использования, диагностические коды неисправностей и т. д.).

Кроме того, значимую для расследования инцидентов информацию могут содержать пульта дистанционного управления (далее, также – ПДУ), подключенные к ним мобильные устройства, а также накопители информации (карты памяти), установленные в летательных аппаратах.

Для примера ПДУ современных «дронов» фирмы DJI содержат серийный номер самого пульта, серийный номер управляемого БПЛА, IMEI сопряженного мобильного устройства (смартфона), координаты местоположения при работе. Также при расследовании уголовных дел будут иметь значение параметры радиосигнала ПДУ.

Сопряженный мобильный телефон, как правило, содержит полетные данные, материалы, полученные с помощью летательного аппарата, серийные номера БПЛА и ПДУ, а также личную идентификационную информацию.

Что касается исследования карт памяти, устанавливаемых на «дроны», в Центральном аппарате МВД России имеется положительный пример, когда восстановление удаленных видеофайлов специалистами-компьютерщиками, позволило в течение нескольких часов установить владельца «беспилотника», перехваченного в центре Москвы.

Анализом типовой конструкции беспилотных летательных аппаратов, а также вопросов, выносимых следствием, при расследовании преступлений, сопряженных с использованием «дронов», можно выделить пять основных вопросов:

1. Является ли представленный объект беспилотным летательным аппаратом, если да, то каким именно и каковы его основные технические характеристики?
2. Какие идентифицирующие сведения имеет представленный объект?
3. Каким способом изготовлен представленный объект?

4. Содержит ли представленный объект электронные накопители информации, если да, то какие именно?

5. Имеется ли на представленном объекте компьютерная информация о журналах работы, геолокации, скорости и направлении движения (полета)?

Основным источником криминалистической информации на борту БПЛА будет электронная начинка. При этом требуется оценка технического состояния, определение работоспособности, функционального назначения и способа производства. Также в некоторых случаях необходимо интерпретировать компьютерную информацию, например, выделить из массива информации координаты и другие показатели полетных данных.

В большой степени все эти задачи решает судебная радиотехническая экспертиза [7, с. 20].

Сегодня в экспертно-криминалистических подразделениях системы МВД России 78 экспертов в 51 регионе занимаются таким видом экспертиз, 43 региона оборудованы специализированной радиотехнической лабораторией – комплекс для исследования радиоэлектронных устройств «Удовольствие» (ЗАО «РНИЭЦ», г. Санкт-Петербург).

Вместе с тем существует необходимость совершенствования компетенции экспертов, занимающихся производством судебных радиотехнических экспертиз. У радиотехников в настоящее время отсутствуют знания, необходимые для грамотного описания исследуемых БПЛА: радиотехник не умеет отличать спойлеры от закрылок и интерцепторов, терминология в этой области крайне сложна: далеко не каждый сможет отличить лонжероны от элеронов или элевонов.

Необходимо создать единую классификацию БПЛА. Например, сегодня чаще всего встречаются две системы классификации БПЛА: Международная, установленная UVSИ (Association for Unmanned Vehicle Systems International, до 2004 г. организация называлась Европейской ассоциацией по беспилотным системам – EURO UVS) и отечественная созданная для Министерства обороны Российской Федерации. При этом отечественная не претендует на повсеместное применение, а иностранная на территории РФ не ратифицирована.

В настоящее время в мире отсутствуют многофункциональные инструменты, которые собирают и анализируют данные, формируемые БПЛА. Более того, исходя из разнотипности и разнородности применяемых компонентов появление такого инструментария маловероятно.

Отдельно стоит указать на необходимость соблюдения мер личной безопасности при исследовании БПЛА:

1) исследуемый объект может содержать взрывоопасные вещества (неразорвавшиеся боеприпасы, элементы самоликвидации, мины-ловушки и т. д.);

2) силовая установка или топливные баки летательного аппарата могут содержать вредные или взрывоопасные вещества (например, не отработавшие элементы твердотопливного двигателя или топливо для жидкостных ракетных двигателей на основе азотнокислых окислителей;

3) БПЛА могут содержать средства радиоэлектронной борьбы, уровень сигнала которых превышает предельно допустимые нормы.

Существенной проблемой для исследования «беспилотников» является отсутствие в экспертно-криминалистических подразделениях системы МВД России

специалистов, владеющих необходимыми компетенциями, и их востребованность в ИТ-отрасли создают трудности для качественного исследования «дронов».

Учитывая изложенное, при производстве судебных экспертиз, в которых объектом является БПЛА, необходимо следовать следующим рекомендациям:

- 1) соблюдать меры безопасности при исследовании БПЛА;
- 2) соблюдать условия хранения изъятых аппаратов;
- 3) использовать для исследования в первую очередь оборудование и программное обеспечение, специально разработанное для криминалистических целей, а также обеспечивающее полный доступ к информации.

Таким образом, в связи с увеличением количества случаев применения БПЛА в криминальных целях необходимо продолжить анализ их представления в качестве объектов криминалистических экспертиз, а также изучить вопрос оснащения экспертно-криминалистических подразделений системы МВД России ридерами транспондеров и другим соответствующим оборудованием. Также необходима разработка методических рекомендаций по исследованию БПЛА для использования при производстве радиотехнических экспертиз и исследований, обучении экспертов по программам дополнительного профессионального образования сотрудников МВД России и подготовке учебно-методических материалов по направлению радиотехнических экспертиз.

Список литературы

1. Воздушный кодекс Российской Федерации от 19 марта 1997 г. № 60-ФЗ (ред. от 29.12.2022) // СПС «КонсультантПлюс».
2. Постановление правительства Российской Федерации от 11 марта 2010 г. № 138 «Об утверждении федеральных правил использования воздушного пространства Российской Федерации» (ред. от 02.12.2020) // СПС «КонсультантПлюс».
3. Авиация: Энциклопедия / гл. ред. Г. П. Свищев. М. : Большая Российская энциклопедия, 1994.
4. Завалов О. А., Маслов А. Д. Современные винтокрылые беспилотные летательные аппараты : учебное пособие. М. : Изд-во МАИ-ПРИНТ, 2008.
5. Мартин Д. Дроны: первый иллюстрированный путеводитель по БПЛА. М. : Изд-во ЭКСМО, 2018.
6. Шеваль В. В. Беспилотные летательные аппараты как носители оборудования комплексных систем наблюдения / под ред. М. Н. Красильщикова. М. : Изд-во МАИ-ПРИНТ, 2010.
7. Щербак В. М., Чуринов Р. А., Петров Е. А., Замараев Е. В. Методика исследования объектов радиотехнической экспертизы : методика. М. : ЭКЦ МВД России, 2019.
8. URL: https://supercam.aero/assets/cache_image/assets/resourceimages/159/450_video_gray_42312323_1500x1000_05f.png (дата обращения: 19.04.2023).
9. URL: <https://kronshtadt.ru/assets/components/phpthumbof/cache/STEL6321-min.d47961c9fd24b08c6311073fb20a622e2.jpg>.
10. URL: https://zala-aero.com/upload/iblock/6ae/zala-421_22-_1_.jpg.

Братищева В. В.¹,

курсант Московского областного филиала

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Миронов В. Л.,

преподаватель кафедры оперативно-разыскной деятельности ОВД

и применения информационных технологий

Московского областного филиала

Московского университета МВД России имени В.Я. Кикотя

ПРИМЕНЕНИЕ OSINT В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

OSINT (Open Source INTelligence – разведка по открытым источникам) – это методология, включающая в себя поиск и сбор данных из общедоступных источников, а также их анализ для получения дополнительной информации о цели исследования.

История OSINT берет свое начало в декабре 1941 г., когда в США службами мониторинга трансляций зарубежных источников начался сбор и изучение радиопрограмм: сотрудниками велась запись радиотрансляций, осуществлялся их перевод для дальнейшего предоставления в ряд ведомств военного подчинения. Такие данные стали еженедельными отчетами. Как пример работы – исследование корреляции стоимости апельсинов в Париже и уровня успешности бомбардировок железнодорожных мостов.

В июле 1958 г. в СССР вышел журнал «Огонек», темой номера в котором стало бурное индустриальное развитие Урала. Одна из опубликованных фотографий явилась отправной точкой, по которой аналитики ЦРУ восстановили схему энергоснабжения всего Уральского региона.

Следующий этап развития OSINT – период с 2005 по 2009 г. В США создается центр, занимающийся анализом разведматериалов, находящихся в открытом доступе. Это был период бурного роста интернета, социальных сетей, что обусловило увеличение массива информации, находящегося в общем доступе.

Период 2016–2019 гг. технологию OSINT открыли для себя бизнесмены, политические компании, правоохранительные органы, инвесторы, службы безопасности.

Сбор информации в рамках OSINT можно проводить пассивными и активными методами.

Используя пассивные методы, вы никак не выдаёте себя и то, что вы ищите. Поиск ограничивается контентом на сайте объекта исследования, архивной или кешированной информацией, незащищенными файлами.

Активные методы предполагают инициативное взаимодействие с компьютерами и программным обеспечением исследуемой инфраструктуры. При этом ис-

¹ © Братищева В. В., 2023.

пользуются специализированные инструменты для получения доступа к открытым портам, сканирование уязвимостей и серверных веб-приложений. В этом случае ваши действия могут быть зафиксированы.

Источники информации для OSINT обобщенно можно разделить на две группы.

1. Открытые данные, к которым относятся новостные колонки, ряд подкастов, информация компании открытого доступа, блоги, социальные сети, информация из интернет-сообществ. Все это находится в открытом доступе в интернете и может быть найдено посредством стандартной поисковой системы.

2. Документация, хранимая в неиндексируемом сегменте интернета, но, тем не менее, доступная для публичного просмотра. Примером такой документации могут являться:

- информация, которая может быть представлена в ответ на запрос (отчетность, стенограммы пресс-конференций, доклады, публичные заявления и т. д.);
- материалы, на которые была оформлена подписка (статьи в СМИ, информация из почтовых рассылок, проходящая по специализированным сервисам);
- метаданные, получаемые посредством использования специализированного инструментария при проведении аналитической работы с исходными данными.

Характерная особенность OSINT заключается в уникальности каждой поисковой задачи, отсутствии жестких шаблонов и алгоритмов, которые могут использоваться в расследовании. Технология индивидуальна для решения каждой задачи.

Один и тот же способ получения информации может применяться для решения разных задач. Например, анализ фотографии может осуществляться для идентификации изображенных на ней людей, получения сведений о месте и времени съемки, выявления признаков монтажа, разоблачения фейков и др.

Верно и обратное – одна и та же задача может быть решена разными способами. Например, выявить аккаунты одного и того же человека на разных ресурсах можно путем сопоставления никнейма, адреса электронной почты или аватарки.

Очевидно, что при решении сложных поисковых задач происходит обработка большого количества данных, которую весьма затруднительно осуществить в ручном режиме. Поэтому автоматизации поиска информации уделялось много внимания на протяжении всей истории OSINT. На сегодняшний день можно выделить два вида решений, каждое из которых обладает определенными достоинствами и недостатками.

1. Поисковые боты. Большинство из них работает в Telegram. Как правило, реализуют поисковые запросы в достаточно узкой предметной области. Например, исследуют адрес электронной почты или телефонный номер по многочисленным утечкам информации. Или сканируют различные ресурсы для поиска совпадений имени пользователя (никнейма).

2. Платформенные решения. Помимо поисковых машин, содержат в себе аналитические модули и инструменты визуализации данных, за счет чего позволяют существенно повысить автоматизацию расследований. Наиболее известными являются:

- Shodan – поисковая система, которая позволяет искать в сети оборудование различных типов, главным образом интернет-вещи (веб-камеры, маршрутизаторы и иные «умные» устройства);

- Maltego – позволяет собирать информацию о сетевых объектах (сайтах, аккаунтах, доменах, IP-адресах и т. п.), находить связи между ними и представлять все это в наглядном графическом виде;

- Snoop Project – одно из лучших решений для поиска по никнейму.

Не отстают и российские разработчики:

- Avalanche – система автоматизированного интернет-мониторинга, осуществляет мониторинг ключевых СМИ, соцсетей, телеграм-каналов, darkweb, тендеров, судов, правительственных сайтов.

- Виток-OSINT – осуществляет поиск в СМИ, блогах, форумах, социальных сетях и в файлах веб-браузера Tor, строит и визуализирует взаимосвязи между объектами поиска.

Перечень инструментария OSINT будет не полным, если не упомянуть еще о двух решениях. Во-первых, это OSINT Framework, представляющий собой иерархичный каталог, который содержит ссылки на различные OSINT-инструменты, разбитые по категориям, зачастую используемые аналитиками, маркетологами, частными детективами и обычными пользователями для поиска и анализа мультимедийных ресурсов, геолокации, логинов и никнеймов, IP-адресов, метаданных, адресов электронной почты и т. д.

Во-вторых, Google Dorks. Это набор расширенных поисковых операторов Google, которые уточняют параметры поиска, а также позволяют найти общедоступные, но скрытые данные.

Таким образом, профессиональный OSINT – это целая совокупность платформ и инструментов, используя которые пользователь имеет возможность искать, собирать, анализировать, исследовать любые данные, следить за динамикой изменений, сравнивать результаты по разным показателям и т. д.

Применительно к правоохранительной деятельности можно выделить ряд задач, решение которых методами OSINT является весьма эффективным.

1. Поиск людей, точнее, каких-либо сведений, позволяющих идентифицировать человека, определить его местонахождение, круг общения, место работы или учебы, интересы и т. п. Наибольший интерес для поиска представляют номер телефона, адрес электронной почты, никнейм, фото лица, аватарки.

Большинство сервисов при регистрации нового пользователя требуют указать номер телефона и (или) электронную почту, что делает эти сведения ключевыми в сборе информации о человеке.

Использование пользователем одного и того же никнейма на разных ресурсах позволяет логически связать аккаунты. Этот поиск можно осуществлять вручную или использовать специальные инструменты, например сайт namechk.com, который проверит наличие одинакового никнейма почти на сотне ресурсов.

Схожая ситуация складывается при поиске по лицу или аватарке. На рынке представлено большое количество решений, использующих разные алгоритмы распознавания лиц и ориентированные на разные соцсети. Заинтересовавшимся рекомендуем для начала обратиться к решениям FindFace и Search4Faces.

Развитие электронных сервисов, предоставляемых государственными органами и коммерческими структурами, объективно приводит к легальному появлению в открытом доступе обезличенных персональных данных. Их использование в совокупности с иной информацией позволяет сделать вывод о принадлежности данных конкретному человеку. Например, имя и отчество можно узнать по номеру телефона (используя систему быстрых платежей) или по государственному регистрационному знаку принадлежащего человеку транспортного средства (в этом случае станет известна еще и дата рождения).

2. Поиск местоположения. Источником исходных данных чаще всего служат фотографии. В этом случае анализируются метаданные файла, которые возможно содержат географические координаты места съемки, а также само изображение на наличие значимых элементов (узнаваемые здания, элементы рельефа местности и т. п.). В интернете существует достаточно большое количество ресурсов, позволяющих просматривать и редактировать метаданные файлов, поисковые сервисы Яндекс и Google можно использовать для поиска изображений и просмотра панорам улиц.

Кроме того, определенную информацию о местонахождении интересующего лица может дать IP-адрес его устройства при подключении к интернету.

3. Получение информации о юридических лицах и индивидуальных предпринимателях. В сети широко представлены сервисы по проверке и анализу контрагентов (СПАРК, СТАР, Rusprofile и многие другие), которые не только аккумулируют сведения о хозяйствующем субъекте (ИНН, ОГРН, коды классификаторов, дата создания, ФИО руководителя, финансовые результаты деятельности, участие в госзакупках и др.), но и предоставляют аналитическую информацию, позволяющую выявить аффилированность и установить бенефициаров. Данные ресурсы активно используются в раскрытии и расследовании преступлений в сфере экономики.

4. Разоблачение фейков. Фейковая информация, как правило, содержит изображения либо уже публиковавшиеся в интернете, либо созданные под конкретную ложь. В первом случае раскрыть дезинформацию может помочь уже упоминавшийся поиск изображений в Яндексе или Google, а также ресурс Wayback Machine (archive.org), который хранит архивные версии сайтов, сделанные в разное время. Во втором случае выявить постановочное фото можно путем анализа элементов изображения и их сопоставления с прилагающимся текстом. В этой ситуации могут быть использованы самые разнообразные инструменты: анализ метаданных, поиск по лицу, сайты с метаданными.

В правоохранительной деятельности OSINT может применяться при борьбе с такими явлениями, как:

- организованная преступность;
- кража персональных данных;
- вымогательство;
- отмывание денег;
- нарушения прав интеллектуальной собственности;
- терроризм и экстремизм;
- педофилия и другие.

Использование OSINT в борьбе с преступностью существенно повышает ее эффективность, особенно при проведении крупных международных расследований. Ярким примером является проведенная в 2014 г. совместная операция ФБР и Европола «Onymous» по массовому закрытию криминальных рынков в DarkNet. В результате были ликвидированы более 410 скрытых сервисов и 27 различных сайтов, арестованы 17 человек, изъяты биткойны на сумму \$ 1 млн, золото, наличные деньги и наркотики.

В нашей стране в последние годы реализуется ряд мероприятий, направленных на внедрение OSINT в деятельность правоохранительных органов. Так, например, в 2021 г. было подписано соглашение между концерном «Автоматика», АО «Национальная инжиниринговая корпорация» и компанией «Ти Хантер» о создании информационно-аналитической платформы анализа по открытым источникам данных. Продукт планируется передать правоохранительным органам и крупным компаниям для расследования киберпреступлений.

Не остается в стороне и МВД России. На данный момент основное внимание уделено организации обучения сотрудников полиции. Осуществляется повышение квалификации сотрудников, задействованных в противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий по программам «Методы киберразведки», «Поисковые системы и конкурентная разведка в Интернете» и «Безопасность информационных технологий».

Подводя итог, отметим, что цифровизация государственного управления, общественной и частной жизни сопровождается формированием большого количества ресурсов, накапливающих разнообразную информацию практически о всех значимых событиях. В этом контексте разнообразие методологии OSINT открывает широкие возможности ее применения в правоохранительной деятельности, в первую очередь при выявлении, пресечении, раскрытии и расследовании преступлений.

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*

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВАМ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ И ОТДЕЛЬНЫЕ ПУТИ ИХ РЕШЕНИЯ

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

Показательно, что за истекшие шесть лет уровень преступности в данной сфере увеличился с 90 587 в 2017 году до 522 065 в 2022 году. Зафиксированная негативная тенденция подтверждается увеличением с 4 % в 2017 году до 26 % в 2021 году удельного веса таких преступлений в общем числе зарегистрированных.

Значительное количество из всех зарегистрированных преступлений данного вида составляют мошенничества, совершенные с использованием средств мобильной связи. В 2022 г. это 212 963 преступления или 40.6 % от всех киберпреступлений.

Изучение информации, поступившей из территориальных органов предварительного следствия МВД России, выявил следующие наиболее распространенные проблемы в расследовании таких 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.).

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.

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.

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

¹ © Гончар В. В., 2023.

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

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

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

Кроме того, не совершенна работа сотрудников правоохранительных органов на стадии проверки сообщения о преступлении.

Так, целесообразно придерживаться следующих рекомендаций.

Следователю и/или дознавателю в ходе работы в составе СОГ целесообразно:

1. Провести опрос и принятие заявления пострадавшего. В объяснении в обязательном порядке необходимо отражать подробный хронометраж всех событий, последовательность действий потерпевшего при поступлении звонка или в ходе общения потерпевшего с преступником посредством сети Интернет.

В ходе опроса необходимо выяснить максимальное количество обстоятельств хищения: время и место преступления, номера банковской карты или счета, возможная запись голоса преступника и иные имеющиеся данные.

2. При хищении денежных средств с использованием услуг удаленного доступа управления банковским счетом выясняется у потерпевшего о подключении к банковскому счету услуги удаленного доступа управления банковским счетом (к примеру, мобильный банк):

- если услуга подключена самим потерпевшим, то с какого времени и каким способом она подключена (посредством заявления о подключении в офисах банковских учреждений или посредством банкоматов);

- с какого времени потерпевший пользуется абонентским номером, к которому данная услуга подключена, так как не исключается перевыпуск номера оператором связи после истечения шести месяцев неиспользования абонентского номера с оформлением номера на иное лицо;

- проводит осмотр мобильного устройства потерпевшего на предмет установления типа его программного обеспечения, наличия в нем собственной антивирусной программы и ее активности;

- в ходе опроса выясняет наличие возможности выхода в интернет с мобильного устройства;

- истребует у потерпевшего договор на банковское обслуживание карты, со счета которого произошло списание денег;

- истребует у потерпевшего детализацию соединений его абонентского номера.

Детализацию соединений номера потерпевшего можно получить в ходе осмотра места происшествия посредством услуги «личный кабинет» на сайте оператора сотовой связи лично пострадавшим.

Признаками хищения при наличии в мобильном устройстве вредоносной программы будут служить смс-сообщения, направляемые на сервисные номера банка с абонентского номера потерпевшего, которые будут видны только при получении детализации соединений его абонентского номера.

В рамках осмотра места происшествия производится осмотр мобильного телефона, устройства удаленного доступа потерпевшего на предмет сохраненных смс-сообщений, абонентских номеров, с использованием которых происходило общение, сохраненных страниц журнала посещений сети Интернет. Фиксация производится путем крупномасштабной фотосъемки.

Сотрудник органа дознания в ходе работы в составе СОГ:

1. Ознакомившись с обстоятельствами совершения преступления и исходя из индивидуальных особенностей того или иного способа хищения:

1.1. С помощью сайта Федерального агентства связи «Россвязь» или иного устанавливает принадлежность оператору и региону абонентских номеров, использовавшихся при совершении мошенничества.

1.2. Исходя из возможностей оперативно-технических подразделений, направляет запрос на установление принадлежности интересуемых абонентских номеров, с указанием дат активации и отключения.

2. При перечислении денежных средств на счет банковской карты, в рамках материала доследственной проверки в соответствии с ч. 5 ст. 26 ФЗ «О банках и банковской деятельности», подготавливается ходатайство в районный суд по месту дислокации органа внутренних дел о проведении ОРМ «наведение справок» с целью получения сведений о владельце банковской карты и движении денежных средств по счету карты. В случаях перевода денежных средств со счета карты потерпевшего проводятся аналогичные мероприятия с целью установления дальнейшего движения денег, без запроса на получение сведений о владельце карты. Детализированный отчет по счету карты может быть предоставлен самому потерпевшему по его заявлению, поданному в офис, где данная карта ему была выдана. Сроки выдачи ответов гражданам и объем предоставляемых в них сведений законом не регламентированы.

В целях ускорения получения сведений необходимо рекомендовать потерпевшему написать в присутствии сотрудника ОМВД претензию и с ней обратиться в отделение банка, где была выдана банковская карта, о чем отобразить соответствующее обязательство.

Список литературы

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.

Кияева Е. Ю.¹,

слушатель Института судебной экспертизы

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Горбулинская И. Н.,

заместитель начальника кафедры технико-криминалистического

обеспечения экспертных исследований

учебно-научного комплекса судебной экспертизы

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКИХ ПОДРАЗДЕЛЕНИЙ

В настоящее время, когда информационные технологии становятся неотъемлемым элементом любой сферы, не является исключением и судебно-экспертная деятельность. Безусловно, пока еще рано говорить о ее полной цифровизации, но определенные информационные технологии на современном этапе уже используются достаточно активно. Проанализируем основные из них [8, с. 104].

1. Формирование и применение узкоспециализированных автоматизированных информационно-поисковых систем (АИПС), которые содержат определенные объекты экспертизы.

Среди рассматриваемых систем можно назвать, например, такие как «Металлы» (система, содержащая описание составов металлов и сплавов и сферу их использования), «Обувь» (система, содержащая ключевые характеристики подошв обуви) и т. д. С помощью данных систем при производстве судебной экспертизы эксперт может получить необходимую информацию для исследования, сравнительные образцы и т. д.

2. Создание и применение систем анализа изображений, в которые могут быть включены и программы, посредством которых осуществляются идентификационные и диагностические исследования. Таких систем достаточно много, среди наиболее известных и часто применяемых можно назвать следующие:

– дактилоскопические. Рассматриваемые системы дают возможность устанавливать личность человека по следам рук. К ним относятся такие системы, как «Папилон» – запатентованный способ автоматического распознавания и установления тождества папиллярных узоров пальцев и ладоней рук. Программа гарантирует стабильно высокие показатели надежности и избирательности поисков в базе данных больших объемов, исключая предварительный отбор дактилокарт и следов по их качеству. Также на АДИС ПАПИЛОН возложено ведение дактилоскопических учетов, идентификация личности по отпечаткам пальцев рук, идентификация личности по словесному описанию, идентификация нео-

¹ © Кияева Е. Ю., 2023.

познанных трупов по фрагментарному отображению следов пальцев и ладоней рук. АДИС ПАПИЛОН кодирует следы рук, формирует и передает на просмотр эксперту рекомендательные списки для их анализа и принятия окончательного решения [7].

– применяемые при производстве портретных экспертиз. Системы данного вида (системы «Портрет 2005», «Образ++», «СОВА») позволяют формировать композиционные портреты разыскиваемых лиц, конструируя их по тем описаниям, которые дают потерпевшие. Значительное число элементов, имеющихся в данных системах (к примеру, лица в очках, с бородой или усами), автоматизация процесса, при которой элементы в кратчайшие сроки и без особых усилий присоединяются друг к другу и в совокупности демонстрируются лицу, составляющему портрет, позволяют достигать значительного сходства полученного изображения с разыскиваемым, что, безусловно, повышает эффективность деятельности по поиску таких лиц. Также данные системы позволяют осуществлять поиск спустя значительное время, осуществлять реконструкцию лиц по черепу и т. д.

В Московском метрополитене запущена система видеонаблюдения, реализуемая командой экспертов по машинному обучению VisionLabs, которая способна распознавать лица. В возможности данной системы входит идентификация по признакам внешности, что позволяет выявлять разыскиваемых лиц. Команда VisionLabs не первый год признается лидирующей на международном конкурсе ChaLearn Face Anti-spoofing Attack Detection Challenge. Уже сегодня активно используются разработка и внедрение систем идентификации человека по биометрическим данным (система «Безопасный город»), т. е. субъект может быть идентифицирован по определенным признакам, которые весьма разнообразны (строение тела, черты лица, сетчатка глаза, папиллярные узоры, голос и др.). Если такие системы достигнут максимальной эффективности, то со временем необходимость в проведении портретной экспертизы будет отсутствовать, так как программа будет способна сама провести идентификацию;

– используемые при подготовке иллюстраций к заключению эксперта. Например, программ РАСТР позволяет упростить, значительно ускорить и автоматизировать процесс подготовки иллюстраций к заключению эксперта. Данную программу используют при производстве дактилоскопического, баллистического, почерковедческого, трасологического исследования, систему также можно использовать при производстве судебно-медицинской экспертизы. Источниками изображений для данной программы могут быть: файлы стандартных форматов (BMP, TIFF, JREG); файлы формата АДИС ПАПИЛОН; системный буфер обмена; изображения, полученные с помощью планшетного сканера и т. д. РАСТР способен обрабатывать как цветные изображения, так и черно-белые [6]. Мощные инструменты программы по обработке исходных изображений предоставляют эксперту иллюстрации для экспертного заключения;

– автоматизирование процесса обработки и сбора экспериментальных сведений, получаемых при выполнении различных исследований (баллистических, автотехнических, инженерно-технических и др.) с помощью различных специализированных устройств, объединенных с компьютером.

В рамках данного направления возможно выделение следующих элементов:

1. Программно-аппаратные комплексы, используемые для обработки различных видов анализа (к примеру, лазерного, спектрального), осуществляемого в рамках криминалистических экспертиз материалов, веществ, изделий; в целях определения групповой принадлежности малых количеств горюче-смазочных материалов по спектрам поглощения в ультрафиолетовой и видимой зонах спектра и др.

2. Системы, применяемые в рамках производства баллистических судебных экспертиз («КОНДОР– М», «Арсенал», «Балэкс»), которые дают возможность осуществлять сравнительный анализ следов на пулях и гильзах в трех измерениях, позволяют обрабатывать значительный объем данных.

3. Системы для фоноскопического исследования, с помощью которых возможна идентификация личности по фонограмме устной речи. К примеру, по уголовному делу по факту кражи транспортного средства Т., впоследствии потерпевшему, поступали звонки с предложением выкупить его транспортное средство, данные речевые сообщения были записаны. Впоследствии при установлении подозреваемого Д. была произведена фоноскопическая судебная экспертиза, согласно заключению которой голос на фонограмме с требованиями о выкупе принадлежит Д. [5].

Также с помощью данных систем возможно производить анализ акустической обстановки, шумов, условий, при которых производится звукозапись; идентифицировать средства, с помощью которых осуществлялась аудиозапись; повышать разборчивость речевых фонограмм, их качество. В числе таких систем можно назвать «Диалект», «ОТExpert», «Justiphone», «ИКАР Лаб» [1, с. 109].

В то же время нельзя не отметить, что имеются все предпосылки для более активного использования технологий в экспертной деятельности. В частности, многие годы правоприменители и научное сообщество ведут речь и возможности внедрения в судебно-экспертную деятельность Лабораторной информационной системы управления (ЛИМС) [2, с. 10]. Данная система, к примеру, уже достаточно давно и успешно используется полицией США, в рассматриваемую базу сосредоточены все проведенные экспертные исследования.

Отстаивая целесообразность внедрения рассматриваемых технологий в судебно-экспертную деятельность в России, исследователи называют следующие прогнозируемые положительные аспекты такого решения:

- минимизация отрицательного влияния человеческого фактора (субъективизма) при производстве экспертных исследований;
- сокращение сроков производства судебных экспертиз.

В то же время, совершенствуя и расширяя использование информационных технологий в экспертной деятельности, следует учитывать, что соответствующие базы данных (которые видится необходимым расширять, наполнять нужной информацией), являются лишь форматом сбора и хранения информации. Действующая система не предназначена для того, чтобы выдавать конкретный результат производства экспертизы (исключение составляют лишь отдельные системы, которые позволяют четко определить принадлежность следа путем их сравнительного сопоставления). Все те данные, которые помещены в базу данных, подвер-

гаются анализу с помощью различных дополнительных инструментов, путем их изучения, сопоставления экспертом. Современные технологии не выполняют за эксперта его работу, они лишь – вспомогательное средство.

Исследователями отмечается, что применение искусственного интеллекта может влечь за собой неправильные выводы в силу того, что проводится неправильный анализ объектов, в особенности если информация избыточна или, наоборот, недостаточна. Такая проблема, в частности, отмечается в работе систем распознавания лиц. Все сказанное свидетельствует о необходимости тщательного контроля анализа сведений, сосредоточенных в базах данных. Поэтому и представляется, что обработкой информации, по крайней мере, в настоящее время должен заниматься эксперт.

Как уже отмечалось, внедрение в судебно-экспертную деятельность ЛИМС может позволить разрешить многие вопросы. В частности, уже неоднократно поднимался вопрос о необходимости создания базы данных экспертных учреждений по родам и видам экспертиз, с современной и необходимой информацией. В настоящее время нередки ситуации, когда об определенных экспертных учреждениях информация имеется, но при обращении в них лица, производящие расследование, узнают о том, что отдельные виды экспертиз в них настоящее время не проводятся. Или, напротив, в экспертных учреждениях появились новые возможности, стали проводиться те судебные экспертизы, специалистов по которым ранее не было, но органы расследования не владеют информацией о том, что в данные экспертные учреждения могут быть назначены какие-либо судебные экспертизы, и вынуждены искать те учреждения, куда их надлежит назначить.

Также существует необходимость формирования базы экспертных заключений в качестве основных причин, по которым это не удастся сделать до настоящего времени, исследователи называют недостатки законодательного регулирования, проблемы практической реализации, однако, представляется, что все указанные проблемы преодолимы, и их необходимо разрешать, поскольку создание таких баз позволит существенно оптимизировать судебную экспертную деятельность. Конечно, при этом следует задаться целью ввести специальный доступ для ограниченного числа лиц к каждому заключению эксперта.

Зарубежный опыт свидетельствует о том, что подобный подход является весьма эффективным и позволяет существенно оптимизировать экспертную деятельность. В частности, во Франции используется платформа *Oralex*, которая предназначена для цифровизации судебно-экспертной деятельности, позволяет взаимодействовать суду и лицами, участвующими в деле. При этом каждая информация, начиная с вынесения определения о назначении судебной экспертизы, отправляется в систему в формате pdf, с момента размещения ее на платформе нет никакой возможности внесения изменений в данную информацию.

Таким образом, можно сделать следующие выводы. На современном этапе развития судопроизводства, безусловно, существует необходимость в цифровизации судебно-экспертной деятельности. Это обусловлено процессом развития науки и техники, появлением новых объектов, исследования, развитием методологии судебной экспертизы. Значимую роль в оптимизации экспертной деятель-

ности играют различные базы, в которых накапливается, хранится, анализируется и структурируется информация.

Предполагается, что в настоящее время производство судебных экспертиз или даже их существенной части перекладывать на искусственный интеллект недопустимо, но все же информационные технологии могут иметь существенное значение для снижения различных затрат на экспертную деятельность.

Список литературы

1. Воронин С. А. Практика и перспективы применения информационных технологий в судебной экспертизе // Международное научное издание Современные фундаментальные и прикладные исследования. 2016. Т. 2. № 2 (21).
2. Идзиковский В. И., Горшкова Е. А. ЛИМС – автоматизированная система управления для лаборатории, или нечто большее? // Современная лабораторная практика. 2012. № 3 (19).
3. Интервью начальника ЭКЦ МВД России генерал-лейтенанта полиции А. В. Шишко радиостанции «Милицейская волна» 1 марта 2019 г. Сайт Министерства внутренних дел Российской Федерации. URL: <https://xn--b1aew.xn--p1ai/document/16093018>.
4. Новые информационные технологии в судебной экспертизе : учебное пособие / Э. В. Сысоев, А. В. Селезнев, И. П. Рак, Е. В. Бурцева. Тамбов : Издательство Тамбовского государственного технического университета, 2006.
5. Приговор Кузьминского районного суда г. Москвы от 23 апреля 2019 г. по делу № 1-47/2019 // <https://sudact.ru/>.
6. Система подготовки изображений для заключений и экспертиз «РАСТР». URL: <http://www.bnti.ru/des.asp?itm=4355&tbl=01.09>.
7. Системы ПАПИЛОН. Разработка, внедрение и сопровождение биометрических систем. URL: <http://www.papillon.ru/>.
8. Тараскаев С. А. Современное состояние и перспективы применения информационных технологий в судебно-экспертной деятельности // Юридическая наука. 2019. № 8.

Гребнева А. С.¹,

*доцент кафедры технико-криминалистического
обеспечения экспертных исследований
учебно-научного комплекса судебной экспертизы
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

Ромашенко О. Л.²,

*преподаватель кафедры технико-криминалистического
обеспечения экспертных исследований
учебно-научного комплекса судебной экспертизы
Московского университета МВД России имени В.Я. Кикотя*

О НЕКОТОРЫХ ОСОБЕННОСТЯХ ТЕХНОЛОГИИ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Специалист получает статус эксперта по определенному уголовному делу, потому что по данному делу необходимо провести определенные исследования с целью получения ответов на конкретные вопросы, необходимые для всестороннего и полного раскрытия и расследования преступления, лицом, ведущим расследование по уголовному делу. Также важно отметить, что судебная экспертиза проводится для получения ответов на вопросы, которые требуют специальных знаний, определения фактов, необходимых для вынесения более грамотного решения в конкретном деле. Целью проведения судебной экспертизы является обеспечение честного и справедливого рассмотрения дела. Судебная экспертиза в области информационных технологий предусматривает проведение исследования определенных информационных объектов, в том числе переносных носителей информации, персональных компьютеров, ноутбуков, электронных планшетов, смартфонов, серверов, другого сетевого оборудования, а также восстановление удаленной, поврежденной и защищенной информации, исследование аппаратного состояния оборудования, поиск и анализ данных на исследуемых носителях, и так далее.

Результаты судебной экспертизы могут использоваться в качестве доказательств и помочь суду принять правильное решение в деле. Поэтому постановка вопросов эксперту – важный аспект при проведении судебной экспертизы. При постановке вопросов эксперту необходимо учитывать фактические обстоятельства дела, технические возможности проведения экспертизы и компетенцию эксперта. Это означает, что если дело требует проведения экспертизы в определенной области знаний, то вопросы должны быть поставлены таким образом, чтобы эксперт мог предоставить соответствующую экспертную оценку на основе своей специализации и опыта. При постановке вопросов эксперту нужно учесть

¹ © Гребенева А. С., 2023.

² © Ромашенко О. Л., 2023.

все существенные факторы, которые могут повлиять на решение дела, и сформулировать вопросы таким образом, чтобы они позволили получить объективную и достоверную информацию от эксперта. Исходя из изложенного, при назначении судебной компьютерно-технической экспертизы, а также любой другой судебной экспертизы, в ходе проведения которой изучается различная компьютерная информация, лицу, ведущему расследование данного дела, необходимо выбрать такое экспертное учреждение, подходящее по профилю специализации, или какого-то конкретного судебного эксперта, который обладает необходимыми специальными знаниями в этой области.

Достаточно часто следователями экспертиза назначается в государственные экспертные учреждения, не имеющие специалистов в нужной области, или частным экспертам, не обладающим необходимой квалификацией. Также многочисленны случаи постановки перед экспертами вопросов, выходящих за пределы их специальных познаний и требующих назначения комплексной экспертизы.

Говоря непосредственно о технологии исследования экспертом компьютерной информации и разнообразных цифровых устройств, хочется обратить внимание, что методика проведения данных компьютерно-технических экспертиз предполагает проведения определенных необходимых мероприятий по защите сохранности данной цифровой информации. Среди необходимых для этого действий можно выделить несколько пунктов, которые необходимо соблюдать: а) при соединении изъятого носителя цифровой информации к тестовому компьютеру, который используется судебным экспертом для проведения исследования, задействуются аппаратные средства блокировки уничтожения или сохранения данной информации; б) необходимо копирование всей цифровой информации судебным экспертом на специально выделенные зоны на тестовом компьютере. По другому данное действие называется созданием образа исследуемого носителя цифровой информации. Именно данный образ и исследует в дальнейшем судебный эксперт, а не работает непосредственно с изъятой информацией на изъятом носителе. Вся работа судебного эксперта должна проводиться непосредственно с использованием специализированного программного обеспечения, использование которого должно быть соответственно обосновано и описано в заключении эксперта [3].

Заключение эксперта первоначально не обладает какой-то особенной юридической силой, поэтому оценивается по общим правилам, как и все доказательства в соответствии с ч. 1 ст. 88 УПК РФ. Оценка доказательств – это процесс анализа и проверки всей имеющейся информации в уголовном деле, включая результаты экспертиз, показания свидетелей, материалы документации и т. д. с целью определения их достоверности и достаточности для принятия определенного процессуального решения.

Ведущий ученый Ю. Г. Корухов писал: «Достоверность заключения эксперта надо искать в нем самом вне связи с другими доказательствами». С одной стороны, можно согласиться с этим высказыванием, ведь заключение эксперта можно назвать особым видом доказательств, которое предполагает проведение экспертом научных исследований с использованием специальных знаний, это вызывает особые трудности при их оценке [5]. Экспертные исследования самостоятельны

и независимы, но нельзя быть точно уверенным, что раз они основаны на научных расчетах и фактах, то не нужно сомневаться в их достоверности. Экспертное заключение должно оцениваться на общих основаниях, как и все остальные предоставленные доказательства, полученные законным путем, и поэтому не должно иметь никаких преимуществ перед другими доказательствами [6].

Анализ правомерности применения в качестве доказательства экспертного заключения состоит из следующих позиций:

а) оценка обоснованности самих выводов содержанию самого исследования. Данные выводы эксперту необходимо основывать на всестороннем, объективном анализе и исследовании предоставленных объектов [9]. Если использовать эксперту только апробированные методики при проведении экспертизы, то данный факт будет являться основанием для признания данного заключения допустимым доказательством.

Доказательства, полученные с нарушением закона, не могут быть приобщены к материалам уголовного дела и не могут приниматься для рассмотрения судом и исключаться из перечня доказательств, соответственно, и само заключение эксперта, полученное при использовании этих незаконных материалов, не будет иметь юридической силы и будет исключено из доказательств по делу;

б) необходимость соблюдения процессуального порядка назначения и проведения необходимой судебной экспертизы. Данные действия регламентируются несколькими статьями уголовно-процессуального законодательства.

Так, УПК нашей страны предполагает возможность ознакомления подозреваемого и обвиняемого как с самим постановлением о назначении экспертизы (часть 3 ст. 195 УПК РФ), разъясняя ему его права при производстве экспертизы (ст. 198 УПК РФ), так и с самим заключением эксперта (ст. 206 УПК РФ). Часть 2 ст. 283 УПК РФ предусматривает возможность сторонам задать свои вопросы эксперту в письменном виде в ходе судебного разбирательства. Кроме этого, в ст. 217 УПК РФ предусмотрена возможность ознакомления обвиняемого и его защитника с материалами уголовного дела в конце расследования до его передачи в суд. Здесь хочется обратить внимание, что невозможно ознакомление с информацией, снятие и получение копии информации, содержащейся на носителях цифровой информации, хранящихся при уголовном деле, в случае если они были предметом компьютерно-технической экспертизы и хранящихся на электронных носителях, признанных по делу вещественными доказательствами, без использования специализированного криминалистического программно-аппаратного комплекса. Это обосновано тем, что любое подключение носителей информации после проведения судебных компьютерно-технической экспертизы без использования указанного выше специализированного криминалистического программно-аппаратного комплекса может повлечь нарушение целостности содержимого носителей информации [4].

В результате комплексной всесторонней оценки экспертного заключения формируются его значение и доказательственная сила по определенному уголовном делу. При анализе заключения компьютерно-технической экспертизы необходим особый подход, ведь данная экспертиза строится на применении узкоспециализированных специальных знаний в этой области при исследовании предостав-

ленных эксперту материалов. Субъекты оценки указанных доказательств зачастую не обладают специальными знаниями в этой области, и поэтому в процессе оценки необходимо четкое соблюдение требований закона и научных принципов. В процессе оценки заключения эксперта учитываются такие факторы, как квалификация эксперта, методы и средства исследования, достоверность и объективность полученных данных, убедительность выводов, их соответствие с установленными фактами и правилами науки.

Таким образом, технология экспертного исследования, заключение по судебной экспертизе в области информационных технологий, оценка заключения эксперта по такого рода исследованиям, несмотря на общие процессуальные и научные подходы, имеют ряд важных особенностей.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 25.03.2022, с изм. от 19.05.2022).
2. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (с изм. и доп.).
3. Апелляционное постановление Судебной коллегии по уголовным делам Московского городского суда от 25 ноября 2013 г. по делу № 10-12204.
4. Апелляционное определение Судебной коллегии по уголовным делам Московского городского суда от 22 июня 2015 г. по делу № 10-7831/2015.
5. Аверьянова Т. В. Судебная экспертиза : курс общей теории. М., 2008. С. 468.
6. Белкин Р. С. Криминалистическая энциклопедия / Р. С. Белкин. М., 2000. С. 69.
7. Грабова К. А. Роль компетентности эксперта в арбитражном процессе / К. А. Грабова. Текст: непосредственный // Научный аспект. 2020. № 3. С. 154–160.
8. Доказывание при правоприменении посредством правосудия в Российской Федерации : монография. 5-е изд., испр. и доп. / под ред. В. Н. Галузо. М. : ТЕИС, 2021. С. 189–190.
9. Овсянников И. В. Категория вероятности в судебной экспертизе и доказывании по уголовным делам : дис ... д-ра юрид. наук. М., 2001.
10. Холявка Н. И. Проблемы назначения и проведения судебной экспертизы в гражданском судопроизводстве // Молодой ученый. 2022. № 24 (419). С. 280–282.

Егоров Д. А.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

ПРИМЕНЕНИЕ КВАНТОВЫХ ТЕХНОЛОГИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С развитием информационных технологий возросла необходимость в обеспечении безопасности информационных систем. В данной статье рассматривается применение квантовых технологий в области обеспечения системы информационной безопасности.

Квантовые технологии имеют потенциал изменить информационную безопасность в будущем, их возможности связаны с особенностями квантовой механики, которые отличаются от классической физики. Кроме того, квантовые технологии обладают высокой степенью надежности и защищенности от внешних воздействий. Для понимания работы квантовых технологий в информационной безопасности необходимо разобраться в таких терминах, как квантовые биты (кубиты), квантовые каналы связи и квантовые алгоритмы.

Квантовые биты (кубиты) – это основные единицы информации в квантовых вычислениях. Они отличаются от классических битов тем, что могут находиться в суперпозиции нескольких состояний одновременно и обладают квантовым свойством, называемым квантовой корреляцией или «спутанностью», которое позволяет проводить операции над несколькими кубитами одновременно. Еще одним применением квантовых технологий в системах информационной безопасности является квантовое случайное число. Квантовое случайное число используется для генерации криптографических ключей и случайных чисел. Эта технология стала широко известна после выхода телефона компании Samsung. Samsung Galaxy A Quantum – это телефон, выпущенный в 2020 г., который был разработан совместно с корейским оператором связи SK Telecom и оснащен квантовым блоком защиты [1]. Квантовый блок защиты включает в себя квантовый генератор случайных чисел (QRNG) и квантовый криптографический процессор, который может использоваться для шифрования данных на уровне аппаратного обеспечения. QRNG генерирует случайные числа на основе квантовых явлений, что делает их невозможными для предсказания и защищает данные от взлома. Кроме того, квантовый криптографический процессор может использоваться для

¹ © Егоров Д. А., 2023.

создания квантовых криптографических ключей, которые могут быть использованы для шифрования и дешифрования данных на уровне аппаратного обеспечения.

Как подчеркнул генеральный директор компании «ИнфоТеКС» Андрей Чапчаев: «Получение разрешения на опытную эксплуатацию ViPNet Quandor – это новая веха развития квантовой криптографии в России. За квантовыми технологиями и основанной на них криптографии мы видим большое будущее. Они могут стать фундаментом системы информационной безопасности нашей страны, поэтому мы продолжим инвестировать в развитие и совершенствование наших квантовых разработок» [2].

Плюсы квантовых технологий обеспечения безопасности:

– Безопасность: Квантовые технологии позволяют создавать защищенные криптографические системы, которые не могут быть взломаны с помощью традиционных методов, таких как перебор паролей или анализ трафика.

– Скорость: Квантовые технологии обеспечивают быстрое шифрование и расшифрование данных, что может значительно повысить производительность и эффективность систем безопасности.

– Устойчивость: Квантовые технологии могут быть использованы для создания более устойчивых и надежных систем защиты информации, которые не будут уязвимы для внешних атак и могут предотвращать взломы [4].

Прогнозы относительно развития квантовых технологий в сфере информационной безопасности обнадеживающие. Развитие квантовых технологий в обеспечении информационной безопасности может изменить парадигмы национальной и международной безопасности и является перспективной и многообещающей сферой.

Однако, несмотря на все преимущества, существует необходимость в дальнейшем исследовании и разработке квантовых технологий, чтобы они стали более доступными и простыми в использовании для разных пользователей.

Таким образом, квантовые технологии защиты информации уже сегодня показывают большой потенциал для решения проблемы безопасности в цифровой среде. Дальнейшее развитие этой области будет иметь важное значение для обеспечения информационной безопасности во всех сферах деятельности.

Список литературы

1. Официальная презентация Galaxy A Quantum от компании Samsung // Samsung. URL: <https://www.samsung.com/us/mobile/galaxy-a71-5g/>.
2. Официальная презентация Galaxy A Quantum от компании Samsung // Центра компетенций НТИ по направлению «Квантовые технологии» на базе МГУ им. М.В. Ломоносова. URL: <https://quantum.msu.ru/ru/press/news/2021-12/quandor-operation>.
3. Отличная квантовая механика : учебное пособие. М. : Альпина фикшн, 2019. С. 319.
4. Квантовые технологии в телекоммуникационных системах. Ростов н/Д, Южный Федеральный университет, 2021.

Коняхин Д. И.¹,

курсант факультета подготовки

специалистов в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Дворянкин О. А.²,

старший преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

РОЛЬ ЧЕЛОВЕЧЕСКОГО ФАКТОРА В КИБЕРБЕЗОПАСНОСТИ С УЧЕТОМ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Роль человеческого фактора оказывает огромное влияние на успех и неудачу в системе кибербезопасности. На человека воздействуют люди как напрямую в визуальном общении, так и посредством искусственного интеллекта (далее – ИИ), т. е. через различные программы. Они нацеливаются на уязвимости человека, против которого ведут кибератаку, или людей, против которых также ведут кибератаки, т. е. ищут слабые стороны, благодаря которым стремятся получить о нем или о них конфиденциальную информацию.

На данный момент идет серьезное увеличение различных информационных угроз через информационные технологии интернета с различными сценариями на государственный орган или компанию, в которых зачастую самой доступной точкой входа или доступа (влияния и манипулирования) становится обычный человек. И как было отмечено выше, основное желание преступников – это стремление получить о структуре или ее сотруднике (сотрудниках) необходимую конфиденциальную информацию.

В этой связи преступник (преступники) использует следующие технологии:

Первое: Случайная атака.

Второе. Недостаточная мотивация сотрудников.

Рассмотрим недостатки и уязвимости человеческого фактора при работе с кибербезопасностью:

– человек не может одновременно проанализировать большое количество данных, *как это может сделать ИИ;*

– человек может допускать ошибки из-за усталости, стресса или просчетов, *в то время как ИИ не подвержен таким факторам;*

– *в отличие от ИИ,* человек может не быть в курсе современных угроз и трендов в области кибербезопасности, а также может не сработать на со-

¹ © Коняхин Д. И., 2023.

² © Дворянкин О. А., 2023.

ответствующем уровне при недостаточных знаниях и опыте в данной области.

Перейдя от человека к компьютеру, т. е. ИИ, нужно понять, почему сейчас это настолько популярно и какую же роль он там занимает.

Роль искусственного интеллекта в кибербезопасности становится все более ценной, поскольку эта технология может помочь улучшить безопасность информационных систем и снизить риски кибератак.

Некоторые из способов, которыми ИИ может помочь в защите информации, включают:

- обнаружение и предотвращение кибератак: многие системы ИИ могут обнаруживать аномальное поведение и предупреждать об угрозах безопасности до того, как они станут серьезными проблемами;
- мониторинг безопасности: ИИ может непрерывно мониторить информационные системы и анализировать данные по безопасности, чтобы выявлять уязвимости и улучшать системы безопасности;
- распознавание вредоносных программ: ИИ может распознавать вредоносные программы и блокировать их, чтобы предотвратить потенциальные угрозы безопасности;
- автоматизация процессов защиты информации: ИИ может автоматизировать процессы защиты информации, например, анализируя логи и определяя потенциальные проблемы, что позволяет сократить время, необходимое для реагирования на угрозы;
- разработка систем безопасности: ИИ может помочь разработчикам систем безопасности создавать более эффективные и защищенные системы, используя данные и аналитику по информационной безопасности.

Несмотря на плюсы работы ИИ, можно выделить ряд недостатков его работы при кибербезопасности:

- ИИ не может применять эмпатию или интуицию, что часто нужно, когда речь идет об оценке окружающей среды и проверке неявных угроз на фоне социальной и взаимной обусловленности;
- какой бы совершенной не был ИИ, у него всегда есть ограниченности в понимании лингвистических нюансов, которые человек может достаточно легко распознать;
- ИИ, как и любые компьютерные системы, уязвимы к кибератакам и могут быть компрометированы.

Таким образом, можно сделать вывод, что человек и ИИ имеют как свои положительные стороны, так и отрицательные, но при этом если две эти экосистемы будут работать совместно и дополнять друг друга, комбинируя свои способности, а не соревноваться в достижении результатов, то и положительных результатов будет значительно больше.

Некоторые способы использования ИИ в кибербезопасности, чтобы помочь человеческому фактору включают:

1. Анализ больших объемов данных с помощью ИИ, чтобы автоматизировать процессы анализа и выявления угроз.
2. Использование машинного обучения для создания более точных моделей поведения и выявления отклонений.

3. Применение ИИ для разработки и тестирования сквозных стратегий по обеспечению безопасности, что поможет снизить человеческий фактор в рискованных ситуациях.

4. Создание ИИ-алгоритмов, которые могут помочь автоматизировать процессы уведомлений и исправления уязвимостей.

5. Становление ИИ для прогнозирования и выявления потенциальных киберугроз, что поможет заранее предпринимать необходимые меры по повышению безопасности.

6. Использование ИИ для проведения автоматизированного сканирования уязвимостей в компьютерных системах, в которой применяются различные методы сканирования и сбора данных.

7. Применение ИИ для мониторинга активности пользователей в компьютерных системах. ИИ может обнаруживать подозрительное поведение, такое как попытка несанкционированного доступа к конфиденциальной информации или внесение изменений в системные настройки без соответствующих разрешений. Человек же может использовать эту информацию для принятия мер по блокированию доступа, обучения пользователей правилам и профилактике вредоносных действий.

В заключение необходимо отметить, что использование ИИ в кибербезопасности может существенно улучшить защиту информации, однако для обеспечения максимальной эффективности необходим человеческий фактор. Но самое важное – это полноценная и совместная работа человека с искусственным интеллектом.

Список литературы

1. Боровская Е. В. Основы искусственного интеллекта. URL: <http://lib.tau-edu.kz/wp-content/>.
2. Человеческий фактор в информационной безопасности. URL: <https://habr.com/ru/articles/344542/>.
3. Google's AI-powered Cybersecurity Solution Is Now Generally Available. URL: <https://venturebeat.com/2021/07/29/googles-ai-powered-cybersecurity-solution-is-now-generally-available/>.

Завьялова А. А.¹,

*доцент кафедры технико-криминалистического
обеспечения экспертных исследований*

учебно-научного комплекса судебной экспертизы

Московского университета МВД России имени В.Я. Кикотя,

кандидат химических наук

Завьялов В. В.²,

член Совета Организации ветеранов ЭКЦ МВД России,

кандидат химических наук,

профессор Академии военных наук

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ХОДЕ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ НАРКОТИЧЕСКИХ СРЕДСТВ ПО УСТАНОВЛЕНИЮ ОБЩЕГО ИСТОЧНИКА ПРОИСХОЖДЕНИЯ

Действенная борьба с незаконным оборотом наркотических средств, психотропных веществ, их прекурсоров, а также сильнодействующих и ядовитых веществ (далее также – наркотики) в современных условиях уже практически невозможна без активного и широкого использования передовых информационных технологий. В первую очередь данные технологии необходимы для сбора, обработки, аккумуляции и последующего эффективного и оперативного использования огромных массивов информации о наркотиках, которые представляют собой постоянно пополняющийся широкий спектр различных химических соединений, растений, грибов и препаратов на их основе, их химическом составе, физико-химических свойствах и биологической активности, фармакокинетики и фармакодинамики, а также методах их производства, включая используемые для этого оборудование и реагенты, и внешнем виде, в котором они попадают на нелегальный рынок, в том числе способах их упаковки, таблетирования и иных приемах придания наркотикам «товарного вида» и применяемых для этого технических средствах. Данная информация при ее грамотном использовании сотрудниками правоохранительных органов, в частности экспертами-криминалистами, позволит установить общий источник происхождения различных образцов наркотиков, изымаемых из нелегального оборота, что в свою очередь чрезвычайно важно для выявления всей цепи наркотрафика в целях полного пресечения этой противозаконной деятельности [1].

В свое время в экспертно-криминалистических подразделениях как органов внутренних дел, так и других правоохранительных органов Российской Федерации в соответствии с совместным приказом ФСКН России, МВД России, ФСБ России, ФТС России от 27 декабря 2012 г. № 535/1143/679/2664 «Об утверждении Положения о порядке формирования и использования единой базы данных

¹ © Завьялова А. А., 2023.

² © Завьялов В. В., 2023.

по химическому составу значительных изъятий наркотических средств и психотропных веществ и коллекции изображений и описаний отличительных признаков упаковок наркотических средств и психотропных веществ» была организована работа по формированию единых информационных баз данных, которые содержат сведения, характеризующие химический состав образцов, изъятых из нелегального оборота наркотических средств и психотропных веществ, а также изображения и сведения об отличительных признаках их упаковок. В системе ФСКН России такая база данных получила название «Сигнатура». Практическое ее использование позволяло при сравнении физико-химических свойств, поступивших на исследование образцов наркотиков и индивидуализирующих признаков их упаковок с имеющимися в базе сведениями, установить общность происхождения вновь изъятых из незаконного оборота образцов с ранее изъатыми. Сформированная на основании проверки по «Сигнатуре» информация позволяла сориентировать оперативные и следственные подразделения о принадлежности реализаторов наркотиков к определенным организованным преступным сообществам, «специализирующимся» на данном виде противозаконной деятельности [1].

Представляется целесообразным продолжить реализацию приведенного межведомственного нормативного правового акта в полном размере. При этом возможности системы «Сигнатура» необходимо не только полностью восстановить, возложив функцию по ее ведению на экспертно-криминалистические подразделения органов внутренних дел, но развивать дальше, увеличивая как объем аккумулируемой в ней информации, так и ее спектр [3; 4]. При этом на первых порах можно ориентироваться в данных вопросах, например, информационно-поисковую систему «АИПСИН АнтиНаркотики» (далее – ИПС «АИПСИН»), разработанную белорусскими коллегами как один из элементов или механизмов осуществляемой в настоящее время наркополитики, имеющей в первую очередь превентивный характер противодействия незаконному обороту законодательно контролируемых химических соединений. Необходимо отметить, что данная система уже давно и успешно используется не только в Белоруссии, но и в нашей стране, однако ее применение в России носит до сих пор несистемный и по большей части инициативный характер.

Задача ИПС «АИПСИН» состоит в оказании содействия реализации механизмов информационного обеспечения подразделений правоохранительных органов с учетом как их специфики, так и значимости решаемых задач в режиме реального времени. При этом ИПС «АИПСИН» имеет высокий легитимный статус и формируется согласно стандартам ISO, ГОСТ и требованиям различных сертифицирующих и научно-экспертных организаций и не нуждается в дополнительной сертификации на территории Российской Федерации.

В настоящее время информация, необходимая для идентификации появляющихся на незаконном рынке потенциально опасных веществах, уже включена в базы данных ИПС «АИПСИН», которые постоянно обновляются в режиме реального времени. При этом подобная информация практически отсутствует в иных, схожих с ИПС «АИПСИН», программных продуктах, что делает ИПС «АИПСИН» уникальным инструментом для борьбы с наркоугрозой. При ис-

пользовании ИПС «АИПСИН» эксперты-криминалисты смогут проводить превентивное изучение всей доступной информации по потенциальным к контролю веществам [5].

Таким образом, развитие информационных технологий в сфере борьбы с незаконным оборотом наркотиков, а в первую очередь в части экспертно-криминалистического сопровождения соответствующих оперативно-разыскных мероприятий, процессуальных действий и в целом всего спектра усилий правоохранительных органов, в данной сфере позволит вывести работу по защите населения нашей страны от наркоугрозы, которая является одной из важнейших угроз для национальной безопасности Российской Федерации, на качественно иной более высокий уровень, соответствующий современным вызовам преступного мира. У нашей страны появится, наконец, возможность создать всеобъемлющую общегосударственную систему борьбы с наркопреступностью, насущная потребность в которой давно назрела, и о необходимости в которой все громче требует гражданское общество. Учетом того, что Российское государство никогда не чуралось действительно положительного зарубежного опыта при построении собственных государственных и общественных систем, примерным ориентиром при построении такой системы можно взять достаточно успешный европейский опыт функционирования системы раннего предупреждения о наркоопасности, в которую включены подразделения органов правопорядка, учреждения здравоохранения – морги, станции скорой помощи, больницы, наркодиспансеры, научные организации, предприятия фармацевтической и химической промышленности 30 стран (рис. 1).



Рис. 1. Структура европейской системы раннего предупреждения о наркоопасности

Эта система предполагает постоянный обмен информацией обо всех случаях обнаружения новых синтетических наркотиков, ее анализ и принятие адекватных мер реагирования. Целесообразно изучить возможность использования данного опыта в нашей стране. В первую очередь это касается организации взаимодействия с системой здравоохранения в целях оперативного представления органам внутренних дел сведений о выявленных в ходе химико-токсикологических исследований новых наркотиках или их метаболитах.

Использование информационных систем позволит более оперативно и достоверно идентифицировать новые психоактивные вещества, а коллегам из оперативных подразделений поможет в работе по поиску, выявлению и пресечению путей наркотрафика и деятельности подпольных лабораторий.

Список литературы

1. Завьялова А. А., Завьялов В. В. Комплексный подход к экспертному установлению общего источника происхождения наркотиков. Бутлеровские сообщения. № 12. Т. 64. Казань, 2020. С. 98–103.
2. Завьялова А. А., Завьялов В. В. Комплексный методический подход к реализации технико-криминалистического обеспечения выявления возможных путей наркотрафика. «Технико-криминалистическое обеспечение раскрытия и расследования преступлений» // Сборник статей по итогам международной научно-практической конференции, проводимой в рамках деловой программы Международной выставки «Интерполитех-2019», 22–23 октября 2019 г. М. : Московский университет МВД России имени В.Я. Кикотя, 2020. С. 157–161.
3. Завьялова А. А., Завьялов В. В. Возможности комплексного сравнительного исследования наркотических средств и психотропных веществ для установления общего источника их происхождения // Экспертная практика: М. : ЭКЦ МВД России, 2016. № 80. С.78–90.
4. Криминалистическое исследование упаковок и таблетированных форм наркотических средств и психотропных веществ в целях установления общего источника происхождения : методические рекомендации / [В. В. Завьялов и др.]. М. : ЭКЦ МВД России.
5. Завьялова А. А., Завьялов В. В., Гладырев В. В. Возможности использования передового опыта экспертной службы республики Беларусь в практической деятельности экспертно-криминалистических подразделений органов внутренних дел Российской Федерации на примере системы «Айпсин-Антинаркотики» // Сотрудничество в сфере экспертной деятельности. Материалы Международного круглого стола. 2018. С. 82–84.

Шилов М. А.¹,

*курсант факультета подготовки сотрудников
для подразделений по охране общественного порядка
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Смирнов В. М.,

*старший преподаватель кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук*

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТИ ДЛЯ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНОЙ СЕТЕВОЙ АКТИВНОСТИ

В настоящее время существует множество проблем с отражением атак в киберпространстве. Особенно часто атакам подвергаются сети, принадлежащие предпринимателям и бизнесменам. В данной статье описан новый способ отражения атак с помощью нейросетей.

Модели, основанные на данных сетевых временных рядов, являются одним из наиболее популярных в последние годы методов, используемых для систем обнаружения сетевых вторжений. Большинство данных временных рядов имеют нелинейные. Несколько методов машинного обучения использовались для создания нейросети, которая смогла бы отражать кибератаки. Однако в некоторых исследованиях отмечается, что эти статистические методы не учитывают взаимосвязь между данными и в основном полагаются на отбор признаков, что делает их неэффективными для использования в режиме реального времени, где они демонстрируют более низкие показатели обнаружения.

В настоящее время широко используются методы глубокого обучения, такие как сверточные нейронные сети и рекуррентные нейронные сети. Сверточная нейронная сеть – это класс нейронных сетей с глубоким обучением, который в основном основан на таком математическом понятии, как «свертка». Архитектура сверточной нейросети состоит из входного и выходного слоев и нескольких скрытых слоев. Скрытые слои обычно представляют собой сверточные слои, имеющие функцию активации, за которой следует объединение слоев, которые помогают уменьшить размерность данных. Рекуррентные нейронные сети еще раньше продемонстрировали свои возможности в приложениях обработки естественного языка, таких как, например, машинный перевод. Такая сеть позволяет работать с последовательностями произвольной длины. Таким образом, в рекуррентной нейронной сети сигналы могут передаваться в обоих направлениях, создавая петли в сети.

Сверточные нейронные сети способны повысить производительность по сравнению с другими методами машинного обучения; способность сверточных

¹ © Шилов М. А., 2023.

нейронных сетей изучать сложные внутренние структуры может быть адаптирована для фондовых рынков.

Как правило, сверточные нейронные сети применяются для изучения пространственных/высокоуровневых признаков набора данных, в то время как слои двунаправленной нейронной сети с долгой краткосрочной памятью используются для изучения признаков временных рядов. Объединение этих моделей позволит осуществить распознавание конкретной атаки. Для выполнения классификации распознавание проводится по пяти классам – Нормальный (обычный трафик, отсутствие атак), DoS-атаки (отказ в обслуживании), атаки зондированием, атаки от корневого сервера к локальному и атаки от пользователя к корневому каталогу.

Нейронная сеть с двунаправленной долгосрочной памятью – это модель, которая получает информацию о последовательности в обоих направлениях – назад, из конца в начало или вперед, из начала в конец. Двунаправленный режим отличается от обычной однонаправленной сети. Такой подход позволяет сети лучше обучаться на каждом этапе, что приводит к лучшему изучению признаков.

Модель состоит из слоя одномерной сверточной нейронной сети, а также нескольких слоев двунаправленной нейронной сети с промежуточными слоями. Идея состоит в том, чтобы использовать слой одномерной сверточной нейронной сети и слой объединения, что позволит сократить набор параметров и свободных переменных с целью извлечения признаков с меньшим использованием ресурсов. Наконец, уменьшение числа параметров позволит значительно сократить продолжительность обучения.

Слои двунаправленной нейронной сети используются для изучения как прямых, так и обратных данных временных рядов со скрытыми слоями, использующими два блока, имеющие один и тот же вход и связанных с одним и тем же выходом. Один из блоков обрабатывает временные ряды в прямом направлении, а другой – в обратном.

Два слоя двунаправленной нейронной сети в модели расположены таким образом, что размер ядра удваивается. Согласно схеме модели первый двунаправленной нейронной сети начинается с 64 нейронов, а следующий и последний слой двунаправленной нейронной сети – со 128. Причина использования такого числа узлов заключается в том, чтобы модель могла лучше понять взаимосвязь долговременных зависящих от времени признаков, изученных первым одномерным слоем сверточной нейронной сети, который обеспечивает лучшее извлечение признаков и более быстрое время обучения модели. Как правило, сверточные нейронные сети и рекуррентные нейронные сети, используемые в комбинации, имеют более высокую вероятность переобучения и плохо работают на тестовом наборе. Чтобы держать это под контролем, модель обеспечивается перекрестной проверкой. Перекрестная проверка – это метод, разделяющий данные на блоки. Как средний, так и лучший показатели доли верных откликов модели при решении задачи обнаружения подозрительной сетевой активности с округлением до сотых составили 0,99, что соответствует 99 % верно классифицированных экземпляров. С величиной ошибки в 0,026 можно сделать вывод о высоком качестве классификации сетевых атак в наборе данных с использованием предложенной модели.

Таким образом, итоговые показатели точности на неизученных данных демонстрируют превосходство предложенной модели нейронной сети (99 %) по сравнению с остальными используемыми методами.

Такая нейронная сеть имеет большое превосходство над уже существующими в следующем:

- быстрая обучаемость;
- выделение не только отдельных признаков, но и систем этих признаков, что позволяет более точно определять вид совершаемой атаки;
- быстрая реакция на совершаемые атаки;
- быстрый подбор способа отражения совершаемой атаки.

Таким образом, при сочетании двух моделей нейронных сетей образуется совершенная новая нейронная сеть, которая имеет в себе преимущества каждой из представленных моделей. Новая модель позволяет сделать прорыв в защите информации, особенно полезной окажется для бизнесменов и предпринимателей, хотя может найти свое применение во многих отраслях. Для этого ее стоит лишь переобучить, а этот процесс не займет много времени.

Список литературы

1. Azizjon M., Jumabek A., Kim W. 1D CNN-based Network Intrusion Detection with Normalization on Imbalanced Data, 2020, P. 218–224.
2. Khan R., Zhang X., Alazab M., Kumar R. An improved convolutional neural network model for intrusion detection in networks, in 2019 Cybersecurity and Cyberforensics Conference (CCC), 2019, P. 74–77.
3. Liao H., Lin C., Lin Y., Tung T. Intrusion detection system: A comprehensive review, Journal of Network and Computer Applications, Vol. 36, 01-2013, P. 16–24.
4. Nancy P., Muthurajkumar S., Ganapathy S., Kumar S., Selvi M., Arputharaj S. Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks, IET Communications, Vol. 14, No. 5, 2020, P. 888–895.
5. Schuster M., Paliwal K. Bidirectional recurrent neural networks, IEEE Transactions on Signal Processing, Vol. 45, No. 11, 1997, P. 2673–2681.
6. Sultana N., Chilamkurti N., Peng W., Alhadad R. Survey on sdn based network intrusion detection system using machine learning approaches, Peer-to-Peer Networking and Applications, Vol. 12, P. 493–501, 2019.
7. Verma A., Kaushik P., Shrivastava G. A network intrusion detection approach using variant of convolution neural network, ICCES, 2019, P. 409–416.
8. Complete Guide To Bidirectional LSTM (With Python Codes). URL: <https://analyticsindiamag.com/complete-guide-to-bidirectional-lstm-with-python-codes/>.
9. NSL-KDD. Kaggle. URL: <https://www.kaggle.com/hassan06/nsllkdd>.

Калашникова А. А.¹,

преподаватель кафедры информатики и математики

Московского университета МВД России имени В.Я. Кикотя

Соболев А. О.²,

курсант факультета подготовки сотрудников для подразделений

экономической безопасности и противодействия коррупции

Московского университета МВД России имени В.Я. Кикотя

АНАЛИЗ СОЗДАНИЯ КОМПЬЮТЕРНО-МОЗГОВЫХ ИНТЕРФЕЙСОВ ДЛЯ КИБОРГОВ

В данной статье рассмотрено одно из основных направлений работ в области искусственного интеллекта: картирование мозга человека и дальнейшего моделирования работы. Изучены и проанализированы результаты трудов специалистов Brown University, команды Николелиса, Илон Маска и ученых стран Италии, Великобритании и Швейцарии, которые проводили опыты над животными в целях изучения мозговой активности и прогнозирования различных алгоритмов работы системы, работа ученых современного поколения, основанная на создании киборга, которым управлял человек при помощи подачи сигналов через компьютер.

Одним из основных направлений работ в области искусственного интеллекта является разработка по картированию мозга человека и дальнейшего моделирования его работы. Эксперименты по внедрению чипов в мозг ведутся еще с 1990-х гг. и вполне успешно. Впервые технология была разработана в качестве инструмента, обеспечивающего общение без движения.

Отправной точкой в данной области были исследования специалистов Brown University [2], показавшие работу по картированию мозга, что позволяло отслеживать сигналы активности человека при помощи компьютерной техники и впоследствии управлять движениями пальцев рук. Для этого в мозг вживляли небольшие микрочипы, которые регистрировали сигналы моторных нейронов и с помощью разработанного алгоритма передавали сигналы компьютерной технике в реальном времени, благодаря чему начинал функционировать виртуальный заместитель руки, т. е. курсор.

Первыми испытуемыми были обезьяны, которых дрессировали в течение двух лет, чтобы те могли воспроизводить небольшие задачи для изучения мозговой активности и прогнозирования различных алгоритмов. В ходе двухлетней работы с обезьянами-советами команда Николелиса в 2000 г. идентифицировала движения и правильно предсказывала их скорость и направление [3].

Очередным открытием для команды стало замечание, что в функциональной единице присутствует более одного нейрона. Отмечалось, что даже один из лучших одонейронных показателей не мог в полном объеме выполнить анализ популяции нейронов. Сигналы начали усреднять от 7 до 30 нейронов для выяв-

¹ © Калашникова А. А., 2023.

² © Соболев А. О., 2023.

ления оптимального значения при движении имитированной рукой. Изначально обезьяны двигали лапой и курсором на мониторе одновременно. Такие манипуляции обезьяне вознаграждались, т. е. в ходе работы была задействована психика животных. Однако обезьяна в скором времени научилась передвигать курсор исключительно подачей импульсов без повторения лапой, что вывело ученых на новый уровень в познании новейшей технологии того времени.

Ученым из Италии, Великобритании и Швейцарии в 2020 году впервые удалось подключить нейронную сеть, состоящую как из биологических, так и искусственных клеток мозга, которая могла обмениваться данными [5].

Подопытными в данной разработке являлись крысы, передававшие электрические сигналы на искусственно созданные сети из Италии в Швейцарию. Онлайн-сигналы передавались в реальном времени через мемристоры, которые располагались в Великобритании. Ученые разработали алгоритм, позволявший передавать сигналы в обратном потоке, т. е. от искусственно созданных клеток мозга к биологическим.

Таким образом, учеными была разработана система, что способствовала передаче сигналов из мозга мыши по интернету в обе стороны – гибридный мозг. Профессора полагают, что разработка может стать основой нейронного имплантата, который способствовал бы передаче сигналов из биологических в искусственные нейросети для полного понимания друг друга. Разработка направлена на лечение заболеваний головного мозга. В настоящее время технология представляет из себя обычную сеть, но есть все основания полагать, что разработка является шагом к более продвинутому протезированию, в котором будут задействованы нейронные имплантаты.

В результате исследований получилась демонстрация взаимодействия биологических и искусственных нейронов в реальном времени в двух направлениях.

Ученые в 2021 году создали киборга, имевшего микростимулятор с нейронами живого таракана, которому можно задавать путь передвижения дистанционно. Управление происходит через компьютер с передачей сигналов из мозга человека. Таракан-киборг был разработан в ходе хирургической операции, которая не требовала особых усилий для ученых. Насекомое оснастили микростимулятором, включающим в себя заземляющий, левый и правый электрод. Умеренная производительность онлайн-контроля достигалась с помощью прямоугольного импульса, работающего с 1,5 В амплитудой, частотой в 50 Гц, шириной 500 мс и коэффициентом заполнения 50 %.

С данными характеристиками микростимулятора в результате исследования было выявлено, что человек способен управлять киборгом по заранее выстроенным дорогам пути с успешностью в 20 % [1].

В последние несколько лет произошел большой скачок в области компьютерно-мозговых интерфейсов. Это дает надежду больным с инсультом в быстром восстановлении мелкой моторики рук при проведении нейрохирургами безопасной операции с использованием картирования мозга.

В 2016 году Илон Маск запустил проект, который начал разработку прибора, способного передавать по Bluetooth сигналы головного мозга, чтобы управлять компьютером или мобильным телефоном мозговыми импульсами [4].

В 2019 году проект был презентован и следом отправлен на доработку. Компания ориентирована на лечение больных неврологическими заболеваниями. Предполагается, что операция будет занимать не более 10 минут и переноситься крайне не легко. Первые опыты успешно прошли уже на крысах и обезьянах. На данный момент Илон Маск ждет одобрения от Минздрава США для проведения опытов на людях.

Маск уверен в своем проекте и заявляет, что разработка поможет не только больным людям для исцеления, но и в конкуренции с искусственным интеллектом. О плюсах и минусах разработки говорить довольно рано, ведь апробации на людях еще не было, но 09.04.2021 компания опубликовала видеозапись, на которой макака играла в компьютерную игру без помощи приставки, т. е. по средствам передачи сигналов через чип в мозге.

Neuralink (компания Илона Маска по разработке чипов) решили внедрить девятилетней макаке в мозг чип, благодаря чему примат сначала играл в компьютерные игры с помощью приставки и передачи сигналов, позже – без использования приставки. Данные исследования проводились еще 10–16 лет назад, поэтому каким-то грандиозным прорывом в области человечества разработку назвать нельзя. У Илона есть большие надежды и амбиции, ведь передавать сигнал для управления хотят в связке с iPhone, т. е. настраивать канал управления любым устройством силой мысли.

Еще не так давно шли бурные обсуждения между учеными в области искусственного интеллекта – возможно ли обрести искусственному интеллекту сознание? Рассматривая современные технологии и подвиги ученых-нейрологов, можно с уверенностью сказать, что искусственный интеллект будет жить.

Список литературы

1. Интерфейсы мозг-компьютер: обзор современных достижений // Хабр // URL: <https://habr.com/ru/post/564644/>.
2. Компьютерно-мозговые интерфейсы для киборгов // <https://www.kv.by/archive/index2002133402.htm>.
3. Матлис, Ян. Обезьяна думает, робот делает // Computerworld // URL: https://translated.turbopages.org/proxy_u/en-ru.ru.624ecbf5-62c1f56b-fa4194b1-74722d776562/https/www.computerworld.com/article/2589905/monkey--think---robot-do.html.
4. Нейрочип Neuralink: действительно ли мы будем вживлять гаджеты в мозг // РБК // URL: <https://trends.rbc.ru/trends/industry/5f4ce51c9a79475172aeea28>.
5. Хмелева, Алина. Ученые впервые подключили биологические клетки мозга к нейронной сети // Компьютерра 28.02.2020 // URL: <https://www.computerra.ru/254906/uchenye-vpervye-podklyuchili-biologicheskie-kletki-mozga-k-nejroseti/>.

Капшунов Д. С.¹,

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

Научный руководитель:

Калашиникова А. А.,

*преподаватель кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя*

К ВОПРОСУ ИЗУЧЕНИЯ МЕТОДОВ ВЗЛОМА ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И РАЗРАБОТКЕ МЕР ПО ИХ ЗАЩИТЕ

В настоящее время информационные системы являются неотъемлемой частью работы органов внутренних дел (ОВД). Они используются для хранения и обработки большого количества информации, включая личные данные граждан, сведения о преступлениях и расследованиях, а также другую конфиденциальную информацию. Однако с ростом использования информационных технологий появляются все новые методы атак и способы взлома информационных систем. В результате системы ОВД могут стать уязвимыми для кибератак и кражи данных. Цель данной статьи состоит в анализе основных способов взлома информационных систем ОВД и мер защиты от них.

Информационные системы в ОВД – это комплекс программных и аппаратных средств, предназначенных для обработки, хранения и передачи информации в деятельности органов внутренних дел.

Проанализируем основные способы взлома информационных систем ОВД:

1. Фишинг – это мошенническая попытка получить конфиденциальные данные (логины, пароли, номера банковских карт и т. д.) путем подделки электронных писем или сайтов, которые выглядят как официальные. Как правило, фишинг-атаки начинаются с отправки электронных писем, которые могут выглядеть, как будто они отправлены от правительственных учреждений, банков или других организаций. Цель таких атак – убедить пользователей предоставить свои конфиденциальные данные, которые затем могут быть использованы для взлома системы.

2. Вирусы и трояны – это программы, которые могут быть установлены на компьютеры, используемые ОВД, без ведома пользователя. Они могут проникнуть на компьютеры через вредоносные веб-сайты, электронную почту или даже USB-накопители. Эти программы могут служить для установки дополнительного вредоносного ПО, сбора конфиденциальной информации или перехвата управления системой.

3. DDoS-атаки (от англ. Distributed Denial of Service – распределенный отказ в обслуживании) – это атаки, при которых злоумышленники перегружают

¹ © Капшунов Д. С., 2023.

систему большим количеством запросов, что приводит к ее выходу из строя или к снижению ее производительности. Для таких атак часто используются ботнеты – сети компьютеров, зараженных вредоносным ПО, которые управляются из одного центра.

4. Социальная инженерия – это психологический метод атаки, при котором злоумышленники убеждают сотрудников ОВД предоставить конфиденциальную информацию или выполнить определенные действия, которые могут привести к взлому системы. Например, злоумышленники могут позвонить в ОВД, выдавая себя за сотрудников другой организации, и запросить конфиденциальную информацию. Этот метод атаки очень эффективен, так как люди зачастую доверчивы и не задумываются о том, что могут стать жертвами атаки.

5. Недостатки в системах безопасности – это ошибки, которые могут быть обнаружены в системах ОВД и использованы злоумышленниками для взлома системы. Например, это может быть уязвимость в программном обеспечении, слабые пароли, отсутствие защиты от перебора паролей и т. д.

Изучив основные требования и угрозы, можно выделить следующие меры защиты от взлома информационных систем ОВД:

1. Обучение сотрудников ОВД. Сотрудники ОВД должны быть обучены основам информационной безопасности и тому, как распознавать фишинг-атаки, вирусы и трояны, а также как обезопасить свои пароли и личные данные. Обучение должно проводиться регулярно и включать в себя тренировочные упражнения для сотрудников.

2. Использование антивирусного ПО и брандмауэров. Системы ОВД должны быть защищены от вредоносного ПО с помощью антивирусного ПО и брандмауэров. Это позволит защитить систему от вирусов, троянов и других угроз.

3. Использование сильных паролей и двухфакторной аутентификации. Для защиты от перебора паролей, сотрудники ОВД должны использовать сильные пароли, состоящие из различных символов и цифр, а также использовать двухфакторную аутентификацию.

4. Аудит безопасности системы. Регулярный аудит безопасности системы поможет выявить уязвимости и недостатки в системе безопасности, которые могут быть использованы злоумышленниками для взлома системы. Аудит должен включать в себя проверку наличия обновлений и патчей, проверку системных журналов и т. д.

5. Ограничение доступа к конфиденциальной информации. Сотрудники ОВД должны иметь доступ только к той информации, которая необходима для выполнения их служебных обязанностей. Кроме того, доступ к конфиденциальной информации должен быть ограничен и контролируем, чтобы предотвратить несанкционированный доступ.

6. Резервное копирование данных. Регулярное резервное копирование данных поможет предотвратить потерю данных в случае атаки или системного сбоя. Копии данных должны храниться в надежных и защищенных местах.

7. Использование шифрования. Шифрование может использоваться для защиты конфиденциальной информации и данных, которые передаются по сети.

Для шифрования можно использовать различные алгоритмы, такие как AES, RSA и т. д.

8. Мониторинг безопасности системы. Регулярный мониторинг безопасности системы позволит выявлять необычную активность в системе и быстро реагировать на угрозы безопасности. Для мониторинга можно использовать специальные программы, которые будут анализировать журналы системных событий и сетевую активность.

Системы ОВД могут стать уязвимыми для различных методов атак, которые используются злоумышленниками для получения несанкционированного доступа к информации. Для защиты от этих угроз были представлены различные меры, которые могут быть использованы для укрепления информационной безопасности систем ОВД. Особо отметим, что важным элементом обеспечения информационной безопасности является обучение сотрудников ОВД.

В целом рассмотрение данного вопроса показывает, что защита информационных систем ОВД от взлома и несанкционированного доступа является важным вопросом для обеспечения безопасности граждан и предотвращения преступлений.

Список литературы

1. Алексеенко С. П., Баркалов Ю. М. Обнаружение и реагирование на инциденты в инфокоммуникационных системах ОВД // Охрана, безопасность, связь. 2019. Т. 1. № 4 (4). С. 131–135.
2. Канавин С. В., Хохлов Н. С. Анализ рисков нарушения информационной безопасности в информационных, телекоммуникационных системах ОВД // Общественная безопасность, законность и правопорядок в III тысячелетии. 2020. № 6-2. С. 174–177.
3. Основные угрозы информационной безопасности органов внутренних дел // URL: <https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-vooruzhennykh-sil-rf/osnovnye-ugrozy-informatsionnoj-bezopasnosti-organov>.
4. Федеральный закон от 26 июля 2006 г. № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798.
5. Худяков В. В., Альховская А. В. К вопросу об обеспечении кибербезопасности деятельности сотрудников полиции // Проблемы информационного обеспечения деятельности правоохранительных органов : сборник статей IX Всероссийской научно-практической конференции, Белгород, 20 мая 2022 года. Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2022. С. 175–181.

Савоськин Р. А.¹,
тестировщик программного обеспечения компании
ООО «Реинформ Инт.»

ОСНОВНЫЕ ВИДЫ КИБЕРПРЕСТУПЛЕНИЙ И ПЕРВОНАЧАЛЬНЫЕ ДЕЙСТВИЯ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ПРОТИВОДЕЙСТВИЮ ИМ

Значительное количество регистрируемых киберпреступлений в последние годы вынуждает государственные органы, специализирующиеся на противодействии им, вырабатывать новые подходы к данной деятельности.

Из основных рекомендаций можно выделить следующие: неукоснительное соблюдение сотрудниками правоохранительных органов порядка сбора и хранения необходимой доказательной базы по фактам хищений денежных средств; организация оперативного взаимодействия правоохранительных органов с банковскими структурами и порядка их информирования; опрос потерпевшего дознавателем/следователем на первоначальном этапе, проведение изъятия ПК, телефона; назначение криминалистического исследования и в зависимости от результатов проведение ОРМ.

Хищения у юридических лиц можно свести к четырем видам хищений:

1. Подмена ИНН и р/с получателя.
2. Подмена р/с получателя.
3. Замена получателя в счете на оплату.
4. Мошенничество «возврат денежных средств».

Рассмотрим более подробно каждый из этих видов.

1. Подмена ИНН и р/с получателя.

1. Описание схемы мошенничества.
2. Клиент сформировал в 1С платежное поручение на ООО «Ромашка»
3. Клиент экспортировал поручение из 1С в ДБО.
4. Клиент из ДБО отправил в Банк.
5. Банк прислал Клиенту SMS с подтверждением платежа. В SMS указаны все реквизиты получателя. Клиент платеж подтвердил.
6. Банк исполнил поручение.

Позже выяснилось, что в Банк ушло платежное поручение, где БИК банка получателя и счет получателя заменены на ранее Клиенту неизвестные, но наименование получателя осталось неизменным – ООО «Ромашка».

В данном случае мошенничество стало принципиально возможно из-за того, что Клиент даже не пытался сверить цифры р/с и считал платеж легитимным.

Так как сами по себе реквизиты не могут замениться на мошеннические, то требуется криминалистическая экспертиза компьютера клиента. Учитывая, что

¹ © Савоськин Р. А., 2023.

таким мошенничеством уже промышляли преступные кибергруппировки Lurk, Buhtrap и Fibbit, вероятность вирусного заражения компьютера потерпевшего велика.

2. Подмена только БИК и р/с получателя без других изменений реквизитов получателя.

Возможна, если банк получателя не проверяет соответствие ИНН и р/с.

3. Замена получателя в счете на оплату.

1. Клиент заказывает счет на оплату у партнера.
2. Партнер высылает Клиенту счет электронной почтой.
3. Клиент оплачивает счет не глядя.

Позже выясняется, что деньги партнеру не пришли, а партнер отправлял другие реквизиты.

В данном кейсе счет на оплату меняется в электронной почте Клиента или его партнера. Точно так же могут быть подменены реквизиты не полностью, а как в первом кейсе.

4. Мошенничество «возврат денежных средств».

1. Клиент получает на р/с небольшую сумму от неизвестного ранее контрагента.

2. Клиент получает электронное письмо от этого неизвестного контрагента с просьбой вернуть случайно направленные в адрес Клиента деньги. В письме файл с реквизитами.

3. Клиент открывает файл.

4. Клиент вносит в справочник доверенных неизвестного контрагента для возможности вернуть деньги.

5. Клиент возвращает ДС.

Позже выясняется, что с компьютера жертвы стали сами собой отправляться платежи на того, кому ранее возвратили, а ДБО «глючит».

В данном кейсе клиент из файла в почте получает вирус, который впоследствии управляет компьютером. Кроме того, Клиент сам вносит нового получателя в доверенные своего ДБО. Кроме того, «ошибочный» платеж и его возврат фактически обучают систему антифрода Банка, указывая системе, что они партнеры и их операции легитимные.

У следователя есть полномочия «пробить» телефоны, IP и граждан России. Если схожих случаев кибермошенничества накапливается много, то вероятность выйти на мошенников увеличивается. Чтобы работа по «пробивке» не потерялась, по всем случаям кибермошенничества необходимо подключать на сопровождение «К» МВД, так как у «К» ведется внутренняя база. Не исключена вероятность, что в «К» уже знают мошенников.

Порядок расследования вышеизложенных способов хищения у юридических лиц описан в методических рекомендациях о порядке действий в случае выявления хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства клиента, созданных Рабочей группой Ассоциации Российских банков и НП «Национальный платежный совет» по предотвращению мошенничества в платежных системах (Протокол № 1 от 19 июля 2012 г.).

Хищения у физических лиц. Актуальные темы по хищениям в ДБО у физических лиц:

1. Хищение с использованием вирусного заражения мобильного устройства.
2. Хищение с использованием методов социальной инженерии.
3. Хищение с использованием вирусного заражения ПК клиента (фишинг).
4. Хищение с заменой СИМ-карты.

Дознаватель/следователь на первоначальном этапе должен опросить потерпевшего провести изъятие ПК, телефона.

Назначить криминалистическое исследование и в зависимости от результатов, провести ОРМ.

Хищение с использованием вирусного заражения мобильного устройства.

1. Получить объяснение клиента.
2. Провести изъятие мобильного устройства.
3. Клиент должен предоставить:
 - выписку СМС-сообщений от сотового оператора
 - выписку по счету банковской карты
4. Сделать запрос в банк, в котором необходимо запросить:
 - данные о получателе средств;
 - если это номер карты, то предоставить установочные данные на владельца;
 - место обналичивания средств: дата, время, город, номер банкомата, место его установки;
 - если это номер телефона, то подключен ли телефон к картам банка, если да, см. выше.
 - если электронный кошелек, запросить установочные данные на владельца кошелька и движения средств у владельца системы.
5. Назначить криминалистическую экспертизу мобильного устройства на предмет наличия: вируса, данных по управляющим серверам и т. д.
6. Привлечь к оперативному сопровождению сотрудников правоохранительных органов.

Хищение с использованием методов социальной инженерии.

7. Получить объяснение клиента.
8. Клиент должен предоставить:
 - выписку СМС-сообщений от сотового оператора;
 - выписку входящих/исходящих звонков;
 - выписку по счету банковской карты.
9. Если зафиксированы входящие звонки с неизвестных заявителю номеров, запросить операторов о владельце.
10. Сделать запрос в банк, в котором необходимо запросить:
 - данные о получателе средств;
 - если это номер карты, то предоставить установочные данные на владельца;
 - место обналичивания средств: дата, время, город, номер банкомата, место его установки;
 - имелись ли факты переводов с карты получателя похищенных средств на другие карты, если да, то см. выше;

- если это номер телефона, то подключен ли телефон к картам банка, если да, см. выше;
- если электронный кошелек, запросить установочные данные на владельца кошелька и движения средств у владельца системы.
- Данные IP-адреса, с которого осуществлялось хищение средств.
- Запросить интернет-провайдера для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента.
- Проверить, были ли обращения от имени заявителя в службу помощи банка по номерам в п. 9.
- Если звонки были, запросить копии аудиозаписей.

Хищение с использование вирусного заражения ПК клиента (фишинг).

11. Получить объяснение клиента.

12. Клиент должен предоставить:

- выписку СМС-сообщений от сотового оператора;
- выписку входящих/исходящих звонков;
- выписку по счету банковской карты.

13. Если зафиксированы входящие звонки с неизвестных заявителю номеров, запросить операторов о владельце.

14. Сделать запрос в банк, в котором необходимо запросить;

- данные о получателе средств;
- если это номер карты, то предоставить установочные данные на владельца;
- место обналичивания средств: дата, время город, номер банкомата, место его установки.
- Имелись ли факты переводов с карты получателя похищенных средств на другие карты, если да, то см. выше:
- если это номер телефона, то подключен ли телефон к картам банка, если да, см. выше.

– Если электронный кошелек, запросить установочные данные на владельца кошелька и движения средств у владельца системы.

- Данные IP-адреса, с которого осуществлялось хищение средств.
- Запросить интернет-провайдера для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента.
- Проверить, были ли обращения от имени заявителя в службу помощи банка по номерам в п. 9.

– При установлении фактов входящих звонков, с которых проводился «развод» потерпевшего, запросить владельцев.

- Если звонки были, запросить копии аудиозаписей.
- Назначить криминалистическую экспертизу устройства на предмет наличия: вируса, данных по управляющим серверам и т. д.
- Привлечь к оперативному сопровождению Управление «К».

Хищение с заменой СИМ-карты.

15. Получить объяснение Клиента.

16. Клиент должен предоставить:

- выписку СМС-сообщений от сотового оператора;
- выписку входящих/исходящих звонков;

- выписку по счету банковской карты;
- письмо от сотового оператора о факте замены СИМ-карты.

17. Если зафиксированы входящие звонки с неизвестных заявителю номеров, запросить операторов о владельце.

18. Запросить у сотового оператора:

- копию доверенности, по которой осуществлялась замена СИМ-карты;
- данные ЕМЕІ, в который вставлялась замененная СИМ-карта, ее номер;
- вставлялись ли другие СИМ-карты в устройство с этим ЕМЕІ, их номера;
- данные геолокации по ЕМЕІ.

19. Проверить через нотариат подлинность доверенности.

20. При выявлении факта использования поддельной доверенности провести проверку поверенного лица по спец. учетам МВД, в том числе и базам данных МВД (ГИБДД, Трасса, Магистраль и др.).

21. Сделать запрос в банк, в котором необходимо запросить:

- данные о получателе средств;
- если это номер карты, то предоставит установочные данные на владельца;
- место обналичивания средств: дата, время, город, номер банкомата, место его установки.

– Имелись ли факты переводов с карты получателя похищенных средств на другие карты, если да, то см. выше:

– если это номер телефона, то подключен ли телефон к картам банка, если да, см. выше.

– Если электронный кошелек, запросить установочные данные на владельца кошелька и движения средств у владельца системы.

– Данные IP-адреса, с которого осуществлялось хищение средств.

– Запросить интернет-провайдера для получения в электронной форме журналов соединений с Интернет с электронного устройства Клиента

– Проверить, были ли обращения от имени заявителя в службу помощи банка по номерам в п. 9.

– Если звонки были, запросить копии аудиозаписей.

– При установлении факта мошенничества:

– Назначить криминалистическую экспертизу устройства на предмет наличия: вируса, данных по управляющим серверам и т. д.

– Привлечь к оперативному сопровождению правоохранителей.

Еще один вид мошенничества – использование поддельных банковских карт в торгово-сервисной сети.

При расследовании данного вида мошенничества следователь/дознатель должен знать технологию расчетов по операциям с банковскими картами при проведении оплаты товаров и услуг.

После проведения операции покупки товара по банковской карте торгово-сервисное предприятие (далее – ТСТ) составляет платежный документ (запрос) с использованием карты и в режиме on-line передает данный документ в банк для оплаты, далее информация об этой операции также в режиме on-line через платежную систему передается в банк-эмитент этой карты, и при получении одобрения (кода авторизации) банк в конце рабочего дня переводит деньги за покупку

со своего расчетного счета обслуживаемому предприятию. Возмещение денежных средств от банка-эмитента по проведенной операции банк получает через платежную систему в течение 5–7 дней.

После того, как выясняется, что операция была мошенническая, банк-эмитент может опротестовать данную операцию. В этом случае денежные средства снимаются со счета банка-эквайера. Такое опротестование (чарджбэк) может быть представлено в течение 6 месяцев с момента совершения мошеннической операции. По условиям договора предприятием денежные средства с предприятия, как правило, не снимаются. Таким образом, ущерб по мошеннической операции ложится на банк-эквайер.

При расследовании таких преступлений следователю/дознавателю необходимо:

1. Получить объяснения с сотрудников банка.
2. Получить в офисе банка копии чеков по операциям.
3. Получить в офисе банка материалы видеонаблюдения (при наличии).
4. Получить в банке список авторизационных запросов.
5. Получить в банке список финансовых транзакций.
6. Получить в банке/офисе документы о зачислении денежных средств на счет.
7. Получить в банке копии запросов в банки-эмитенты.
8. Получить в банке копии ответов от банков-эмитентов.
9. Получить в банке список операций, объявленных банком эмитентов как мошеннические и выставленных в FRS/SAFE.
10. При наличии задержанных платежных карт провести криминалистическое исследование.
11. Запросить в банке, проводились ли по банковской карте другие операции в других ТСТ. При выявлении таких операций предпринимаются действия, указанные выше.

Список литературы

1. Информационно-аналитические материалы ПАО Сбербанк.
2. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / [В. В. Гончар и др.]. М. : Инфра-М, 2023.

Назаров А. К.¹,

*преподаватель кафедры информационной безопасности
Краснодарского университета МВД России,
кандидат физико-математических наук*

КИБЕРБЕЗОПАСНОСТЬ: ПРОБЛЕМЫ И УГРОЗЫ

С каждым годом растет число кибератак, при этом «ландшафт» киберугроз становится все шире. Потому особенно актуальным становится получение знаний о фундаментальных основах безопасности и приватности, умений производить моделирование угроз и оценку рисков, освоение основ шифрования. В современном мире – мире информационных технологий – важно иметь более глубокие знания основ организации и принципов функционирования операционных систем, а именно, разбираться в особенностях безопасности и приватности операционных систем (например, Windows, Linux, Mac OS X).

Другой особенностью развития киберпространства является наличие в ней программ, ботов, которые работают в автоматическом режиме, сканируют сеть Интернет, находят уязвимости системы и предоставляют эту информацию в открытом доступе. Эти программные продукты позволяют хакерам без особого опыта совершать попытки получить несанкционированный доступ к компьютерным системам с целью украсть, изменить, уничтожить данные или использовать компьютерную систему для проведения дополнительных атак. Причем им достаточно найти одну уязвимость в системе для совершения кибератаки, в то время как сотрудникам по информационной безопасности и обычным пользователям необходимо найти все слабые места в системе, чтобы усилить их защиту. Данный факт только усложняет работу по созданию системы с высоким уровнем защищенности. При этом даже одна успешно совершенная кибератака может привести к огромным потерям (финансовым потерям, утечке информации, потере репутации и т. д.).

Существуют также поисковые системы, с помощью которых можно, в частности, быстро найти уязвимые места устройств в сети Интернет. Так на сайте <https://www.shodan.io/> можно ввести в качестве строки запроса значение «default password», в результате чего мы получим список подключенных к сети устройств, использующих пароль по умолчанию. При этом в результатах запроса отображаются IP-устройства и учетные данные для авторизации. Это может позволить злоумышленнику даже без специальных навыков получить несанкционированный доступ к чужим устройствам.

Еще одной серьезной угрозой, несомненно, можно считать наличие в сети Интернет предложений о продаже готовых наборов эксплойтов для различных типов уязвимостей. Наличие в сети Интернет подобных продуктов также позволяет хакерам без особого опыта совершать кибератаки.

Очевидно, что при наличии в открытом доступе в сети Интернет автоматизированных систем поиска уязвимостей и увеличения числа хакеров повышение

¹ © Назаров А. К., 2023.

цифровой грамотности обычных пользователей, а также соблюдение ими кибергигиены и других мер по предотвращению от кибератак могут оказаться далеко недостаточными для полной защиты своих компьютерных систем. «Ахелесовой пятой» может оказаться, к примеру, уязвимость нулевого дня.

Еще одной потенциальной угрозой можно считать возможное использование искусственного интеллекта в киберпреступлениях, что приведет к качественным изменениям в сфере кибербезопасности.

С учетом вышесказанного можно сделать вывод о необходимости рассмотрения и принятия дополнительных мер по обеспечению кибербезопасности:

1. Усиление контроля в сети Интернет, в том числе использование искусственного интеллекта с целью поиска киберпреступников, содействующих им лиц, для анализа действий пользователей, анализа содержимого сайтов, предотвращения кибератак, для усиления защиты информационных систем и т. д. Использование искусственного интеллекта (как киберпреступникам, так и защитниками правопорядка) представляет собой новую эру в развитии киберпространства.

2. Изменение протоколов обмена данными. Существующие и используемые на сегодняшний день правила обмена данными уже давно доказали на практике, что они не обеспечивают должного уровня безопасности. Назрела необходимость пересмотра, замены протоколов обмена данными на современные, созданные с учетом нынешних реалий и всего спектра киберугроз.

3. Принятие новых правовых мер по борьбе с киберпреступностью. Такие меры должны быть приняты как на государственном уровне, так и международном.

В связи с постоянным и быстрым развитием киберпространства, усложнением программных средств, развитием информационных технологий будут появляться новые уязвимости, которыми могут воспользоваться киберпреступники. Наличие у них в арсенале ботов, искусственного интеллекта только усложняет ситуацию. Возможным решением этих проблем может стать создание нового безопасного «киберПодпространства», функционирующего по новым правилам обмена данными, обеспечивающим безопасность и «прозрачность» работы в сети.

Список литературы

1. Н. Хауз. Полный курс по кибербезопасности : секреты хакеров. Т. 1 / Н. Хауз 2017.
2. Винокуров С. А. Основы кибербезопасности : учебник / С. А. Винокуров [и др.]. Воронеж, Воронежский институт МВД России, 2022.

Куриленко Ю. А.¹,

*заместитель начальника кафедры информатики и математики
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук*

Михайлова В. Д.²,

*курсант Института судебной экспертизы
Московского университета МВД России имени В.Я. Кикотя*

КИБЕРШПИОНАЖ – УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сегодня мы живем в эпоху интернет-революции. Никогда еще человечество не было так взаимосвязано и не имело такого широкого доступа к одним и тем же инструментам и информации. Будучи движущей силой глобализации и современного прогресса, интернет обеспечивает мгновенный доступ к информации и связь с ней, одновременно создавая новую среду для культурного обмена. Однако Интернет также создает новые риски, связанные с угрозой информационной безопасности. В процессе компьютеризации кибершпионаж стал опасной проблемой: доступность информации привела к ее неизбежной утечке.

Кибершпионаж – несанкционированное получение информации с целью личного, экономического или военного превосходства, осуществляемое с использованием обхода (взлома) систем компьютерной безопасности с применением вредоносного программного обеспечения [1]. Угрозы кибершпионажа становятся активнее, поскольку интернет и гаджеты играют все более важную роль в жизни каждого человека. Сегодня почти вся информация находится на электронных носителях, что позволяет злоумышленникам совершать киберпреступления с целью получения конфиденциальных данных, государственной тайны, кражи финансовых данных и банковских карт, а также личных данных. Атаки кибершпионов в основном направлены на несанкционированные данные государственных или коммерческих организаций, поскольку это наиболее ценная информация. Цель таких атак – попытка похитить корпоративные, промышленные и военные секреты, информацию о разработках в различных отраслях, важные промышленные и производственные объекты, данные о механическом оборудовании и телекоммуникациях, а также сведения о транспортной инфраструктуре. В. В. Путин на заседании коллегии Федеральной службы безопасности в 2014 г. определил, что «объектом шпионажа являются перспективные отечественные технологии и разработки, планы строительства и развития Вооруженных Сил и оборонно-промышленного комплекса, важнейшие политические и экономические сведения» [2]. В основном кибершпионаж осуществляется путем взлома через интернет и локальные сети, намного реже – через физический доступ. Вредоносные и шпионские программы, программы-импланты, а также целевые атаки являют-

¹ © Куриленко Ю. А., 2023.

² © Михайлова В. Д., 2023.

ся основными методами, используемыми для незаконного получения данных. Эта деятельность может нарушить работу государственных учреждений, федеральных агентств и предприятий.

С 2000 года число хакерских атак ежегодно увеличивается. Согласно отчету телекоммуникационной компании Verizon по кибершпионажу (за период с 2014 года по 2021 год) в 2020 году по сравнению с 2019 использование программ-вымогателей увеличилось на 6 %, количество фишинговых атак – на 11 %, самый большой рост составляет взлом учетных данных – 61 %. В 88 странах было выявлено 79 тысяч инцидентов, средняя стоимость атаки составила 21 тысячу долларов, при этом в 95 % ущерб составляет от 60 тысяч до 48 миллионов рублей. По данным отчета, в большинстве случаев кибершпионаж осуществляется с целью кражи личных, учетных, медицинских и платежных данных [3].

Многие считают, что проблему кибершпионажа можно решить через установленные брандмауэры – технологические барьеры, защищающие сеть от несанкционированного доступа. Брандмауэры, несомненно, фильтруют данные, поступающие в сеть, и не позволяют злоумышленникам получить доступ к конфиденциальной информации. Однако они менее полезные и значимые в ограничении неспециализированных хакеров. Еще одна проблема, возникающая при использовании брандмауэров так же, как и при использовании антивирусных программ, – это пренебрежительное отношение к безопасности на уровне пользователей. Пользователь может начать ощущать себя непобедимым за своим «экраном» или антивирусной программой и перестает уделять внимание защите своих данных или предотвращению вторжений в будущем.

Проблема безопасности в условиях постоянных угроз кибератак, безусловно, насущная. По нашему мнению, будущее безопасности заключается в защите данных и соединений на уровне отдельного компьютера. И задействование искусственного интеллекта здесь занимает одну из главных позиций. К примеру, использование методов и возможностей искусственного интеллекта в специальных самоорганизующихся мультиагентных роевых системах (SOMAS), которые способны самосинхронизироваться. Такая система помогает работать агентам без централизованного контроля. Вместо традиционного планирования «да»/«нет» агенты способны принимать решения на основе фактической ситуации, научившись на своем опыте через симуляторы. Данные роевые программы намного эффективнее в обеспечении второй линии защиты, чем соответствующие человеческие аналоги, поскольку они обучаются во много раз быстрее [4].

Следует также рассмотреть вопрос аутентификации пользователей. Аутентификация в киберпространстве – процесс проверки личности пользователя перед предоставлением доступа определенному компьютеру или интернет-сети. Основным видом такой проверки являются пароли пользователя, однако это не всегда предотвращает угрозу кибершпионажа. Именно по этой причине рекомендуется устанавливать многофакторную защиту доступа к сети, поскольку в таком случае хакерам приходится получать несанкционированный доступ сразу к нескольким устройствам аутентификации одновременно, что затрудняет атаку злоумышленников.

Наконец, есть возможность перейти в частное интернет-пространство, а также сократить количество существующих сетей. Каждое государственное учреждение и корпоративное предприятие эксплуатируют множество отдельных сетей, при сокращении которых количество незащищенных соединений и пересечений между самими сетями уменьшается и, следовательно, приводит к повышению безопасности данных от угрозы кибершпионажа.

Несмотря на то что кибершпионаж представляет собой серьезную угрозу, его можно уменьшить путем внедрения новых технологий безопасности.

Список литературы

1. Википедия. Кибершпионаж // URL: <https://ru.wikipedia.org/wiki/Кибершпионаж>.
2. Заседание коллегии Федеральной службы безопасности // URL: <http://www.kremlin.ru/events/president/news/17516>.
3. Дарья Каспарьянц. Обзор ежегодного отчета компании VERIZON по результатам расследования утечки данных и первого отчета по кибершпионажу // URL: <https://rdc.grfc.ru/2021/07/verizon-report/>.
4. Ерофеева В. А., Иванский Ю. В., Кияев В. И. Управление роом динамических объектов на базе мультиагентного подхода // Компьютерные инструменты в образовании. 2015. № 6. С. 34–42.

Лустин В. И.¹,

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

ЗАЩИТА ИНФОРМАЦИИ. ВИБРОАКУСТИЧЕСКИЙ КАНАЛ

Виброакустический канал утечки информации образуется из-за воздействия акустических сигналов, возникающих при ведении разговоров в выделенном помещении, на строительные конструкции (стены, потолки, полы, двери, оконные рамы и т. п.) и инженерно-технические коммуникации (трубы водоснабжения, отопления, канализации, воздуховоды и т. п.), которое вызывает в них упругие (вибрационные) колебания, которые и регистрируются датчиками средства разведки [1].

При разговоре волна распространяется и колеблется об ограждающие конструкции, такие как системы отопления, оконные проемы и т. п. при помощи специальных стетоскопов злоумышленник может преобразовывать эти колебания в акустический сигнал. Борьба с прямым акустическим каналом происходит за счет звукоизоляции помещений. К примеру, уплотнение дверных косяков, дополнительный слой звукоизоляционных материалов на все поверхности помещения, уплотнение оконных проемов. Для защиты от виброакустического канала используются любые средства, которые уменьшают колебания, к примеру, резиновые вставки на стены. А к активному методу в основном относятся генераторы шума. Также устанавливаются виброгенераторы на ограждающие конструкции, которые «сбивают» колебания.

Организационные мероприятия – мероприятия по защите информации, которые подразумевают использование специально созданных технических средств, предназначенных для защиты информации. К главным организационным мероприятиям причисляются определение пределов контролируемой зоны, т. е. той зоны, в которой без наблюдения и сопровождения не могут находиться люди, автомобили и прочая техника, не имеющих специальных пропусков.

Чтобы злоумышленник не мог получить доступ к интересующему его объекту, создается организация контроля и ограничения доступа к информационным системам и защищаемым помещениям, выставление постов охраны и видеонаблюдения, а также любые другие меры, направленные на защиту.

Технические мероприятия – мероприятия по защите информации, предусматривающие осуществление особых технических решений, а также использование особых технических средств. Технические мероприятия исполняются с использованием пассивных и активных средств защиты. Они ослабляют уровень информационного сигнала, который может перехватить злоумышленник. Существует множество видов аппаратуры для перехвата акустической информации.

¹ © Лустин В. И., 2023.

Меры по защите от утечки информации направлены на закрытие каналов утечки информации посредством снижения уровня информационного сигнала или снижения отношения сигнал/шум в местах, где возможно размещение переносных средств разведки или их обнаружителей до значения, которое делает это невозможным, т. е. заставляет изолировать сигнал с помощью средств разведки и вести с помощью пассивных или активных средств защиты [2].

К техническим мероприятиям, осуществляемым с помощью пассивных средств, относят:

- контроль и ограничение доступа на объекты технической голосовой побочной информации (ТГПИ), а также закрепленные за ними помещения;
- установку технических устройств и систем контроля и ограничения доступа на объекты ТГПИ, а также закрепленные за ними помещения;
- установку технических устройств и систем контроля и ограничения доступа на объекты ТГПИ в охраняемые помещения;
- звукоизоляцию охраняемых объектов [3; 4].

Для снижения риска утечки информации по виброакустическому каналу специалистам по защите информации необходимо максимально ослабить речевой сигнал от источника звука, который поступает на коммуникации, служащие средой его распространения, где он может быть перехвачен.

Первым решением будет архитектурно-дизайнерское:

- покрытие стен пористой штукатуркой;
- использование штор или жалюзи;
- установка дверей с двойной рамой;
- установка шумогенераторов.

Поиск устройств для извлечения информации затруднен из-за проблем с доступом в помещение, где вполне возможно могут быть установлены встроенные устройства, но когда проблема решена, специализированные устройства осуществляют поиск запоминающих устройств с помощью демаскирующих щитов. Существуют многофункциональные локаторы, способные обнаруживать большинство типов встроенных устройств, предназначенных для считывания данных с различных инженерных каналов утечек, в том числе виброакустических. Лучше выбирать бытовую технику, несертифицированные китайские аналоги менее надежны.

Оснащение помещения защитой от протечек из виброакустических каналов может сильно ударить по бюджету. Для снижения затрат необходимо совмещать защиту от виброакустических и акустических утечек и проводить превентивные меры, не полагаясь на обнаружение встроенных устройств.

Защита от акустических и виброакустических каналов утечки информации предполагает использование двух видов средств: пассивных и активных. При использовании пассивных средств защиты гарантируется звукоизоляция помещения. В рассматриваемом помещении такие средства предлагается использовать по минимуму, так как любого рода реконструкция помещения повлечет за собой большие затраты на создание защитной системы. Самым важным моментом в конструкции пассивной защиты является стена с окнами, так как она выходит на улицу. При этом имеется контролируемая зона, что в свою очередь исключает

прямое прослушивание. Не исключаем возможности прослушивания и с верхних этажей [5].

Поэтому рекомендуется использовать следующие средства:

- использовать для обшивки потолка плиты из гранулированной минеральной ваты. Предварительно заделайте все щели в потолке;
- вместо используемых жалюзи в защищаемом помещении можно использовать тканевые шторы, так как они обладают лучшей звукоизоляцией, чем пластиковые жалюзи или рольставни;
- установить двойную дверь;
- использовать звукопоглощающий материал для дверной панели.

Звукоизоляция корпусов защитных помещений, их систем вентиляции и кондиционирования должна обеспечивать отсутствие возможности подслушивания разговоров, ведущихся внутри, извне защищаемого помещения. Поскольку все вышеперечисленные меры защиты информации от утечки по акустическим и виброакустическим каналам недостаточны, а дополнительные пассивные средства защиты непригодны, необходимо использовать метод активной акустической или виброакустической шумовой маскировки.

Для этого должны использоваться сертифицированные средства активной защиты. В такой защите нуждаются окна, стены, двери, потолки и батареи.

Пассивные методы защиты информации обычно реализуются при строительстве или реконструкции зданий, на этапе разработки проектных решений, что позволяет заранее учитывать типы строительных конструкций, способы связи и оптимальные места размещения помещений компании. Если пассивная защита здания технически невозможна или не соблюдаются требуемые нормы защиты от шума, применяются активные защитные меры.

Список литературы

1. Разработка системы технической защиты информации : учебное пособие / [В. И. Аверченков и др.]. Брянск : Брянский государственный технический университет, 2012.
2. Технические средства и методы защиты информации : учебник для вузов / [А. П. Зайцев и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. М. : ООО Издательство Машиностроение, 2009.
3. Титов А. А. Инженерно-техническая защита информации : учебное пособие. Томск : Томский государственный университет систем управления и радиоэлектроники, 2010.
4. Торокин А. А. Инженерно-техническая защита информации : учебное пособие. М. : Гелиос АРВ, 2005.
5. Хорев А. А. Способы и средства защиты информации : учебное пособие. М. : МО Российской Федерации. 2000.

Климова Е. К.¹,

слушатель института судебной экспертизы

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Виноградова Н. И.,

доцент кафедры технико-криминалистического обеспечения

экспертных исследований

учебно-научного комплекса судебной экспертизы

Московского университета МВД России имени В.Я.Кикотя,

кандидат химических наук, доцент

ИННОВАЦИОННЫЙ ПОДХОД В ОПРЕДЕЛЕНИИ ДЕФЕКТОВ МАТРИЦ В СЪЕМОЧНЫХ УСТРОЙСТВАХ

Увеличение объема визуальной информации в современном мире не вызывает сомнений. Наиболее простым способом запечатления визуальной информации является цифровая фотография.

Преступный мир также не стоит на месте. В значительном количестве преступлений фигурирует цифровая фотография. Возможность идентификации съемочного устройства, на котором было сделано изображение, в значительной мере облегчила раскрытие и расследование преступлений.

Одним из основных этапов создания цифровой фотографии является формирование изображения на матрице. Проходя через систему линз, свет попадает на матрицу – микросхему фотокамеры, на которой находятся светочувствительные элементы, преобразующие свет в электрический сигнал. Данные элементы могут с течением времени «изнашиваться» в результате эксплуатации и отображаться на фотоизображениях в виде точек, нарушающих общую композицию [1]. Неисправные пиксели, отображаемые на фотографии, получили названия «горячие» и «битые» пиксели.

«Горячие пиксели» проявляются в виде цветных точек и могут возникать и исчезать в зависимости от различных факторов. «Битые» пиксели могут быть постоянно белыми либо постоянно черными, независимо от выдержки, ISO, температуры и других факторов. Устойчивость отображения и неповторимый (случайный) характер возникновения дает возможность использовать «битые пиксели» для идентификации матрицы съемочного устройства.

Проверить наличие дефектных пикселей матрицы можно опытным путем. Устанавливаются следующие параметры фотосъемки: чувствительность ISO – 50, разрешение максимальное для конкретной модели, сжатие изображения с минимальными потерями, режим съемки – без вспышки. Объектив закрыт непрозрачной заслонкой (шторкой), гарантирующей полную светонепроницаемость. Делается несколько снимков с максимальным возможным временем экспозиции [2].

¹ © Климова Е. К., 2023.

При исследовании непосредственно съемочного устройства на предмет дефектов матрицы предпочтительнее осуществлять фотосъемку в формате RAW, так как данный формат содержит необработанные данные об электрических сигналах с фотоматрицы цифрового фотоаппарата [3]. Использование метода на изображениях, представленных в формате JPEG, снижает точность работы в связи с тем, что используемый алгоритм сжатия с потерями основан на устранении высоких частот в изображении, что приводит к размытию изображения, и, соответственно, увеличению ложных срабатываний при обнаружении особых точек.

Так как эксперту на исследование могут приходить различные объекты, необходимо исследовать оба формата. В полученных экспериментальных снимках всех форматов важно точно дифференцировать «горячие» пиксели от «битых», так как для идентификации могут быть использованы только «битые» пиксели.

В изображениях формата RAW для определения природы пикселя необходимо произвести вычисление среднего значения пикселей, принадлежащих пикселям матрицы, имеющим одинаковый цвет светофильтра, после чего выполнить сравнение полученного значения со значением пикселя по формуле:

$$D = \left| \frac{S_{x,y+2} + S_{x,y-2} + S_{x+2,y} + S_{x-2,y}}{4} - S_{x,y} \right|,$$

где $S_{x,y}$ – интенсивность освещенности пикселя с координатами (x,y). Если полученная интенсивность освещенности D меньше интенсивности освещенности искомого пикселя, то пиксель считается «битым»; если больше – «горячим» [2].

Точное разграничение «битых» и «горячих» пикселей необходимо ввести и для изображений формата JPEG. Установить природу дефекта сложно, так как формат сохраняет изображение со сжатием, но для криминалистических нужд необходимо разграничить два этих понятия.

Есть и другая проблема, связанная с регламентацией неисправных пикселей. Форумы фотолюбителей косвенно доказывают, что наличие «битых» пикселей даже у новых фотокамер не является редкостью и у крупных производителей, таких как Canon, Nikon и Sony. Официальных данных, согласно которым матрицу фотокамеры можно признать браком, нет.

Для фотолюбителей «горячие» и «битые» пиксели являются помехой. Поэтому пользователи стремятся маскировать дефекты различными способами.

Первый способ – ремапинг («Mapping pixel» или «remap»). Данная процедура применима к цифровым фотоаппаратам. «Mapping pixel» – программа, определяющая местонахождение «битых» пикселей, получающая информацию с соседних, исправных пикселей. Она перепрограммирует пиксель, делая его «зависимым». «Зависимые» пиксели – жаргонный термин, означающий зависимость конкретного пикселя от значения его окружающих.

Таким образом, ремапинг не чинит матрицу, а только скрывает дефекты, за счет этого снижается качество изображений. Неосведомленный покупатель фотоаппарата, бывшего в употреблении, рискует приобрести устройство низшего

качества, чем заявлено. Аналогичные программы встроены в значительную часть современных смартфонов.

Второй способ – обработка изображений после съемки при помощи программ. Установление первоначального содержания обработанных изображений выходит за рамки фототехнической экспертизы и требует специальных знаний в области программирования.

Подводя итоги вышеизложенного, можно сформулировать ряд проблем:

1. Отсутствие регламентации матриц съемочных устройств, продажа производителями фотоаппаратов с дефектами матриц.
2. «Маскирование» дефектных пикселей матриц съемочных устройств, мешающее исследованию матриц экспертом-фототехником и вводящее в заблуждение потребителя.
3. Сложность идентификации съемочного устройства из-за сжатия в формате JPEG.
4. Отсутствие критериев отнесения пикселей к «горячим» и к «битым» для изображений формата JPEG.

В рамках экспертной инициативы предлагаю следующие решения:

1. Создать ГОСТ, регламентирующий количество дефектных пикселей матриц новых съемочных устройств. Схожее явление – дефектные пиксели электронных визуальных дисплеев (экранов устройств). Они регламентированы ГОСТ Р 52324-2005 (ИСО 13406-2:2001) «Эргономические требования к работе с визуальными дисплеями, основанными на плоских панелях». ГОСТ для матриц съемочных устройств можно создать аналогично данному.

2. «Ремапинг» «битых» пикселей или другое их маскирование, предшествующее осуществлению снимка, считаю необходимым запретить или сопровождать соответствующим программным обеспечением, позволяющим установить, какие именно пиксели являются дефектными и подверглись обработке. Данное обеспечение целесообразно предоставить пользователям, чтобы каждый покупатель мог удостовериться в соответствии качества покупаемого товара с заявленным.

3. Предлагаю создавать отечественные программы для обработки изображений в формате RAW. Исследованием интернет-ресурсов установлены тенденции к массовому использованию формата RAW при создании цифровых изображений, в том числе смартфонами. Это обусловлено расширенными возможностями обработки исходного изображения, высоким качеством полученного изображения за счет отсутствия сжатия. Например, смартфоны Samsung Galaxy S20 Ultra, Xiaomi Mi 10 Ultra, Huawei P40 Pro Plus, и OnePlus 8 Pro уже снабжены возможностью съемки в данном формате. Популяризация данного формата приведет к его использованию, в том числе, и среди злоумышленников.

4. Для изображений формата JPEG считаю необходимым разработать критерии отнесения пикселей к «горячим» или к «битым». В случае невозможности выведения точной формулы предлагаю на основе экспериментальных данных принять пороговое значение освещенности, позволяющее классифицировать данные понятия.

Создание регламентации актуально на данном этапе, так как в условиях сложившейся политической обстановки значительно больше внимания уделяется отечественным производителям. В данный момент в России рынок съемочных устройств и смартфонов крайне мал, а потому так необходимо сформулировать регламент именно сейчас, на этапе разработки техники.

Список литературы

1. Аминова Е. А. Разработка и анализ алгоритмов идентификации источников цифровых изображений : дис. ... канд. техн. наук. Ярославль, 2018.
2. Кулешов С. В., Аксенов А. Ю., Зайцева А. А., Подход к идентификации источника снимков с цифровых камер [Текст] / С. В. Кулешов, А. Ю. Аксенов, А. А. Зайцева // Инновационная наука = Innovation science : 2015. № 12. С. 82–86.
3. Raw формат изображения URL: [https://ru.wikipedia.org/wiki/Raw_\(Raw формат изображения\)](https://ru.wikipedia.org/wiki/Raw_(Raw_формат_изображения)).

Миляев Г. А.¹,

курсант факультета подготовки специалистов

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, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

По сведениям статистики, приведенной ГИАЦ МВД за 2022 г., количество преступлений в сфере информационно-телекоммуникационных технологий увеличилось. Происходит будто планомерный рост количества таких преступлений [1]. В свою очередь стоит отметить тот факт, что раскрываемость таких преступлений растет. Это происходит за счет того, что сотрудники стали чаще сталкиваться с такими преступлениями, получать опыт при их раскрытии, осваивать собственные методики раскрытия таких преступлений. Особое внимание хочется уделить тому, что сотрудники также стали верно проводить компьютерные экспертизы различных технических устройств, будь то компьютер, телефон, планшет или же запоминающие устройства [2].

Перед компьютерной экспертизой стоит ряд задач, которые она должна решать [3]. Основные из них – это установление факта произошедшего события, осуществление доступа к данным, находящимся на том или ином техническом устройстве или носителе информации, дальнейшее исследование извлеченных данных с устройства, особенности этих данных, при каких условиях они были созданы, и так далее. Возможности компьютерной экспертизы практически безграничны в отношении технических устройств, после ее проведения можно получить любую нужную и интересующую правоохранителей информацию [4].

Имея то количество информации, которая может дать компьютерная экспертиза, сотрудники могут достоверно знать и понимать особенности совершения преступления, а также, что данное преступление могло быть совершено с помощью определенного устройства, находящегося в определенном месте. Последующее нахождение преступника и его задержание существенно упрощаются после получения результатов компьютерной экспертизы [5].

Говоря о проведении компьютерной экспертизы, так же хочется отметить тот факт, что данное техническое мероприятие может осуществляться на территории

¹ © Миляев Г. А., 2023.

Российской Федерации как государственными, так и некоммерческими организациями. Это следует из ч. 2 постановления Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 – «Под негосударственными судебно-экспертными учреждениями следует понимать некоммерческие организации, созданные в соответствии с Гражданским кодексом Российской Федерации и Федеральным законом «О некоммерческих организациях»» [6]. Однако этот факт порождает определенное количество проблем.

Первая проблема заключается в том, что механика проведения компьютерной экспертизы не регламентируется законодательно. Это значит, что некоммерческие организации зачастую могут проводить и проводят экспертизы по собственным методикам, что существенно отличается от методик экспертно-криминалистических центров правоохранительных органов. Из-за этого они могут проводиться не совсем корректно, что может повлиять на качество его проведения и результаты этого технического мероприятия на его качество.

Следующим проблемным моментом является тот факт, что некоммерческие организации не имеют собственной, официальной, научно-технической базы, не жели правоохранительные органы. В свою очередь наличие такого фундамента позволяет экспертам действовать согласно общепринятым правилам и истинам, которые были проверены временем и опытом.

Подводя итоги, хотелось бы еще раз обозначить, что проведение компьютерной экспертизы должно быть законодательно урегулировано, потому что это порождает определенное количество проблем, которые влияют на результаты проведения компьютерной экспертизы. Нужно выработать строгие методики, которые являлись бы обязательными для исполнения всеми организациями как государственными, так и негосударственными.

Список литературы

1. Центр по проведению судебных экспертиз и исследований автономная некоммерческая организация «Судебный Эксперт». URL: <https://sudexpa.ru/expertises/informatcionno-kompiuternaia-ekspertiza/>.
2. Компьютерно-сетевая экспертиза // URL: <https://rtmtech.ru/services/setevaya-ekspertiza/>.
3. Уголовно процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 14.04.2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_.
4. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_.
5. ГОСТ Р 57429-2017 Судебная компьютерно-техническая. Термины и определения.
6. Постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_.

Кубасов И. А.¹,
профессор кафедры информационных технологий
Академии управления МВД России,
доктор технических наук, доцент

РАЗВИТИЕ И ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В настоящее время четвертой научно-технической революции, в условиях цифровой трансформации МВД России информационные технологии (ИТ) занимают особое место и выполняют важную роль в повышении эффективности информационно-аналитического обеспечения оперативно-служебной деятельности органов внутренних дел Российской Федерации (ОВД).

Внедрение ИТ коренным образом изменяет методы работы органов, предоставляя им эффективные инструменты для борьбы с преступностью, управления данными и обмена информацией для принятия более эффективных решений [1]. Так, информационные технологии произвели революцию в способах сбора, обработки и анализа судебных доказательств. Цифровые инструменты позволяют извлекать и анализировать данные с электронных устройств, таких как мобильные телефоны и компьютеры, что может помочь следователям в раскрытии дел. Например, ОВД могут использовать передовые аналитические инструменты для обработки больших объемов данных и получения информации в целях принятия решений и управления операциями [2; 3]. Также могут использовать передовые технологии наблюдения, такие как системы распознавания лиц и номерных знаков, для выявления подозреваемых и отслеживания их перемещений.

Ведомственные информационные системы позволяют собирать, хранить и анализировать огромные объемы данных о схемах совершения преступлений, подозреваемых и преступной деятельности [4; 5]. Полученные данные используются для выявления очагов преступности, прогнозирования преступной деятельности и разработки стратегий борьбы с преступностью. Эти системы также помогают выявлять тенденции и модели преступной деятельности, что позволяет более эффективно реагировать на преступления.

Информационные технологии обеспечивают расширение возможностей в области внутреннего и внешнего взаимодействия. С помощью ИТ органы внутренних дел могут более эффективно управлять своей деятельностью. От управления подразделением и технологическим оборудованием до отслеживания запасов и управления финансами.

Информационные технологии применяются и в образовательной деятельности для расширения возможностей в области обучения. Например, используя онлайн-платформы обучения и инструменты моделирования, ИТ предоставляют сотрудникам ОВД реалистичный и увлекательный учебный опыт.

¹ © Кубасов И. А., 2023.

Также могут предоставлять виртуальную реальность и дополненную реальность для имитации сценариев реального мира и улучшения результатов обучения.

С учетом основных задач дальнейшего развития ИСОД МВД России, указанных в «Основных направлениях дальнейшего развития единой системы информационно-аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы» [6] и Ведомственной программы цифровой трансформации МВД России на 2023–2025 годы [7], весьма актуальным является дальнейшее развитие и внедрение инновационных информационных технологий.

Так, МВД России реализуется пилотный проект федерального проекта «Искусственный интеллект» Национальной программы «Цифровая экономика Российской Федерации» по выявлению признаков серийности преступлений [8]. Это яркий пример цифровой трансформации, так как имеет место глубокая реорганизация всех процессов расследования и раскрытия серийных преступлений с использованием цифровых инструментов: данных и информационных технологий [9]. Признаками данной цифровой трансформации являются:

1) создание новой цифровой платформы – информационной системы выявления признаков серийности преступлений, интегрированной с другими ведомственными информационными сервисами и обеспечивающей многостороннее взаимодействие пользователей по обмену информацией, с тем чтобы оптимизировать процессы, повысить эффективность оперативно-служебной деятельности МВД России;

2) применение в разрабатываемой системе «сквозных» технологий: технологий искусственного интеллекта и больших данных;

3) принятие решений о принадлежности того или иного преступления к серии на основе анализа структурированных и неструктурированных данных: материалов уголовных и административных дел, заключений экспертов, судебных решений, а также заявлений граждан, оперативных сводок и аудиоматериалов и др.

Можно выделить несколько основных перспективных направлений развития информационных технологий в деятельности ОВД:

1. Цифровизация процессов делопроизводства и управления данными.

Органы внутренних дел имеют дело с большим объемом данных, включая судимости, материалы дел и многие другие документы. Оцифровка этих записей и внедрение цифровых систем управления данными могут повысить эффективность и точность поиска информации, увеличить скорость расследований.

2. Широкое использование искусственного интеллекта (ИИ) во всех направлениях оперативно-служебной деятельности ОВД.

Технологии ИИ могут помочь органам внутренних дел быстро выявлять закономерности и аномалии в данных, что может помочь в расследовании и раскрытии преступлений, выявлении противоправных действий.

3. Разработка и развитие мобильных приложений.

Мобильные приложения могут быть разработаны для облегчения общения между сотрудниками ОВД и другими правоохранительными органами. Эти приложения могут включать в себя такие функции, как GPS-слежение, системы опо-

вещения и платформы обмена сообщениями, которые могут повысить эффективность операций и повысить общую оперативность органов внутренних дел.

4. Внедрение и развитие биометрических технологий.

Биометрические технологии, такие как распознавание лиц, сканирование отпечатков пальцев и распознавание радужной оболочки глаза, анализ ДНК и т. д., могут использоваться для более быстрой и точной идентификации подозреваемых и преступников. Эти технологии также могут быть использованы для предотвращения фальсификации личных данных и обеспечения возможности проверки органами внутренних дел личности лиц, причастных к преступной деятельности. Тем не менее следует использовать их осторожно с надлежащим контролем, чтобы избежать потенциального неправомерного использования и нарушения конфиденциальности.

5. Использование больших данных и аналитики.

Органы внутренних дел могут использовать аналитику больших данных для анализа больших объемов данных и выявления тенденций и закономерностей, которые могут иметь значение для уголовных расследований. Это может привести к более эффективным стратегиям предупреждения преступности и реагирования на нее.

6. Внедрение технологии блокчейн.

Технология блокчейн может использоваться для повышения безопасности и прозрачности операций ОВД. Создавая децентрализованный и защищенный от несанкционированного доступа учет всех действий органа внутренних дел, технология блокчейна может помочь снизить риск коррупции, улучшить подотчетность и обеспечить справедливое и прозрачное проведение расследований.

7. ИТ в обеспечении кибербезопасности.

С ростом использования технологий в работе полиции возникает потребность в надежных мерах кибербезопасности. Органы внутренних дел должны установить безопасные системы и протоколы для защиты конфиденциальных данных и предотвращения кибератак [10].

В целях эффективного внедрения и развития инновационных информационных технологий в деятельности ОВД предлагается следующий алгоритм.

1. Проведение комплексной оценки потребностей в ИТ, которые необходимы органу внутренних дел для достижения своих целей и решения оперативно-служебных задач. Эта оценка должна включать обзор текущих процессов и систем, интервью с заинтересованными сторонами и анализ пробелов в текущем и желаемом состояниях.

2. Выработка ИТ-решений. На основе оценки потребностей следует разработать конкретные ИТ-решения, необходимые для удовлетворения потребностей органа внутренних дел. ИТ-решения должны соответствовать «Основным направлениям дальнейшего развития единой системы информационно-аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы» [4] и включать дорожную карту реализации, оценку необходимых ресурсов, показатели и критерии оценки эффективности внедрения ИТ-решений.

3. Выделение ресурсов, необходимых для реализации ИТ-решений, включая финансирование, человеческие ресурсы и инфраструктуру. Это может включать

обеспечение дополнительного финансирования или перераспределение существующих ресурсов.

4. Разработка и внедрение ИТ-решений. Это могут быть такие решения, как системы управления делами, инструменты анализа данных или мобильные приложения для сотрудников на местах. Решения должны быть масштабируемыми, безопасными и удобными для пользователей.

5. Обучение и программно-техническая поддержка. Следует провести обучение сотрудников по эффективному использованию новых ИТ-решения. Это должно включать обучение тому, как вводить данные в новые системы, как анализировать данные, как использовать и технически поддерживать новые технологии.

6. Мониторинг и оценка эффективности ИТ-решений для обеспечения их соответствия потребностям органов внутренних дел. Это может включать в себя сбор отзывов от заинтересованных сторон, анализ данных из новых систем и внесение корректировок в ИТ-решения по мере необходимости.

7. Непрерывное совершенствование и развитие. Следует постоянно улучшать ИТ-решения, чтобы они оставались эффективными. Это может включать обновление систем, добавление новых функций или внедрение новых технологий по мере их появления.

Таким образом, успешное внедрение и развитие ИТ в органах внутренних дел требует системного и стратегического подхода. Следуя предложенному алгоритму, органы внутренних дел могут определять свои потребности в ИТ, разрабатывать и внедрять решения, а также постоянно развивать ИТ-возможности для эффективного решения оперативно-служебных задач.

В заключении следует отметить, что внедрение и развитие информационных технологий коренным образом меняют характер деятельности органов внутренних дел. Внедряя цифровые решения, технологии искусственного интеллекта, мобильные приложения, биометрические технологии, аналитику больших данных и технологию блокчейн и т. д., органы внутренних дел могут существенно повысить эффективность своей деятельности и в конечном счете способствовать укреплению общественного порядка и созданию более безопасного общества.

Список литературы

1. Кубасов И. А. Информационные технологии в следственной и судебно-экспертной деятельности. В сборнике : Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации. Сборник научных статей по материалам международной научно-практической конференции / под ред. Ю. В. Гаврилина, Ю. В. Шпагиной. М., 2021. С. 171–177.

2. Кубасов И. А., Лекарь Л. А., Кондрущенко О. М. Перспективные направления применения методов анализа больших данных в информационно-аналитическом обеспечении оперативно-разыскной деятельности. В сборнике : Стратегическое развитие системы МВД России: состояние, тенденции, перспективы. Сборник статей Международной научно-практической конференции / под общ. ред. И. Г. Чистобородова, А. Л. Ситковского, В.О. Лапина. 2020. С. 436–442.

3. Кубасов И. А., Лекарь Л. А. Поиск и анализ больших данных в социальных сетях и Интернете для информационно-аналитического обеспечения оперативно-розыскной деятельности // Оперативно-розыскной портал: право и технологии. 2022. № 2 (2). С. 16–19.
4. Кубасов И. А., Стрельников Ф. И., Лунев Ю. С. Вопросы повышения эффективности использования автоматизированных дактилоскопических учетов при раскрытии и расследовании преступлений // Вестник Воронежского института МВД России. 2020. № 2. С. 231–236.
5. Кубасов И. А., Пучков Г. Ю. Основы математической модели надежности функционирования инфокоммуникационных систем внутренних дел Российской Федерации // Научно-технический портал МВД России. 2022. № 3 (43). С. 16–22.
6. Основные направления дальнейшего развития единой системы информационно-аналитического обеспечения деятельности МВД России на период с 2020 по 2024 годы, утвержденные исполняющим обязанности Министра внутренних дел Российской Федерации генералом полиции Российской Федерации В. А. Колокольцевым 21.01.2020.
7. Распоряжение МВД России от 25 января 2023 г. № 1/649 «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2023–2025 годы».
8. Национальная программа «Цифровая экономика» // АНО «Цифровая экономика». URL: <https://data-economy.ru>.
9. Кубасов И. А., Шапкин А. В., Рябев И. В. Внедрение технологий искусственного интеллекта для обработки больших данных в сфере внутренних дел. Вестник МВД России. 2021. № 5. С. 110 – 117.
10. Солодуха Р. А., Атласов И. В., Кубасов И. А. Стеганоанализ цифровых изображений : монография. Воронеж : Воронежский институт МВД России. 2022. 172 с.

Макеев В. А.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Булгаков В. Г.,

начальник кафедры естественнонаучных дисциплин

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук, доцент

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА РАСПОЗНАВАНИЯ ЧЕЛОВЕКА ПО РАДУЖНОЙ ОБОЛОЧКЕ

Исследования радужной оболочки начались в XX веке: сама идея использовать эту часть глаза для идентификации личности была предложена американским глазным хирургом Франком Буршем еще в 1936 г., хотя запатентовать и реализовать ее смогли только через полвека офтальмологами Леонардом Фломом и Араном Сафиром в 1987 г. [5]. Сегодня использование радужной оболочки в качестве биометрического идентификатора становится все более популярным благодаря современным методам исследования и распознавания.

Для исследования радужной оболочки используются различные методы, такие как фотографирование, сканирование, исследования в ультрафиолетовой области и др. Самым популярным и эффективным методом является фотографирование. Если рассмотреть радужную оболочку под микроскопом, то мы увидим, что она имеет рисунок, который состоит из различных линий, точек и кривых. Такой рисунок является уникальным для каждого человека, как отпечатки пальцев.

Для получения изображения радужной оболочки используется специализированная камера, которая имеет высокое разрешение и световую систему для получения четкого изображения. Камера располагается вблизи глаза человека и устанавливается на определенном расстоянии, чтобы получить максимальную четкость изображения. При этом обычно используются инфракрасные источники освещения, которые позволяют легко заметить и зафиксировать все детали радужной оболочки [2, с. 100–102].

Но одной из основных и трудно решаемых проблем в использовании радужной оболочки для идентификации личности является изменение радужки в течение времени. Эти изменения могут быть вызваны возрастом, современные методы исследования и распознавания радужной оболочки создают широкие перспективы для развития биометрических технологий в будущем. В последние годы исследователи разрабатывают различные математические методы как для уменьшения влияния этих изменений, так и для улучшения точности распознавания.

¹ © Макеев В. А., 2023.

Для распознавания радужной оболочки используются различные математические методы, такие как множественные методы, методы машинного обучения, статистические методы и другие. Многие из этих методов используются в сочетании с искусственным интеллектом и позволяют добиться высокой точности распознавания.

Основным математическим методом идентификации личности на основе радужной оболочки является ее математический анализ. Данный анализ применяется для извлечения информации из изображения радужки с целью создания уникального шаблона личности. Этот шаблон используется для сопоставления с другими шаблонами радужки с целью идентификации личности. Важнейшим этапом математического анализа радужной оболочки является сегментация изображения радужки, т. е. своеобразное разделение ее на составляющие. Сегментация позволяет выделить радужную оболочку из остальных элементов глаза, таких как зрачок и белок глаза. После сегментации применяются различные математические методы для извлечения информации, таких как особые точки радужки, текстуры и контуры [4, с. 68–72].

Один из наиболее популярных методов распознавания радужной оболочки, применяющих математические вычисления и формулы, – это метод фильтрации Габора. Этот метод основан на использовании фильтров, которые работают наподобие фильтров Фурье и позволяют выделить определенные частоты радужной оболочки. А с учетом физических явлений и последующей помощью математических формул можно исследовать и выделять индивидуальные признаки каждой радужной оболочки. Кроме того, при использовании данного метода возможно учитывать взаимодействие факторов света и тени на изображении радужной оболочки [1, с. 147–149].

Было выявлено, что одним из ключевых этапов алгоритмов распознавания является извлечение признаков. Так, одним из ключевых математических методов при распознавании радужной оболочки является использование множественных методов обнаружения этих признаков. Этот метод позволяет выделить основные черты радужной оболочки, такие как геометрические признаки (длина и ширина), текстурные признаки, статистические признаки и использовать их для дальнейшего анализа и распознавания [3]. После получения основной информации не исключается использование одновременно нескольких методов обнаружения признаков радужной оболочки для идентификации личности. Для классификации образов радужной оболочки могут использоваться различные методы оптимизации. Наиболее популярными являются методы оптимизации на основе генетических алгоритмов и методы на основе кластеризации. Оба метода позволяют выделить группы образов на основании их уникальных черт, что в свою очередь позволяет повысить точность распознавания.

Современные методы распознавания радужной оболочки все чаще используют методы машинного обучения, такие как искусственные нейронные сети, методы опорных векторов и другие. По мере обучения нейросетей эти методы более гарантированно позволяют классифицировать изображения радужной оболочки и добиться высокой точности распознавания. В современном мире существует огромное множество и других различных математических методов и алгоритмов

для обработки изображений радужной оболочки с целью идентификации личности. Можно упомянуть один из наиболее широко используемых методов – метод локальных бинарных шаблонов (Local Binary Patterns, LBP) в сочетании с методом классификации, таким как метод опорных векторов (Support Vector Machines, SVM). Другими используемыми методами являются метод главных компонент (Principal Component Analysis, PCA), метод масштабирования вейвлет-преобразований (Wavelet-Scale-Space, WSS) и метод детектирования границ (Edge Detection).

Заключение: Распознавание человека по радужной оболочке в современности является крайне эффективным способом биометрической идентификации. Современные методы исследования и распознавания радужной оболочки позволяют добиться высокой точности и скорости работы системы. Математические методы, такие как анализ, методы машинного обучения, оптимизации и обнаружения признаков и многие другие, а также их комбинации значительно повышают эффективность распознавания. Данное направление постоянно будет совершенствоваться, и при должном использовании законов математики оно будет стремиться только к созданию инновационных методов и средств идентификации человека не только по радужной оболочке, но и другим признакам.

Список литературы

1. Применение спектров текстурной картины для изучения и классификации неоднородных структур : / [Е. А. Абраменко и др.] // Известия Алтайского государственного университета. 2010. № 1–2. С. 147–149.
2. Третьяков И. Н., Минакова Н. Н. Алгоритм разграничения доступа по радужной оболочке глаза для решения задач контроля доступа к информационным ресурсам // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1-1. С. 100–102.
3. Петров И., Минакова Н. Сравнительный анализ методов некооперативного распознавания радужной оболочки глаза // Известия Алтайского государственного университета, 1, № 1 (89). URL: <http://izvestiya.asu.ru/article/view/%282016%291-29016%291-01.5>.
4. Павельева Е. А., Крылов А. С. Алгоритм сравнения изображений радужной оболочки глаза на основе ключевых точек // Информатика и ее применение. 2011. № 1. С. 68–72.
5. Википедия: аутентификация по радужной оболочке глаза. URL: https://ru.wikipedia.org/wiki/Аутентификация_по_радужной_оболочке_глаза.

Маликов С. А.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

НЕКОТОРЫЕ ПРОБЛЕМНЫЕ ВОПРОСЫ В СФЕРЕ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Искусственный интеллект – это область компьютерных наук, которая занимается разработкой алгоритмов и систем, способных имитировать интеллектуальные способности человека, такие как распознавание образов, обучение, планирование и принятие решений. На сегодняшний день он используется в различных областях, включая медицину, финансы, производство, транспорт и многие другие.

Одной из основных областей применения искусственного интеллекта является машинное обучение (Machine Learning), которое позволяет компьютерам извлекать знания из данных, на основе которых они могут принимать решения и делать предсказания [1]. Машинное обучение используется в различных задачах, таких как классификация, кластеризация, предсказание и рекомендации.

Еще одной областью, в которой применяется машинное обучение, является обработка естественного языка (Natural Language Processing, NLP), которая позволяет компьютерам понимать и генерировать естественный язык. Эта технология используется для создания различных приложений, таких как переводчики, чат-боты и системы распознавания речи.

Искусственный интеллект также широко применяется в компьютерном зрении (Computer Vision), которое позволяет компьютерам обрабатывать и анализировать изображения [2]. Эта технология используется в различных областях, таких как медицина, автоматизированное вождение, навигация и видеонаблюдение.

Непрозрачность моделей может быть вызвана различными факторами, такими, как:

1. Сложность моделей: некоторые модели могут быть очень сложными и иметь множество параметров, которые трудно интерпретировать.
2. Недостаток данных: иногда модели могут быть обучены на недостаточном количестве данных, что может привести к неожиданным результатам или недостаточной уверенности в принимаемых решениях.
3. Наличие ошибок: модели могут содержать ошибки, которые могут привести к неправильным выводам.

¹ © Маликов С. А., 2023.

4. Отсутствие стандартов: на данный момент не существует универсальных стандартов для создания прозрачных моделей, что может привести к различиям в том, как модели интерпретируются.

Решением проблемы непрозрачности моделей может быть использование более прозрачных и интерпретируемых моделей, таких как деревья, решений, линейные модели или нейросети с интерпретируемой архитектурой. Также могут быть использованы методы объяснения принимаемых решений, например, методы локальной интерпретации, которые позволяют объяснить, почему модель приняла определенное решение для конкретного наблюдения. В целом для успешного развития необходимо учитывать эту проблему и работать над ее решением, чтобы обеспечить доверие и принятие в обществе.

Например, модели машинного интеллекта могут быть предвзятые, если они обучаются на данных, которые содержат искажения или дискриминацию. Поэтому важно разрабатывать методы для обнаружения и устранения предвзятости [3].

Искусственный интеллект является одним из наиболее активно развивающихся направлений в науке и технологиях в настоящее время. Различные проблемы, такие как непрозрачность моделей, проблемы безопасности и конфиденциальности, ответственность и этика, а также сложность внедрения, являются вызовами для развития и применения искусственного интеллекта в различных областях [4].

Кроме того, важно продолжать работу над развитием технологий для создания и внедрения моделей, а также обучения персонала, который будет работать с этими моделями. В целом проблемы, связанные с развитием и применением искусственного интеллекта, требуют комплексного подхода и совместных усилий со стороны научного сообщества, правительственных и бизнес-структур. Решение этих проблем позволит обеспечить дальнейшее развитие искусственного интеллекта и его успешное использование в различных сферах.

Список литературы

1. Технологии машинного обучения: примеры современных тенденций // Хабр URL: https://habr.com/ru/companies/kauri_iot/articles/518974/.
2. Компьютерное зрение: от распознавания текста до изучения космоса // Yandex Cloud. URL: <https://cloud.yandex.ru/blog/posts/2022/05/computer-vision>.
3. Баррат Д. Последнее изобретение человечества: искусственный интеллект и конец эры Homo sapiens : [пер. с англ.] / Д. Баррат. 2-е изд. М. : Альпина нон-фикшн, 2018. С. 212.
4. Демкин В. И. История и перспективы развития нейронных сетей / В. И. Демкин, Д. К. Луков // Вестник современных исследований. 2018. № 6.1 (21). С. 366–368.

Васильев Р. А.¹,

курсант факультета подготовки

специалистов в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Булгаков В. Г.,

начальник кафедры естественнонаучных дисциплин

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук, доцент

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ РАСПОЗНАВАНИЯ МИМИКИ ЧЕЛОВЕКА

Распознавание мимики человека – это процесс идентификации и анализа различных выражений на лице, которые могут отражать эмоциональное состояние, интенсивность боли, уровень стресса и другие аспекты психического состояния человека. Разработка эффективных методов для распознавания мимики является актуальной задачей, которая находит применение во многих областях, таких как медицина, психология, реклама и др.

Один из подходов к решению этой задачи – использование математических методов и алгоритмов машинного обучения. Разберем различные математические методы, используемые в распознавании мимики человека.

Математические методы

1. Метод гибкого сравнения на графах (Elastic graph matching).

Метод гибкого сравнения на графах, известный как Elastic graph matching, является одним из математических методов, используемых для распознавания мимических выражений. Он основан на использовании графовой модели представления мимических выражений и методах поиска сходства между ними.

Для начала необходимо представить мимические выражения в виде графовых моделей. Каждый граф представляет одно конкретное выражение. Вершинами графа являются точки на лице, например, уголки глаз, носа, рта и другие зоны. Ребром являются коннекторы между этими точками, которые связывают их вместе, образуя форму мимического выражения [1, с. 96–98].

Затем Elastic graph matching метод пытается сопоставить графы, находя наиболее оптимальное сходство между вершинами и ребрами графов. Это делается путем вычисления расстояния между графами. При этом учитываются изменения положения вершин и ребер на исходных графах, находящиеся в пределах разумных значений.

Один из основных преимуществ метода гибкого сравнения на графах заключается в том, что он способен автоматически адаптировать граф к множеству раз-

¹ © Васильев Р. А., 2023.

личных размеров изображения лица и изменениям формы лица. Это делает его полезным для распознавания мимических выражений в разных условиях.

Однако этот метод требует больших вычислительных мощностей и может быть неэффективным при обработке большой базы данных изображений. Однако, благодаря своей высокой точности и надежности, метод гибкого сравнения на графах все еще остается популярным выбором для распознавания мимических выражений в некоторых областях, особенно в научных исследованиях [2].

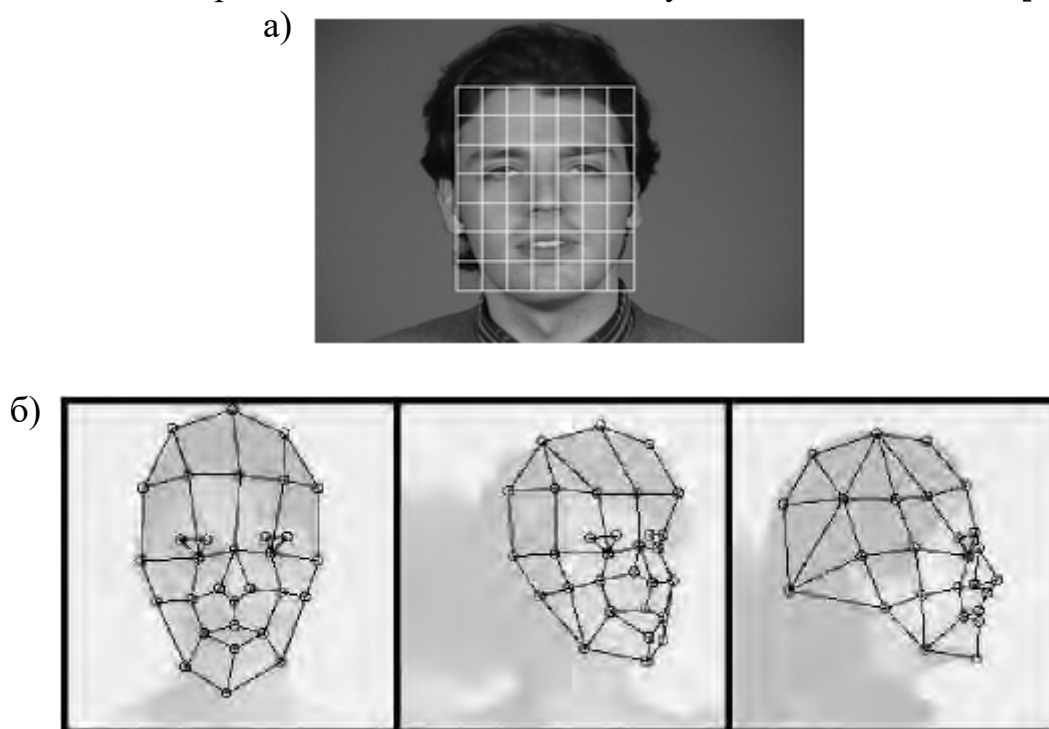


Рис. 1. Пример структуры графа для распознавания лиц:

а) регулярная решетка; б) граф на основе антропометрических точек лица

2. Метод главных компонент (РСА).

Метод главных компонент (РСА) является одним из наиболее широко используемых подходов в области анализа данных и машинного обучения. Он может быть использован для распознавания мимики человека на основе анализа изображений лица. РСА работает путем нахождения линейных комбинаций исходных переменных, которые объясняют наибольшую дисперсию в данных. Для распознавания мимики человека исходными переменными могут быть пиксели изображения, представляющие лицо. Для применения РСА для распознавания мимики человека сначала необходимо подготовить данные, включающие изображения лиц людей с различными выражениями мимики. Затем необходимо выполнить предварительную обработку данных, такую как выравнивание лиц и удаление фона. Далее алгоритм РСА применяется для извлечения главных компонент изображения. Главные компоненты могут быть использованы для разделения изображения на зоны, отвечающие за различные выражения лица (например, улыбку, грусть, злость и т. д.) [2].

Наконец, для распознавания мимики человека извлеченные главные компоненты могут быть использованы для обучения классификатора, который будет определять, какое выражение мимики соответствует конкретному набору извлеченных главных компонент.

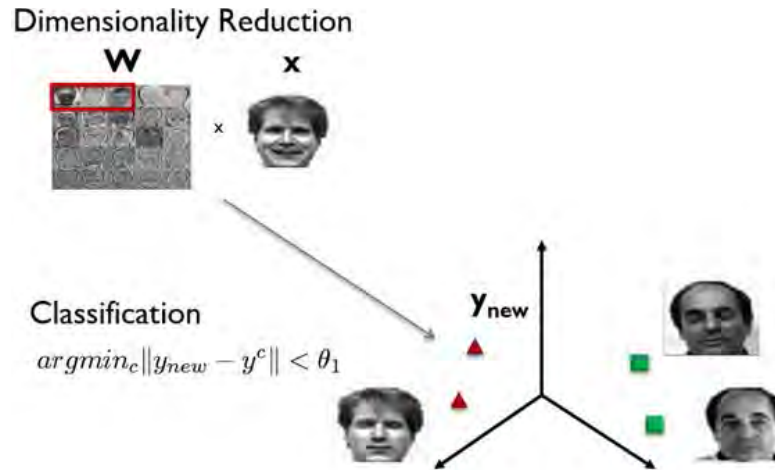


Рис. 2. Пример отображения лица в трехмерное метрическое пространство, полученном по трем собственным лицам, и дальнейшее распознавание

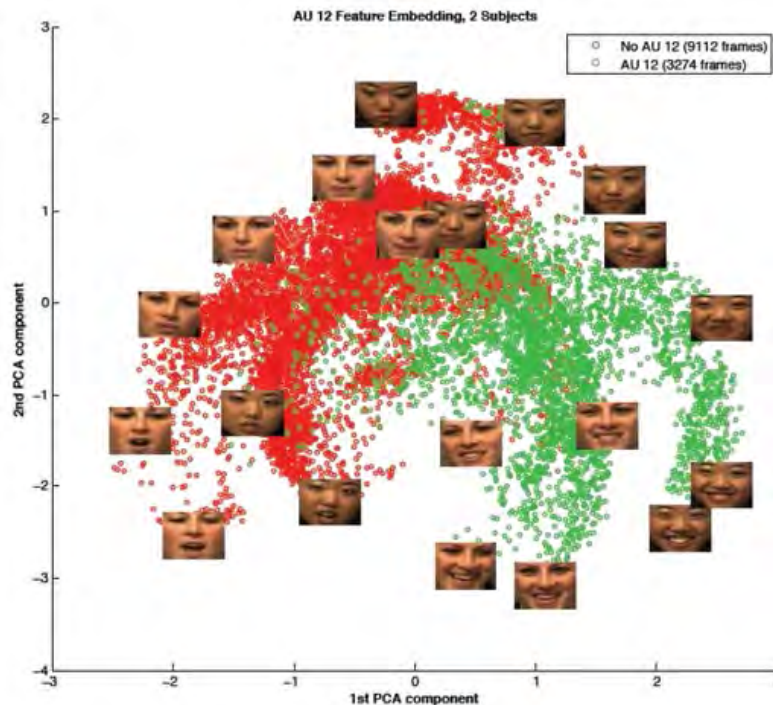


Рис. 3. Пример работы метода PCA

3. Вектор признаков.

Вектор признаков при распознавании мимики лица играет важную роль, так как он содержит информацию, необходимую для классификации выражения лица. Каждый признак в векторе признаков соответствует определенной характеристике лица, которая характеризует выражение, такое как угол наклона глаз, яркость кожи и т. д.

Определение оптимального набора признаков является ключевой задачей в разработке систем распознавания мимики. Хорошо выбранный набор признаков позволяет улучшить точность распознавания, а также снизить количество данных, которые необходимо обрабатывать в реальном времени.

Вектор признаков важен также при применении методов машинного обучения для распознавания мимики. Машинное обучение предполагает, что система

может обучаться на основе примеров, и для этого нужно иметь возможность извлечения определенных признаков из данных. Вектор признаков позволяет сформировать образец, на основе которого нейронная сеть или другой алгоритм машинного обучения может обучаться.

4. Метод Виолы-Джонса.

Метод Виолы-Джонса – это алгоритм компьютерного зрения, который используется для распознавания лиц и мимики человека. Он основан на использовании каскада классификаторов, каждый из которых определяет наличие определенной характеристики (например, глаза, нос, рот) на изображении. Это позволяет быстро и точно определять положение и форму лица, а также выражение мимики (например, улыбка или гримаса). В основе метода Виолы-Джонса по поиску лица лежат идеи: интегральное представление изображения по признакам Хаара, метод построения классификатора на основе алгоритма адаптивного бустинга и метод комбинирования классификаторов в каскадную структуру [3, с. 297–304].

Алгоритм проходит через несколько этапов:

1. Детектирование ориентированных границ (edge detection) на изображении.
2. Разбиение изображения на маленькие блоки, которые называются «окнами».
3. Применение каскада классификаторов к каждому окну.
4. Если окно содержит лицо или выражение мимики, то оно сохраняется для дальнейшей обработки.
5. Дополнительная обработка для уточнения определения формы лица и выражения мимики.

Этот метод широко используется в различных областях, где требуется быстрое и точное распознавание лиц и мимики, включая анализ эмоций, системы безопасности, а также в индустрии развлечений.

Распознавание мимики человека – это одна из задач компьютерного зрения, которая имеет много применений в таких областях, как игровая индустрия, медицина, системы безопасности и другие. Существует множество программных средств, которые позволяют распознавать мимику, но в этой статье мы рассмотрим несколько известных и часто используемых из них.

1. Affectiva – это программа для распознавания и анализа эмоций, которая использует компьютерное зрение и другие технологии машинного обучения. Affectiva позволяет распознавать различные выражения мимики, такие как улыбка, гримаса и другие. Она также может определять эмоциональное состояние человека на основе мимики и других факторов, например речи.

2. Emotient – это программа для распознавания лица и мимики, которая использует технологии распознавания лица и машинного обучения, чтобы определить наличие и тип выражений мимики, таких как улыбка, гримаса, злость и другие. Emotient может использоваться в таких областях, как игровая индустрия, медицина, системы безопасности и другие.

3. Microsoft Cognitive Services – это когнитивный сервис от Microsoft, который позволяет распознавать лица и выражения мимики. Microsoft Cognitive Services использует алгоритм распознавания лиц и машинного обучения, чтобы

определять наличие и тип выражений мимики, таких как улыбка, гримаса, кислая мина и другие.

4. OpenCV – это открытая библиотека компьютерного зрения, которая поддерживает распознавание лица и мимики. Она предоставляет множество алгоритмов и инструментов для анализа изображений и распознавания лица и мимики, включая алгоритм Виолы-Джонса. OpenCV также предоставляет поддержку для разных языков программирования, таких как C++, Python, Java и других.

5. Kairos – это программа распознавания лица и выражений мимики, которая использует методы глубокого обучения для достижения высокой точности и быстродействия. Kairos может использоваться в таких областях, как системы видеонаблюдения, игры и другие.

6. Amazon Rekognition – это сервис для анализа изображений, который может распознавать выражения мимики, эмоции и другие характеристики лица на фото и видео. Amazon Rekognition может использоваться в таких областях, как системы безопасности, анализ клиентов и другие.

Распознавание мимики может иметь широкий спектр применений в таких областях, как медицина, психология, игровая индустрия, маркетинг и другие. В медицине, например, распознавание мимики может помочь в диагностике и лечении психических расстройств. В игровой индустрии распознавание мимики может использоваться для улучшения игрового интерфейса и повышения иммерсии игроков. В маркетинге распознавание мимики может быть полезным для анализа реакций потребителей на рекламные материалы и продукты.

Таким образом, развитие методов и средств для распознавания мимики человека имеет большую практическую ценность и может иметь значительный вклад в различные области науки и технологии.

Список литературы

1. Частикова В. А., Титова А. А. Обзор методов идентификации людей на основе изображений лиц (2022).
2. Анализ существующих подходов к распознаванию лиц. URL: <https://habr.com/ru/companies/synesis/articles/238129/>.
3. Lienhart R., Kuranov E., Pisarevsky V. : Empirical analysis of detection cascades of boosted classifiers for rapid object detection. In : PRS 2003, P. 297–304 (2003).

Медведев В. А.¹,

*преподаватель кафедры социально-экономических
и гуманитарных дисциплин Ленинградского областного филиала
Санкт-Петербургского университета МВД России*

СОВРЕМЕННОЕ СОСТОЯНИЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В современном мире информационные технологии играют огромную роль в жизни общества. Однако они также стали доступными и для разного рода преступников, которые используют их для своих злонамеренных целей. Время не стоит на месте, и вместе с ним развиваются и преступления. Современные технологии позволяют преступникам использовать информационные системы и интернет для совершения различных киберпреступлений, таких как кража личных данных, мошенничество, распространение вредоносных программ и многое другое. В результате возникают преступления, которые совершаются при помощи информационных технологий и которые нередко остаются безнаказанными. В связи с этим расследование преступлений, связанных с использованием информационных технологий, представляет собой непростую задачу для правоохранительных органов. Необходимо не только иметь достаточно знаний в области информационных технологий, но и располагать соответствующими инструментами для проведения расследования.

Свои корни данный вид преступлений берет в период появления ЭВМ, первое преступление с использованием компьютера было зафиксировано в 1960-м г. Вообще историю развития информационной преступности можно условно разделить на два этапа: первый этап – с момента появления первой ЭВМ и до 1990-х гг. и второй этап – с 1990 г. по сей день. Именно в 90-х гг. киберпреступность начинает развиваться ускоренными темпами. Естественно, это связано с активным распространением интернета по всему миру.

С появлением нового вида преступности начали появляться новые методы борьбы с ней, а также потребовалось создать нормативно-правовую базу, которая давала бы определение новообразовавшемуся понятию. Международная организация ООН дает такое определение киберпреступности – это любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети. Также регулирует данную область и международная конвенция Совета Европы, в которой указано четыре вида информационных преступлений, определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

1. Незаконный доступ (ст. 2).

¹ © Медведев В. А., 2023.

2. Незаконный перехват (ст. 3).
3. Вмешательство в данные (ст. 4).
4. Вмешательство в систему (ст. 5).

Проанализировав современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий, а также применение новых инструментов, таких как нейронные сети, для более эффективной борьбы с преступлениями данной категории, можно отметить, что в современном мире наблюдается тенденция роста так называемой киберпреступности по определенным направлениям. По итогам 2022 г. на 21 % больше зарегистрировано преступлений по факту сбыта наркотиков через интернет. Увеличилось также количество заведомо ложных сообщений об акте терроризма, 92 % из них совершены дистанционно. Также сообщается, что раскрываемость преступлений, совершенных с использованием цифровых технологий, в 2022 г. повысилась на 4,4 %. В целом же количество преступлений, зарегистрированных за 2022 г., снизилось по сравнению с прошлым годом на 1,9 %. За этот период сотрудниками правоохранительных органов было раскрыто более 1 млн преступлений.

Как следует из данных МВД, в 2022 г. количество преступлений, совершенных с помощью информационно-телекоммуникационных технологий, в том числе пластиковых карт, мобильной связи, компьютерной техники, пошло на убыль впервые с 2017-го. Позитивную динамику эксперты связывают с повышением осведомленности людей о методах злоумышленников, а также спадом активности преступников весной 2022 г. на фоне спецоперации России на Украине. Однако специалисты предупреждают, что такая тенденция вряд ли сохранится.

В России идет активная борьба с киберпреступностью, уже в 1998 г. в структуре МВД было сформировано автономное подразделение, которое специализируется на раскрытии и расследовании преступлений в сфере высоких технологий. Следующим шагом по борьбе с киберпреступностью было создание специального управления, которое было предназначено для борьбы с информационными преступлениями. Направлениями деятельности данного управления являлись: борьба с разработкой, внедрением и использованием вредоносных программ, противодействие преступлениям, совершаемым в сфере IT-технологий, пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет. Однако, несмотря на принимаемые меры в данной области, имеется комплекс нерешенных проблем:

Первой выделяемой проблемой является – неудовлетворительный уровень технического оснащения подразделений, специализирующихся на расследовании киберпреступлений. Это является, действительно, очень серьезной проблемой, поскольку на сегодняшний день отделы по борьбе с киберпреступностью не оснащены всем необходимым оборудованием. Это создает препятствия в поиске доказательств и в принципе усложняет расследование по делу в данной области. Необходимо осознавать, что обе противоборствующие стороны обладают одним инструментом борьбы, т. е. фундаментальным условием результативности работы правоохранительных органов здесь служат инновации, их активное внедрение и использование.

Также достаточно проблематично идентифицировать преступника или преступников в тех случаях, когда преступление совершено с использованием незащищенной сети передачи данных. Злоумышленники способны подменить учетные данные сети, что делает их нахождение практически невозможным.

Недостаточная техническая и информационная грамотность следователей, привлекаемых к расследованию и раскрытию киберпреступлений, что в свою очередь мешает успешному расследованию подобных дел. Данную проблему можно объяснить тем, что сегодня не обучают юристов высокотехнологичным дисциплинам, этот пробел в знаниях не позволяет эффективно вести работу в сфере информационной преступности.

И последней выделяемой проблемой является низкий уровень обращения граждан с заявлением о совершенном киберпреступлении. Это обусловлено тем, что граждане попросту не верят, что их дело можно решить. Кроме того, в случае обращения в правоохранительные органы потерпевшие зачастую не могут предоставить минимально необходимые данные, что говорит нам о низком уровне просвещенности населения в информационной сфере.

В заключение можно отметить, что в современном мире ситуация с преступлениями, совершаемыми с использованием информационных технологий, является очень актуальной и требует повышенного внимания со стороны правоохранительных органов. Технологический прогресс и возможности, которые он предоставляет, позволяют злоумышленникам все более изощренно совершать преступления и скрывать следы своей деятельности. Однако вместе с тем новые технологии и инструменты для защиты от преступных действий также развиваются и совершенствуются. Необходимо совершенствовать методы и технологии расследования преступлений с использованием информационных технологий, что позволит повысить эффективность борьбы с киберпреступностью и защитить интересы общества.

Список литературы

1. Коломоец А. В. Проблемы в раскрытии киберпреступлений / А. В. Коломоец // Правовое образование : Сборник научных статей / под ред. И. В. Бухаровой, А. А. Никитиной. Т. 16. Ростов н/Д : Ростовский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования Всероссийский государственный университет юстиции в г. Ростове-на-Дону, 2021. С. 373–378.
2. Тимакина Ю. А. Основные направления внедрения информационных технологий в деятельность МВД России, 2020.
3. Тимакина Ю. А. Использование достижений в области искусственного интеллекта в информационном обеспечении органов внутренних дел, 2019.

Мирзахмедов Д. М.¹,

*слушатель факультета подготовки иностранных специалистов
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Заринова Э. Р.,

*доцент кафедры естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат физико-математических наук*

О ПРАКТИЧЕСКОМ ПРИМЕНЕНИИ ПОСЛЕДОВАТЕЛЬНОСТИ ФИБОНАЧЧИ

В работе предлагается практическое применение последовательности Фибоначчи [1], будет использована теорема Цеккендорфа и фибоначчиева система счисления.

Теорема Цеккендорфа [2; 3] позволяет представить любое число n в виде суммы некоторых чисел из последовательности Фибоначчи. Введем обозначение $j \gg k$, что будет эквивалентно записи $j \geq k + 2$, тогда

$$n = F_{k_1} + F_{k_2} + \dots + F_{k_r}, k_1 \gg k_2 \gg \dots k_r \gg 0, \quad (1)$$

где $F_{k_1}, F_{k_2}, \dots, F_{k_r}$ – числа Фибоначчи.

Например, число 1 000 000 представимо в виде (2):

$$1\,000\,000 = 832\,040 + 121\,393 + 46\,368 + 144 + 55 = F_{30} + F_{26} + F_{24} + F_{12} + F_{10}. \quad (2)$$

Для представления числа используется «жадный» алгоритм, где сначала выбирается наиболее близкое число последовательности Фибоначчи, близкое к заданному, но меньше его, затем для их разницы выбирается следующее число, наиболее близкое к разнице чисел, но меньше этой разницы, и т. д. Так, теорема о представлении числа через числа Фибоначчи приводит к фибоначчиевой системе счисления.

Любое натуральное число n представимо в виде последовательности нулей и единиц

$$n = (b_m b_{m-1} \dots b_2)_F, \text{ где } n = \sum_{k=2}^m b_k F_k. \quad (3)$$

Можно наблюдать в этой системе счисления отсутствие двух единиц подряд. Представим первые 20 чисел через такую фибоначчиеву систему счисления.

$1 = (000001)_F$	$6 = (001001)_F$	$11 = (010100)_F$	$16 = (100100)_F$
$2 = (000010)_F$	$7 = (001010)_F$	$12 = (010101)_F$	$17 = (100101)_F$
$3 = (000100)_F$	$8 = (010000)_F$	$13 = (100000)_F$	$18 = (101000)_F$
$4 = (000101)_F$	$9 = (010001)_F$	$14 = (100001)_F$	$19 = (101001)_F$
$5 = (001000)_F$	$10 = (010010)_F$	$15 = (100010)_F$	$20 = (101010)_F$

¹ © Мирзахмедов Д. М., 2023.

Представленный ранее миллион через числа Фибоначчи может быть представлен и с помощью двоичного представления $2^{19} + 2^{18} + 2^{17} + 2^{16} + 2^{14} + 2^9 + 2^6$. $(1000000)_{10} = (10001010000000000010100000000)_F = (11110100001001000000)_2$. (4)

Представление через фибоначчьеву систему счисления требует больше битов, поскольку не допускаются две единицы подряд, но в остальном эти представления идентичны.

Определим понятие «кодového слова» Фибоначчи. Кодовым словом Фибоначчи числа будем называть представление Цеккендорфа с обратным порядком его цифр с добавлением еще одной единицы в конец [4], т. е. каждое закодированное слово будет заканчиваться двумя единицами, и таким образом удачно определяется конец кодового слова. В представлении через числа Фибоначчи используются F_n с натуральными индексами n .

Кодовое слово для цифры 1 определяется следующим образом. Единица является первым числом Фибоначчи с натуральным индексом n , как определили ранее $1 = (000001)_F = (1)_F$, в конец кодового слова добавляется 1. Кодируя единицу на входе, на выходе – 11.

Исследуя следующее число 2. $2 = (000010)_F$. Для кода нужно «перевернуть число», получив 01 и добавив к нему в конец единицу. В итоге получается число 011.

Для двузначного числа 11, являющегося суммой чисел Фибоначчи 8 и 3, имеем: $11 = 8 + 3 = F_6 + F_4 = (10000)_F + (100)_F = (10100)_F$.

Переворачивая число, получим 00101 и в конец добавляется еще одна единица, в итоге для числа 11 получается кодовое слово 001011.

Отметим, что данный код является самосинхронизирующимся, и если поток данных восстанавливается, то наличие концевого бита, равного единице, позволяет кусочно восстановить код и дешифровать впоследствии его. Такой подход можно считать более привлекательным, хотя данный код более объемный, чем двоичный.

Список литературы

1. Фибоначчи // Wikipedia. URL: <https://ru.wikipedia.org/wiki/Фибоначчи> (дата обращения: 20.04.2021).
2. Кнут Д., Паташник О., Грэм Р. Конкретная математика. Основание информатики. М. : Мир. 703 с., ил. 1998.
3. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. 2012.
4. Кодирование Фибоначчи // Wikipedia. URL: https://ru.abcdef.wiki/wiki/Fibonacci_coding (дата обращения: 12.04.2023).

Миронов В. Л.¹

*преподаватель кафедры оперативно-разыскной деятельности ОВД
и применения информационных технологий
Московского областного филиала
Московского университета МВД России имени В.Я. Кикотя*

ДИПФЕЙК КАК ВЕРОЯТНЫЙ ИНСТРУМЕНТ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

Термин «дипфейк» (англ. deep fake) образован от слов Deep learning (глубинное обучение) и Fake (подделка). Дипфейки создаются с помощью технологий искусственного интеллекта, применяемых для синтеза звуков, изображений и видео. В двух последних случаях один фрагмент интегрируется в другой, в результате чего получается сгенерированное фото или видео.

Для создания дипфейков чаще всего используются генеративно-сопоставительные сети, которые состоят из двух нейронных сетей. Одна сеть (генеративная) создает фальшивый объект (изображения, аудио или видео), а другая (дискриминативная) определяет их подлинность. Обе сети обучаются на полученных результатах и с каждой новой попыткой все лучше справляются со своими задачами.

Дипфейк-технологии становятся все доступнее – в настоящее время существует большое количество как интернет-ресурсов, так и приложений, позволяющих создавать дипфейки. При этом дипфейк-технологии за последние годы существенно эволюционировали в части повышения реалистичности сгенерированных объектов, поэтому риски и угрозы их бесконтрольного применения выглядят весьма серьезными.

В чем же заключается потенциальная опасность дипфейков? Почему их опасаются политики и публичные личности, юристы и бизнесмены, журналисты и многие другие? Выделим несколько основных угроз, сопроводив их примерами последних лет.

1. Фальсификация выступлений политических, общественных и религиозных лидеров.

В 2017 г. было создано поддельное видео с Б. Обамой, в котором он рассказал о том, что такое дипфейк, а также оскорбил действующего президента США. В 2018 г. в Интернете появилось фейковое видео, созданное бельгийской политической партией Socialistische Partij Anders, в котором Д. Трамп обратился к жителям Бельгии с призывом не признавать Парижское соглашение по климату. Несмотря на то что качество дипфейка было весьма посредственным, видео вызвало множество комментариев, в которых выражалось возмущение тем, что американский президент решил повлиять на климатическую политику Бельгии. Гораздо лучшим качеством отличается опубликованное два года назад организацией Represent.Us фейковое видео с Ким Чен Ыном, в котором лидер КНДР иронично рассуждает о судьбе мировой демократии.

Хотя в приведенных примерах отсутствует формальное нарушение законов, можно легко представить себе и более серьезные намерения авторов дипфейков.

¹ © Миронов В. Л., 2023.

Наиболее серьезные опасения вызывает потенциал использования технологий создания дипфейков для разжигания конфликтов, массовых гражданских беспорядков и подрыва национальной безопасности [1]. Например, во многих странах можно провоцировать межэтнические или межконфессиональные столкновения, выкладывая в социальные сети фейковые видео, где представитель определенной группы высказывается или осуществляет иные действия, которые могут быть восприняты другими как оскорбление.

2. Появление новых способов мошенничества. Наибольшее опасение вызывает безопасность дистанционного банковского обслуживания, основанного на биометрической идентификации и аутентификации клиентов. Сдерживающим фактором пока является отсутствие массового использования банками биометрической системы. В то же время с помощью технологии дипфейков возможно организовывать звонки якобы от руководителей, бизнес-партнеров, близких людей с целью перевода денежных средств. В этом случае дипфейки представляют реальную опасность, особенно если они совмещены с подменой телефонного номера. Так, бухгалтер одного из предприятий получила сообщение от своего директора, чтобы она срочно с ним связалась по видеосвязи. При этом в момент звонка она общалась не с реальным руководителем, а использовалась технология дипфейков. В итоге по поручению «руководителя» бухгалтер осуществила перевод 100 тыс. долларов [2].

3. Компрометация личности, клевета, шантаж. В 2017 г. впервые в Интернете в социальной сети Reddit были опубликованы порнографические видеоролики, в которых лица порнозвезд были заменены лицами голливудских знаменитостей. Кстати, именно тогда и появился термин «Deep fake». Создание порнографических фото и видео является самым распространенным использованием технологии дипфейков – в 2019 г. доля фальшивого порно оценивалась в 96 %. В 2019 г. было выпущено приложение DeepNude для Windows, которое открыло еще одно направление в порнографических дипфейках – удаление одежды с изображений женщин.

Доступность указанных технологий привела к их широкому распространению. В правовом поле можно выделить два негативных сценария. Первый – фальшивый контент (фото или видео) создается и публикуется в Интернете без прямого умысла причинить вред объекту съемки. Такая ситуация характерна, главным образом, в отношении медийных личностей (киноактрис, певиц, спортсменов и т. п.). Второй сценарий – фейк создается и распространяется как «порно из мести». В этом случае налицо прямой умысел на причинение морального или материального (например, путем шантажа) вреда жертве фальсификации, в роли которой может оказаться кто угодно: бывшая подруга, требовательная начальница, скандальная соседка и т. п.

Очевидно, что областью порно сюжетная линия дипфейков не ограничивается. В качестве компрометирующего материала могут использоваться самые разные условия и обстановки: веселые застолья, состояние опьянения, массовые мероприятия и прочее.

Также не стоит считать, что за дипфейком всегда скрывается что-то личное. В бизнес-сфере дипфейки могут использоваться как форма черного пиара, например, жертву могут подставить в компрометирующее видео.

К вышеперечисленным видам вероятного противоправного использования дипфейков можно добавить обход аутентификации по Face ID, в результате которого злоумышленник получает доступ к конфиденциальной информации взломанного аккаунта.

Говоря о выявлении дипфейков, можно отметить, что оно сопряжено с рядом проблем, причины которых весьма разнообразны. Некоторые из них лежат в области психологии. Например, большинство людей достаточно доверчивы и склонны безоглядно доверять надежным, как им кажется, источникам информации. В совокупности с любопытством, повышенному интересу к определенным персонам или событиям это приводит к тому, что появившаяся информация изначально воспринимается как достоверная. Поэтому основой оценки информации на подлинность должна стать критичность мышления. Вспомним изречение Рене Декарта: «Подвергай все сомнению».

Выявить дипфейк можно двумя способами: путем визуального обнаружения артефактов или посредством использования специального программного обеспечения.

Несмотря на существенное повышение качества дипфейков, многие из них все еще можно выявить при внимательном рассмотрении деталей изображения. Выделим несколько групп признаков, по которым можно определить поддельное фото или видео:

- лицо – очень редкое моргание, неестественное движение глаз, блики в глазах отсутствуют или не совпадают, лицо замирает на доли секунды, артикуляция не соответствует произносимым словам;
- эмоции не соответствуют речи;
- движения не соответствуют темпу речи;
- неестественная поза (лицо в анфас, туловище повернуто);
- зубы, волосы, очки – зачастую содержат видимые дефекты;
- качество изображения – неестественный тон кожи, неправильные тени, нечеткий стык шеи и головы.

Программное обеспечение, предназначенное для выявления дипфейков, позволяет выявлять искусственные изменения, которые могут быть невидимы для человеческого глаза. Алгоритмы работы этих программ, основанные обычно на сверточных нейронных сетях, весьма разнообразны: анализ бликов и отражения в глазах, выражения лица и мимики, исследование визем (визуального выражения того, как произносится тот или иной звук). Также применяется частотный анализ изображения, на основе метода дискретного косинусного преобразования (известен, например, по алгоритму сжатия JPEG).

Необходимость разработки отечественных программ для выявления дипфейков нашла свое отражение в утвержденной в декабре 2022 г. «дорожной карте» «Новое общесистемное программное обеспечение», согласно которой Правительство Российской Федерации в ближайшие два года профинансирует разработку нескольких проектов по распознаванию сгенерированного контента (дипфейков). Однако ряд экспертов скептически оценивают реализуемость этих планов [3].

Крупные кампании, обрабатывающие чувствительные данные, уже заняты реализацией собственных проектов. Например, Сбербанк России в 2022 г. запа-

тентовал алгоритмы выявления дипфейков, которые в 98 % случаев способны обнаружить синтетические изменения изображений лиц людей в видео [4]. В январе 2023 г. социальная сеть «ВКонтакте» объявила, что разрабатывает технологию распознавания дипфейков. Появится возможность проверить загруженные на платформу фотографии или ролики на наличие манипуляций, связанных с лицом, например, изменения в редакторах или замены одного человека на другого. Пользователи смогут самостоятельно проводить проверку видео и изображений на достоверность.

Однако следует понимать, что даже при условии разработки и внедрения эффективных алгоритмов по обнаружению дипфейков загруженный хоть и ненадолго в интернет, фальсифицированный контент вполне способен нанести непоправимый ущерб в силу высокой скорости распространения информации в Интернете.

В завершение коснемся вопроса об ответственности за использование дипфейков, повлекшее причинение морального или материального вреда. В настоящий момент законодательство Российской Федерации не содержит соответствующих норм. В то же время актуальность данной проблемы обусловила разработку законопроекта, предполагающего внесение поправок в ст. 63 «Обстоятельства, отягчающие наказание», ст. 158 «Кража», ст. 159 «Мошенничество», ст. 160 «Присвоение или растрата чужого имущества», ст. 163 «Вымогательство» Уголовного кодекса Российской Федерации. Согласно предлагаемым изменениям использование дипфейков при совершении указанных преступлений будет считаться обстоятельством, отягчающим уголовную ответственность, а также являться квалифицирующим признаком при совершении указанных преступлений.

Дипфейки – это не хорошо и не плохо. Это инструмент, с помощью которого можно сделать образовательный видеосюжет или развлекательный контент. Но в руках злоумышленника дипфейки превращаются в грозное оружие, последствия применения которого могут быть весьма масштабны. Очевидно, что в ближайшее время дипфейки способны значительно изменить ландшафт киберугроз. Они уже сейчас используются в политических кампаниях для манипулирования аудиторией, и это лишь вопрос времени, когда преступники применят подобный метод к состоятельным частным лицам и бизнесу [5].

Список литературы

1. Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия : Государственное и муниципальное управление. 2020. Т. 7. № 4. С. 379–386.
2. Развитие методики синтеза изображения Deepfake. URL: <https://files.sberdisk.ru/s/guv59wzboE2t8VM>.
3. Разработчики систем для распознавания видеофейков в РФ получают гранты. URL: <https://habr.com/ru/news/708696>.
4. Сбер запатентовал технологии по распознаванию дипфейков. URL: <https://rospatent.gov.ru/ru/news/sber-dipfeyk-17082022>.
5. Ларина Е. С., Овчинский В. С. Криминальная жизнь дипфейков. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfeykov.

Козаева К. И.¹,

курсант

Московского областного филиала

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Миронов В. Л.,

*преподаватель кафедры оперативно-разыскной деятельности ОВД
и применения информационных технологий*

Московского областного филиала

Московского университета МВД России имени В.Я. Кикотя

ИНДУСТРИЯ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА НА СОВРЕМЕННОМ ЭТАПЕ

Тот факт, что современные технологии активно используются для совершения преступлений, не является открытием. Одним из наиболее ярких примеров является телефонное мошенничество с целью кражи персональных данных граждан и данных их банковских карт.

Преступные сообщества, занимающиеся телефонным мошенничеством, имеют четкую организационную структуру, в основе которой находится call-центр, оснащенный компьютерами, многоканальными линиями связи, оборудованием подмены номеров. Для определения потенциальной жертвы используются ранее украденные базы данных с персональными данными граждан.

В настоящее время наиболее активный телефонный трафик мошеннических звонков исходит с территории Украины. Это происходит по следующим основным причинам:

- наличие межнационального конфликта между Россией и Украиной на фоне проведения специальной военной операции;
- отсутствие между странами соглашения об экстрадиции лиц, подозреваемых и обвиняемых в совершении преступлений.

Очевидным является факт того, что трафик мошеннических телефонных звонков стал инструментом хищения средств россиян с целью финансирования вооруженных сил Украины.

По данным Банка России, в III квартале 2022 г. в результате мошеннических действий граждане Российской Федерации перевели злоумышленникам денежные средства в размере 4 млрд руб., что является рекордным показателем [1].

Для осуществления мошеннического звонка используется специализированное программное обеспечение, позволяющее подменить номер абонента, осуществляющего исходящий звонок.

Также мошенники приобретают в Даркнете базы данных российских организаций (банков, маркетплейсов, служб доставки и т. п.), которые, как правило, содержат такие персональные данные, как:

¹ © Козаева К. И., 2023.

- фамилия, имя и отчество;
- контактные данные (номер телефона, адрес электронной почты);
- место жительства.

Телефонные мошенники работают по заранее утвержденному шаблону, что позволяет осуществлять психологическое давление на жертву с целью хищения денежных средств, хранящихся на банковских картах.

Мошенничество с использованием телефона реализуется путем задействования мошенниками технических средств IP-телефонии, позволяющих подменять исходящий номер, отображающийся на дисплее телефона у потенциальной жертвы.

Телефонное мошенничество реализуется по множеству разнообразных сценариев, основными из которых являются следующие.

1. Мошенник под видом сотрудника службы безопасности банка (чаще всего звонят от имени Сбера) сообщает потенциальной жертве о попытке подозрительных действий со стороны третьих лиц в отношении ее счетов и банковских карт и предлагает перевести все средства на «безопасный счет». В конце 2021 г. заместитель правления Сбера С. Кузнецов отметил: «сейчас доля мошеннических звонков из-за рубежа достигла 70 %, при этом такие call-центры «работают» исключительно по гражданам России. Главный источник звонков – территория Украины, еще конкретнее – город Днепр, бывший Днепропетровск. Там большое количество русскоговорящей молодежи, а возможностей честного заработка, очевидно, не хватает» [2]. С началом проведения специальной военной операции количество звонков с территории Украины существенно снизилось, однако в 2023 г. вновь увеличилось.

2. Мошенник под видом сотрудника правоохранительных органов сообщает потенциальной жертве о пресечении противоправных действий со стороны третьих лиц в отношении ее банковских карт и в рамках следственных мероприятий рекомендует убедиться в безопасности средств путем проведения транзакций по карте.

3. Мошенники работают сразу по двум схемам. Сначала звонит сотрудник службы безопасности банка и сообщает о том, что от его имени был взят кредит, и, чтобы разобраться, переключает на сотрудника правоохранительных органов, который предлагает сообщить жертве свои персональные данные для уточнения информации по поводу взятия кредита.

Мошенники сообщают жертве о том, что ее родственник попал в беду и ему срочно требуется медицинская помощь и дорогостоящие лекарства, на которые нужно перевести определенную сумму денег. Или же родственник стал виновником аварии и нужно срочно перевести деньги, чтобы его не привлекли к ответственности.

Для организации эффективного противодействия организованным преступным группам, осуществляющим телефонные мошенничества, правоохранительным органам необходимо знать организацию их деятельности, роли участников, способы обналичивания денежных средств и т. п. Существенную помощь в данном вопросе оказало выявление мошеннического call-центра в г. Бердянске.

Во время специальной военной операции на Донбассе в апреле 2022 г. был обнаружен пустующий офис. Оказалось, что в неприметном здании находился один из крупнейших мошеннических call-центров Украины. В сменном режиме в нем «трудилось» около 300 человек. Для получения доступа к информации, хранящейся на жестких дисках call-центра, и помощи в расследовании правоохранительные органы обратились к экспертам Сбера. Обладая огромным опытом расследования компьютерных преступлений, эксперты банка идентифицировали большинство сотрудников call-центра. Изучив терабайты информации, эксперты получили полное представление о структуре и организации работы центра, источниках данных о гражданах Российской Федерации звонков, а также о технологиях и сценариях обмана [3]. Так, для ведения диалога преступники применяли около 150 различных сценариев.

Работники call-центра, непосредственно совершающие телефонные звонки, делятся на три группы.

«Холодники» обзванивают людей по слитым в Интернет базам телефонов. У них две основные задачи: выяснить материальное положение жертвы и параллельно его встревожить, напугать, таким образом, заставляя сотрудничать. Например, человеку сообщают о подозрительном снятии денег с его банковских карт, представляются следователями и говорят о возбуждении уголовного дела и т. д.

«Клосеры» бывают двух типов: одни работают с личными деньгами жертвы, другие специализируются на принуждение жертвы взять в банке кредит и перечислить его мошенникам. Вторые – это уже высший пилотаж, очень опытные люди.

Чем больше денег сумеют вытащить из жертвы мошенники, тем больший бонус вся команда звонивших получит по итогу «закрытия» разводки. Обычно руководители call-центров оставляют своим работникам до 20 % от суммы украденного.

Еще один тип мошенников, участвующих в аферах, – «мены». Как правило, это люди, хорошо знающие определенный регион страны, владеющие информацией о структуре власти области или края, ключевых региональных фигурах, именах начальников отделений банков, органов МВД, знающие географию города жертвы, они всегда в курсе последних городских новостей и т. д.

Задача этих мошенников помочь своим подельникам убедить в реальности происходящего засомневавшуюся жертву, они засыпают ее своими знаниями о том, на какой улице находится тот или иной банк, как туда пройти или проехать, называют реальные фамилии. Попытки жертвы подловить звонящего «банковского работника», «следователя» или «трейдера из венчурной компании» на лжи упираются в детальное знание «меном» региональных реалий. При этом «мены» могут вообще никогда не бывать в регионе своей «приписки» – они скрупулезно изучают город, область или республику через Интернет.

Техническое оснащение мошенников довольно просто: компьютер с базами данных, несколько специализированных программ, наушники с микрофоном. В основе их деятельности – IP-телефония с виртуальными номерами телефонов и возможность их подмены.

Сегодня не нужно покупать какое-то безумно дорогое специальное оборудование или быть гением информатики, в Интернете есть множество сервисов, готовых решить данные задачи.

Базы с данными потенциальных жертв мошенники обычно покупают в Даркнете. Стоимость их стартует от нескольких тысяч рублей и достигает десятков миллионов, все зависит от количества, качества и, самое главное, актуальности информации.

Самые дешевые базы клиентов сайтов бесплатных объявлений. Из них можно узнать имя человека, его номер телефона, электронную почту, а по тому, что он продает, косвенно понять материальное положение. С таким ресурсом нужно работать дополнительно: самостоятельно искать дату рождения, ИНН, прописку и другие нужные для преступников данные.

Дороже всего обходятся банковские документы, которые в числе прочих персональных данных будут содержать счета, размеры долговых обязательств, заложенные недвижимость и автомобили. Обзавестись подобными базами для мошенника, это большая удача, они очень экономят время на холодных звонках и в целом удешевляют процесс нелегальной наживы.

Основной контингент call-центров составляет молодежь в возрасте 18–25 лет [4]. Устраиваясь в такие фирмы, практически все они прекрасно знают, чем им предстоит заниматься. Для современной молодежи это возможность без необходимости тратить годы на образование и наработку опыта сразу зарабатывать приличные деньги. Поэтому вопросы морали их беспокоят в последнюю очередь.

Обналичивание денежных средств в call-центрах происходит через сервисы «Яндекс. Кошелек», «QIWI Кошелек», «WebMoney», «BTC-кошелек» или через банковские карты дропов.

Таким образом, индустрия телефонного мошенничества в настоящее время по-прежнему остается одной из актуальных угроз для россиян, что требует интенсификации дальнейших усилий со стороны правоохранительных органов по выявлению и пресечению деятельности мошеннических call-центров.

Список литературы

1. Мошенники похитили со счетов россиян рекордную сумму. URL: <https://lenta.ru/news/2022/11/24/4bln/>.
2. В Сбере заявили, что доля мошеннических звонков из-за рубежа достигла 70 %. URL: <https://tass.ru/ekonomika/12967881>.
3. Мошеннический call-центр «Бердянск». URL: <http://www.sberbank.ru/common/img/uploaded/kibrary/investigations/berdyansk.pdf>.
4. Вам звонок из Днепра: как устроен мир телефонных жуликов с Украины. URL: <https://life.ru/p/1561941>.

Перепелица Е. А.¹,

*слушатель 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

ОСНОВНЫЕ СПОСОБЫ УСТАНОВЛЕНИЯ ЛИЧНОСТИ С ПОМОЩЬЮ ИНФОРМАЦИОННО-ПОИСКОВЫХ СИСТЕМ

В настоящее время информационно-поисковые системы стали неотъемлемой частью нашей повседневной жизни. Мы используем их для поиска информации о товарах и услугах, новостях, развлечениях, учебных материалах, а также для многих других целей. Одним из возможных способов использования информационно-поисковых систем является установление личности человека.

В данной статье рассматриваются основные способы установления личности посредством использования информационно-поисковых систем. Они включают в себя поиск по имени, фамилии и другим персональным данным, анализ социальных сетей и использование открытых баз данных.

Существуют различные способы установления личности пользователя в Интернете. Один из основных способов – это анализ поисковых запросов, которые были сделаны пользователем. Информационно-поисковые системы хранят данные о поисковых запросах, а также о посещенных сайтах, которые могут быть использованы для установления личности пользователя.

Например, если пользователь делает запросы на тему лечения определенных заболеваний, это может указывать на его здоровье и состояние здоровья. Если пользователь ищет информацию о путешествиях в определенные регионы, это может указывать на его местонахождение или интересы.

Поиск по имени и фамилии является наиболее очевидным и распространенным способом установления личности. Для этого достаточно ввести имя и фамилию человека в поисковую строку и получить результаты, связанные с этими данными. Результаты могут включать в себя социальные сети, блоги, веб-страницы, новостные статьи, статьи в онлайн-журналах и другие источники.

Анализ социальных сетей также является эффективным способом установления личности. Социальные сети содержат множество персональных данных, таких как имя, фамилия, дата рождения, место жительства, место работы и т. д. Анализ данных социальных сетей может помочь определить интересы, хобби,

¹ © Перепелица Е. А., 2023.

образ жизни и другие характеристики человека, которые могут быть полезными для установления его личности.

Открытые базы данных, такие как базы данных регистрации автомобилей, базы данных налоговых служб, базы данных государственных организаций и т. д., также могут быть использованы для установления личности человека. Эти базы данных содержат персональные данные, такие как имя, фамилия, дата рождения, адрес и другие данные, которые могут быть использованы для установления личности человека.

Еще один способ установления личности – это использование информации о местоположении человека. С помощью информационно-поисковых систем можно определить место работы, место жительства, места, где человек учился, посещал различные мероприятия, и т. д. Эти данные также могут помочь в установлении личности и выяснении дополнительной информации о человеке.

Также с помощью информационно-поисковых систем можно исследовать интересы, хобби и привычки человека. Поиск информации о музыкальных предпочтениях, спортивных интересах, культурных событиях, которые посещал человек, позволят установить его личность и лучше понять его предпочтения.

Однако необходимо учитывать, что использование информационно-поисковых систем для установления личности может нарушать право на конфиденциальность и защиту персональных данных. Также не всегда информация, найденная в Интернете, может быть точной или актуальной. Поэтому важно учитывать не только полученную информацию, но и ее источники, а также производить проверку полученных данных.

Как итог, установление личности пользователя в Интернете может быть достигнуто путем комбинации различных источников информации, включая поисковые запросы, собранные данные из других источников, а также множество других параметров.

Для защиты от установления личности пользователя можно использовать такие методы, как использование виртуальных частных сетей (VPN), использование анонимных браузеров или поисковых систем, использование фильтров рекламы и т. д.

Одной из основных проблем установления личности с помощью информационно-поисковых систем является необходимость корректной идентификации и проверки источника полученной информации. В современном мире люди часто оставляют свои персональные данные в различных онлайн-сервисах, таких как социальные сети, интернет-магазины, форумы и т. д. При этом пользователи могут использовать псевдонимы, никнеймы и другие способы скрыть свою реальную личность.

Кроме того, некоторые люди могут использовать в сети Интернет специальные программы и технологии для скрытия своего IP-адреса или использования виртуальных частных сетей, что делает их идентификацию еще более сложной.

Еще одной проблемой являются недостаточная точность и актуальность информации, полученной из поисковых систем. В связи с тем, что Интернет постоянно меняется и обновляется, информация, полученная через поисковую систе-

му, может быть устаревшей или неполной. Кроме того, существует вероятность, что информация может быть искажена или неправильно интерпретирована.

Еще одной проблемой является недостаточная защита персональных данных пользователей. Как правило, поисковые системы собирают и хранят большое количество информации о пользователях, включая их запросы, историю поиска и другие данные. При этом существует риск, что эта информация может быть украдена или использована для незаконных целей.

Наконец, установление личности через информационно-поисковые системы также может нарушать права и свободы граждан, включая право на конфиденциальность, свободу выражения и доступ к информации. Поэтому при использовании информационно-поисковых систем необходимо учитывать эти проблемы и принимать меры для обеспечения безопасности и конфиденциальности данных пользователей.

В заключение можно сказать, что информационно-поисковые системы могут быть полезным инструментом для установления личности и поиска дополнительной информации о человеке. Однако необходимо соблюдать права на конфиденциальность и защиту персональных данных, а также производить проверку полученной информации.

Список литературы

1. Кушнир И. В. Оперативно-розыскная деятельность. М., 2010.
2. Данилов А. Л. Информационно-поисковые системы : учебник. М., 2018.
3. Кораблев В. Н. Оперативно-розыскная деятельность. М., 2021.
4. Компьютерные технологии в правоохранительной деятельности : учебное пособие / под ред. Л. В. Тузовой. М., 2020.
5. Современные информационные технологии в правоохранительной деятельности : учебное пособие / под ред. А. Г. Воронина. М., 2021.
6. Воронин А. Г., Воронина А. В., Пащенко Н. А. Информационные технологии в правоохранительной деятельности : учебник. М., 2018.

Руденко М. П.¹,

*командир отделения факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Толстых М. Ю.,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий*

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук

О ВОПРОСАХ РАЗРАБОТКИ СОБСТВЕННЫХ СИСТЕМ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (DLP) ДЛЯ ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ОВД

Процесс цифровизации становится ключевым направлением развития государства, в том числе и правоохранительных органов. В связи с чем возникает проблема обеспечения безопасного и эффективного внедрения программных средств для решения служебных задач. Защита конфиденциальных данных от несанкционированных воздействий является актуальной задачей и связана с внешними и преимущественно с внутренними угрозами. Несмотря на постоянное совершенствование методов противодействия им, чрезвычайно сложно обеспечить полную защищенность важных данных. Решением проблемы является контроль сотрудников при работе с информацией посредством мониторинга их активности системой предотвращения утечки данных.

Data Loss Prevention (далее – DLP) – это система предотвращения утечки защищаемой информации из организации. Она представляет собой программный или программно-аппаратный комплекс, с помощью которого системные администраторы могут отслеживать и контролировать попытки несанкционированных действий с данными: их изменение, копирование, передачу во внутренней сети и за ее пределы. Система позволяет контролировать действия всех подключенных хостов в сети, фиксировать активность использования социальных сетей, пересылки e-mail сообщений, а при попытке распространения защищаемой информации блокировать пользователя и оповещать администратора, тем самым снижая риск утечки важных данных. Основной целью DLP-систем являются поддержание и выполнение всех требований политики конфиденциальности и безопасности информации, которые существуют в той или иной организации.

В ходе служебной деятельности правоохранительные органы получают и используют информацию ограниченного доступа, утечка которой наносит ущерб как отдельным гражданам, так и обществу в целом. Так, например, получение

¹ © Руденко М. П., 2023.

незаконного доступа к автоматизированным информационно-поисковым системам МВД может привести к изменению и удалению записей в базах данных или разглашению информации, содержащейся в них. Традиционные средства защиты, такие как антивирусы или межсетевые экраны, не способны противостоять внутренним угрозам. Следовательно, ликвидировать все причины утечки служебной информации не представляется возможным, и возникает необходимость применения обязательных мер для их предотвращения, в том числе установка специализированных защитных DLP-систем.

Для достижения поставленных задач в обеспечении информационной безопасности подразделений МВД России использование новейших DLP-систем представляется необходимой мерой и предполагает:

- контроль за отправкой документов на печать, копирование информации на флеш-носитель и ее удаление;
- контроль и блокировка отправки сообщений по электронной почте, мессенджерам, социальным сетям;
- контроль использования автоматизированных рабочих мест сотрудниками в личных целях;
- блокирование нежелательных программ, вредоносного программного обеспечения;
- контроль локальных соединений с использованием технологий беспроводной связи (Wi-Fi, Bluetooth, GPRS);
- контроль использования FTP-соединений.

Системы DLP подразделяются на три основных типа, в зависимости от архитектуры подсистемы контроля: сетевые (шлюзовые), агентские и гибридные (комбинированные).

Первый тип характеризуется наличием шлюза – центрального сервера. Система устанавливается на отдельном персональном компьютере (далее – ПК) или сервере между коммутатором рабочей станции корпоративной сети и прокси-сервером, осуществляющим доступ к глобальной сети. Настройка заключается в подключении хоста и перенаправлении трафика с рабочих станций на него. При такой топологии весь сетевой трафик проходит через DLP-систему, и в зависимости от режима работы, может пропустить его дальше в Интернет либо заблокировать. Сетевые DLP-системы имеют два режима работы: блокирование и мониторинг.

Системы, работающие в режиме блокировки, позволяют защищать информацию от утечек в интернет-сервисах, работающих через протоколы: HTTP, FTP, SMTP и другие. При работе в режиме мониторинга обрабатывается дублированный трафик от коммутатора и сохраняется в журнале для последующего анализа сотрудниками отдела информационной безопасности. Таким образом, контролируется трафик корпоративной сети, но происходящее на конечных хостах определить невозможно.

Шлюзовые DLP-системы обладают высокой степенью защищенности от сторонних вмешательств, предотвращая риски несанкционированного доступа к аппаратным компонентам и изменение настроек, к которым есть доступ только у определенных сотрудников, администрирующих локальную сеть.

Агентские DLP-системы отличаются наличием программ-агентов на хостах сотрудников, осуществляющих контроль за их активностью в процессе использования автоматизированных рабочих мест.

Комбинированные или гибридные DLP-системы обладают возможностями двух ранее упомянутых и представляют повышенный интерес для многих компаний. Объединяя функции агентской и сетевой части, в результате получаем мощный инструмент по предотвращению утечек информации из корпоративной сети.

Применение DLP-системы правоохранительными органами для обеспечения полной защиты данных от утечек предполагает наличие функций как сетевых, так и агентских систем, поэтому рекомендуется использовать системы комбинированного типа. Подход к выбору программно-аппаратного обеспечения требует тщательного анализа функциональных возможностей программного комплекса, необходимого для работы организации: изолированность от глобальной сети Интернет, степень секретности охраняемой информации, количество автоматизированных рабочих мест и так далее.

Повсеместное внедрение усовершенствованных DLP-систем в подразделения МВД России станет эффективным средством обеспечения защиты информации от утечки. Системы автоматизированного контроля помогут получить фактические данные о поведении сотрудников, обнаружить случаи несанкционированных действий с информацией, предотвратить инсайдерские угрозы и защитить данные от утечек, связанных с человеческим фактором.

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
4. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
5. Баранов А. С. Использование систем предотвращения утечек данных в организациях // Молодой ученый. 2020. № 48 (338). С. 15–16. URL: <https://moluch.ru/archive/338/75562/>.

Филимонова Ю. В.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОСОБЕННОСТИ ПОЛУЧЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПРИ РЕАЛИЗАЦИИ АТАК ТИПА MITM

Конституция РФ выступает в качестве правовой основы для ведения оперативно-разыскной деятельности, так как закладывает важнейшие принципы отношений между правоохранительными органами и гражданами в сфере борьбы с преступностью. К таким принципам относятся признание государством высшей ценностью прав и свобод человека (ст. 2), равенства граждан перед законом (ст. 19), соблюдение норм международного права в области обеспечения прав человека (ст. 17), обеспечение права на неприкосновенность частной жизни, личную и семейную тайну (ст. 23). Также в качестве основы можно рассматривать Федеральный закон № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон об ОРД), Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции», УК РФ, Закон Российской Федерации от 17 января 1992 г. «О прокуратуре Российской Федерации», Федеральный закон от 3 апреля 1995 г. «О федеральной службе безопасности» и многие другие НПА.

Основываться данная деятельность должна не только на конституционных принципах законности уважения и соблюдения прав и свобод человека и гражданина а также на принципах конспирации сочетания гласных и негласных методов и средств.

В настоящее время существуют разные средства, которые могут быть использованы для разработки и сбора информации. В качестве одного из таких средств наибольший интерес представляет глобальная сеть Интернет, используемая пользователями для связи между собой. Помимо этого, в сети хранится большое количество разной информации и ее используют в качестве социальной среды для общения. Чаще всего информация, которая расположена в Интернете, носит позитивный или развлекательный характер, однако размещенная информация может носить и негативную окраску. При этом в первую очередь стоит отметить, что в сети можно найти информацию, содержащую признаки какого-либо преступления, которая может помочь при их раскрытии и расследовании.

¹ © Филимонова Ю. В., 2023.

Полученную из сети информацию правоохранные органы не могут использовать в качестве доказательств, но данная информация может помогать раскрывать преступления. Проведенный анализ показывает, что сейчас информация, которая расположена в сети, может быть использована как основа для правового регулирования полученной информации в сети.

На сегодняшний день оперативно-разыскная деятельность находится в поиске новых источников, которые можно использовать для поиска информации, с целью последующего использования таких данных, как доказательства по делу. Связано это с тем, что на законодательном уровне не установлен процесс, который может быть использован для вовлечения таких данных в дело.

Данные, которые были непосредственно получены при использовании сети Интернет, должны быть получены в результате проведения ОРМ. Но сейчас не установлена суть данных мероприятий, не прописаны и не установлены те средства, которые могут быть для этого использованы.

Все это говорит о необходимости проведения анализа данных мероприятий, дать им четкое обоснование. Данные вопросы должны быть рассмотрены в научной литературе, при этом необходимо принимать во внимание ту практику, которая сложилась в стране.

Анализ проведенных исследований показывает, что данным направлением занимаются несколько ученых. В монографии, созданной петербургскими учеными, установлено, что оперативно-разыскные мероприятия по каналам связи являются отдельной категорией мер, регулируемых законодательством об оперативно-разыскной деятельности. Эти меры имеют специфичный характер проведения и правового регулирования. Кроме того, под оперативно-разыскными мероприятиями на каналах связи понимаются операции по контролю за почтовыми отправлениями, телеграфными сообщениями, прослушиванию телефонных разговоров, а также извлечению информации из технических каналов связи.

Одной из важнейших характеристик Интернета является перенос среды из реального мира в виртуальное пространство. Этот двойственный характер – средства связи и виртуальной среды – формирует новый уровень реальности, который нельзя отождествлять с материальным миром. Поэтому очень важно рассматривать Интернет, главным образом, как виртуальную среду и расширять существующие правовые нормы на объекты виртуальной реальности. Необходимо обратить внимание на то, что правовое регулирование в области материального мира, в частности борьба с преступностью, должно также охватывать Интернет. Становится очевидно, что официальная позиция государства сводится к необходимости признания важности переносимости правовых норм из материального мира в Интернет.

Множество объектов и видов деятельности в Интернете свидетельствует о возможности существования ОРД с широкой гаммой видов. Интернет содержит информацию, привлекающую ОРД, формирующуюся при подготовке и совершении преступлений в реальном мире, что расширяет сферу действия ОРД. В Интернете информация, которая может заинтересовать органы, осуществляющие ОРД, появляется в результате подготовки и совершения преступлений в реальном мире, что значительно расширяет сферу деятельности ОРД.

Однако важно отметить, что ОРД в интернете не должна восприниматься только как удаление информации из технических каналов связи, проводимое на основе правового регулирования. ОРД должна существовать в интернете в различных формах и условиях доступа к информационным объектам, а также содержание информационного обмена, реализуемого в ходе ОРД, должны отличаться от предоставляемых услуг в интернете.

Подводя итог, можно сказать, что оперативно-разыскная практика существенно разнообразна, но также идет по пути разнообразных форм и видов мошенничества в интернете, а не буквального понимания его как коммуникационной сети с трактовкой всех действий только как изъятия информации из технических каналов связи.

Список литературы

1. Кушнир И. В. Оперативно-розыскная деятельность. М., 2010.
2. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.).
3. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (с изменениями и дополнениями).
4. Шаров В. И. Оперативно-розыскные мероприятия в сети Интернет // Общество и право. 2018. № 2 (64). URL: <https://cyberleninka.ru/article/n/operativno-rozysknye-meropriyatiya-v-seti-internet>.
5. Мовчан А. В. Отдельные аспекты применения компьютерной разведки в оперативно-розыскной деятельности // Проблемы правоохранительной деятельности. 2014. № 2.
6. Голубев В. В. Интернет и оперативно-розыскная деятельность // Законодательство. 1999. № 11.
7. Паламарчук А. В. Правовое регулирование правоотношений в сети Интернет. URL: <http://genproc.gov.ru/documents/nauka/document-72010>.
8. Глава Минкомсвязи: виртуальная преступность должна караться реально. URL: <http://24news.club/2015/10/15/glava-minkomsvyazi-virtualnaya-prestupnost-dolzha-karatsya-realno>.
9. URL: http://www.consultant.ru/cons/document/cons_doc_LAW_155995/3d0cac60971a511280.
10. ФСБ сможет проводить оперативно-разыскные мероприятия в Интернете. URL: <http://pravo.ru/news/view/90524>.

Панков Е. С.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОТДЕЛЬНЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ОТКРЫТЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

Киберпреступность является серьезной угрозой для государства, компаний, организаций и граждан. Она может привести к утечке конфиденциальной информации, потере денежных средств, прерыванию работы важных систем и другим негативным последствиям. В настоящее время существует множество методов противодействия киберпреступности, включая использование открытых источников информации.

Открытые источники информации представляют собой публично доступные источники данных, которые могут использоваться для получения информации о компаниях, организациях, людях и других субъектах. К таким источникам могут относиться государственные базы данных, сайты, социальные сети, блоги, форумы и другие ресурсы. Они могут содержать ценную информацию, которая может быть использована для выявления уязвимостей и предотвращения кибератак.

Одним из методов использования открытых источников информации является мониторинг социальных сетей. Киберпреступники могут использовать социальные сети для сбора информации о своих жертвах, поэтому мониторинг активности в социальных сетях может помочь выявить потенциальные угрозы. Это может включать отслеживание упоминаний о компании или ее сотрудниках, мониторинг хештегов и обсуждений, связанных с кибербезопасностью, и т. д.

Открытые источники информации могут быть использованы для мониторинга подозрительной активности в интернете. Это может включать мониторинг форумов, где обсуждаются техники кибератак, отслеживание продажи украденной информации на теневых рынках и т. д. Эта информация может быть использована для определения новых угроз и разработки мер по их предотвращению.

Кроме того, открытые источники информации могут использоваться для создания базы данных известных киберпреступников и их методов. Это может помочь идентифицировать уязвимости и принимать меры по их предотвращению.

¹ © Панков Е. С., 2023.

Также такая база может использоваться для сравнения с новыми угрозами и определения их возможного происхождения.

Использование открытых источников информации является важным методом противодействия киберпреступности. Данные источники позволяют получить ценную информацию о компаниях, организациях и киберугрозах, которая может быть использована для выявления уязвимостей, предотвращения кибератак, получения важной информации о других обстоятельствах преступления. Однако необходимо помнить, что использование открытых источников информации требует тщательного анализа и верификации, чтобы убедиться в ее достоверности. Кроме того, использование открытых источников информации должно соответствовать законодательству о защите персональных данных и правам на конфиденциальность.

Список литературы

1. URL: https://www.infowatch.ru/sites/default/files/publication_file/analiticheskiy-otchet-strategii-kiberbezopasnosti.pdf.
2. URL: <https://cyberleninka.ru/article/n/kiberbezopasnost-ugrozy-vyzovy-resheniya>.
3. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/>.
4. URL: https://codernet.ru/articles/security/kiberprestupleniya_v_bankovskoj_sfere_samyie_izvestnyie_sluchai/.
5. URL: <https://cyberleninka.ru/article/n/kiberprestupnost-v-bankovskoy-sfere-tendentsii-i-osobennosti-rassledovaniya>.

Полякова О. С.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Овчинский А. С.,

профессор кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

доктор технических наук, профессор, Академик РАЕН

АНАЛИЗ ДАННЫХ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Современной правоохранительной деятельности не обойтись без использования современных технологий и методов обработки и анализа больших объемов данных. С каждым годом все больше преступлений совершаются с использованием интернет-ресурсов и социальных сетей, что требует от следователей и оперативников быстро адаптироваться к новым тенденциям и находить информацию во всевозможных источниках. В данной работе будет рассмотрен вопрос анализа данных из открытых источников в раскрытии и расследовании преступлений, особенности такого анализа, а также приведены практические примеры использования данного подхода в процессе раскрытия и расследования преступления.

Существует масса источников информации, которыми человек пользуется каждый день. Самыми известными являются социальные сети и мессенджеры. У каждого человека есть как минимум один аккаунт в какой-либо социальной сети или мессенджере, в котором указано настоящее имя и фамилия, а иногда и фотографии, дата рождения, открытый список друзей и сообществ. Мониторинг социальных сетей – мощный инструмент при анализе и сборе данных о человеке. Также можно найти огромное количество слитых в открытый доступ баз данных, которые хранят персональные данные человека. Эти базы данных сливают недобросовестные операторы связи, владельцы интернет-сервисов и так далее. В XXI веке интернет хранит информацию о каждом человеке на Земле.

OSINT (Open Source Intelligence) – разведка по открытым источникам.

Источниками информации для OSINT могут служить:

1. Открытые данные (новости, подкасты, записи в блогах, социальных сетях и других интернет-сообществах, информация о доступных из Интернета портах и т. д.), которые можно найти в сети с помощью поисковых систем, в том числе специализированных, таких как Shodan.

¹ © Полякова О. С., 2023.

2. Предназначенные для публичного использования документы из невидимого сегмента сети:

- материалы, предоставляемые по запросу (отчеты, записи пресс-конференций, доклады, публичные заявления);
- материалы, предоставляемые по подписке (статьи в отраслевых журналах, почтовые рассылки через специализированные сервисы);
- метаинформация, которую можно получить с помощью специализированных инструментов или при анализе других материалов (например, из комментариев в коде программ).

Также рассмотрим такой раздел OSINT, как SOCMINT.

SOCMINT (или социальная медиа разведка) – это подраздел OSINT, фокусирующийся на сборе и мониторинге данных в социальных сетях. Информации в социальных сетях много, ниже представлена классификация:

1. Открытая

- посты;
- фотографии;
- личные данные, размещаемые в профиле (дата рождения, город проживания, семейное положение и т. д.).

2. Частная

- личные сообщения.

Любой поиск информации начинается с некоторого начального набора данных. В данной курсовой работе это будут фамилия, имя, номер телефона, домашний адрес и фотография.

Источниками информации о человеке могут быть:

- 1) он сам: аккаунты в социальных сетях, блог и т. п.;
- 2) государство: базы данных налоговой, судебных приставов, судов и т. п.;
- 3) иные источники (друзья, враги, СМИ, работодатель и т. п.).

Теперь можно приступить к алгоритму сбора информации о человеке.

Первым делом по имени и фамилии можно найти человека во всех популярных социальных сетях, конечно, если он там зарегистрирован. Такой способ является не результативным, так как с определенным набором фамилии и имени будут найдены около 1 000 людей, что не облегчит поиск определенного человека. Также человек может быть не зарегистрирован в социальных сетях, так что найти его будет невозможно.

Далее по ФИО можно произвести поиск в Яндекс или Google. Вводя ФИО, поисковая страница выдает зарегистрированные ИП на такие имена, а также профили в социальных сетях. Можно сделать вывод, что искать в поисковике лишь по имени и фамилии не эффективно, так как поиск предлагает слишком много вариантов других людей.

Имея ФИО человека, можно узнать, каким бизнесом он владеет. На сайте налоговой есть сервис по поиску предпринимателей по имени и фамилии. С помощью этой информации мы можем узнать, чем примерно занимается человек. Кроме того, в базе открыто хранится номер ИНН. Первые его четыре цифры являются кодом подразделения ФНС. Ищем его в Google или Яндекс и выясняем, в каком городе человек зарегистрировал ИП. С помощью сайта

ФНС можно по ФИО найти все зарегистрированные ИП, их ОГРН и ИНН, регион, в котором зарегистрировано предприятие, дату включения в реестр и дату исключения.

Также человека можно найти в базе МВД (<https://мвд.рф/wanted>), особенно если он вызывает опасения. У МВД есть для этого бесплатный сервис, только для поиска придется указать год рождения. Данное поле можно заполнить наугад, если знать примерный возраст.

Практически любой номер можно полноценно пробить в интернете. Да так, что о владельце получится узнать не только различную персональную информацию, но и получить его фото.

Социальные сети самый большой источник информации о вас. Так как именно там вы, быть может, когда-то давно или же в настоящий период времени размещаете информацию о себе, своих интересах, хобби; где можно увидеть круг ваших друзей и знакомых; где можно посмотреть ваши фотографии, музыку и видео – вся информация в совокупности позволит:

- 1) сформировать комплексный образ вашей личности и статус в обществе;
- 2) узнать, что является главным в жизни и какие приоритеты;
- 3) определить адрес, где проживаете или чаще всего бываете;
- 4) выяснить номер телефона (ваш, членов семьи и близких друзей);
- 5) скачать и сохранить графические материалы (которые поспособствуют дальнейшему поиску информации).

В заключение хочется отметить, что анализ данных из открытых источников имеет огромный потенциал в области раскрытия и расследования преступлений. Использование современных методов и технологий обработки данных позволяет значительно увеличить эффективность работы правоохранительных органов и сократить время, затрачиваемое на расследование.

Подводя итог, можно сказать, что анализ данных из открытых источников становится неотъемлемой частью работы правоохранительных органов и будет продолжать развиваться и совершенствоваться в будущем.

Список литературы

1. ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения» от 01.05.2020 // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200172576>.
2. Беляевский И. К. Маркетинговое исследование: информация, анализ, прогноз : учебное пособие. М. : Финансы и статистика, 2019.
3. Гасанов Э. Э. Интеллектуальные системы. Теория хранения и поиска информации : учебник для бакалавриата и магистратуры / Э. Э. Гасанов. М. : Юрайт, 2016.
4. Гатчин Ю. А., Сухостат В. В., Куракин А. С., Донецкая Ю. В. Теория информационной безопасности и методология защиты информации. 2-е изд., испр. и доп. СПб. : Университет ИТМО, 2018.
5. Поликарпов Е. С. Основы компьютерной разведки : учебное пособие. М., 2020.

Смолянинов В. А.¹,

*курсант факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

Севастьянов Д. С.²,

*командир отделения факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

Котова Н. А.³,

*курсант факультета подготовки специалистов
в области информационной безопасности*

Московского университета МВД России имени В.Я. Кикотя

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

ПРОБЛЕМЫ ИССЛЕДОВАНИЯ ПАМЯТИ КВАНТОВОГО КОМПЬЮТЕРА

По мере того, как квантовые компьютеры все больше становятся реальностью для современного человека, становится все более важной разработка методов криминалистического анализа их квантовой памяти. Потенциал вычислений квантовых компьютеров также вызывает опасения по поводу их использования в преступной деятельности, такой как взлом, кража данных и шпионаж. Однако исследование следов в таких системах вызывает проблемы из-за хрупкой природы квантовых состояний и ограниченного знания квантового состояния до измерения.

Квантовый компьютер – это вычислительное устройство, которое использует явления квантовой механики (квантовая суперпозиция, квантовая запутанность) для передачи и обработки данных.

Рассматривая квантовые компьютеры, необходимо изучить одно из главных их отличий от обычных технических устройств: квантовые компьютеры используют в своих расчетах определенные свойства квантовых систем, такие как запутанность и суперпозиция. Свойство запутанности позволяет определить два кубита в состояние, при котором становится невозможным описать один кубит

¹ © Смолянинов В. А., 2023.

² © Севастьянов Д. С., 2023.

³ © Котова Н. А., 2023.

без учета состояния другого. Если исходом измерения первого кубита оказывается 0, то при последующем измерении второго кубита со стопроцентной вероятностью будет получен исход 1 [3, с 73]. Необходимо отметить, что ученые ИТМО предложили универсальный способ для генерации квантовых корреляций и запутанных состояний. Он позволяет динамически влиять на параметры системы и задавать желаемые характеристики фотонов, например, явления группировки или антигруппировки. Исследование открывает возможности для кодирования запутанных состояний в сверхпроводящих кубитах и обработки квантовой информации в оптических чипах следующего поколения [5].

Однако вместе с этими преимуществами возникают и новые проблемы. Например, фиксация информации на квантовых компьютерах является гораздо более сложной задачей, чем на обычных компьютерах. Это связано с тем, что квантовые биты очень чувствительны к внешним воздействиям, таким как электромагнитные поля, излучение и т. д. Эти воздействия могут вызвать ошибки в обработке данных и привести к искажению результатов вычислений.

Благодаря квантовой запутанности квантовый компьютер с 79 запутанными кубитами имеет число состояний 10^{23} степени, т. е. 100 секстиллионов, с 263 кубитами такая машина могла бы представлять столько одновременных состояний, сколько протонов во вселенной, в то время как обновление до 400 кубитов может содержать всю информацию, закодированную во вселенной.

Вычисления производятся посредством манипуляций, называемых квантовыми вентилями, с амплитудами кубитов.

Вентили могут быть однокубитные и двухкубитные. Также существуют универсальные наборы вентиляей, с помощью которых можно выполнить любое квантовое вычисление. Вентили в квантовом компьютере выполняются последовательно, но иногда некоторые амплитуды волновых функций нужно сохранить для более позднего этапа вычислений. Для данного действия нет возможности использовать классическую память, так как при производстве измерений вся волновая функция кубита редуцируется до одного результата, после чего становится невозможным оперировать амплитудами его волновой функции. Более того, в квантовой физике действует запрет на клонирование состояния: невозможно создать точную копию квантового состояния. Единственным вариантом синхронизации операций оказывается создание задержки в выполнении вентиля для этого кубита.

Переходя к самому криминалистическому исследованию информации в квантовых компьютерах, стоит отметить тот факт, что постановка следователем вопросов для эксперта не должна претерпеть существенные изменения, так как на любом устройстве именно информация имеет главенствующее значение.

Стоит обратить повышенное внимание на процесс обнаружения, фиксации и изъятия информации с квантовых устройств.

На данный момент существует несколько методов обнаружения и фиксации информации на квантовых компьютерах. Один из вариантов – использование специальных средств защиты данных, которые отслеживают любые изменения состояния устройства и предпринимают необходимые меры, если что-то необычное происходит.

Также существуют методы, связанные с квантовым шифрованием, которое позволяет надежно защитить передаваемую информацию. Суть этого метода заключается в блокировании доступа к незакодированной информации во время передачи и обработки данных. Однако, несмотря на приемлемую эффективность такого метода, у него есть определенные слабости, которые могут быть использованы хакерами, работающими с квантовыми компьютерами.

Одной из основных проблем в квантовом криминалистическом анализе является тот факт, что квантовые состояния хрупки и могут быть легко нарушены внешними воздействиями – проблема декогеренции. Изменения температуры или электромагнитные помехи могут привести к тому, что квантовое состояние потеряет свою когерентность и станет неотличимым от случайного шума, что затрудняет восстановление информации из квантовой памяти, подвергшейся внешним воздействиям. Это означает, что традиционные криминалистические методы, такие как клонирование или визуализация памяти, могут быть неприменимы к квантовой памяти.

Еще одна проблема заключается в том, что квантовая память по своей сути вероятностна. В отличие от классической памяти, где каждый бит имеет определенное значение 0 или 1, кубит с определенной вероятностью может находиться в суперпозиции обоих состояний.

Наконец, существует проблема квантовой запутанности. Свойство запутанности, описанное выше, определяет, что информация, хранящаяся в одном кубите, может быть распределена по нескольким кубитам, что затрудняет восстановление исходной информации из одного кубита.

В результате можно сделать вывод, что обеспечение безопасности хранения и обмена информацией на квантовых компьютерах – сложная задача, которая требует внимательного изучения особенностей устройства и создания новых алгоритмов и инструментов.

Список литературы

1. Rietsche R., Dremel C., Bosch S. et al. «Квантовые вычисления. Электронные рынки», 2022. С. 2525–2536.
2. Нильсен М., и Чуанг И. Квантовые вычисления и квантовая информация: выпуск к 10-летию, 2010. С. 33–34.
3. Прескилл Дж. Квантовая информация и квантовые вычисления. Т. 1 / Дж. Прескилл. Ижевск : НИЦ «Регулярная и хаотическая динамика», 2008. С. 73.
4. Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. Ижевск : НИЦ «Регулярная и хаотическая динамика», 2001. С. 71–92.
5. Новостной сайт университета ИТМО. URL: <https://news.itmo.ru/ru/science/it/news/13012/>.

Филимонов А. А.¹,
ведущий специалист
Управления специальных экспертиз
Центра экспертизы и координации информатизации

СОЗДАНИЕ ПЕРСОНАЛЬНЫХ ЭКСПЕРТНЫХ ИНСТРУМЕНТОВ ИССЛЕДОВАНИЯ ЦИФРОВЫХ ДАННЫХ В СРЕДЕ РАЗРАБОТКИ JUPYTER NOTEBOOK НА ЯЗЫКЕ PYTHON

В рамках компьютерно-технической экспертизы (далее – КТЭ) эксперты исследуют носители и собственно цифровую информацию различного характера и структуры.

Отметим, что экспертное исследование в рамках КТЭ возможно условно представить в виде граф-цикла (рис. 1), где вершины – объект исследования (далее – ОИ), специализированное криминалистическое программное обеспечение (далее – СПО), соответствующие результаты обработки ОИ с помощью СПО (далее – РОСПО), эксперт (специалист, проводящий экспертизу) и соответствующие результаты обработки РОСПО экспертом (далее – РОЭ). Очевидно, что указанный цикл обычно разрывается по итогам соответствующей итерации на этапе РОЭ в случае получения достаточного объема данных для вывода по поставленным относительно ОИ вопросам либо в случае необходимости смены инструмента исследования. В иных случаях с учетом полученных данных происходит смещение фокуса исследования и начинается новый цикл.

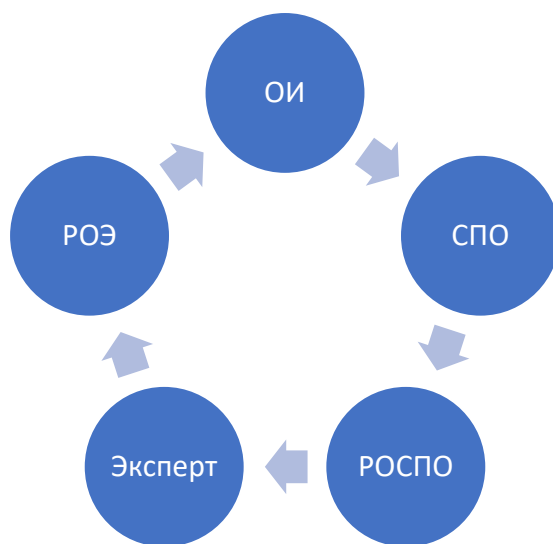


Рис. 1. Условная схема обработки ОИ с использованием СПО

Смена инструмента в рамках цикла исследования часто обусловливается необходимостью решения отдельных частных экспертных задач, инструменты решения которых не реализованы в используемом СПО.

¹ Филимонов А. А., 2023.

В указанных случаях экспертами используются либо возможности СПО в части написания программного кода обработки необходимых данных внутренним скриптовым языком (при наличии реализованной функциональности), либо сторонние средства разработки программного обеспечения.

При этом особое значение для экспертов возможность создания инструментов решения частных экспертных задач принимает в условиях отсутствия или значительного устаревания имеющихся в наличии коммерческих криминалистических программных и программно-аппаратных комплексов.

В такие моменты возникает вопрос выбора средств создания инструментов решения частных экспертных задач, а именно – языка и среды программирования.

Данный выбор осложняется наличием различного рода объективных ограничений как связанных с квалификацией эксперта, так и с различного рода требованиями к собственно выбираемым средствам.

Так, естественно, разработка соответствующих программных инструментов требует от проводящего экспертизу специалиста серьезных знаний в области программирования, структур данных и алгоритмов. Кроме того, имеются и иные требования, в том числе, например, требования, связанные с обеспечением возможности положительного результата последующей процессуальной оценки соответствующего заключения [1, ст. 88].

В совокупности с зачастую ограниченными сроками проведения экспертных исследований вышеизложенное означает, что используемые в их рамках средства создания инструментов решения частных экспертных задач должны быть свободнораспространяемыми и, одновременно, позволяющими не увеличивать сроки производства, в том числе они должны быть доступными для оперативного изучения и не должны быть перегружены функционалом.

С учетом изложенного, а также исходя из потребностей экспертов не только в оперативном получении качественного конечного результата обработки информации, но и из необходимости документирования хода обработки соответствующих материалов, сформулируем основные требования к языку и среде программирования.

Так, очевидно, что основными значимыми требованиями к языку программирования с учетом описанных выше целей являются следующие:

- возможность свободного легального использования;
- простота синтаксиса;
- возможность автоматического определения типа и связывания с ним переменных в момент присваивания значения (динамическая типизация);
- возможность автоматического выделения памяти для объектов в целях использования создаваемой программой и освобождение памяти от неиспользуемых объектов (автоматическое управление памятью);
- значительное количество стандартных и дополнительных реализованных библиотек;
- возможность использования кода, написанного на иных языках.

То есть, фактически, язык программирования должен обеспечивать возможность концентрации эксперта непосредственно на программировании необхо-

димого функционала разрабатываемого программного средства без отвлечения на нюансы управления типами и памятью, а также предоставлять возможность использования в программах значительного количества уже реализованного функционала как в виде библиотек, так и в виде кода на иных языках программирования.

Основными значимыми требованиями к среде программирования исходя из описанных выше целей являются следующие:

- кроссплатформенность;
- простой интерфейс;
- поддержка наиболее распространенных языков программирования;
- возможность комбинировать в едином рабочем пространстве исполнимый код, комментарии к коду, вывод исполнения кода в различных форматах, а также промежуточные/итоговые выводы по результатам анализа того или иного этапа исследования;
- возможность формирования (в том числе разметки) структурированного итогового выходного документа исходя из содержания рабочего пространства для создания аналитического отчета по исследованию, например, в виде приложения к заключению, без использования либо с минимальным использованием дополнительного программного обеспечения.

Исходя из сформированных выше требований к языку программирования возможно лучшим выбором в данном случае является язык программирования «Python» – один из самых популярных в настоящее время языков, используемых, в том числе в анализе данных и машинном обучении.

Python обладает, в том числе, следующими основными свойствами [2]:

- является свободнораспространяемым языком программирования;
- является высокоуровневым языком программирования;
- является языком программирования общего назначения;
- имеет динамическую типизацию;
- имеет автоматическое управление памятью;
- имеет значительное количество реализованных функций в стандартной и дополнительно подключаемых библиотеках;
- позволяет использовать код на иных языках.

В качестве среды разработки (программирования) лучшим выбором в настоящее время, по мнению автора, является Jupyter Notebook.

Исходя из сведений на официальном сайте проекта [3] указанный программный продукт является веб-приложением для создания вычислительных документов и обмена ими с простым, оптимизированным интерфейсом.

Кроме того, среда разработки Jupyter Notebook обладает следующими основными свойствами:

- является свободнораспространяемой средой разработки;
- является кроссплатформенной средой разработки;
- имеет простой, не перегруженный элементами интерфейс;
- предоставляет возможность выбора языка программирования;
- предоставляет возможность интерактивного вывода исполнения кода (HTML, изображения, видео, LaTeX и др.);

- предоставляет возможность использования инструментов обработки больших данных (Apache Spark от Python, R и Scala);
- предоставляет возможность использования инструментов обработки больших данных с помощью pandas, scikit-learn, ggplot2 и TensorFlow.

С учетом заявленных возможностей, в том числе объединения в едином рабочем пространстве программного кода и интерактивного вывода исполнения данного кода в виде HTML, LaTeX, изображений и видео, указанное программное обеспечение можно признать подходящим для использования в качестве прикладной среды программирования эксперта КТЭ для решения частных экспертных задач путем разработки персональных экспертных инструментов.

Jupyter Notebook является веб-приложением. Вместе с тем у него есть возможность и локальной работы – для ее реализации необходимо установить соответствующее серверное программное обеспечение на локальный персональный компьютер. Подключение к среде и дальнейшая работа происходят с использованием браузера.

Установка на локальный компьютер может быть осуществлена из Python путем использования системы управления пакетами `pip` и соответствующей команды (`pip install notebook`). Альтернативным способом является использование дистрибутива Anaconda, изначально ориентированного на работу с данными, и поставляемого с предустановленными основными необходимыми библиотеками и инструментами, в том числе «Jupyter Notebook».

Работа с Jupyter Notebook начинается с создания файла документа («ноутбука»), который будет отображать рабочую среду исследования эксперта в соответствующей степени, в том числе код, комментарии и вывод по результатам исполнения кода, если такой вывод предусмотрен. Собственно файл имеет расширение «`ipynb`» и формат «`json`».

После создания новой рабочей среды (файла «ноутбука») в ней содержится один характерный элемент – ячейка.

Отметим, что фактически рабочая среда Jupyter Notebook формируется из таких ячеек, которые могут быть нескольких основных видов, в том числе:

- ячейки Code;
- ячейки Markdown.

Тип ячейки необходимо выбирать при ее создании и в случае необходимости переопределять в процессе работы с использованием интерфейса среды разработки. Интерпретация содержимого ячейки средой зависит от ее вида. На рис. 2 выделен элемент интерфейса (элемент под условным номером 2), с использованием которого устанавливается тип ячейки.

Комбинация ячеек указанных выше видов позволяет сформировать структурированную рабочую зону (рабочее пространство), в рамках которой решается конкретная частная экспертная задача.

Рассмотрим возможности ячеек типов Code и Markdown подробнее.

Ячейки Code содержат код на языке программирования ядра и комментарии к нему (ядром по умолчанию является Python).

Под ячейкой Code располагается ячейка вывода по результатам исполнения кода в ячейке. Выходные данные могут представлять собой текст, изображение, графики или HTML-таблицы.

Таким образом при программировании ячейки в целях визуализации результата выполнения кода возможно использовать различные средства форматирования выводимой информации.

На рис. 2 приведен пример прямого вывода текстового содержания объекта (список списков) и его форматированный вывод (см. разделы 2 и 3 соответственно) с использованием дополнительных программных модулей, в частности «Pandas».

По умолчанию исполнение ячеек Code выполняется в порядке их следования и фиксируется средой программирования слева от ячеек – метки вида «In[n]», где n – порядковый номер исполнения ячейки.

Вместе с тем в любой момент времени произвольная ячейка Code может быть исполнена экспертом для решения части конкретной исследовательской задачи без перезапуска иных ячеек¹. Таким образом, достигается повышенный уровень интерактивности разработки.

Указанная особенность использования ячеек Code является важным свойством Jupyter Notebook в целом, так как позволяет исследователю последовательно выполнять необходимые действия, получать и фиксировать предварительные и итоговые данные, а в случае необходимости вносить необходимые коррективы в код конкретных ячеек с их последующим запуском на исполнение без необходимости перезапуска всего кода рабочего пространства.

Данное свойство позволяет, например, не производить импорт данных каждый раз, когда необходимо провести какие-то манипуляции с данными, что значительно ускоряет работу с данными и разрабатываемым программным обеспечением.

Рассмотрим особенности ячеек Markdown.

Ячейки Markdown содержат текст, который может быть отформатирован с использованием языка разметки Markdown и HTML.

Основные возможности формирования и форматирования содержания рабочего пространства Jupyter Notebook с использованием ячеек данного типа, которыми стоит воспользоваться в рамках разработки, включают в себя: формирование заголовков, отступов, маркеров и разрывов строк; выделение жирным шрифтом и курсивом; создание упорядоченных и не упорядоченных списков; создание таблиц; вставка изображений.

Приведем необходимый для реализации указанных возможностей порядок действий.

Для формирования заголовков необходимо добавить перед текстом соответствующих ячеек нужное количество символов «#» (количество зависит от уровня заголовка).

¹ Стоит отметить, что в ходе разработки необходимо учитывать изменение переменных по результатам исполнения конкретной ячейки, так как они могут использоваться программным кодом иных ячеек.

Для добавления отступов необходимо поместить перед текстом символ «>».

Для формирования маркеров необходимо добавить в текст ячейки: символ «-» с одним пробелом после него (результат – круглый маркер с заливкой); символ «-» с пробелом до/после него (результат – квадратный маркер с заливкой); табуляция и символ «-» с пробелом до/после него (результат – круглый маркер без заливки).

Для добавления разрывов строки необходимо добавить в месте обрыва строки тег «
».

Для добавления выделения жирным шрифтом необходимо поместить предназначенный для выделения текст между тегами «» и «», между «**» и «**» или между «__» и «__».

Для добавления выделения курсивом необходимо поместить предназначенный для выделения текст между тегами «<i>» и «</i>», между «*» и «*» или между «_» и «_».

Для добавления упорядоченного списка необходимо поместить элементы списка между тегами «» и «», которые в свою очередь поместить между тегами «» и «».

Для добавления неупорядоченного списка необходимо поместить элементы списка между тегами «» и «», которые в свою очередь поместить между тегами «» и «».

Для добавления таблицы необходимо строки таблицы поместить между тегами «<tr>» и «</tr>», элементы заголовка поместить между тегами «<th>» и «</th>», элементы строк поместить между тегами «<td>» и «</td>».

Добавление изображения осуществляется с использованием тега с указанием ссылки на файл (src) и его размера (width, height).

На рис. 2 приведены примеры результатов отдельных указанных выше действий (см. разделы 3.1–3.4).

Отметим, что при работе с заголовками в рабочем пространстве целесообразно использовать расширение «Table of contents», позволяющее отображать навигацию по созданным заголовкам в соответствии со сведениями о них в ячейках «Markdown» (рис. 2, элемент под условным номером 1).

Полученное итоговое содержание рабочего пространства может быть экспортировано и приложено к заключению эксперта. Предусмотрены следующие виды экспорта: «PDF via HTML (.pdf)», «AsciiDoc (.asciidoc)», «HTML (html)», «HTML with toc (html)», «LaTeX (tex)», «Markdown (md)», «Notebook (ipynb)», «PDF via LaTeX (.pdf)», «PDF via HTML (.pdf)», «reST (rst)», «Python (py)», «Reveal.js», «slides (slides.html)» и «PDF via HTML (.html)».

На рисунке 2 приведен пример сформированного рабочего пространства, с оформленными заголовками и отдельными примерами формирования и форматирования текста в ячейках «Markdown». Кроме того, выделены зоны отображения заголовков в панели навигации (элемент под условным номером 1), элемент интерфейса для выбора типа ячейки (элемент под условным номером 2), элемент интерфейса для активации отображения панели навигации по содержанию рабочей среды (элемент под условным номером 3), а также сведения о порядке исполнения ячеек «Code» (элементы под условными номерами 4–6).

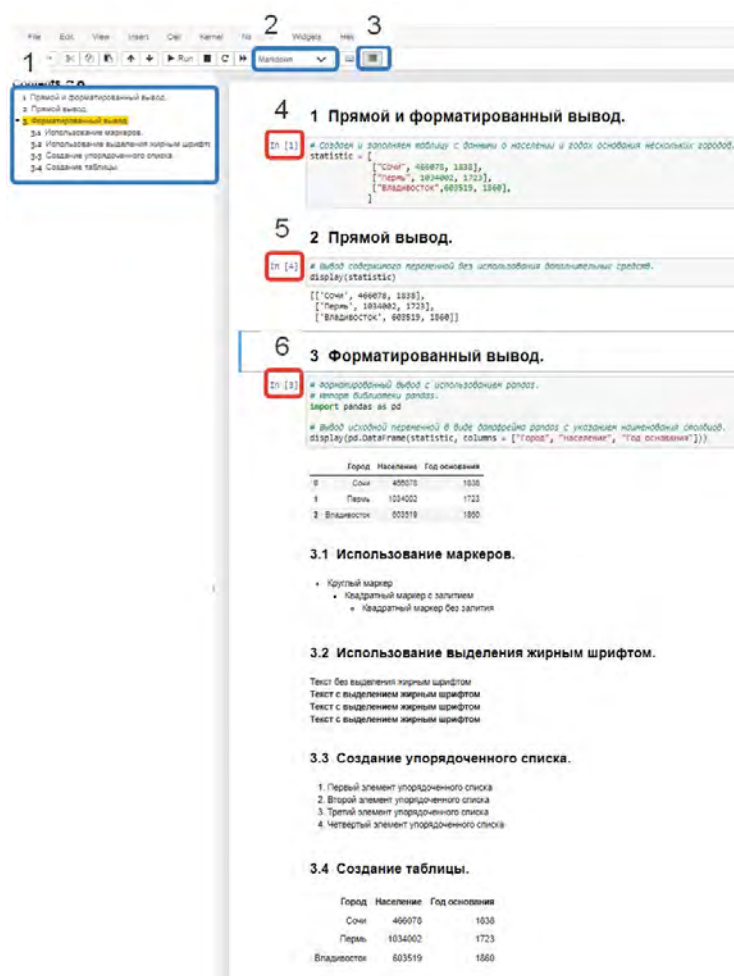


Рис. 2. Пример сформированного рабочего пространства
Jupyter Notebook

Таким образом, среда разработки Jupyter Notebook является удобным инструментом решения частных экспертных задач в части разработки персональных экспертных инструментов на языке «Python», позволяющим:

- объединять в едином рабочем пространстве программный код, его вывод, аналитическую составляющую исследования, а также навигацию по соответствующим разделам рабочей среды;
- по итогам исследования формировать соответствующий выходной отчетный документ, содержащий собственно программный код, вывод по результатам его исполнения, а также экспертную аналитику промежуточных и итоговых результатов.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174-ФЗ (ред. от 18.03.2023) // // НПП «Гарант-сервис». URL: <https://internet.garant.ru/#/document/12125178/paragraph/53424899/doclist/3170/1/0/f4e31cca-dbb9-4f74-9e03-1bd32f8a4348/%D0%A3%D0%9F%D0%9A:8>.
2. Python.org: [сайт]. URL: <https://www.python.org>.
3. Project Jupyter: [сайт]. URL: <https://jupyter.org>.

Пучков Г. Ю.¹,

ведущий научный сотрудник

ФКУ НПО «Специальная техника и связь» МВД России,

кандидат технических наук

ОСОБЕННОСТИ СОЗДАНИЯ СЕРВИСОВ ИСОД МВД РОССИИ В ИНТЕРЕСАХ ОПЕРАТИВНЫХ СЛУЖБ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

В современных условиях ускорения темпов научно-технического прогресса четко проявляются тенденции компьютеризации, создания разветвленных систем обработки данных, включающих в себя ЭВМ, информационные системы и компьютерные сети. Информатизация затрагивает практически все стороны государственной и общественной жизни, в том числе и играет важную роль в автоматизации процессов оперативно-разыскной деятельности (далее – ОРД).

Неслучайно в последнее время по инициативе подразделений центрального аппарата МВД России, занимающихся ОРД, значительно активизировалась деятельность по созданию новых типов специального программного обеспечения, предназначенного для решения разнообразных задач по раскрытию и предотвращению преступлений [1].

В настоящее время реализация данного программного обеспечения осуществляется в виде сервисов Единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России).

В общем случае сервис ИСОД МВД России, создаваемый в интересах оперативных подразделений органов внутренних дел, представляет собой базу данных для хранения оперативно значимой информации и современные инструменты для ее обработки.

Как правило, база данных аккумулирует сведения о персональных данных лиц, совершивших преступления, находящихся в розыске, попавших в поле зрения правоохранительных органов в ходе оперативно-разыскной деятельности, а также информацию о совершенных преступлениях и местах преступлений [2].

Принципиальным моментом является то, что все сервисы ИСОД МВД России разрабатываются с использованием технологии «тонкого клиента». До недавнего времени подразделения территориальных органов МВД России на областном уровне имели собственные базы данных (далее – БД), сформированные сотрудниками данных подразделений. В результате в системе МВД России сформировалось и используется большое количество региональных БД, не связанных друг с другом. Это не позволяет осуществлять поиск и получение оперативной информации в автоматическом виде из БД других регионов.

Технология «тонкий клиент» предполагает создание единой для всех абонентов сервиса (централизованной) базы данных, которая вместе с инструментарием

¹ © Пучков Г. Ю., 2023.

ем для обработки хранящихся в ней данных размещается в центре обработки данных ИСОД МВД России. На клиентских местах устанавливается программное обеспечение лишь для формирования запросов, команд на соответствующую обработку информации, хранящейся в базе данных, получения и отображения результатов поиска и обработки данных.

Централизованная БД сервиса формируется путем миграции данных из региональных БД и постоянно обновляется сотрудниками территориальных органов МВД России. Таким образом, сотрудник любого региона страны имеет доступ к информации, поступившей в БД из любого другого региона. Это существенно повышает эффективность ОРД, особенно по преступлениям, совершенным так называемыми «гастролерами», серийными убийцами и т. д. Таким образом, все сервисы ИСОД МВД России как созданные, так и планируемые в настоящее время к разработке, будут иметь общую техническую базу, поскольку разворачиваются на серверных мощностях центра обработки данных ИСОД МВД России, и использовать общую для всех архитектуру – «тонкий клиент».

Анализ требований технических заданий на создание специального программного обеспечения (далее – СПО) в интересах оперативных служб показывает, что большая часть требований к СПО касается вопросов получения, хранения и обработки информации, получаемой в автоматизированном виде от кредитных организаций, операторов сотовых систем связи и сервисов ИСОД МВД России. Реализация данных требований в каждом сервисе ИСОД МВД России, закрепленном за конкретной службой, приводит к необходимости осуществления одних и тех же работ в разных ОКР, а в дальнейшем и в рамках модернизации данных сервисов.

Учитывая изложенное, представляется целесообразным разработать в интересах оперативных служб базовое СПО, которое позволяло бы получать оперативно значимую информацию через единый базовый сервис ИСОД МВД России. Это позволит существенно повысить степень унификации программного обеспечения, снизить затраты на разработку и дальнейшую модернизацию необходимого программного обеспечения.

Опыт создания и использования базовых сервисов ИСОД МВД России имеется. В рамках разработки государственной информационной системы миграционного учета были созданы подсистемы, которые в настоящее время доступны для всех служб и подразделений органов внутренних дел Российской Федерации. К ним относятся:

Сервис нормативно-справочной информации, который позволяет получать сведения об объектах единой системы классификации и кодирования МВД России (НСИ);

Единый базовый сервис сведений о физических лицах, который позволяет получать сведения о физических лицах (ЕСФЛ);

Единый базовый сервис сведений о юридических лицах, который позволяет получать сведения о юридических лицах (ЕСЮЛ);

Подсистема внешнего взаимодействия (ПВВ), которая позволяет обеспечить автоматизацию взаимодействия с внешними системами и сервисов ИСОД МВД России между собой;

Централизованная подсистема отчетности и бизнес-аналитики (ЦПОиБА), которая позволяет обеспечить построение фиксированных отчетов, произвольных отчетов (на основе структуры соответствующей БД), предоставление современных инструментов бизнес-анализа, построение табличных и графических форм отображения результатов анализа статистической информации.

Первый опыт использования указанных базовых сервисов показывает, что это было своевременное и правильное решение. Вместе с тем в ходе работ по их сопряжению с другими сервисами ИСОД МВД России выяснилось, что базовый сервис должен строиться, как отдельный самостоятельный объект. В противном случае необходимость его доработки влечет за собой изменение контрольной суммы исходного СПО всего сервиса, в состав которого он входит, и появление всех связанных с этим неприятностей (проведение типовых испытаний, сертификация во ФСТЭК России и т. д.).

Учитывая изложенное, в настоящее время для решения задач информационного обмена с кредитными организациями и операторами сотовых систем связи предлагается создать базовый сервис «Цифровая платформа». В рамках работ по его созданию планируется разработать и разместить в системе межведомственного электронного взаимодействия (далее – СМЭВ 3) типовые виды сведений, которые позволят сотрудникам различных оперативных служб использовать общие вычислительные и транспортные ресурсы для получения оперативнозначимой информации от различных организаций и предприятий, подключенных к СМЭВ 3.

Важным направлением создания базовых сервисов ИСОД МВД России в интересах оперативных служб можно считать разработку федеральной информационной системы биометрических учетов (далее – ФИСБУ), которая началась в 2022 г. Целью работы является создание универсального сервиса ИСОД МВД России, предоставляющего возможность сотрудникам оперативных служб осуществлять идентификацию личности человека по изображению лица, дактилоскопической и геномной информации, содержащейся в едином банке биометрических учетов МВД России, создаваемом в рамках данной ОКР.

Планируется, что банк биометрических учетов будет содержать дактилоскопическую информацию об отпечатках и следах пальцев (ладоней) рук, данные об изображении лиц, попавших в поле зрения правоохранительных органов.

Доступ к геномной информации планируется осуществлять путем формирования при помощи соответствующих инструментов ФИСБУ запросов к сервису ИСОД МВД России «Объединенная поисковая федеральная система генетической идентификации «Ксенон-2».

Кроме этого, через ФИСБУ планируется осуществлять доступ к аналогичной информации, хранящейся в банках данных других ФОИВ, а именно:

- межгосударственном информационном банке;
- федеральной ГИС «Единая система идентификации и аутентификации» (ЕСИА);
- едином центре хранения и обработки данных г. Москвы (ЕЦХД);
- единой биометрической системе (ЕБС);

- государственной автоматизированной информационной системе «Сфера»;
- единой государственной информационной системе обеспечения транспортной безопасности (ЕГИС ОТБ).

Важным направлением данной работы является осуществление миграции дактилоскопической информации, хранящейся в банках данных территориальных органов МВД России, в единый банк биометрических учетов.

Другим перспективным направлением создания базовых инструментов ИСОД МВД России является разработка сервиса для определения криминального облика подозреваемого. Речь идет об использовании возможностей интернет сети:

по получению информации об объекте интереса, содержащейся в электронных средствах массовой информации, социальных сетях и других источниках, находящихся в интернет сети в открытом доступе, таких как:

- установка базовых сведений об объекте интереса и его окружении;
- анализ деятельности объекта интереса и его окружения;
- установка связей между интересующими объектами;
- вовлеченность объекта интереса в социальные и бизнес-процессы;
- проведение анализа оперативной обстановки в регионе;
- анализ деструктивных течений;
- анализ протестной активности;
- анализ социальной напряженности в регионах;
- составление психологических портретов объектов интереса, групп пользователей, объединенных по тем или иным признакам, представляющих оперативный интерес.

Создание такого сервиса ИСОД МВД России в качестве базового позволит оперативным сотрудникам различных служб использовать одни и те же технологии искусственного интеллекта, модели и методики анализа больших данных.

В заключение необходимо отметить, что унификация процессов получения в интересах оперативных служб органов внутренних дел оперативно значимой информации за счет создания и использования базовых сервисов ИСОД МВД России позволит существенно сэкономить время и финансовые ресурсы, предусмотренные на внедрение методов поиска, обработки и анализа информации, упростить процесс эксплуатации СПО и уменьшить объем задействованных на эти цели средств вычислительной техники.

Список литературы

1. Пучков Г. Ю., Сергеева С. В., Дудникова Е. В. Специальное программное обеспечение для автоматизации деятельности подразделений МВД России по борьбе с незаконным оборотом наркотических средств. Полицейский вестник Всероссийского института повышения квалификации сотрудников МВД России № 1 (6). 2022. С. 63–69.
2. Основные направления создания информационной системы для идентификации личности по фенотипическим признакам человека // [В. О. Благов и др.] // Вестник РГГУ. 2021. № 2. С. 37–46.

Ромашкин Т. Р.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Атласов И. В.²,

профессор кафедры естественнонаучных дисциплин

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

доктор физико-математических наук, профессор

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВНЕДРЕНИЯ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ПРИ ОРГАНИЗАЦИИ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ АТАК

Стеганография (от греч. *στεγανός* – скрытый + *γράφω* – пишу; буквально «тайнопись») – наука, позволяющая автору спрятать передаваемые им данные в некотором контейнере, тем самым скрыв сам факт передачи информации. В стеганографии существует два типа материалов: сообщение и носитель. Сообщение – это секретные данные, которые должны быть скрыты, а носитель – это материал, в котором содержится сообщение.

Текстовая стеганография основана на выбранном тексте обложки и изменении свойств текста обложки, таких как пунктуация или правописание, для скрытия информации. Чаще всего информация может содержаться в пробелах и непечатаемых символах. Использование знаков препинания было предложено как способ сокрытия битов. Метод кодирования со сдвигом строк представляет собой редактирование документа с помощью смещения положения строк по вертикали на странице текстового документа для уникализации его кода.

Стеганография со сдвигом слов является одним из наиболее важных методов. Поскольку он не изменяет первоначальный смысл текста и работает быстро и просто, широко используется сдвиг слов. Он нажимает на положение слова или, другими словами, изменяет длину пространства внутреннего мира, чтобы вставить секретное сообщение.

При извлечении секретной информации описанный выше метод требует сравнения пробелов в полученном тексте с пробелами в исходном «чистом» тексте. Брассил и др. предложили идею «управления пространством» в ссылке, которая заставляет текст stego становиться саморасширяющимся. Предполагается, что пробелы в строке равны друг другу. Таким образом, алгоритм сохраняет соседние пространства позиции встраивания (до и после) неизменными во время фазы встраивания. Эти два пространства называются «управляющими пространствами». На этапе извлечения алгоритм сравнивает положение встраивания с управ-

¹ © Ромашкин Т. Р., 2023.

² © Атласов И. В., 2023.

ляющими пробелами, чтобы определить, увеличивается или уменьшается положение встраивания в пространство. Однако этот метод заметно изменяет длину текстовой строки.

Стеганография – это в основном передача зашифрованного сообщения, текста или файла, скрытого внутри другого файла, называемого «носителем», который может быть чем угодно, от простого расширения блокнота до файла, содержащего некоторые аудио– или визуальные носители. Медиафайлы более совместимы с выполнением необнаруживаемой стеганографии. Файл изображения может быть изменен до сотого пикселя, чтобы закодировать в нем сообщение, которое было бы невозможно обнаружить, если бы кто-то явно не искал его. Однако для обнаружения любого акта стеганографии создателю конкретного сообщения потребуется упорядочить зашифрованное сообщение, поскольку прямое сообщение будет легко обнаруживаемым. Криптография происходит, когда вы можете видеть информацию, но не понимаете ее. Стеганография происходит, когда информация скрыта. Записка, написанная секретным кодом, является криптографией; записка, написанная невидимыми чернилами, является стеганографией. Люди, обменивающиеся частной или конфиденциальной информацией в Интернете, используют оба метода.

Простым подходом для встраивания информации в изображение обложки является использование младших значащих битов (LSB).

Концепция заключается в том, что если изменить последнее битовое значение пикселя, цвет не будет принимать заметных изменений. Кодирование выполняется с помощью следующих шагов:

1. Преобразование изображения в градации серого.
2. При необходимости изменение размера изображения.
3. Преобразование сообщения в двоичный формат.
4. Инициализация выходного изображения так же, как и входного.
5. Перебор каждого пикселя изображения и выполнение следующего алгоритма:
 - a) преобразование значения пикселя в двоичную систему;
 - b) получение следующего бита сообщения для внедрения;
 - c) сравнение переменных для обновления пикселей выходного изображения;
6. Продолжение обновления картинки на выход до полного внедрения битов.
7. Записываем входное и выходное изображения в локальную систему.

Разница между изображением оригинала и изображением стего будет едва заметна человеку. Основным недостатком является ограниченный размер данных, встроенных в изображение. Методы LSB, реализованные в 24-битных форматах для цветного изображения, трудно обнаружить в отличие от 8-битного формата.

Методы маскировки и фильтрации, обычно ограничиваемые 24 битами или изображениями в оттенках серого, используют другой подход к сокрытию сообщения. Эти методы встраивают информацию в более важные области, а не просто скрывают ее в уровне шума.

В аудиостеганографии секретное сообщение встроено в оцифрованный аудиосигнал, что приводит к незначительному редактированию двоичной последова-

тельности соответствующего аудиофайла. цель состоит в том, чтобы позволить автору тайно отправлять свои данные, скрытые в песне. Рассмотрим некоторые методы интегрирования тайных сообщений в песни, записи голоса, аудиосообщения и другие звуковые файлы.

В настоящее время существует несколько методов, используемых для создания расширенных спектров. К ним относятся Спектр распространения прямой последовательности (DSSS), Спектр распространения с перескоком по частоте (FHSS) и Спектр распространения с перескоком по времени. Каждая техника отличается по своей реализации и имеет определенные преимущества/недостатки. В дополнение к вышесказанному существует ряд гибридных методов, которые предлагают определенные преимущества по сравнению с другими методами или расширяют их полезность. Эти гибриды представляют собой модуляцию с скачкообразной частотой/ прямой последовательностью и скачкообразной частотой во времени. Различные методы расширения спектра используют цифровую кодовую последовательность для процесса модуляции. Кодовая последовательность называется псевдослучайным шумом (PN). Псевдослучайный шум – это сигнал, аналогичный шуму, который удовлетворяет одному или нескольким стандартным тестам на статистическую случайность. Сигнал, по-видимому, не имеет определенной структуры, но на самом деле он состоит из детерминированной последовательности импульсов, которые повторяются через длительный промежуток времени.

Метод скрытия эха имеет два набора параметров: длину сегмента и его эхо-банк. Эхо-банк состоит из набора эхо-ядер, количество которых зависит от типа кодирования. В частности, существуют 2 и 2 эхо-ядра в случае двоичного кодирования и кодирования Мюррея соответственно. Где каждое ядро представляет один символ алфавита. В процессе встраивания аудиосигнал делится на последовательные блоки в соответствии с длиной сегмента. Затем сообщение кодируется в соответствии с используемым алфавитом (двоичным или m-массивом).

Список литературы

1. Хасанов Р. И. Основы стеганографии : учебное пособие. Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2016.
2. Грибунин В. Г., Оков И Н., Туринцев И. В. Цифровая стеганография. М. : СОЛОН-Пресс, 2018.
3. Медведев М. П., Фомина М. А. Стеганография как средство совершения кибератак. Новая наука: От идеи к результату. 2016. № 11–2. С. 121–124.
4. Биккенин Р. Р. Стеганография – современный метод обеспечения безопасности информации. Информация и космос. 2006. № 2. С. 89–93.

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*

СПУФИНГ/СНИФФИНГ HTTPS

В настоящее время большинство веб-сайтов обеспечивают защищенную связь между клиентами и веб-сервером, используя протокол HTTPS. Этот протокол основан на использовании TLS и криптографических алгоритмов, которые обеспечивают шифрование данных точка-точка во время передачи. Более того, протокол позволяет проверить подлинность соединения и обеспечить целостность передаваемых данных, что предотвращает возможность изменения информации злоумышленниками в процессе передачи.

Для пояснения HTTP расшифровывается, как HyperText Transfer Protocol, который представляет собой формально определенный набор правил для обмена данными между клиентом (сетевым ресурсом, который запрашивает данные или услуги) и сервером (ресурсом, который получает запросы и отвечает на них). HTTP – это протокол прикладного уровня в семиуровневой сетевой модели OSI, который стандартизирует коммуникационные функции телекоммуникационных или вычислительных систем, независимо от их внутренней структуры или технологии. Определение и текущая разработка этого протокола в настоящее время находятся под эгидой международной организации под названием Internet Engineering Task Force (IETF). HTTPS (Secure Hypertext Transfer Protocol) – это защищенная версия популярного HTTP (протокола передачи гипертекста). Этот протокол работает на прикладном уровне и основан на HTTP, но с дополнительной безопасностью протокола TLS (на транспортном уровне) для обеспечения сквозной безопасности для всех подключений, от клиентов до веб-серверов.

Такая атака, как удаление SSL, существует, и она заключается в «снятии» TLS-шифрования сообщений, чтобы злоумышленник мог видеть все сообщения в открытом виде, используя HTTP. Это возможно, когда злоумышленник имеет физический доступ к сети или использует программное обеспечение для перехвата трафика. Такие атаки могут привести к серьезным последствиям, таким как утечка конфиденциальной информации и компрометация безопасности данных. Один из способов обнаружения таких атак может быть перехват трафика, выходящего за пределы защищаемой сети, что может выявить инсайдеров или злоумышленников. Однако для защиты от подобных атак необходимо использо-

¹ © Рахмонбердиев Б. Б., 2023.

вать дополнительные методы шифрования данных и защиты сетевых устройств и приложений. Перехват трафика может осуществляться с целью его дальнейшего анализа и выявления утечек, а также для модификации трафика с целью навязывания ложной информации. Все современные сервисы, от электронной почты до сервисов обмена сообщениями работают с использованием зашифрованных протоколов, следовательно, одной из подзадач борьбы с утечкой информации является перехват HTTPS трафика.

Протокол TLS является одним из наиболее часто используемых протоколов для обеспечения безопасной связи. Кроме того, он используется не только в соединениях HTTPS, но и в других протоколах, таких как FTPES (версия FTP с защитой, обеспечиваемой TLS) и даже в протоколах виртуальной частной сети, таких как OpenVPN.

Протокол TLS (и, следовательно, протокол HTTPS на уровне приложения) использует различные криптографические алгоритмы, которые обеспечивают нам следующие характеристики:

Если мы проводим атаку ARP Spoofing и устанавливаем сниффер для захвата всего трафика, то мы можем перехватывать весь сетевой трафик, генерируемый конкретным компьютером (жертвой). В случае использования незащищенных протоколов, таких как HTTP или FTP, злоумышленник может легко просмотреть все ваши сообщения, учетные данные для аутентификации и даже файлы cookie сеанса. Поэтому подключение к открытым Wi-Fi сетям или другим ненадежным сетям представляет риск, так как любой злоумышленник может осуществить атаку «Человек посередине» и получить доступ к вашей информации.

Если мы используем безопасный протокол, например HTTPS, то злоумышленник сможет перехватывать всю информацию, но не сможет прочитать ее содержимое. То есть он не сможет увидеть учетные данные для аутентификации, файлы cookie сеанса или что-либо еще, так как весь трафик зашифрован с помощью сквозного шифрования от клиента до веб-сервера. Благодаря протоколу TLS и криптографическим алгоритмам, таким как AES, наша информация будет надежно защищена и останется конфиденциальной, т. е. будет зашифрована от конца до конца.

Атаки с разделением SSL представляют собой процесс настройки прокси HTTP/HTTPS для «разрыва» защищенного протокола HTTPS, при этом жертва использует незащищенный протокол HTTP, что позволяет злоумышленнику перехватывать и просматривать всю информацию внутри соединения. Для нарушения HTTPS-соединения необходимо выполнить определенный процесс:

1. Для того чтобы перехватить весь сетевой трафик, который отправляет и принимает жертва, мы можем провести атаку ARP Spoofing. Это позволит нам перехватывать весь трафик, отправляемый жертвой, до того, как он будет доставлен до маршрутизатора.

2. Запустить сниффер, такой как WireShark, который является очень хорошим выбором благодаря своей полноте и простоте использования, а также по причине того, что он бесплатен.

3. Проверка правильности работы ARP Spoofing и сниффера, чтобы убедиться в захвате трафика жертвы. Однако мы не сможем видеть HTTPS-трафик,

так как он зашифрован от конца до конца. Мы сможем увидеть только открытый трафик, такой как DNS и ICMP.

Постоянно ведется работа по повышению безопасности TLS. И многие эксперты согласны с тем, что соединения постепенно будут становиться все более безопасными. Это повышает уверенность в будущем HTTPS. Планы по развитию этой технологии в ближайшем будущем включают использование машинного обучения, внедрение клиентских сертификатов и использование возможностей нейронных сетей. Однако пока эти задачи выполняются, необходимо использовать доступные инструменты для защиты от хакерских атак. Специалисты компании Zelenit понимают это и могут помочь вам внедрить наиболее эффективные модели защиты. Дополнительные консультации и помощь можно получить по телефону или через онлайн-сервисы.

Список литературы

1. Модель OSI // medium.com. URL: <https://medium.com/software-engineering-roundup/the-osi-model-87e5adf35e10>.
2. Как sniffить HTTPS-трафик iOS-устройства // habr.com. URL: <https://habr.com/ru/company/dataart/blog/419677/>.
3. Как перехватить защищенный трафик // tech-geek.ru. URL: <https://tech-geek.ru/sniffing-ssl/>.
4. Sniffing HTTPS трафика в Wi-Fi и локальных сетях // forum.antichat.com. URL: <https://forum.antichat.com/threads/345266/>.
5. Три лучших HTTPS-сниффера и декодера [список 2023] // www.raymond.cc. URL: <https://www.raymond.cc/blog/spying-windows-software-by-sniffing-and-decoding-packets-including-ssl-with-ospay/>.

Гуков А. А.¹,

*заместитель начальника отдела по расследованию ДТП
Следственного управления УМВД России
по Одинцовскому городскому округу*

Фареник Д. С.²,

*начальник отдела по расследованию ДТП
Следственного управления УМВД России
по Одинцовскому городскому округу*

Холодков К. И.³,

*ведущий научный сотрудник лаборатории геоинформатики
Института физики Земли имени О.Ю. Шмидта
Российской академии наук,
кандидат технических наук*

Гуков А. А.⁴,

*доцент кафедры тактико-специальной,
огневой и физической подготовки
Московского областного филиала
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В ПРОВЕДЕНИИ ОСМОТРА МЕСТА ПРОИСШЕСТВИЯ ПРИ ДОРОЖНО-ТРАНСПОРТНОМ ПРОИСШЕСТВИИ

Сотрудники следственных органов, прибывающие на осмотр места дорожно-транспортного происшествия (ДТП), постоянно решают две конкурирующие между собой проблемы: с одной стороны, необходимо качественно провести осмотр места ДТП, а с другой стороны, требуется как можно быстрее возобновить движение по автотрассе.

Несомненно, что для следственных органов качественно выполненный осмотр места ДТП имеет приоритетное значение и крайне важен для дальнейшего расследования происшествия, предусмотренного уголовным законодательством Российской Федерации. Неквалифицированное и небрежное проведение этого следственного действия обычно приводит к невозможным утратам следов и вещественных доказательств, так как компенсировать пробелы, допущенные при первоначальном осмотре, путем повторного осмотра чаще всего уже не удастся. При проведении следственных действий следует учитывать, что «характерной

¹ © Гуков А. А., 2023.

² © Фареник Д. С., 2023.

³ © Холодков К. И., 2023.

⁴ © Гуков А. А., 2023.

особенностью места ДТП являются быстрое изменение и уничтожение следовой картины, что предполагает фиксацию в первую очередь следов и объектов, которые подвержены быстрым изменениям из-за атмосферных и метеорологических условий вследствие воздействия проезжающими транспортными средствами и по другим причинам».

В соответствии с российским законодательством и в целях качественного осмотра места ДТП следователю необходимо выполнять многочисленные действия. В том числе: произвести осмотр места происшествия, составив протокол осмотра; составить схему места ДТП; осмотреть и зафиксировать повреждения на (далее – ТС); в том числе детально зафиксировать следы, оставленные на месте ДТП; произвести фотосъемку повреждения на ТС; подготовить рапорт об обнаружении признаков преступления. В случае если в результате ДТП есть погибшие, следователь должен на месте происшествия подготовить постановление о назначении медицинской судебной экспертизы и вручить его транспортировщикам погибших в морг.

Кроме этого, если ДТП произошло в погодных условиях, которые могут измениться (темное время суток или снег, дождь, туман и т. д.), следователь обязан установить общую видимость проезжей части, а также конкретную видимость в данных погодных условиях.

Также на время осмотра места происшествия влияют иные факторы: взаимодействие следователя с различными службами; общение с родственниками пострадавших; отбор объяснения очевидцев ДТП. Все перечисленное необходимо выполнить непосредственно на месте для понимания механизма самого происшествия.

Помимо всего следователь выполняет распорядительные функции по руководству следственно-оперативной группой (СОГ) и координации действий других служб (инспекторов ДПС, дорожных служб, эвакуатору и т. д.).

Нередки случаи, когда на места происшествия по ДТП выезжают следователи, не имеющие специальных знаний в этой области расследования. Это обстоятельство негативно влияет на качество проведения осмотра. Зачастую ими фиксируются только те следы, оставленные ТС (если таковые имеются), которые он видит. И то при условии, что он может их соотнести к следам, оставленным именно этими ТС. Так, например, при наличии в районе места ДТП сколов асфальтного покрытия, осыпи грязи с подкрылков ТС следователями и инспекторами ДПС как следы, оставленные ТС на месте ДТП, не замечаются. Вышеуказанные следы зачастую доказывают непосредственное место столкновения автомобилей, что в первую очередь необходимо выяснять при расследовании ДТП.

Конечно, недостаточность зафиксированных следов возможно восполнить путем допросов понятых, водителей и инспекторов ДПС, участвовавших при осмотре места ДТП, а также назначением комплексной фототехнической и трассологической судебных экспертиз, по фотоснимкам. Но необходимость выполнения указанных процессуальных действий приводит к затягиванию сроков предварительного следствия.

Практика показывает, что при большом объеме задач, выполняемых следователями при осмотре места ДТП, схемы, составленные им вручную, мало информативны и часто плохо читаются. Точность данных, приведенных в них, зача-

стю невысока. Расстояния фиксируются лишь те, которые, по мнению инспектора ДПС или следователя, важны в настоящее время. Несмотря на присутствие на бланке схемы места ДТП масштабной сетки, объекты отображаются без соблюдения масштаба. Поэтому в дальнейшем по такой схеме крайне затруднительно определить дополнительные данные, необходимые для последующего анализа ДТП. Подробное, точное и детальное составление схемы места ДТП для дальнейшего расследования уголовного дела имеет самое важное значение, так как по делам данной категории необходимо в дальнейшем проведение автотехнической судебной экспертизы, на которую при ее производстве опирается эксперт-автотехник. Нередки случаи, когда по результатам проведенной автотехнической судебной экспертизы, экспертом делаются выводы о невозможности дачи заключения ввиду малой информативности осмотра места происшествия, в том числе следов ТС и «привязки» к объектам на схеме.

Все эти обстоятельства, несомненно, влияют на время проведения осмотра места ДТП, соответственно на составление протокола осмотра места происшествия и составление схемы к нему, следовательно время остается незначительное.

Вышеперечисленные обстоятельства побуждают сотрудников следственных органов искать новые, более эффективные методики осмотра места происшествия и фиксации следов ДТП. С этой целью следственным отделом по расследованию ДТП СУ УМВД России по Одинцовскому городскому округу в 2022 г. применялась экспериментальная методика фиксации обстоятельств на месте ДТП при помощи реконструкции трехмерной модели по фотоснимкам, полученных с миниатюрного беспилотного летательного аппарата (БПЛА). При этом в качестве специалиста в области фотограмметрии привлекался сотрудник лаборатории геоинформатики Института физики Земли имени О.Ю. Шмидта Российской академии наук.

Трехмерная модель места ДТП представляет собой набор точек в трехмерном пространстве, образующих транспортные средства, дорожную инфраструктуру и прочие объекты с учетом их местоположения, формы и масштаба. Создание такой модели по данным реально существующих объектов называется реконструкцией. В нашем случае реконструкция производится по серии фотоснимков при помощи методов фотограмметрии. Фотограмметрия позволяет извлечь пространственную информацию о снимаемых объектах за счет отслеживания точек этого объекта на снимках с разным ракурсом. Идея восстановления формы поверхности схожа с принципом бинокулярного зрения. Схематично этот процесс изображен на рис. 1.

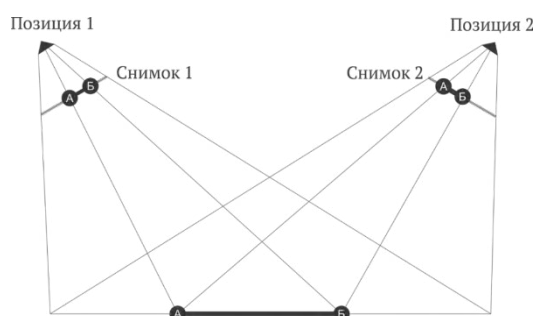


Рис. 1. Принцип восстановления геометрии из двух снимков под разными углами для двумерного случая. А и Б – точки на объекте и на соответствующих снимках

Существует несколько программных инструментов фотограмметрии и трехмерной реконструкции: Agisoft Metashape, RealityCapture и многие другие.

Для того чтобы сохранить реальный масштаб объектов, положение камеры в момент съемки фиксируется при помощи системы радионавигации на борту БПЛА – приемника спутниковых сигналов глобальных навигационных спутниковых систем NAVSTAR/GPS, ГЛОНАСС и COMPASS/Beidou. В результате реконструкции полученная модель может быть исследована на предмет характера повреждений, расстояний между объектами, состояния дорожной инфраструктуры и прочего.

Кроме масштабных трехмерных моделей, могут быть получены ортофотопланы. Ортофотоплан – это фотоизображение местности, составленное из нескольких специальным образом преобразованных фотоснимков.

И трехмерные модели, и ортофотопланы являются геопривязанными, т. е. координаты каждой точки известны, следовательно, возможны любые измерения расстояний и площадей.

На рис. 2 представлены фрагмент трехмерной модели (фото слева) и фрагмент ортофотоплана (фото справа) одного из происшествий. На обоих фрагментах указаны одинаковые измерения.

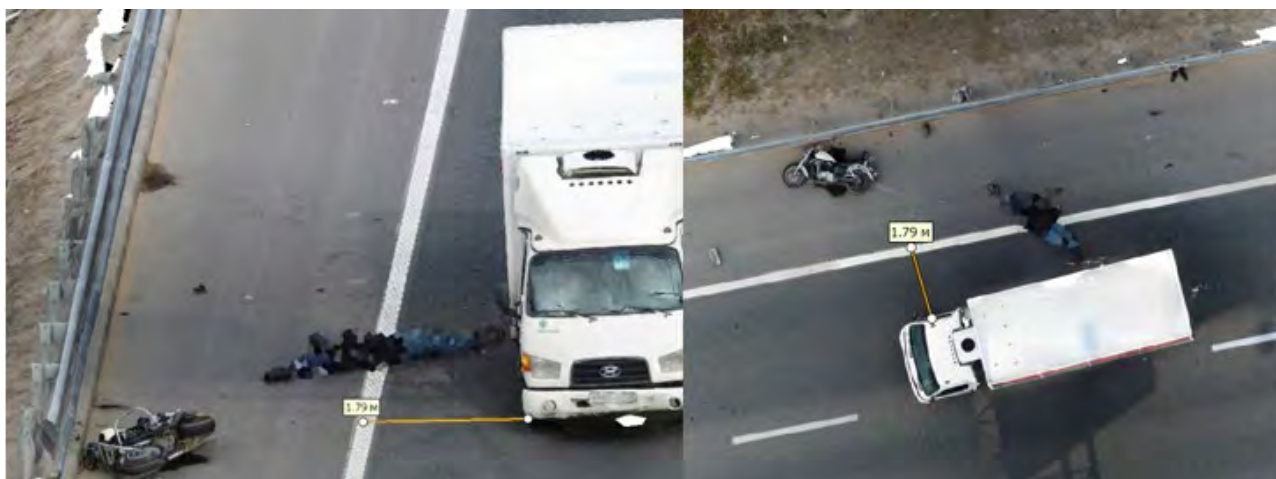


Рис. 2. Измерения, выполненные по трехмерной модели (фото слева) и по ортофотоплану (фото справа)

Для получения трехмерной модели и ортофотоплана необходимы фотографии местности в высоком разрешении с перекрытием — таким, чтобы каждый последующий снимок содержал хотя бы четверть, а лучше треть сцены предыдущего снимка. Кроме этого, каждый снимок должен быть геопривязан, записаны долгота, широта и высота камеры, а также (желательно) угол крена и тангажа камеры относительно горизонта и направления на север.

В нашей работе для получения таких снимков применялся БПЛА DJI Mini 2. При малом весе и возможностью достаточно длительного времени работы на одной батарее он оснащен камерой высокого разрешения (12 Мп) и приемником ГНСС. Процедура получения фотоматериалов достаточно проста: инспектор-оператор приводит в полетное положение БПЛА за 2 минуты и в течение 20 минут (в среднем) получает порядка 200 изображений. Далее изображения

обрабатываются в ПО Metashape. Этот программный инструмент, в частности, позволяет систематизировать и выстроить процедуры получения трехмерной модели и ортофотоплана таким образом, чтобы вмешательство специалиста в области геодезии или фотограмметрии было сведено к минимуму. Полученные трехмерные модели и ортофотопланы затем могут быть исследованы и сохранены для приобщения к материалам дела.

В ходе осмотров мест ДТП сотрудниками следственного отдела также использовались наземные опознавательные знаки, выставленные до фотографирования с указанием расстояния между знаками. Эти расстояния в дальнейшем использовались для контроля точности вычисленных положений и размеров объектов. Опыт показал, что при сравнении расстояний в трехмерной модели и натурно средняя ошибка составляет не более 2 см.

По нашему мнению, предлагаемая экспериментальная методика фиксации обстоятельств на месте ДТП при помощи реконструкции трехмерной модели по фотоснимкам, полученных с БПЛА, имеет ряд преимуществ по отношению к традиционным методам осмотра места ДТП, в том числе:

- результаты осмотра насыщены большей информацией;
- повышаются точность линейных измерений и полнота исследования следов;
- позволяет установить точное местоположение участников движения и пострадавших лиц, используя привязку к местности;
- более рационально используется время, отведенное для сбора данных;
- позволяет в дальнейшем производить реконструкцию места происшествия по ортофотоплану и проводить дополнительные аналитические действия;
- позволяет обнаружить и зафиксировать истинную форму, положение и протяженность тормозных следов автомобилей;
- требуется незначительное время на фотофиксацию места ДТП.

Использование БПЛА при осмотре места ДТП позволит значительно увеличить информативность и достоверность данных, собираемых на месте происшествия за счет возможности перемещения фотокамеры в плоскости, параллельной к дорожному полотну.

За полугодовой период 2022 года Следственным отделом по расследованию ДТП СУ УМВД России по Одинцовскому городскому округу в качестве эксперимента были осмотрены семь мест ДТП с применением предложенной методики. При этом следователем выполнялись все стандартные процедуры на месте происшествия, а руководителями отдела СУ производилась фотофиксация места ДТП с применением БПЛА. В протоколе осмотра места происшествия фиксировалось, что при его осмотре применялся конкретный БПЛА (указывались модель и серийный номер). Далее к протоколу осмотра места происшествия приобщался готовый ортофотоплан.

В дальнейшем по результатам проведенного расследования четырех уголовных дела, где при осмотре места ДТП применялся БПЛА, виновным в данном ДТП лицам предъявлены обвинения и уголовные дела с обвинительными заключениями направлены в Одинцовскую городскую прокуратуру. Материалы уголовного дела содержали: осмотр места происшествия; схему; фототаблицу;

ортофотоплан (результат обработки фотоматериалов с БПЛА), а также иные стандартные необходимые документы. По результатам изучения Одинцовской городской прокуратурой данных уголовных дел каких-либо замечаний не поступало и уголовные дела в порядке ст. 220 УПК РФ с утвержденными обвинительными заключениями направлены в суды для рассмотрения по существу.

Одно уголовное дело прекращено на основании п. 4 ч. 1 ст. 24 УПК РФ (в связи со смертью в данном ДТП лица). По двум материалам проверки отказано в возбуждении уголовного дела в связи с отсутствием состава преступления.

Вывод. Применение современных технологий фиксации обстоятельств на месте ДТП при помощи реконструкции трехмерной модели по фотоснимкам, полученных с БПЛА, позволит следственным органам значительно увеличить информативность и достоверность данных, собираемых на месте происшествия.

Кроме того, данная методика позволит в дальнейшем производить реконструкцию места происшествия по ортофотоплану, а следовательно, и проводить дополнительные аналитические действия.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 14.04.2023) // СПС «КонсультантПлюс».
2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 14.04.2023) // СПС «КонсультантПлюс».
3. Краснопевцев Б. В. Фотограмметрия. М. : УПП «Репрография» МИИГАиК, 2008.
4. Леоненко Р. М. О целесообразности использования беспилотных летательных аппаратов в практике осмотров мест происшествий по делам, связанным с авиакатастрофами // Вестник Московского университета МВД России. 2015. № 9. С. 105–106.
5. Осмотр места дорожно-транспортного происшествия: методические рекомендации (Материал подготовлен Следственным департаментом МВД России совместно с ФГКУ «ЭКЦ МВД России» и ГУОБДД МВД России) // Информационный бюллетень Следственного департамента МВД России. 2013. № 1 (155). С. 91.
6. Суворов Ю. Б. Судебная дорожно-транспортная экспертиза : учебное пособие (ГРИФ). М., Экзамен, Право и Закон. 2003.
7. Цыренова Е. Ж., Ангахаев А. К. Об опыте проведения СУ МВД России по Республике Бурятия осмотров мест происшествий по делам о дорожно-транспортных преступлениях // Информационный бюллетень Следственного департамента МВД России. 2017. № 3 (173). С. 104.

Худяков В. В.¹,

доцент кафедры информатики и математики

Московского университета МВД России имени В.Я. Кикотя

Владимирова В. Э.²,

курсант международно-правового факультета

Московского университета МВД России имени В.Я. Кикотя

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК ОДИН ИЗ МЕТОДОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Вопрос о сущности социальной инженерии в жизнедеятельности общества набирает свою актуальность еще с начала 70-х годов прошлого века [2, с. 1]. Многие ученые считают, что данное явление относится к способу открытого реформирования общества [1]. Действительно, первые разговоры о социальной инженерии возникли на почве возрастания информационных атак на систему телефонных операторов.

Социальная инженерия в современном мире приобрела неконтролируемый характер. Она содержит в себе комплекс методик и техник, основанных на психологическом воздействии, на поведении людей с целью получения конфиденциальной информации [5, с. 1]. Социальная инженерия имеет свою эффективность в том случае, когда возникает потенциальная возможность в совершении ошибки в действии лица, на которого направлено воздействие.

В век цифровых технологий основополагающая информация конфиденциального характера зачастую находится в смартфонах или же на мобильных компьютерах, что повышает риск стать жертвой социальной инженерии.

П. С. Швыряев изучил вопрос киберпреступлений с помощью социальной инженерии и отметил, что неконтролируемой проблемой, на которую стоит обратить внимание, являются постоянные звонки с неизвестных номеров, большая часть из которых от спамеров и мошенников [8].

Однако на практике встречаются иные виды социальной инженерии в сфере киберпреступлений, поэтому целесообразно рассмотреть основные направления социальной инженерии, которые посягаются на правоотношения в сфере компьютерной информации.

Наиболее популярное направление социальной инженерии – это массовая рассылка писем в информационной среде [6, с. 3]. Данное явление называется фишинг (Phishing), где атака направлена непосредственно на угрозу информационной безопасности.

Учитывая прогрессивный рост знаний населения в IT-сфере, киберпреступления по направлению фишинга производятся с использованием комплексных технологий: почтовой и онлайн-овой.

¹ © Худяков В. В., 2023.

² © Владимирова В. Э., 2023.

Почтовая технология имеет место тогда, когда формируется спам-сообщение, предназначенное для массового количества людей, а также содержит в себе информацию, приближенную к действительности. То есть состоит из шаблона сообщений, при этом стоит учитывать тот момент, что фишер представляется якобы от легитимной организации.

Например, благодаря фишинговому набору формируется спам-сообщение по подобию сообщения из Федеральной налоговой службы, однако различие в действительности этого письма заключается в том, что оно содержит в себе ссылку на фишинговый сайт или, иными словами, зеркальный сайт. Если лицо допускает ошибку в поведении, то переходит по прикрепленной ссылке и самостоятельно распространяет о себе личную информацию (заполняет номер карты, код, Ф.И.О.).

Онлайновая технология заключается в создании зеркального сайта, где, например, социальная инженерия будет проявляться в несуществующих товарах по низким ценам. При совершении покупки фишер получает личные данные банковских карт, после чего снимает с них денежные средства и присваивает их себе.

Стоит отметить, что фишинг содержит подвид, который называется «подводная охота». Суть заключается в том, что атака направлена на конкретные лица, где информация о пользователях становится известна благодаря социальным сетям.

Таким образом, фишинг содержит в себе два механизма реализации: первый способ выражен в непосредственном контакте с владельцем компьютерной информации, второй способ выражен в получении информации о персональных данных от третьих лиц, т. е., например, от лица, которое в силу должностных обязанностей имеет доступ к чужим данным.

Вишинг (Vishing) – еще один подвид фишинга, который использует телефонные сети для несанкционированного доступа к компьютерной информации, содержащей в себе как личные и финансовые данные [6, с. 5], так и информацию об организации, сообществах, компаниях. Уникальность данной атаки заключается в том, что используется система интерактивного голосового ответа.

Так, например, мошенник создает с помощью данной системы копию голосового сообщения Банка «ВТБ», где предлагает пользователю позвонить в свой банк по номеру для проверки информации. После чего копия системы отклоняет звонки пользователя и передает в дальнейшем звонок киберпреступнику. Метод социальной инженерии отражен в общении киберпреступника с пользователем в роли сотрудника банка.

Конечной целью злоумышленников, как правило, является получение денежных средств жертвы. Заглушая бдительность своего собеседника, преступник добивается желаемого различными способами, мошеннические схемы регулярно меняются на новые, как только перестают «работать» предыдущие [7, с. 200].

Еще один метод социальной инженерии с использованием телефонной сети является претекстинг. Суть данного направления заключается в том, что киберпреступник действует в соответствии с определенным сценарием.

Например, на телефон бабушки поступает звонок от неизвестного абонента. Киберпреступник представляется близким родственником (дочерью/сыном/

внуком) и со слезами рассказывает, что попал в аварию, находится в больнице и срочно нужны деньги. Из-за того что пожилое население зачастую слабо осведомлено о защите информационной безопасности, оно становится жертвами метода социальной инженерии таким способом.

Стоит понимать, что сценарий с использованием социальной инженерии направлен не только на определенный круг лиц, но и на внутренние ценности индивида. Для кого-то влияние будет происходить через мнимую угрозу для семьи, а для кого-то – через возникшие финансовые трудности, которых наяву нет.

Так, например, под влияние социальной инженерии попал деятель науки Виктор Фомин. Мошенники с целью завладеть его денежными средствами использовали следующий сценарий: сначала произвели звонок под видом сотрудника отдела по борьбе с экономическими преступлениями с целью осведомления об оформленном кредите. Для психологического восприятия информации использовали ложные звонки с Центрального банка Российской Федерации, а также использовали фишинг-схему, где в спам-сообщении был представлен поддельный документ с гербом и печатью, содержащий информацию о том, что профессор стал жертвой мошенников [9].

Анализируя данную схему, можно прийти к выводу, что независимо от внутренних убеждений индивида социальная инженерия оказывает колоссальное влияние на психику. Данная история завершилась тем, что жертва социальной инженерии собственноручно передал денежные средства мошенникам.

Таким образом, подтверждается тот факт, что социальная инженерия содержит в себе элемент ожидания совершения ошибки от жертвы преступления.

Киберпреступники действуют также с помощью внедрения вредоносных программ, например: вымогатель, *Qui pro quo*, «тройанский конь», «дорожное яблоко» [6, с. 6].

Первый тип вредоносного программного обеспечения зашифровывает информацию или файлы пользователя с целью выкупа у киберпреступника.

Второй тип направлен на слабые знания у пользователя в информационных технологиях. Под видом сотрудника технической поддержки киберпреступник с помощью социальной инженерии предлагает установить программу, которая в дальнейшем крадет личные данные пользователя.

Третий тип наиболее всем известен. Суть проявления социальной инженерии заложена в том, что скрытые вредоносные программы поступают от электронных почт знакомых, т. е. от надежного отправителя.

Четвертый тип основан на признаках третьего: несанкционированный доступ к компьютерной информации происходит с помощью внешнего накопителя информации, на котором есть скрытые файлы программы по передаче данных киберпреступнику.

Межсайтовый скриптинг или, иными словами, атака с помощью внедрения вредоносного кода в информационную сеть является популярной техникой среди интернет-пользователей. Киберпреступник берет за основу популярный сайт среди пользователей информационного общества, где, находя ошибку в защите веб-сайта, внедряет вредоносный код, который передает на компьютер преступника информацию о жертвах и поражает сеть пользователя сайта [4].

Анализируя действия киберпреступников, которые используют социальную инженерию в качестве метода несанкционированного доступа к компьютерной информации, выявляются следующие этапы [3]:

- 1) сбор информации (перед тем как совершить противоправное деяние, киберпреступник изучает цель с помощью открытых источников, анализирует общественные интересы);
- 2) выбор жертвы (киберпреступник легко влияет на людей, которые наиболее доверчивы или же у данных лиц есть внутренние переживания);
- 3) подготовка технического решения;
- 4) контакт; установление доверия у жертвы к киберпреступнику.

Безусловно, представление об этапах действия киберпреступника может изменяться в ходе рассмотрения конкретного воздействия, однако одно остается неизменным – влияние на жертву с помощью разных механизмов психологического воздействия.

Соответственно, для того чтобы не стать жертвой социальной инженерии, необходимо соблюдать следующие правила:

- 1) проверять источники, от которых поступила информация;
- 2) не переходить по незнакомым ссылкам;
- 3) зачастую социальная инженерия использует метод срочности, поэтому необходимо обдумывать свои действия перед тем, как их совершить;
- 4) установить антивирус, который будет блокировать несанкционированный доступ к личной информации;
- 5) необходимо следить за своим устройством и обновлять программное обеспечение;
- 6) необходимо расширять свой кругозор о новых способах совершения киберпреступлений;
- 7) не принимать телефонные звонки с подозрительных/незнакомых номеров.

Так, соблюдая банальные правила поведения, можно минимизировать шанс стать жертвой социальной инженерии.

С точки зрения профилактики, предпринимаемой государством, необходимо производить информирование граждан с помощью средств массовой информации, профилактические беседы в компаниях и организациях, закрепить обязательный факультативный предмет в образовательных учреждениях по кибербезопасности.

Список литературы

1. Волков Е. Н. Социальная инженерия: явление и его концептуализация // Вестник Нижегородского университета имени Н.И. Лобачевского. Серия : Социальные науки. 2014. № 3 (35). С. 96–101.
2. Грызунов В. В., Шкреба О. С. Особенности применения технологических методов в социальной инженерии // Техничко-технологические проблемы сервиса. 2018. № 4 (46). С. 90–94.
3. Ламинина О. Г. Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки. 2017. № 2. С. 21–23.

4. Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2020. № 4 (135). С. 135–141.
5. Полуэктова Е. В. Социальная инженерия как совокупность способов и приемов злоумышленного нарушения внутриобъектового режима компании // Инновации и инвестиции. 2018. № 2. С. 260–264.
6. Уникович А. С. Социальная инженерия и кибербезопасность: виктимологический аспект // Психопедагогика в правоохранительных органах : научно-практический журнал. 2021. № 3 (86). С. 346–352.
7. Худяков В. В., Черкасов Р. И. Телефонное мошенничество. Бдительность – залог защищенности // International Law Journal. 2022. Т. 5. № 8. С. 199–203.
8. Швыряев П. С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. Электронный вестник. 2021. № 89. С. 184–196.
9. Mash, новостной портал // URL: <https://mash.ru/news/167503>.
10. Агаев М. М., Куриленко Ю. А. Виды фишинговых атак и способы противодействия // Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел : Сборник материалов Всероссийской научно-теоретической конференции, Ростов-на-Дону, 22 апреля 2022 г. Ростов н/Д : Ростовский юридический институт Министерства внутренних дел Российской Федерации, 2022. С. 95–98.

Кучина А. М.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Булгаков В. Г.,

начальник кафедры естественнонаучных дисциплин

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук, доцент

МАТЕМАТИЧЕСКИЕ МЕТОДЫ АВТОМАТИЗИРОВАННОГО РАСПОЗНАВАНИЯ ДИНАМИЧЕСКИХ ПРИЗНАКОВ ЧЕЛОВЕКА

В настоящее время научные исследования в области математических методов автоматизированного распознавания динамических признаков человека приобретают все большее значение. Новейшие технологии позволяют собирать и анализировать данные о динамических признаках человека, таких как тон голоса, пульс, мимика и многие другие. Эти методы обработки данных могут иметь широкий спектр применений, включая медицину, психологию, безопасность и другие области.

Развитие компьютерных технологий уже сегодня раскрывает значительный потенциал вычисления соотношений при осуществлении фотографической и видеопортретной идентификации [2].

Области применения математических методов автоматизированного распознавания ДПЧ:

1. Тон голоса является одним из самых эффективных динамических признаков для распознавания эмоционального состояния человека. Существуют модели машинного обучения, опирающиеся на данные о тоне и интонации голоса, которые могут использоваться для выявления эмоционального состояния человека, например, нейтральность, радость или гнев. Например, частотный анализ (дает возможность прослушать голос на различных частотах и определить его основную частоту) и анализ формант (обычно они отмечаются на спектрограмме звука как ярко выделенные участки), которые указывают на тональность голоса.

2. Другим эффективным динамическим признаком является мимическая мускулатура. Данные об этом признаке могут быть использованы для выявления состояний человека, таких как улыбка, грусть, удивление или страх. Существуют методы компьютерного зрения, позволяющие распознавать мимическую мускулатуру и преобразовывать ее в цифровой формат. В этих методах применяется использование методов компьютерного зрения и глубокого обучения,

¹ © Кучина А. М., 2023.

чтобы определить расположение краев и дескрипторы лица, а также другие характеристики, такие как мимика и глазные движения. Эти параметры затем анализируются, чтобы определить настроение и эмоцию человека. Такой функцией обладает Realeyes, который построен на самой передовой технологии кодирования лиц и машинного обучения (ML), чтобы предоставить точную оценку внимания и эмоциональной реакции. Она используется для измерения мимики при помощи набора камер, расположенных вокруг юбки или окуляра, которые захватывают изображения глаз. Этот подход позволяет определить настроение и эмоции, выражаемые глазами, которые являются ключевым элементом мимики.

3. В безопасности правоохранительных органах математические методы для автоматизированного распознавания динамических признаков могут быть использованы для идентификации лжецов или людей, находящихся под воздействием стимуляторов. Что позволяет быстро распознать человека, который может представлять потенциальную угрозу. Такой программой является система, запущенная японской компанией NEC, позволяет идентифицировать людей с высокой точностью, даже если они скрывают лицо под маской. Алгоритм проверяет открытые части лица, включая глаза, и, по словам представителей компании, результат производится за менее чем 1 секунду с точностью более 99,9 %.

Математические методы анализа ДПЧ могут быть использованы для поддержки полиции и улучшения ее эффективности в борьбе с преступностью. Один из основных способов применения математических методов распознавания ДПЧ – это анализ видеоматериала с камер на улицах и в общественных местах. Множество различных признаков могут быть обнаружены на видеоматериалах, такие как движения и положения тела, мимика, голос, тон, интонации и другие. Существует множество подходов, главным из которых является использование методов глубокого обучения, чтобы создать модели, позволяющие анализировать ДПЧ и выявлять наиболее важные и характерные признаки.

Возможные области применения математических методов анализа ДПЧ в правоохранительных органах:

1. Использование методов распознавания ДПЧ может существенно увеличить производительность полиции. Обработка видеоматериала может отнимать много времени, и сотрудники полиции не обладают экспертным опытом и компетентностью по распознаванию ДПЧ. Методы автоматизированного распознавания ДПЧ могут сэкономить время и снизить производственные затраты полиции. Автоматизация процессов обработки и анализа ДПЧ позволяет сводить время и ресурсы, а также приводит к получению более точных и объективных данных. Это облегчает и ускоряет работу полиции и позволяет более быстро раскрывать преступления.

2. Кроме того, одним из методов из применений распознавания ДПЧ является идентификация личностей на месте происшествия. Это может помочь полиции в установлении личности потерпевшего, свидетеля или подозреваемого. Методы распознавания ДПЧ могут идентифицировать голоса, мимику и другие физические и эмоциональные признаки, что может помочь выявить лжесвидетелей, принять быстрое и точное решение на месте происшествия, а также могут

быть использованы для обнаружения преступлений и их расследования. Это может быть важным фактором в решении уголовных дел.

3. Существующие методы распознавания ДПЧ также могут быть использованы для обнаружения поведения, которые могут указывать на преступление или другие степени опасности.

4. Методы распознавания ДПЧ также могут использоваться для выявления идентичности свидетелей. Когда сотрудники полиции имеют только описание свидетеля, они могут использовать информацию о признаках, поведении и других динамических признаках, чтобы быстро выявить его личность и получить дополнительную информацию, которая может помочь в расследовании.

5. Результаты анализа ДПЧ могут использоваться в качестве доказательств в судебных процессах, которые особенно важны для правоохранительных органов. Методы автоматизированного распознавания ДПЧ могут использоваться для хранения информации о признаках человека и поведения на различных стадиях расследования. Это позволяет поддерживать связь между определенными событиями, а также помогает в построении цепочки событий, что значительно ускоряет процесс расследования.

В заключение можно сказать, что математические методы автоматизированного распознавания динамических признаков человека являются важным инструментом для полиции в борьбе с преступностью. Они позволяют снизить количество преступлений и улучшить эффективность работы полиции в расследовании подвижности преступлений. Это означает, что применение технологий распознавания ДПЧ будет иметь существенное влияние на создание более безопасного общества в будущем.

Список литературы

1. Иваницкий М. Ф. Движения человеческого тела (Анатомические очерки). М. : Физкультура и спорт, 1938.
2. Подволоцкий И. Н. Особенности использования математических методов при сравнении признаков внешности человека // URL: http://www.proexpertizu.ru/theory_and_practice/portret/729/.
3. Гросс Г. Руководство к расследованию преступлений. М.: Изд-во НКВД РСФСР, 1930. С. 60, 70–76.
4. Шаова Т. Г., Исмадова Т. И. Классификация элементов и признаков внешности человека // Вестник криминалистики. Вып. 1 (5). М. : Спарк, 2003. С. 64–71.
5. Realeyes запускает Предварительный просмотр, усовершенствованную систему измерения и прогнозирования внимания // URL: https://translated.turbopages.org/proxy_u/en-ru.ru.6c60b395-644e5760-f989e8de-74722d776562/https/www.yahoo.com/now/realeyes-launches-preview-advanced-attention-140100581.html.

Каримов А. К.¹,
*начальник отдела снабжения
компьютерной и инновационной техникой
ООО «Крилак Спецстрой»*

ОТДЕЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ВНУТРЕННИМ НАРУШИТЕЛЯМ НА ПРЕДПРИЯТИЯХ

Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации путем уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты указанной информации может осуществляться сотрудником эксплуатирующей организации, т. е. инсайдером.

Крупные промышленные 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. То есть 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 становятся 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 име-

¹ © Каримов А. К., 2023.

ют представление о системе управления информационной безопасностью организации [3, с. 234].

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, т. е. 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 [2, с. 36].

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) [3, с. 89].

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 счете 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.

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 [4, с. 189].

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 [5, с. 234].

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 решать методологическую задачу представления этой информации в виде, позволяющем использовать ее в оперативно-разыскной и процессуальной деятельности и квалифицировать как определенное правонарушение или преступление.

Говоря о математическом моделировании рассматриваемых процессов, необходимо отметить, что Математическая модель – это математическое уравнение или система уравнений, которая описывает внутренние принципы процесса, происходящего в системе с точки зрения данного исследования.

Большинство взаимодействующих систем в реальном мире слишком сложны, чтобы моделировать их полностью. Следовательно, первый уровень компромисса заключается в определении наиболее важных частей системы. Они будут включены в модель, остальные будут исключены.

Второй уровень компромисса касается объема математических манипуляций. Хотя математика обладает потенциалом для доказательства общих результатов, эти результаты критически зависят от формы используемых уравнений. Использование компьютеров для обработки уравнений модели может никогда не привести к результатам, но оно гораздо более устойчиво к изменениям.

Математическое моделирование может быть использовано по ряду различных причин. Насколько хорошо достигается какая-либо конкретная цель, зависит от состояния знаний о системе.

Примерами диапазона целей являются:

1. Развитие научного понимания через количественное выражение текущих знаний о системе.
2. Проверка эффекта изменений в системе.
3. Помощь в принятии решений, в том числе тактических решений руководителей, стратегические решения планировщиков. При изучении моделей полезно определить широкие категории моделей. Классификация отдельных моделей по этим категориям сразу же говорит нам о некоторых существенных чертах их структуры.

Одно разделение между моделями основано на типе результата, который они предсказывают. Детерминированные модели игнорируют случайные вариации и поэтому всегда предсказывают один и тот же результат с заданной начальной точки. С другой стороны, модель может носить более статистический характер и поэтому может предсказывать распределение возможных результатов. Такие модели называются стохастическими.

Второй метод различения типов моделей заключается в рассмотрении уровня понимания, на котором основана модель. Самое простое объяснение состоит

в том, чтобы рассмотреть иерархию организационных структур в моделируемой системе. Этапы моделирования полезно разделить на четыре широкие категории деятельности, а именно создание, изучение, тестирование и использование.

Важно понимать, что поведение модели может быть описано двумя способами. Качественное описание дает ответ на вопросы о том, «как», в то время как количественное описание отвечает на вопросы о том, «сколько». В целом качественное поведение будет одинаковым для целых семейств моделей и, следовательно, поддается общим результатам. Это заметно контрастирует с количественным поведением, которое часто имеет отношение только к отдельным обстоятельствам.

Качественное поведение моделей, вероятно, будет демонстрировать большее разнообразие, чем соответствующие детерминированные модели. Например, различные реализации стохастической модели популяции могут демонстрировать экспоненциальный рост и спад. Поэтому в случае стохастических моделей важно не только описать среднее поведение, но и описать диапазон типов поведения.

Выделяют следующие основные методы математического моделирования: аналитические; имитационные; эмпирико-статистические; модели, в которых в той или иной форме представлены идеи искусственного интеллекта.

Аналитические модели – это математические модели, которые имеют решение в замкнутой форме, т. е. решение уравнений, используемых для описания изменений в системе, может быть выражено в виде математической аналитической функции.

Аналитическая модель носит количественный характер и используется для ответа на конкретный вопрос или принятия конкретного проектного решения. Различные аналитические модели используются для рассмотрения различных аспектов системы, таких как ее производительность, надежность или массовые свойства. Аналитические модели должны быть выражены с достаточной точностью, чтобы их можно было формально проанализировать, что обычно делается с помощью компьютера. Проверка модели необходима для того, чтобы аналитическая модель была хорошо сформирована, чтобы она могла надежно поддерживать анализ.

Аналитические модели могут быть дополнительно классифицированы как статические или динамические. Статическая модель представляет свойства системы, которые не зависят от времени или верны для любого момента времени. Простой пример – вычисление массы системы из массы ее частей или вычисление статических геометрических свойств системы, таких как ее длина или объем. Массовые или геометрические соотношения могут меняться со временем, но вычисление дается для одного момента времени. Анализируемые свойства могут иметь детерминированные значения или могут включать распределения вероятностей по их значениям.

Динамическая модель – это аналитическая модель, которая представляет изменяющееся во времени состояние системы, такое как ее ускорение, скорость и положение в зависимости от времени. Выбор динамической модели по сравнению со статической моделью зависит от типа вопроса, на который дается ответ.

Методичное формирование структурно-симуляционного прогнозирования и его использование в криминальных социальных системах разрешило сконструировать представления о новой направленности в компьютерном прогнозировании, которое разрешено именовать объектно-структурным прогнозированием.

Объектно-структурное моделирование является последовательным развитием метода структурно-имитационного моделирования. На пути к глубинному общественному, уголовному праву методология структурного имитационного моделирования нуждается в дополнительном развитии.

В криминальных социальных системах и действиях первичными структурными веществами, до этого только, считаются эти объекты как люди. Надлежит подметить, будто эти составляющие—объекты как люди имеют все шансы обладать полностью установленный нрав взаимосвязей.

Выбор методов моделирования зависит от конкретной задачи и вашего набора данных. Данные могут быть вашим самым ценным инструментом. Таким образом, выбор правильных методов анализа данных может стать решающим моментом при прогнозировании преступлений.

Целью анализа чувствительности являются изменение параметров модели и оценка связанных с изменениями в результатах модели. Этот метод особенно полезен для выявления слабых мест модели. Затем они могут быть усилены экспериментами или просто отмечены и приняты с осторожностью в любом применении. Если модель особенно проста, возможно, удастся дифференцировать результат по каждому параметру в свою очередь. Производные дают точную скорость изменения прогнозов относительно параметров. При использовании более сложных моделей лучше избегать дифференцирования и применять численные методы.

Оценка сложных моделей часто может занять много компьютерного времени. Когда модель приходится оценивать повторно, мы можем допустить некоторую потерю точности в оценке, если это сократит время, затрачиваемое на оценку. Очевидно, что требуется разумное приближение к модели, но когда мы вспомним, что сама модель является только приближением, мы поймем, что небольшая потеря деталей не должна сильно беспокоить, если она достаточно ускоряет вычисления.

Необходимо разработать некоторое приближение, упростив или обобщив модель математически. Все более распространенным примером этого является использование так называемых уравнений замыкания для обобщения статистики стохастической модели. Поскольку уравнения замыкания являются дифференциальными уравнениями (приближенные), результаты многих стохастических симуляций получаются при стоимости, примерно равной одному запуску детерминированной модели.

Альтернативный подход является как простым, так и более общим, но может противоречить сути. Нужно провести эксперимент, в котором из модели будут получены прогнозы для тщательно выбранных значений управляющих переменных. Дальше рассмотреть результаты разработанного эксперимента и подгонять к нему эмпирическую поверхность отклика. Использовать подогнанную поверхность для оценки результатов модели правонарушителя инсайдера в будущем.

Список литературы

1. Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс».
2. Гончар В. В., Орлова А. А. Особенности расследования преступлений, совершаемых в сфере информационных технологий // Безопасность бизнеса. М., 2021. С. 25–29.
3. Смирнов Д. В. Методы поиска признаков инсайдера в BIG DATA : дис. ... канд. тех. наук. М., 2021.
4. Мешков М.В., Есина А.С., Гончар В.В. и др. Предварительное следствие в органах внутренних дел : учебное пособие. М. : Московский университет МВД России, 2007.
5. Предварительное следствие в органах внутренних дел : учебник / [М. В. Мешков и др.]. М. : Юнити-Дана, 2021.

Поташов М. Р.¹,

старший преподаватель

кафедры технико-криминалистического обеспечения

экспертных исследований

учебно-научного комплекса судебной экспертизы

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук

О ВОЗМОЖНОСТЯХ ИСПОЛЬЗОВАНИЯ ЛИНЕЙКИ ПРОГРАММНЫХ ПРОДУКТОВ «АИПСИН» В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

С каждым днем растет количество преступлений, совершаемых с использованием современных информационных технологий. Преступные сообщества активно пользуются достижениями научно-технического прогресса в целях сокрытия незаконной деятельности и расширения сфер влияния. Особенно активно такие технологии используются при совершении мошенничества и незаконного оборота наркотиков. Очевидно, что борьба с организованной преступностью невозможна без внедрения в служебную деятельность органов внутренних дел передовых технологий, призванных эффективно справляться с совершенствующимися день ото дня возможностями представителей организованной преступности.

Одной из самых востребованных линеек, предназначенных для информационной поддержки экспертных подразделений органов внутренних дел, является семейство продуктов «АИПСИН». Данная система является, по сути, уникальным продуктом на всем постсоветском пространстве и в текущий момент времени не имеет аналогов. Разработчиками «АИПСИН» непрерывно проводится научно-исследовательская работа с ведущими научными, образовательными и экспертными институтами на территории России, Белоруссии и стран СНГ.

Линейка продуктов «АИПСИН» позволяет решать целый комплекс задач, включающий в себя:

- совершенствование теоретической подготовки экспертов;
- создание программного обеспечения для нужд конкретного заказчика;
- квалифицированная экспертная помощь в разработке нормативных правовых актов;
- формирование специализированных баз данных;
- разработка методик исследования веществ и др.

Среди перспективных продуктов «АИПСИН» являются программные комплексы:

- «АИПСИН Культурные ценности» – продукт, предназначенный для организации мер по предотвращению незаконного вывоза за границу предметов, представляющих не только культурную, художественную или историческую ценность, но и являющихся национальным достоянием;

¹ © Поташов М. Р., 2023.

– «АИПСИН Взрывчатка» – продукт, предназначенный для идентификации и анализа взрывчатых веществ и боеприпасов. Система позволяет установить тип и состав взрывчатого вещества. Позволяет оценить груз, проходящий через границу, на наличие веществ, которые могут служить компонентами для изготовления взрывчатых веществ. Автоматизирует процесс идентификации боеприпасов и взрывчатых веществ, многократно ускоряя работу контрольных органов и устраняя ошибки, связанные с человеческим фактором;

– «АИПСИН Алкоголь» – продукт предназначен для идентификации и анализа алкогольной продукции, изучение ее качества, определения фальсификации различного уровня, определение соответствия заявленному наименованию. Призван облегчить процедуру производства и реализации готовой продукции, снизить риски использования некачественного сырья и готовой продукции, выявить риски на данном рынке и прочее.

Несмотря на наличие широкой линейки продуктов, самым востребованным в органах внутренних дел является программный комплекс «АИПСИН АнтиНаркотики», который представляет собой многоцелевой комплекс, представленный как в локальной, так и в сетевой версиях, используемый правоохранительными органами Республики Беларусь, Российской Федерации и стран ЕАЭС. Система предоставляет уникальные, не имеющие аналогов среди производителей программного обеспечения и баз данных возможности определения наркотических и психотропных веществ, их метаболитов и прекурсоров.

В базе данных комплекса представлено описание свыше 40 тысяч веществ, хотя в списке запрещенных, ограниченных и контролируемых веществ их не более 600 [1]; собрано свыше 3 тысяч аналитических методик исследования; количество представленных масс-спектров веществ превышает 30 тысяч; массив литературных источников исчисляется десятками тысяч, коллекция приведенных синонимов веществ более 300 тысяч, кроме того, представлены фотографические изображения свыше 45 тысяч подконтрольных объектов. Уникальность «АИПСИН АнтиНаркотики» состоит в том, что система содержит набор информационных модулей в сочетании со специальными поисковыми механизмами и многоуровневыми запросами. Его интеллектуальная поисковая система выполняет поиск, выбирает и отображает необходимую информацию, а также проверяет актуальность путем сравнения экспериментальных данных с информацией, содержащейся в более чем ста отдельных базах данных. Структура «АИПСИН» предусматривает, помимо прочего, подключение внешних каналов информации, в том числе от аналитического оборудования.

Сетевая версия «АИПСИН АнтиНаркотики» автоматически уведомляет в пределах разрешенного доступа о задержаниях, предметах, веществах, способах транспортировки и т. д. запрещенных веществ, собирает, обменивает, хранит и анализирует экспертную информацию с выходом на «профилирование объектов». Система «АИПСИН АнтиНаркотики», по сути, огромный, постоянно пополняемый массив данных, включающий в себя:

– базу библиотек масс-спектров неконтролируемых психоактивных веществах, которые имеют серьезную потенциальную опасность;

- возможность установления статуса контроля вещества и автоматического формирования всей имеющейся информации по веществу;
- возможность извлечения и идентификации спектров искомых веществ в присутствии высокого фонового сигнала и обработки хроматограмм с различным расширением;
- установление статуса контроля вещества по структурной формуле;
- отнесение рассматриваемого вещества к производному наркотического средства или психотропного вещества в соответствии с критериями отнесения к этим производным;
- возможность получения справочной информации начиная от химических свойств, заканчивая синтезом по всем известным наркотическим средствам, психотропным веществам и их прекурсорам [2].

В условиях развития информационных технологий, «АИПСИН АнтиНаркотики» является, по сути, безальтернативным программным продуктом, позволяющим в кратчайшие сроки выявлять и идентифицировать имеющиеся в незаконном обороте вещества, при этом сводя вероятность ошибок, связанных с человеческим фактором, практически до нуля.

Список литературы

1. Постановление Правительства Российской Федерации от 30 июня 1998 г. № 681 «Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации» (ред. от 15.05.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_19243/ (дата обращения: 26.03.2023).
2. Официальный сайт АИПСИН. <https://aipsin.com/aipsinfamily/> (дата обращения: 26.03.2023)

Баранова А. А.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Толстых М. Ю.,

доцент кафедры специальных информационных технологий

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук

ФЕЙКОВЫЕ СООБЩЕНИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном мире с высокой скоростью разрабатываются новые технологии и расширяется информационное пространство. Вместе с их ростом общество сталкивается с такой проблемой, как распространение фейковой² информации. Стремительное продвижение такого вида информации происходит в первую очередь в глобальной сети Интернет посредством мессенджеров и социальных сетей, что является неотъемлемой частью жизни каждого современного человека, обладающего различными гаджетами (компьютерами, планшетами, смартфонами и т. п.).

Использование цифровых инструментов для информирования людей и активизации гражданского обсуждения становится менее эффективным из-за деструктивной работы злоумышленников, которые используют социальные и цифровые платформы для создания и распространения фейков. Правовое регулирование этого явления пока не полностью разработано, но достоверность информации все еще является ключевой проблемой. Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. уделяет большое внимание формированию информационного пространства, основанного на знаниях, где гражданам предоставляется доступ к объективной, достоверной и безопасной информации [1].

Достоверная информация – это факты, подтвержденные юридическими процедурами и соответствующие действительности. Недостоверная общественно значимая информация – это сообщения, которые не соответствуют действительности и могут создать угрозу жизни и здоровью граждан. Социальные сети – распространенный источник информации, но они также стали основным источником фейковых новостей. Борьба с дезинформацией включает проверку достоверности информации перед ее распространением. Для проверки достоверности

¹ © Баранова А. А., 2023.

² Под «фейковой» информацией в данной работе понимаются сведения, которые не соответствуют действительности, т. е. лживая, ложная, фальсифицированная информация, дезинформация.

подозрительной информации можно просмотреть сведения об авторе. Нужно изучить количество сообщений/публикаций автора и активность его учетной записи. Также следует проверить другие сообщения автора на наличие деятельности ботов, которые могут публиковать сведения в любое время суток и из разных частей мира.

Emergent.Info – онлайн-инструмент, который проверяет слухи и заговоры в Интернете. Он отслеживает информацию, публикуемую на новостных сайтах, и анализирует ее, чтобы определить, является ли она достоверной или нет. Emergent.Info также отслеживает изменения, внесенные в статьи после их первой публикации.

MBFC Factchecking – веб-сайт, который проводит проверку фактов по важным политическим и другим вопросам. Он анализирует прозрачность и свободу прессы в стране происхождения и историю фактических отчетов сайта.

FakerFact – инструмент искусственного интеллекта, который оценивает цель и характеристики информации на основе рейтинговых критериев. Рейтинги включают в себя повестку дня, журналистику, мнение и сатиру.

В последнее время рост фальшивых и поддельных сообщений и новостей, распространение в медиа и социальном пространстве дезинформации критически оценивается и вынуждает научно исследовать данную ситуацию: эксперты стремятся, прежде всего, понять теоретическую значимость феномена фейковой информации, а регуляторы – осуществить ее правовую регламентацию. Несмотря на то что проблема фейковой информации признана во всем мире, эффективные методы борьбы с ней все еще нуждаются в исследовании и разработке.

Список литературы

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О стратегии развития информационной безопасности в Российской Федерации на 2017–2030» // НПП «Гарант-сервис».
2. Коробеев А. И., Жмуров Д. В. Кибервиктимология фейка: первичное досье // Вестник Томского государственного университета. 2021. № 471. С. 250–257.
3. Смирнов А. А. Глубокие фейки. Сущность и оценка потенциального влияния на национальную безопасность // Свободная мысль. 2019. № 5 (1677).
4. Шульц Э. Э. Фейковые новости в современных коммуникационных процессах // Вестник РУДН. Серия : Государственной и муниципальное управление. 2022. Т. 9. № 3. С. 262–273.
5. Манойло А. В. Фейковые новости как угроза национальной безопасности и инструмент информационного управления // Вестник московского университета. Политические науки. 2019. № 2. С. 37–44.
6. Распопова С. С., Богдан Е. Н. Фейковые новости: природа происхождения // Вестник Челябинского государственного университета. 2017. № 11 (407). С. 48–53.

Батоев В. Б.¹,
старший научный сотрудник
СТУС МВД России,
кандидат юридических наук, доцент

ИСПОЛЬЗОВАНИЕ АППАРАТНО-ПРОГРАММНОГО КОМПЛЕКСА «БЕЗОПАСНЫЙ ГОРОД» ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ

В современных условиях видеонаблюдение становится все более эффективным средством противодействия преступности. Правоохранительные органы ежедневно эффективно решают задачи по борьбе с преступностью с использованием систем видеонаблюдения [1; 2; 4; 6 и др.]. Это обусловлено тем, что видеонаблюдение в современных условиях выступает необходимым инструментом организации общественных процессов в различных направлениях. Трудно представить ситуацию, при которой видеокамеры отсутствовали бы при осуществлении контроля за деятельностью работников, технологических процессов, правил дорожного движения, при обеспечении охраны в местах массового скопления людей, на объектах транспорта и др. [3, с. 28; 5, с. 73; 7, с. 63; 8, с. 237].

Анализ практики использования систем видеонаблюдения в деятельности государственных органов показывает, что в данное время продолжается процесс создания, внедрения и использования аппаратно-программного комплекса (далее – АПК) «Безопасный город». К числу основных задач данного АПК относятся реализация комплекса мер, направленных на создание технологической основы по устранению рисков в сфере обеспечения общественного порядка и безопасности; налаживание непрерывного информационного взаимодействия информацией о состоянии природных, технологических и иных условий; проведение мониторинговых мероприятий и др., а также решение задач по выявлению и раскрытию преступлений и административных правонарушений в рамках функционирования правоохранительного сегмента (далее – ПС) данного АПК.

Об эффективности использования ПС АПК «Безопасный город» могут свидетельствовать обобщенные статистические данные Главного информационно-аналитического центра МВД России.

По данным ГИАЦ МВД России, на территории Российской Федерации в 2022 г. всего было зафиксировано с помощью АПК «Безопасный город» 97 470 132 преступлений и административных правонарушений, которые более наглядно представлены в табл. 1.

¹ © Батоев В. Б., 2023.

Таблица 1

**Количество преступлений и административных правонарушений,
зафиксированных с использованием АПК «Безопасный город»**

Федеральный округ	Количество преступлений и административных правонарушений	В том числе с использованием	
		Систем видеонаблюдения	Комплексов ЦАФАП
ЦФО	62 020 144	8 145	61 763 322
СЗФО	4 048 561	6 575	4 041 606
СКФО	6 211 918	3 781	6 208 132
ЮФО	2 523 992	6 353	2 517 634
ПФО	8 014 908	7 099	8 004 775
УФО	3 752 644	2 119	3 747 439
СФО	8 486 534	3 459	8 483 073
ДВФО	2 411 431	1 249	2 410 174
Всего по России	97 470 132	38 780	97 176 155

Представленные данные в зависимости от количества фактов регистрации противоправных деяний могут указывать на необходимость дальнейшего развития и внедрения АПК «Безопасный город» в регионах Российской Федерации. Обращает на себя внимание лидирующие позиции, которые занимают регионы из Центрального федерального округа.

Далее предлагаем рассмотреть количественно-качественные показатели использования АПК «Безопасный город» при раскрытии преступлений, которые представлены в табл. 2.

Таблица 2

**Количество преступлений,
раскрытых с использованием ПС АПК «Безопасный город»**

Федеральный округ	Количество раскрытых преступлений	Количество преступлений, по которым лица, их совершившие, были задержаны в результате их отслеживания по системе ПС АПК «Безопасный город» по результатам онлайн-просмотра	Количество преступлений, по которым лица, их совершившие, были задержаны на месте преступления по информации из АПК «Безопасный город»
ЦФО	13 144	9	108
СЗФО	5 182	290	245
СКФО	37	7	0
ЮФО	372	0	0
ПФО	1 661	8	2
УФО	684	21	0
СФО	486	10	0
ДВФО	569	2	0
Всего по России	22 135	347	355

Изучение данных из представленной таблицы указывают на необходимость не только повсеместного оснащения субъектов Российской Федерации системами видеонаблюдения АПК «Безопасный город», но и приведения условий его

эксплуатации к современным техническим реалиям. Иными словами, использование АПК «Безопасный город» необходимо синхронизировать с технологиями искусственного интеллекта, технологиями биометрической идентификации и др.

Таким образом, вопросы создания, внедрения и развития АПК «Безопасный город» требуют принятия дальнейших мер по расширению сферы использования. Безусловно, такие меры потребуют привлечения дополнительных финансовых и материальных затрат со стороны всех задействованных в этом субъектов, что в итоге позволит создать базовые условия для формирования соответствующего уровня информационного обеспечения деятельности правоохранительных органов при решении задач борьбы с преступностью.

Список литературы

1. Гришаков А. Г. Деятельность участкового уполномоченного полиции по профилактике административных правонарушений и раскрытию преступлений с использованием систем видеонаблюдения // Алтайский юридический вестник. 2019. № 1 (25). С. 39–43.
2. Долженко Н. И. Использование видеонаблюдения в расследовании преступлений // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2018. № 6 (97). С. 117–119.
3. Жвалевич С. Н., Токарев А. Ю. О некоторых вопросах использования систем видеонаблюдения в профилактике и раскрытии преступлений // В книге: Актуальные проблемы предупреждения и раскрытия имущественных преступлений. Тезисы докладов республиканского научно-практического семинара. Редакция: Ю. П. Шкаплеров [и др.]. 2014. С. 28–29.
4. Жихорев В.С. Тактика получения доказательственной информации с систем видеонаблюдения при расследовании преступлений, совершаемых на улице // В сборнике : Международная научно-практическая конференция «Преступность в СНГ: проблемы предупреждения и раскрытия преступлений». сборник материалов. 2019. С. 196–198.
5. Кисляков С. В. Использование информации с камер видеонаблюдения на первоначальном этапе расследования дорожно-транспортного преступления // Академическая мысль. 2018. № 2 (3). С. 72–74.
6. Майорова О. В. Использование изображений, полученных с камер видеонаблюдения, в ходе расследования и раскрытия преступлений // Академическая мысль. 2020. № 1 (10). С. 72–74.
7. Майорова О. В., Каримова И. А. Проблемы использования видеоизображений лиц, полученных с камер видеонаблюдения, в ходе расследования и раскрытия преступлений // Энциклопедия судебной экспертизы. 2019. № 4 (23). С. 63–71.
8. Шашкова И. А. Пределы допустимого вмешательства в частную жизнь посредством использования камер видеонаблюдения в целях раскрытия преступлений // В сборнике : Уголовно-процессуальный кодекс Российской Федерации: достижения и проблемы применения. Сборник научных статей V Международной студенческой научно-практической конференции. Юго-Западный государственный университет. 2019. С. 236–241.

Данилова Е. А.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

ЭВОЛЮЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ И ИХ ВЛИЯНИЕ НА СОВРЕМЕННЫЕ МОДЕЛИ БЕЗОПАСНОСТИ

Вредоносное программное обеспечение – один из наиболее распространенных методов, используемых киберпреступниками для проникновения в компьютерные системы и компрометации их. История возникновения вредоносных программ восходит к 1971 году, когда программист Боб Томас создал первый известный компьютерный вирус «Creeper». По мере того, как персональные компьютеры становились все более доступными и набирали популярность, появлялись все новые и новые вредоносные программы.

В 90-х годах прошлого века с развитием сети Интернет началась новая эра вредоносного программного обеспечения, они перестают быть безобидными и начинают делиться на виды в зависимости от принципов функционирования.

Одним из наиболее известных стали черви, и если первые черви создавались в качестве экспериментов, то современные – предназначены за редким исключением для вредоносных целей. Черви используют уязвимости популярных программ, применяя сетевые протоколы для своего распространения.

Еще одним видом вредоносного программного обеспечения стали макровирусы. Их отличительной особенностью стало то, что они должны не только попасть на компьютер пользователя, но и быть запущены им.

Шпионские программы появились в начале 2000-х годов на фоне растущего использования сети Интернет. Они часто поставлялись в комплекте с другим программным обеспечением, обычно в результате бесплатных или условно-бесплатных загрузок. В дистрибутиве с полезным программным обеспечением содержалось и вредоносное, они распаковывались и устанавливались одновременно. Современные шпионские программы расширили свой функционал, они могут отслеживать действия пользователей в социальных сетях, приложениях для обмена сообщениями, а также заражение может происходить без непосредственного физического доступа.

Программы-вымогатели. Они обычно распространяются через электронную почту. Заражение происходит в тот момент, когда пользователь откры-

¹ © Данилова Е. А., 2023.

вает вложенный zip-файл. После активизации вредоносного программного кода троян «садится» в память компьютера, а дальше сохраняет себя в папку с профилем пользователя (AppData, LocalAppData) и добавляет ключ в реестр для того, чтобы гарантировать запуск программы при каждом включении компьютера.

Эволюция вредоносных программ за последнее столетие была постоянной проблемой для специалистов по компьютерной безопасности. С первых дней существования вируса и до современных атак программ-вымогателей. Авторы вредоносных программ постоянно внедряют инновации, чтобы опережать меры безопасности, а развитие искусственного интеллекта и машинного обучения дало им новые инструменты для создания более эффективных и целенаправленных атак.

Список литературы

1. Борисов М. А., Заводцев И. В., Чижов И. В. Основы программно-аппаратной защиты информации : учебное пособие, изд. 3-е, перераб. и доп. М. : ЛЕНАНД, 2014. URL: http://artlib.osu.ru/web/books/content_all/842.pdf?ysclid=lg10n3c5vx121729830 (дата обращения: 07.04.2023).
2. Исаев А. Р. Компьютерные вирусы как площадка для киберпреступлений и шпионажа. 2016. № 10. С. 99–110. URL: <https://www.elibrary.ru/item.asp?id=27541476>.
3. Красноярчук В. И. Из истории появления первых компьютерных вирусов. Сборник трудов конференций : III Национальной научно-практической конференции ; Керчь, 2021. С. 456–460. URL: <https://www.elibrary.ru/item.asp?id=47308829> (дата обращения: 07.04.2023).
4. Цыганков И. А. Компьютерные вирусы: история, классификация, противодействие / Региональная информатика и информационная безопасность, СПб., Вып. 4. 2017. С. 369–370. URL: <https://www.elibrary.ru/item.asp?id=35276249> (дата обращения: 11.04.2023).

Клочкова Е. Н.¹,

доцент кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

УЯЗВИМОСТИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, ОСНОВАННЫХ НА ИСПОЛЬЗОВАНИИ НЕЙРОННЫХ СЕТЕЙ

В последние десятилетия происходит бурное развитие информационных технологий. То, что еще в прошлом веке считалось фантастикой, на сегодняшний день уже реализовано и активно внедряется в повседневную жизнь. Одним из популярных направлений развития информационных технологий стало создание так называемого искусственного интеллекта, реализованного с использованием нейронных сетей. В настоящее время все чаще можно слышать о том, что та или иная задача решается с помощью искусственного интеллекта или для ее решения была построена и обучена нейронная сеть.

В настоящее время существует уже огромное количество программных реализаций нейросетей, некоторые из них созданы крупными IT-компаниями, вкладывающие огромные средства в их разработку, другие – новичками, которые решили попробовать свои силы в области создания искусственного интеллекта. Области применения нейронных сетей постоянно расширяются. Среди основных задач, для решения которых сегодня используются нейронные сети, можно выделить: распознавание и обработка изображений, распознавание и синтез речи, прогнозирование, анализ различных данных, принятие решений и т. д. Алгоритмы на основе нейросетей защищают информационные системы от атак злоумышленников и помогают выявлять незаконный контент в сети.

Преимущества использования искусственного интеллекта, построенного на основе нейронных сетей, очевидны. Хорошо обученная нейросеть способна полностью концентрироваться на поставленной задаче, игнорируя постороннюю, не относящуюся к делу информацию. Она продолжает сохранять работоспособность в случае утраты отдельных элементов. Еще один несомненный плюс – это высокая скорость работы и принятия решения. Нейронной сети не нужен отдых, и чем больше она работает (т. е. в итоге обучается), тем точнее получаемые результаты. В то же время необходимо помнить, что предлагаемые решения не являются абсолютно точными, всегда существует вероятность ошибки. Поэтому возможности нейронной сети желательно использовать как дополнение к другим методам достижения поставленной цели.

Системы искусственного интеллекта, основанные на использовании нейронных сетей, все больше проникают в нашу жизнь, и поскольку они интегрируются во все большее количество отраслей, необходимо рассмотреть, на сколько они уязвимы перед различными угрозами безопасности.

¹ © Клочкова Е. Н., 2023.

Начнем с отравления данных. Для работы любой нейронной сети она должна быть обучена на качественных наборах данных. Если на этапе обучения в систему будут попадать, кроме правильных данных, также ошибочные, то это может привести к тому, что при решении реальной задачи система в некоторых случаях будет совершать грубые ошибки, последствия от которых в зависимости от системы могут быть совершенно разными.

Отличительными особенностями данной угрозы является то, что она закладывается на этапе обучения. Для ее реализации необходимо иметь доступ к данным, а также злоумышленник должен иметь представление о принципах построения нейронных сетей и способах ее обмана.

Если не считать ситуаций, когда разработчики сознательно неправильно обучают систему, то отравление данных может произойти в следующих случаях:

1. Использование данных краудсорсинг-платформ.

Создание выборки для обучения нейронной сети является длительным, дорогостоящим процессом. Для его упрощения создаются специальные платформы, на которых любой желающий может за небольшую плату поучаствовать в разметке данных. Такая разметка никогда не бывает «чистой». Большинство ошибок выявляются с использованием различных статистических методов. Но теоретически возможна ситуация сговора между несколькими разметчиками, когда они совершают одни и те же ошибки. Как результат, используемые статистические методы оказываются бессильными, и сеть обучается на неправильных данных.

2. Использование предобученных моделей.

В открытом доступе в настоящее время выложено огромное количество полуфабрикатов-архитектур нейронных сетей. Для ускорения процесса создания нейронных сетей очень часто разработчики берут такую предобученную модель, меняют последние слои под конкретные задачи, а основной массив весов при этом остается без изменений. В том случае, если изначальная модель была обучена неправильно, то и конечная модель также будет срабатывать с ошибками.

3. Порча данных при обучении в облаке.

Большие нейронные сети не могут быть обучены на обычном компьютере, поэтому некоторые разработчики используют облачные сервисы. В этом случае злоумышленник может получить несанкционированный доступ к обучающим данным и модифицировать их.

Еще одна угроза безопасности интеллектуальных систем, основанных на использовании нейронных сетей, связана с реализацией атаки на уклонение. Основная цель реализации угрозы: заставить сеть выдавать неверные ответы в определенных ситуациях. Атаки уклонением можно делить на разные группы: по желаемому ответу, по доступности модели и по способу подбора помех.

Как известно, восприятие информации человеком и нейронной сетью различается. Зачастую два изображения визуально одинаковые для человека, трактуются сетью совершенно по-разному. При реализации атаки на уклонение перед злоумышленником стоит цель ввести в заблуждение сеть, чтобы она воспринимала объект по-другому, а человек при этом никакой разницы не замечал.

До текущего момента при рассматривании существующих угроз нами делалось предположение, что основная цель, стоящая перед злоумышленником,

заклучалась в нарушении работоспособности модели путем различных манипуляций над данными. Но существует и другой аспект, на который необходимо обратить внимание. Для того чтобы модель эффективно работала, она должна быть хорошо обучена, и учить ее лучше всего на реальных данных. Поскольку в настоящее время системы искусственного интеллекта, основанные на нейронных сетях, используются в различных отраслях, то «обучающие» примеры представляют ценность своим количеством содержащейся в них информации.

Если рассматривать угрозы безопасности с этой точки зрения, то возможны реализации следующих видов атак: атака на установление принадлежности и атака путем инверсии модели.

Атака установления принадлежности предполагает, что злоумышленник пытается определить, применялись ли конкретные данные для обучения модели. Угроза здесь заключается в том, зная о наличии информации, в системе может быть предпринята попытка ее извлечения.

Атака путем инверсии модели предполагает также получение обучающих данных из обученной модели. При таком виде атаки используют возможности, предоставляемые реализацией обработки последовательностей в запросах. В том случае, если в обучающей выборке содержались какие-либо персональные данные, то в момент написания запроса они могут отобразиться в автодополнении.

В заключение хотелось бы отметить, что системы искусственного интеллекта, основанные на нейронных сетях, пока еще очень молоды. Область их применения быстро расширяется, и можно предположить, что в ближайшие годы таких систем станет значительно больше, они станут «умнее», начнут решать все более сложные задачи, количество, содержащейся в них информации, будет возрастать. И если разработчиков в настоящее время интересуют зачастую только технические решения вопросов, то злоумышленников – открывающиеся возможности, поэтому о безопасности таких систем необходимо задумываться уже сейчас.

Список литературы

1. Насколько уязвим искусственный интеллект? // URL: <https://habr.com/ru/company/smartengines/blog/528686/>.
2. Нейронные сети: практическое применение // URL: <https://habr.com/ru/post/322392/>.
3. Обзор уязвимостей нейронных сетей // URL: <https://d-russia.ru/obzor-ujazvimostej-nejronnyh-setej.html>.

Клочкова А. М.¹,
студент кафедры
цифровых технологий и информационных систем
Московского авиационного института
(национальный исследовательский университет)

Максимов Н. А.²,
доцент кафедры
цифровых технологий и информационных систем
Московского авиационного института
(национальный исследовательский университет),
кандидат технических наук, доцент

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ЗАЩИЩЕННОЙ, КИБЕРИМУННОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ KASPERSKY OS ДЛЯ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ МОБИЛЬНЫМ РОБОТОМ

Бурное развитие таких технологий, как машинное зрение, искусственный интеллект привело к тому, что автоматизация, которая ранее была характерна только для промышленных производств, распространяется на все новые отрасли. Пандемия также ускорила внедрение цифровых технологий во все сферы жизни. Все чаще человека заменяют роботы. Если в начале своего развития роботы отличались своей громоздкостью и ограниченным функционалом, то на текущий момент появилось огромное количество мобильных роботов, призванных выполнять широкий круг задач, таких как доставка грузов, клининг, картографирование окружающей среды и т. д. Отдельно стоящей задачей становится появление роботов, способных работать в условиях, опасных для жизни человека.

Одним из таких вариантов становится использование управляемых беспилотных аппаратов, которые могут осуществлять как мониторинг содержания токсичных веществ в атмосфере, так и поиск взрывчатых веществ с использованием дополнительного оборудования.

Мобильные роботы могут выполнять поставленные задачи либо автономно, либо полуавтономно (под управлением оператора). В зависимости от поставленной задачи автономное управление может быть предварительно запрограммировано на устройстве без наличия обратной связи об окружающей обстановке, может иметь ограниченную или очень сложную обратную связь с датчиками. Для реализации автономного управления необходима разработка большого количества алгоритмов, размещения значительного количества всевозможных датчиков. В связи со сложностью разработки и программирования создание автономного робота является достаточно дорогостоящей задачей. При этом зачастую такие роботы имеют значительные ограничения по функциональному назначению.

¹ © Клочкова А. М., 2023.

² © Максимов Н. А., 2023.

Полуавтономные роботы на сегодняшний день являются наиболее востребованными. Отличительной особенностью таких роботов является то, что, кроме задач, которые он «решает» самостоятельно, обязательно присутствуют задачи, которые контролируются человеком. Различают следующие типы управления:

- по кабелю;
- по кабелю и с применением встроенного в робот микроконтроллера;
- по Ethernet;
- при помощи ИК-пульта;
- радиоуправление;
- по Bluetooth;
- по WiFi;
- при помощи сотового телефона.

Управление по кабелю является самым простым способом, с помощью которого оператор может контролировать передвижения робота. Преимуществами таких роботов становится то, что обычно они практически не имеют электроники, очень простые, могут нести дополнительную нагрузку. В то же время основной их недостаток – это то, что передвижение ограничено длиной троса, который при этом еще может и запутаться.

Размещение на роботе микроконтроллера позволяет запрограммировать робота на более сложное поведение, позволяя в некоторых ситуациях принимать решение без непосредственного участия человека. В данном случае к недостаткам, рассмотренным выше, добавляется увеличение стоимости робота за счет дополнительной электроники.

Все остальные типы управления основаны на использовании беспроводного соединения. Преимущество которого связано с тем, что расстояние до оператора не ограничивается длиной кабеля, он уже может, находясь на значительном (безопасном) расстоянии, через систему видеонаблюдения и различные датчики контролировать и отслеживать движение, состояние робота. Исключение составляет управление при помощи ИК-пульта, где требуется прямая видимость между приемником и передатчиком для осуществления управления и управление по Bluetooth, радиус действия которого ограничен приблизительно 10 метрами.

Давая возможность увеличить расстояние между человеком и роботом, беспроводной канал связи в то же время становится одним из наиболее уязвимых элементов робототехнического комплекса. При использовании дистанционно-управляемой роботизированной техники могут возникать проблемы, связанные с необходимостью обеспечения безопасности соединения между аппаратом и оператором. Несанкционированный доступ (просмотр, подмена, перехват и подавление помехами), направленный на нарушение работоспособности робота, может привести в некоторых случаях к критическим последствиям.

В настоящее время основными методами защиты каналов беспроводной связи мобильных роботов специального назначения являются:

- криптографические методы;
- использование VPN;
- применение широкополосных сигналов;
- изменение параметров радиосигнала.

Общим недостатком криптографических методов является сложность аппаратной реализации при увеличении размерности ключа, а также наличие задержки по времени, связанной с шифрованием/дешифрованием сообщений, что может оказаться недопустимым в реальной ситуации. Для методов, основанных на применении VPN, характерны дороговизна те же недостатки, что и для криптографических методов.

Использование метода широкополосных сигналов также не лишено недостатков – это недостаточная защищенность от несанкционированного доступа, незначительное количество последовательностей и отсутствие возможности периодической смены используемых сигналов.

К общим недостаткам рассмотренных методов также следует отнести изначальное предназначение сетей для решения задач информационного обмена широкого круга пользователей, что может вызывать сложности их применения в специальных целях.

В качестве одного из возможных решений данной проблемы может быть предложено разрабатывать программное обеспечение, осуществляющее управление роботизированными устройствами с использованием защищенной, кибериммунной операционной системы Kaspersky OS.

Данная операционная система представляет из себя операционную систему, архитектурно ориентированную на системное решение проблемы киберзащиты технологических процессов. Уязвимость традиционных операционных систем связана с тем, что они проектировались без четкого представления о безопасности. Особенностью Kaspersky OS стало то, что при создании проблемы безопасности выступали в ней в качестве основополагающих.

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 заключение хотелось бы отметить, что область применения роботизированной техники постоянно и быстро расширяется, повышаются сложность и ответственность решаемых задач, поэтому задачи обеспечения защищенного взаимодействия между роботом и оператором будут выходить на первый план.

Список литературы

1. Березников Д. В., Закиев А. А., Магид Е. А. Система обеспечения автономного возвращения колесного робота при потере связи с удаленным оператором // URL: <https://cyberleninka.ru/article/n/sistema-obespecheniya-avtonomnogo-vozvrascheniya-kolyosnogo-robota-pri-potere-svyazi-s-udalennym-operatorom/viewer>.
2. Жук А. П., Осипов Д. Л., Гавришев А. А., Бурмистров В. А. Анализ методов защиты от несанкционированного доступа беспроводных каналов связи робототехнических систем // URL: <https://cyberleninka.ru/article/n/analiz-metodov-zaschity-ot-nesanktsionirovannogo-dostupa-besprovodnyh-kanalov-svyazi-robototekhnicheskikh-sistem/viewer>.
3. Жуков Р. Обзор Kaspersky IoT Secure Gateway, шлюза для построения безопасных систем интернета вещей // URL: <https://www.anti-malware.ru/reviews/Kaspersky-IoT-Secure-Gateway>.

Кондрашечкин Р. В.¹,

*доцент кафедры оперативно-разыскной деятельности ОВД
и применения информационных технологий*

Московского областного филиала

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

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Условия развития современного общества невозможно представить без использования новых технологий и технических решений, таких как искусственный интеллект, которые способны обеспечивать дальнейшее поступательное развитие общества и государства.

Прорывом в области развития информационных технологий может стать цифровое государственное управление, которое развивается под началом Правительства Российской Федерации во главе с М. В. Мишустиним, по словам которого внедрение цифровых технологий в элементы управления государством обеспечит Российской Федерации вхождение в мировую экономику как одной из лидирующих стран [1].

В научной литературе существуют различные научные подходы к пониманию технологии искусственного интеллекта (далее – ИИ).

Американский исследователь Николас Д. Райт под термином «искусственный интеллект» понимает «совокупность технологий, связанных с ИИ, например, определенный ИИ, машинное обучение, большие данные и цифровые вещи, которые вместе предоставляют мощные, широкие и новые возможности. В узком смысле ИИ представляется как анализ данных для моделирования некоторого аспекта мира, где выводы из этих моделей затем используются для прогнозирования и предвидения возможных будущих событий. Важно отметить, что программы ИИ не просто анализируют данные так, как они были изначально запрограммированы. Вместо этого они учатся на данных, чтобы разумно реагировать на новые данные и соответствующим образом адаптировать свои результаты. В конечном счете ИИ – это обеспечение компьютеризированным системам поведения, как поведения, присущего разумному человеку [2].

В научных трудах А. В. Понкин, А. И. Редькин дают свою интерпретацию ИИ, которую раскрывают как сложную кибернетическую компьютерно-программно-аппаратную систему с когнитивно-функциональной архитектурой и собственными или релевантно доступными (приданными) вычислительными мощностями, необходимых емкостей и быстродействия, которая включает в себя электронную, в том числе – виртуальную, электронно-механическую, био-электронно-механическую или гибридную функции [3].

В. А. Тирранен поясняет, что ИИ предполагается определять как свойство интеллектуальной системы, которое включает компьютерные программы и искус-

¹ © Кондрашечкин Р. В., 2023.

ственные нейронные сети, выполняющие функции и решающие задачи, в том числе специально не оговоренные, которые могут самообучаться и адаптировать свое поведение под воспринимаемые внешние условия, а также способные принимать решения исходя из условий и поставленных целей [4].

Новые технологии также разрабатываются и внедряются в деятельности правоохранительных органов в целях противодействия преступности. Искусственный интеллект хорошо справляется с распознаванием закономерностей и аномалий, поэтому может быть надежным инструментом обнаружения угроз.

Известный российский ученый С. С. Овчинский справедливо утверждал, применение современных информационных технологий должно поднять оперативно-разыскную и разведывательную деятельность правоохранительных органов на новый качественный уровень. Это должно найти выражение в формировании новых эффективных подходов в борьбе с организованной преступностью и в противодействии преступности как в сфере «высоких технологий» так и в информационных сферах [5].

В. С. Овчинский и Е. С. Ларина под ИИ понимают вычислительную платформу для выполнения конкретных, заранее заданных функций и решения задач. Это может быть некое устройство превращения любой – визуальной, акустической, текстовой и т. п. – информации к цифровому виду, с последующей обработкой этой цифровой информации методами статистики и дискретной вычислительной математики и получение ответа в интуитивно понятном для человека виде. Именно ИИ является основой для сбора, хранения и обработки информации [6].

На наш взгляд, рассмотренные выше определения ИИ сложны для восприятия и избыточно конкретизированы для правоприменителя.

Считаем, что с позиции правоприменителя целесообразно под технологиями ИИ понимать способность высокотехнической системы повторять некие функции, присущие человеку, которые будут обеспечивать самообучение ИИ и определять поиск и определение решений без специально заданного заранее алгоритма, направленные на получение при выполнении определенных задач обработки данных, такие результаты, которые будут сопоставимы с разумной деятельностью личности.

Мы полагаем, что разрабатываемая система ИИ, являясь важным элементом в деятельности государственных органов и правоохранительной системы в целом, и должна соответствовать требованиям доступности, своевременности, понятности и полноты информации о ней, причем как для общества, так и для участников правоотношений.

Учитывая важность анализируемого нового правового института, автор в рамках данного исследования рассматривает как постановку проблемы вопросы правового обеспечения использования ИИ в правоохранительной деятельности, на необходимость решения которой обращается внимание научного сообщества и правоприменителя.

Представляется важным проанализировать нормативную правовую регламентацию применения новых технологий в правоохранительной деятельности.

Концептуальные основы внедрения и применения ИИ нашли отражение в нормативном-правовом закреплении: Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. [7]; Доктрине информационной безопасности Российской Федерации [8]; Стратегии научно-технического развития Российской Федерации [9]; Национальной стратегии развития искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») [10]; Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 гг. и на перспективу до 2025 г. [11].

В настоящее время информационные системы, программы, технологии ИИ используются в оперативно-разыскной деятельности.

За последние четыре года остаток нераскрытых преступлений с использованием информационно-телекоммуникационной среды составил более 1 млн (1 094 842), а их удельный вес от всего массива нераскрытых преступлений за указанный период (3 581 582) превышает 30 %. По итогам 2021 г. почти 42 % (388 607 из 933 308, в 2020 г. – 45 %, в 2019-м – 23 %) нераскрытых преступлений относится именно к этой категории.

Таким образом, количество преступлений, совершаемых с использованием информационно-телекоммуникационной среды, неуклонно растет, что вызывает серьезное беспокойство.

Исследователи И. Л. Хромов, Н. А. Кузьмин отмечают тот факт, что в современном мире ИИ становится важным инструментарием ОРД в противодействии преступности. Это обусловлено тем, что на ИИ невозможно повлиять каким-либо образом. Его невозможно подкупить или убедить в чем-то, а также скрыть выявленное преступление. Используемые ИИ определенные решения по выполнению задач обусловлены конкретными алгоритмами работы, которые достаточно сложно изменить или перенастроить [12].

Стратегией экономической безопасности Российской Федерации до 2030 г., утвержденной Указом Президента Российской Федерации от 13 мая 2017 г. № 208 [13], приоритетным направлением государственной политики является повышение эффективности бюджетных расходов. Исходя из Концепции повышения эффективности бюджетных расходов в 2019–2024 гг. формирование бюджетной политики государства происходит в соответствии с показателями государственных программ Российской Федерации. МВД Российской Федерации участвует в реализации ряда государственных программ, при этом является ответственным исполнителем государственной программы Российской Федерации «Обеспечение общественного порядка и противодействия преступности.

Постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313 утверждена государственная программа «Информационное общество» [14], участие в реализации которой должны принимать все федеральные органы исполнительной власти, в том числе, правомочные на осуществление оперативно-разыскной деятельности.

Общий объем ассигнований направленный на реализацию данной Программы в период с 2014–2024 гг. за счет средств федерального бюджета, составит свы-

ше 1,6 трлн рублей. В 2020-м г. заложены в бюджет – 236 338 125,9 тыс. рублей, в 2021-м – 259 265 385,6 тыс. рублей. В соответствии с паспортом подпрограммы № 3 «Безопасность в информационном обществе» один из ключевых показателей в 2020 г. это 100 %-й охват контрольными мероприятиями операторов связи, представляющих услуги доступа к информационно-телекоммуникационной сети Интернет.

В соответствии с Посланием Президента Российской Федерации Федеральному Собранию Российской Федерации от 15 января 2021 г. на основании Федерального закона от 24 апреля 2020 г. № 123-ФЗ [15] с 1 июля 2020 г. сроком на пять лет в г. Москве проводится эксперимент по внедрению технологий искусственного интеллекта.

В п. 2 ч. 1 ФЗ № 123 «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в ст.ст. 6 и 10 Федерального закона «О персональных данных» указано, что под ИИ следует понимать технологические решения, которые позволяют имитировать определенные когнитивные, включая самообучение и поиск решений без заранее заданного алгоритма, функции человека и получать результаты при выполнении конкретных задач, которые будут сопоставимы как минимум с результатами интеллектуальной деятельности человека.

Под машинным обучением понимается методика анализа данных, которые позволяют аналитической системе обучаться в ходе решения множества сходных задач. Средства машинного обучения способны строить прогнозы, опираясь на сведения о развитии событий в прошлом.

Рассматриваемый процесс должен включать в себя следующие элементы – системы информации; ИТС; информационно-коммуникационную структуру и специальные средства обработки информации; заданное программное обеспечение; специальные сервисы по обработке информации.

Использование современной технологии ИИ обеспечит создание нового института общественных отношений, направленных на право регулирования новых технологий ИИ для борьбы с преступностью.

С учетом использования и внедрения новых технологий ИИ в ОРД важной задачей выступает осуществление ведомственного контроля и надзора за соблюдением законов в ОРД при использовании новых технологий.

В. С. Овчинский справедливо отмечает тот факт, что в современных условиях применения правоохранительными органами сложных цифровых технологий, которые могут при неправомерном их использовании иметь потенциальную угрозу информационной безопасности общества. С целью предупреждения формирования отрицательных тенденций общество должно иметь полномочия контроля за деятельностью правоохранительных органов, которые должны быть максимально открыты и подконтрольны обществу. Возникающие этические проблемы, связанные с работой органов правопорядка, должны быть решены с помощью применения новых технологических решений, регулирования правоотношений и контроля со стороны общественности [16].

В зарубежных странах системами с использованием технологий ИИ считаются системы с удаленной биометрической идентификацией граждан, автоматической оценкой кредитоспособности, т. е. системы, которые могут осуществлять моделирование, поведение человека, его поведения в интернет-пространстве и в быту при помощи ИИ. Подобные технологии ИИ используются полицией зарубежных стран, а их порядок регламентирован национальным законодательством.

Применение новых технологий ИИ и новых технологических решений должно найти отражение в действующем оперативно-разыскном законодательстве и нормативных правовых актах, что, несомненно, будет способствовать повышению уровня противодействия преступности, а также закреплять правовую систему гарантий обеспечения законности при использовании технических решений на базе ИИ в противодействии преступности и защите общества и государства от противоправных посягательств.

Список литературы

1. Мишустин: цифровизация госуправления поможет Российской Федерации войти в число лидеров мировой экономики: // ТАСС. URL: <http://tass.ru>.
2. Николас Д. Райт Интеллектуальная биология; Джорджтаунский университет; Университетский колледж, Лондон; Новая Америка // Технологические, политические, глобальные и творческие перспективы. Изд. : Air University Press. 2019.
3. Понкин А. В., Редькин А. И. Искусственный интеллект с точки зрения права // Вестник РУДН. Серия : Юридические науки 2018.
4. Тирранен В. А. Преступления с использованием искусственного интеллекта // Развитие теорий. 2019. № 3 (17). С. 10–13.
5. Овчинский С. С. Оперативно-розыскная информация. Теоретические основы информационно-прогностического обеспечения оперативно-розыскной и профилактической деятельности правоохранительных органов по борьбе с организованной преступностью. М., 1993.
6. Овчинский В. С., Ларина Е. С. Искусственный интеллект. Большие данные. Преступность («Коллекция Изборского клуба»). М. : Книжный мир, 2018.
7. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «КонсультантПлюс».
8. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».
9. Указ Президента Российской Федерации от 1 декабря 2016 г. № 642 «О Стратегии научно-технологического развития Российской Федерации» // СПС «КонсультантПлюс».
10. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс».

11. Распоряжение Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года» // СПС «КонсультантПлюс».

12. Хромов И. Л., Кузьмин Н. А., Завьялов И. А. Перспективные направления использования искусственного интеллекта в оперативно-розыскной деятельности. М., 2020. С. 95–96.

13. Указ Президента Российской Федерации от 13 мая 2017 г. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // СПС «КонсультантПлюс».

14. Постановление Правительства Российской Федерации от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество»» // СПС «КонсультантПлюс».

15. Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // СПС «КонсультантПлюс».

16. Овчинский В. С. Этика и «цифра»: этические проблемы цифровых технологий. М. : РАНХиГС, 2020.

Лопухов В. В.¹,

старший преподаватель

кафедры естественнонаучных дисциплин

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

**ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ
ОБЕСПЕЧЕНИЕ
КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ
ПРОЦЕССА РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ
НА ПРИМЕРЕ ОРГАНИЗАЦИИ РАБОТЫ
ПОДРАЗДЕЛЕНИЙ ГУ МВД РОССИИ ПО Г. МОСКВЕ**

Москва как самый крупный мегаполис в России характеризуется наибольшими миграционными, финансовыми потоками, а также количеством совершаемых преступлений, которые вызывают большой общественный резонанс по всей стране.

Отмечается повышение квалификации совершаемых преступлений, смещение их в сферу информационных технологий. МВД России адекватно реагирует на изменения структуры преступности, расширяются и создаются новые структурные подразделения для раскрытия и расследования преступлений с использованием информационных технологий. Это позволяет сохранять положительную динамику раскрываемости. В ГУ МВД России по г. Москве успешно функционируют специализированные оперативные подразделения, от районного до уровня главка, осуществляющие информационно-аналитическое обеспечение оперативно-разыскных мероприятий, сотрудники которых в данном выступлении будут именоваться – оперативные аналитики.

В 2022 г. на территории города Москвы совершено 138 180 преступлений (-3,8 %), раскрыто 45 тыс. Тяжкие и особо тяжкие преступления сократились на 12 %, раскрываемость которых составила 37,1 %.

Зарегистрировано 50 503 (-10,4 %) преступлений, совершенных с использованием информационно-телекоммуникационных технологий, раскрыто их на четверть больше, раскрываемость возросла на 6 % и составила 23,2 %.

С использованием информационных технологий раскрыто 26 400 преступлений, рост составил 14 %, из которых почти половина (10 262) тяжких и особо тяжких, в том числе 105 убийств, 356 УПТВЗ, 8 549 краж 5 285 мошенничеств, 1 007 грабежей, 2 663 преступлений, связанных с наркотиками.

С использованием системы видеонаблюдения, в которой функционирует более 228 тысяч камер, раскрыто около 9 тысяч преступлений, из которых 52 убийства, 188 факта умышленного причинения тяжкого вреда здоровью, 281 разбойное нападение и 639 грабежей.

¹ © Лопухов В. В., 2023.

**Сведения о количестве предварительно расследованных преступлений
с использованием АПК «Безопасный город»:
систем видеонаблюдения за 12 месяцев 2021–2022 гг.**

Вид преступления		Всего преступлений		
		прошлый год	текущий год	В абс. цифрах
всего		6 862	9 006	2 144
предварительное следствие обязательно		4 348	6 276	1 928
тяжких и особо тяжких		2 405	3 685	1 280
убийство, покушение на убийство		49	52	3
умышленное причинение тяжкого вреда здоровью		144	188	44
изнасилование, покушение на изнасилование		37	46	9
кража		3 433	4 235	802
из них	с проникновением	233	262	29
	в том числе в квартиры	99	82	17
	транспортных средств	57	67	10
	в том числе автомобилей	46	52	6
мошенничество		847	1674	827
грабеж		511	639	128
разбой		214	218	4
вымогательство		14	14	
хулиганство		56	90	34
хранение оружия		8	17	9
преступления экономической направленности		304	989	685
преступления связанные с наркотиками		251	390	139

Существенным результатом информационно-аналитического обеспечения было прямое участие оперативных аналитиков в выявлении и раскрытии, совместно с Центром по противодействию экстремизму Главка, преступления по ст. 210 УК РФ (организация преступного сообщества).

В полученном задании оперативные аналитики имели неполные данные организатора преступной группы, которая вымогала у одного из учредителей крупной энергетической компании сначала 30 млн рублей, затем 150 млн, при этом угрожая физическим насилием, рабством на Северном Кавказе и т. д. Также были получены некоторые телефонные номера и другие разрозненные сведения о преступниках. С использованием базы данных «Записная книжка», информационных массивов лиц, прошедших оперативное документирование в районных ОМВД, в постоянном контакте с оперативными сотрудниками были установлены члены преступной группы, составлены схемы прямых и косвенных связей, были установлены другие эпизоды преступной деятельности данной группы. Получаемые ими деньги шли на финансирование экстремистской деятельности религиозного характера.

В работе активно использовалась экономическая база «СПАРК», эту базу ГУ МВД России по г. Москве оплачивал с 2011 г., а с 2015 г. появилось подключение к базе данных D&B, содержащей сведения о зарубежных фирмах.

Несложное, но классическое, успешное раскрытие оперативные аналитики сделали, работая по убийству с расчленением неизвестной гражданки.

Дворником в мусорном контейнере было найдено расчлененное тело. Обнаруженный среди частей тела фрагмент пальца принадлежал гражданке Ефремовой Г. П., 1956 г.р., ранее судимой. На нее интересной информации получено не было. Оперативный аналитик установил, по информации ЗАГС, что в 1984 году Ефремова сменила фамилию на Сучкову в связи с замужеством, получил фотоизображения, по которым была установлена личность трупа.



Рис. 1. Фото Ефремовой Г. П.

В ходе проведения дальнейших оперативно-аналитических мероприятий уже в отношении гражданки Сучковой была получена информация о ее прямых и косвенных связях и возможном адресе проживания, которая была использована сотрудниками ОУР при раскрытии данного преступления. Далее была установлена гражданка Зверьянская Г. Д., 1965 г.р., подруга убитой, которая была изобличена в том, что, исполняя свой коварный замысел, на почве личной неприязни, вызванной завистью, с помощью ножа убила Сучкову, а затем с целью сокрытия преступления в ванной комнате ее расчленила и в полиэтиленовых пакетах вывезла и выбросила в мусорный контейнер.

Активное участие в раскрытии преступлений принимают оперативные аналитики территориальных подразделений окружного и районного уровней.

Характерным примером совместной работы сотрудников ГУ и УВД по Юго-Западному округу является раскрытие разбойного нападения на двух сотрудниц «Почты России» (Меркушину С. С. и Иванову Н. Н.) и похищения у них 250 тыс. рублей.

Так, сотрудником ОМВД России по району Северное Бутово с использованием АПК «Безопасный город» был получен «скриншот», на котором изображена автомашина преступника. Низкое качество изображения позволило установить только марку автомобиля – «Тойота» темного цвета.



Рис. 2. Скриншот с изображением автомобиля

С использованием базы данных ГИБДД была сделана выборка автомашин марки «Тойота», выезжающих с территории района Северное Бутово в период совершения преступления. Путем исключения были выбраны две автомашины, похожие на искомую, и далее совместно УВД по ЮЗАО проведены соответствующие оперативно-аналитические мероприятия и по базе данных лиц, прошедших оперативное документирование, были установлены и впоследствии изобличены злодеи – Колесников Е. О. и Карпов И. В., первый из которых задержан, а второй объявлен в федеральный розыск.

Хорошие раскрытия сделали сотрудники УВД по Западному округу г. Москвы с использованием интернет-ресурсов и имеющихся информационных массивов.

Так, на улице Староволынская был обнаружен труп Кравченко С. В., 1995 г.р., со множественными ножевыми ранениями. В ходе оперативно-аналитических мероприятий сотрудниками было установлено его место жительства, что он являлся студентом 2 курса МГУ им. Ломоносова, вел активную переписку в социальных сетях. С помощью имеющихся возможностей установлена предполагаемая квартира и компьютер, с которого на электронную почту убитого систематически поступали сообщения. В ходе дальнейших аналитических мероприятий из зарегистрированных в данной квартире лиц был выявлен Савченко Д. С., 1995 г.р., который по данным оперативных сводок угрожал физической расправой своей бывшей сожительнице Шкариной Н. В., 1995 г.р. за связь с впоследствии убитым Кравченко. Дальнейшие ОРМ и обыск, проведенные сотрудниками УР, выявили в месте его жительства вещи убитого Кравченко – ключи, паспорт, планшетный компьютер.

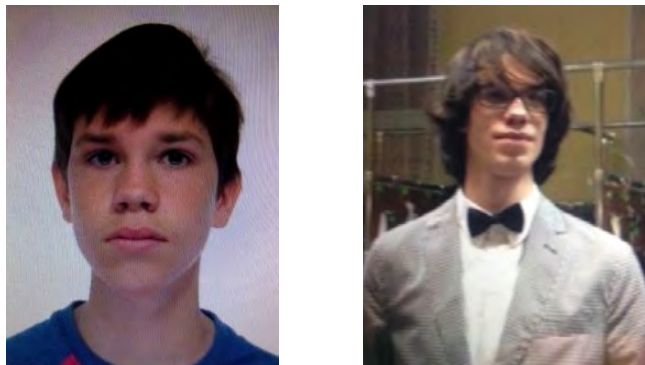


Рис. 3. Фото погибшего

На берегу Москвы-реки с повреждениями головы обнаружен труп Турыгинова А. В., 1987 г.р. В ходе изучения записей с видеокamer наблюдения ст. м. «Филевский Парк» сотрудниками УВД по ЗАО было установлено, что незадолго до смерти потерпевшая выходила из станции метро с двумя неизвестными. С целью установления ее связей был проведен мониторинг сети Интернет и путем сравнения фотоизображений было установлено, что один из молодых людей, выходящих из метро, схож с фотографией одного из знакомых убитой – Ростовцевым Д. С., 1996 г.р., зарегистрированным в г. Краснодаре и находящемся в федеральном розыске по ст. 159 УК РФ. Оперативно-аналитические мероприятия в отношении него позволили установить его родственников и адрес фактического проживания – г. Королев М.О. Дальнейший анализ сети позво-

лил установить второго подозреваемого – Фомина А. А., 1995 г.р. Основываясь на этой аналитической информации, сотрудниками ОУР оба были задержаны и им предъявлены обвинения по ч. 4 ст. 111 УК РФ.

Немаловажен вклад оперативных аналитиков Москвы в выявление и раскрытие хищений денежных средств с банковских карт путем использования услуги «900» Сбербанка России.

Свой преступный умысел мошенники реализовывали, используя тот факт, что при смене номера мобильного оператора «Билайн» услуга «900» по управлению своей банковской картой без соответствующего заявления в Сбербанк оставалась подключенной на старом номере, который уходил в повторную продажу. В г. Зеленограде было выявлено более 100 таких эпизодов, в Юго-Западном округе – 20.

Описанные примеры не содержат сложной, красивой аналитики, которая получается, к сожалению, редко, в единичных случаях. Но они являются типовыми и массовыми, и именно этого ждут оперативные службы.

Существенным резервом в раскрытии имущественных преступлений в Москве, как и, наверное, в России в целом, являются учет и работа с наркозависимыми лицами, которым постоянно нужны деньги для приобретения и употребления наркотиков. Начальником ГУ МВД России по г. Москве этому вопросу уделяется значительное внимание.

При этом анализ деятельности органов внутренних дел по раскрытию и расследованию преступлений, связанных с незаконным оборотом наркотических средств, показал, что полученная оперативными аналитиками оперативнозначимая информация в ходе проведения опросов лиц, причастных к указанной категории преступлений, используется не в полной мере.

В связи с этим в целях систематизации процедуры опроса данной категории лиц в УВД по Юго-Западному округу был разработан и внедрен в других окружных управлениях специальный опросный лист.

Опросник состоит из трех блоков:

- информация о лице, задержанном за хранение наркотического средства;
- информация о способе и месте приобретения наркотика;
- сведения в отношении сбытчика наркотических веществ.

Позиции, содержащиеся в вышеуказанных блоках, были перенесены в формат Excel с целью дальнейшей обработки внесенной информации, с использованием функции «фильтр» данной офисной программы.

Основными позициями, по которым осуществляется выборка, с целью установления серийности являются:

- имя и криминальная кличка сбытчика;
- номер мобильного телефона сбытчика;
- номер qіwі-кошелька или банковской карты, на которые были переведены денежные средства.

В случае установления серийности сотрудник изучает остальные характеризующие личность преступника позиции. Работа ведется с целью получения обобщающей информации, которая позволит установить полные установочные данные фигуранта.

Пример: на территории оперативного обслуживания ОМВД по Энскому району выявлено четыре факта использования одного и того же номера мобильного телефона с целью приобретения наркотического средства «героин». При этом в трех случаях было указано имя сбытчика «Саид». В одном случае сбытчиком являлся мужчина азиатской внешности, которому на вид 35–40 лет, в пользовании у которого находится автомашина марки «Лада Приора» темно-зеленого цвета, с фрагментом номера «343».

Сотрудниками УВД в ходе проведения оперативно-аналитических мероприятий по имеющейся информации была установлена личность фигуранта, его местонахождение, родственные и криминальные связи.

Инициативное оперативно-аналитическое исследование направлено в ОУР УВД с целью использования полученной информации в ОРД. В дальнейшем поступило уведомление о заведении дела оперативного учета по окрасу «незаконный оборот наркотических средств» в отношении данного лица.

Также было выявлено три факта совпадения по номерам мобильного телефона в отношении лица, осуществляющего сбыт курительный смесей «спайсов», путем закладок на территории оперативного обслуживания одного из ОМВД.

Полученные сведения также были направлены в ОУР ОМВД с целью проведения технических мероприятий, направленных на установление лица, использующего данный мобильный номер. Затем были проведены оперативно-аналитические мероприятия в отношении фигуранта, сведения о котором были получены в ходе проведенных ОРМ.

Необходимо отметить, что данные результаты работы были достигнуты на основании информации, сбор которой осуществлялся в течение 1,5 месяцев. В созданный информационный сегмент в отношении наркозависимых лиц внесена информация в отношении 269 фигурантов.

Полученный результат достигнут благодаря тесному взаимодействию сотрудников УР территориальных органов МВД России на районном уровне с оперативными аналитиками в части предоставления опросных листов после проведения бесед с доставленными лицами, с целью дальнейшего внесения полученной оперативноразнозначимой информации в информационные массивы.

Данная работа особенно ценна и востребована, поскольку давно уже сбыт наркотиков происходит дистанционно, без физического контакта продавца и покупателя, через закладки и электронные платежи.

Вышеуказанная методика работы также используется сотрудниками ОМВД по районам в части сбора информации по нераскрытым квартирным кражам, грабежам и разбоям, в том числе «барсеточного типа»; мошенничествам, кражам и угонам автотранспорта.

Данный метод работы позволяет сотрудникам в кратчайшие сроки предоставлять в оперативные подразделения информацию по уголовным делам, которые возможно относятся к серии совершенных преступлений данным лицом.

При осуществлении выборки особое внимание уделяется следующим поисковым критериям:

- способ и место совершения преступления;
- приметы предполагаемого преступника;

- фотокомпазиционные портреты, полученные в инициативном порядке из экспертно-криминалистических подразделений;
- скриншоты, полученные с камер видеонаблюдения, установленные в Московском регионе с использованием АПК «Безопасный город»;
- перечень похищенного имущества.

На основании полученных сведений, сотрудниками также проводится анализ нераскрытых преступлений с целью установления адресов, наиболее подверженных той или иной категории преступлений. Анализируются время совершения преступления, день недели, категория потерпевшего, внешность предполагаемого преступника, которая устанавливается на основании фотороботов, скриншотов и примет, указанных в допросе потерпевшего.

Указанные сведения широко используются сотрудниками наружных служб с целью грамотной расстановки нарядов, используемых в системе единой дислокации. А также работе с лицами, проверяемыми на причастность к ранее совершенным преступлениям. Для сотрудников наружных служб готовятся небольшие буклеты, которые они используют при несении службы.

Список литературы

1. Организация информационно-аналитического обеспечения оперативно-розыскной деятельности органов внутренних дел : учебное пособие / [В. В. Денисов и др.]. М. : Академия управления МВД России, 2017.
2. Букейханов П. Е. Информационные технологии в сфере розыскной работы органов внутренних дел. М., 2002.
3. Шумилов А. Ю. Правовое регулирование оперативно-розыскной деятельности: сборник нормативных актов и документов. М., 2000.

Меняйло Д. В.¹,

*начальник кафедры информационно-компьютерных технологий в деятельности органов внутренних дел
Белгородского юридического института
МВД России имени И.Д. Путилина,
кандидат юридических наук, доцент*

Барсова Е. Р.²,

*курсант факультета правоохранительной деятельности
Белгородского юридического института
МВД России имени И.Д. Путилина*

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ

Коррупция как явление имеет проблемный характер. Но некоторые все же пока задают себе вопрос: «Это болезнь российского общества или же норма жизни?» Стоит однозначно ответить, что коррупция – это негативное явление, которое обременяет жизнь как отдельно взятого лица, так и общества в целом. Коррупция, так называемые «откаты» в бизнесе, бьют по карману простого гражданина, увеличивая стоимость товара на прилавке, либо выполняемой услуги, так как в стоимость товара (услуги) необходимо заложить дополнительные финансовые издержки. И если мы хотим действительно выйти из «коррупционного тупика», то необходимо сформировать в обществе устойчивые представления о «ненормальности» коррупционных проявлений. Пока же, напротив, такие представления в должной степени не характерны для национального правового менталитета россиян.

На борьбу с коррупционными проявлениями как в современной России, так и в иных государствах мирового сообщества приходят информационные технологии. У каждого государства с течением времени были выработаны разнообразные методы по борьбе с представленным негативным социальным явлением. Причем методика подавления отрицательных коррупционных проявлений в каждой стране различна – от смертной казни до отсутствия применения жестких мер воздействия на коррупционеров; от формирования антикоррупционного сознания до создания технологий искусственного интеллекта. При этом следует уточнить, что на сегодняшний день развитые зарубежные страны стремятся к выработке систематизированного и эффективного механизма с внедрением информационно-коммуникационных технологий в соответствующие процессы борьбы с коррупцией. В эпоху цифровизации передовые технологии проникают во все сферы жизнедеятельности человека, обеспечивают возможность создания и применения наиболее совершенных способов противодействия коррупционным проявлениям.

¹ © Меняйло Д. В., 2023.

² © Барсова Е. Р., 2023.

Формирование сотрудничества развитых государств в направлении борьбы с коррупцией посредством применения передовых технологий имеет огромный потенциал для создания и продвижения кардинально новых приемов противодействия коррупционным правонарушениям.

В частности, на сегодняшний день к основным принципам отечественной и зарубежной политики противодействия данному негативному социальному явлению относятся:

- работа с общественностью посредством организации онлайн-дискуссий;
- выявление коррупционеров по средствам мониторинга интернет-пространства;
- обработка больших данных на предмет выявления признаков коррупционных проявлений;
- повышение правовой культуры граждан с помощью информирования общественности о ее праве на сопротивление произволу недобросовестных государственных чиновников;
- создание онлайн-каналов для подачи жалоб о конкретных случаях злоупотреблений полномочиями чиновников;
- автоматизация и цифровизация предоставления государственных услуг;
- открытость деятельности представителей государственной и местной власти.

Формирование передовых подходов по борьбе с коррупцией, подпитываемое цифровой трансформацией политики государств, стало основой для внедрения интересных решений в сфере активного противодействия взяточничеству во всех его проявлениях. Опираясь на практику зарубежных государств, можно с уверенностью сказать, что передовые технологии позволяют снизить ущерб от такой многоаспектной проблемы, как коррупция.

На сегодняшний день политику в направлении борьбы с коррупцией с активным применением IT-технологий осуществляет целый ряд стран, в числе которых США, Япония, Республика Корея, Сингапур, Эстония, Франция, Финляндия и др.

Например, в Республике Корея еще с 1999 г. стала успешно применяться IT-платформа «OPEN», которая позволила гражданам посредством Интернета контролировать процедуру рассмотрения своих обращений чиновниками, а значит, сделала деятельность государственного аппарата более прозрачной и открытой [1]. Внедрение платформы OPEN повлияло на работу госслужащих, ведь риски несправедливых решений по обращениям; затягивание с ответами; требование «дополнительной оплаты» за ускорение процедуры» были сведены к минимуму.

В Сингапуре был выбран иной путь минимизации последствий взяточничества от лица государственных служащих – посредством частичного сокращения государственного аппарата. В частности, в часто посещаемых заведениях произошла замена аппарата чиновников на электронные терминалы для получения услуг и справочной информации. Взаимодействие с государством в стране происходит дистанционно – посредством электронных информационных порталов, интегрированных с мобильными устройствами [1].

Ряд стран международного сообщества приняли решение о привлечении общественности к проблемам взяточничества с помощью создания анонимных каналов связи, с помощью которых обычные граждане передают информацию о соответствующих преступлениях госслужащих. Не обошла эту практику и Австрия, в которой функционирует так называемый «веб-сайт информаторов», действующий через анонимный электронный почтовый ящик.

Далее хотелось бы отметить положительный опыт КНР, в которой с 2012 г. функционировала система искусственного интеллекта Zero Trust. За 7 лет работы, согласно статистике, данная система позволила выявить 8 721 коррупционера (учитывая, что она затронула лишь 1 % административного аппарата Китая) [2]. Основная деятельность ИИ Zero Trust сводилась в анализе социальных отношений госслужащих, специфики принимаемых ими решений. Zero Trust оценивал информацию из 150 баз данных, относящихся к центральному и региональным правительствам.

В распоряжении ИИ была информация о фактах, связанных с незаконной передачей имущества, подозрительными приобретениями ценных бумаг, снос домов, которые были инициированы китайскими чиновниками. Zero Trust отличалась тем, что позволяла считывать информацию с разных источников, именно поэтому попытки подтасовать данные чиновником не могли увенчаться успехом.

Кроме того, система фиксировала подозрительные изменения счетов госслужащих и вычисляла процент вероятности коррумпированной активности с последующим отчетом властям. По словам одного из создателей ценной системы, на данной стадии с «оступившимся» чиновником связывался представитель власти, который уведомлял его о проверке и помогал ему «избежать дальнейших ошибок» [2]. С 2019 года система была упразднена по причине «доставления дискомфорта» госслужащим и вследствие иных недостатков, однако эффективность данного ИИ была неоднократно доказана.

По нашему мнению, принцип действия Zero Trust должен совершенствоваться в дальнейшем, ведь его польза была неоднократно доказана на практике КНР. Устранение проблемных вопросов, обнаруженных в системе, позволит «дистанционно» выявлять злоупотребления госслужащих без создания специальных контролирующих органов.

Среди основных информационных технологий последнего времени, применяемых как в России, так и в иностранных государствах, можно указать на следующие:

1. Предоставление государственных услуг в дистанционном режиме, в рамках так называемого «электронного правительства», а в некоторых случаях и «цифрового правительства». Последнее отличает применение в системе управления цифровых технологий (облачные вычисления, большие данные, искусственный интеллект).

2. Так называемая «Big Data», сущность которой заключается в функционировании цифровых инструментов для обработки значительных по величине объемов информации. Применяется для анализа, расследования и аудита подозрительных финансовых операций. Цифровую платформу на основе действия Big Data в области противодействия коррупции на сегодняшний день успешно

применяют в Будапеште – система анализирует большое количество информации и выявляет аномальные закономерности (подозрительные результаты торгов, отсутствие конкуренции коммерческих организаций и пр.).

Данная система сделает возможным ведение автоматизированного учета статистических данных параметров коррупционных отношений, в том числе: возникающих коррупционных рисков; возможных коррупционных взаимоотношений (потенциального конфликта интересов); статистики коррупционных правонарушений с возможностью привязки к конкретному объему полномочий чиновников и должностных лиц [3, с. 30].

3. Блокчейн и технологии распределенной книги (DLT). Особое значение для надежного управления органами власти социальными и экономическими системами приобретает постоянное совершенствование технологии криптозащиты передаваемой информации. В связи с этим важно отметить широкие антикоррупционные возможности блокчейн-технологий [4, с. 62].

Новеллой в сфере противодействия коррупции в России стало введение новой информационной системы противодействия коррупции «Посейдон». В апреле 2022 года в соответствии с указом Президента Российской Федерации В. В. Путиным была введена в действие информационная система противодействия коррупции «Посейдон», которая призвана при обработке, анализе и сопоставлении информации выявлять признаки коррупционной деятельности [5]. ГИС «Посейдон» состоит из трех элементов. Во-первых, программно-аппаратного комплекса центрального сегмента системы, имеющего профилактическое назначение. Во-вторых, программно-аппаратного комплекса многоцелевого назначения. «Необходим для обеспечения работы внутренних и внешних субъектов «Посейдона» с программно-аппаратным комплексом центрального сегмента системы, а также для автоматизированного ввода, учета и хранения справок о доходах, расходах, об имуществе и обязательствах имущественного характера.». В-третьих, специального программного обеспечение «Справки БК», которое позволяет в автоматизированном режиме собирать информацию от чиновников об их доходах, расходах, об имуществе и обязательствах имущественного характера, и такую же информацию о некоторых членах их семей (супруги и несовершеннолетних детей) [6, с. 252]. Оператором ГИС «Посейдон» является Федеральная служба охраны России. В связи с чем Министерство внутренних дел России осуществляет с данным ведомством взаимодействие по вопросам предоставления и получения информации как в целях собственной безопасности, так и борьбы с коррупционерами и их пособниками. Основная идея ГИС «Посейдон» заключается в системном аккумулировании информации финансового и имущественного характера, анализе данной информации и получении вытекающих из такового анализа выводов. В этом плане наблюдается автоматизированная работа с большими данными (Big Data).

Кроме уже описанных информационных технологий, в Российской Федерации применяются технологии, обеспечивающие сбор доказательственной базы для изобличения лиц, причастных к коррупционным правонарушениям. Это видеофиксация и видеоаналитика в рамках идеи «безопасный город». Например, уже доказали свою эффективность программа ПАРСИВ, специальное программ-

ное обеспечение «Паутина», биометрическая система распознавания лиц в городском транспорте «Сфера» и т. д.

Большое подспорье в правоохранительной деятельности органов внутренних дел и в противодействии коррупции оказывают прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД (служебные сервисы) и система централизованной обработки данных (ЦОД) единой системы информационно-аналитического обеспечения деятельности МВД России.

В рамках противодействия коррупции и иных преступлений интерес представляет и такой инструмент по анализу криптовалютных операций, используемый Росфинмониторингом, как «Прозрачный блокчейн».

Но, как известно, лучше не допустить преступления и провести комплекс профилактических мероприятий, чем бороться с последствиями преступления. В этой связи следует продолжать проведение правового информирования, правового просвещения об истоках и последствиях коррупции как в целом для общества, так и для самого коррупционера в части юридической ответственности. Также следует обратить внимание на цифровизацию антикоррупционной экспертизы при проверке нормативных правовых актов и их проектов на предмет наличия в них коррупциогенных факторов.

Список литературы

1. Евсиков К. С., Суворов А. А., Братчикова Л. Р. Цифровая трансформация противодействия коррупции // Известия ТулГУ. Экономические и юридические науки. 2022. № 1. URL: <https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-protivodeystviya-korrupsii>.
2. Избавит ли искусственный интеллект человечество от коррупции // URL: <https://www.techinsider.ru/science/731753-izbavit-li-iskusstvennyy-intellekt-chelovechestvo-ot-korrupcii/>.
3. Меняйло Д. В., Крупенникова К. К. О противодействии коррупции в условиях цифровой трансформации // Проблемы правоохранительной деятельности. 2022. № 3. С. 28–32.
4. Крупенникова К. К., Меняйло Д. В. Развитие антикоррупционной деятельности в условиях цифровизации государства и общества // Проблемы юриспруденции и педагогики высшей школы в работах молодых ученых : сборник материалов Всероссийской научно-практической конференции, Белгород, 30 ноября 2022 года. Вып. 3. Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. С. 62–66.
5. Указ Президента Российской Федерации от 25 апреля 2022 г. № 232 «О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации» // Собрание законодательства Российской Федерации. 2022. № 18. Ст. 3053.
6. Фарахiev Д. М. Государственная информационная система «Посейдон»: современный взгляд на противодействие коррупции // Вестник Московского университета МВД России. 2023. № 1. С. 250–254.

Папуша Е. Ю.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

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

ПРОБЛЕМЫ ГОЛОСОВЫХ ПОМОЩНИКОВ ПО РАСПОЗНАВАНИЮ DEERFAKE И КАК ЗАЩИТИТЬ СЕБЯ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ВАШИМ ДАННЫМ

Защита голосовых помощников становится все более важной в связи с широким использованием этих устройств в нашей повседневной жизни. Голосовые помощники предназначены для выполнения широкого спектра задач, от установки напоминаний и воспроизведения музыки до управления устройствами умного дома и предоставления информации. По мере того, как голосовые помощники все больше интегрируются в нашу жизнь, возрастает и вероятность того, что атаки поддельных устройств могут причинить вред. Вот несколько причин, по которым защита голосовых помощников крайне важна:

Соображения конфиденциальности. Голосовые помощники всегда прослушиваются, что означает, что они потенциально могут записывать конфиденциальную информацию, которой пользователи могут не захотеть делиться.

Финансовое мошенничество. Голосовые помощники все чаще используются для финансовых операций, таких как совершение покупок и перевод денег.

Физическая безопасность: Голосовые помощники часто используются для управления устройствами умного дома, такими как замки, камеры безопасности и системы сигнализации.

Дезинформация и социальная инженерия. Атаки с использованием подделок могут быть использованы для распространения дезинформации или манипулирования людьми с помощью социальной инженерии.

Уязвимость голосовых помощников к подделкам голоса. Голосовые помощники полагаются на алгоритмы машинного обучения для распознавания и интерпретации человеческой речи.

Защита от голосовых подделок. Защита от голосовых подделок требует сочетания технических и нетехнических мер. Технические меры включают в себя повышение точности алгоритмов распознавания голоса и разработку новых методов обнаружения и предотвращения подделки голоса.

¹ © Папуша Е. Ю., 2023.

Чтобы оценить влияние этих факторов на устойчивость голосовых помощников к атакам подделки, можно провести различные эксперименты. Например, можно использовать различные типы голосовых образцов или TTS-движков для создания мошеннических запросов к голосовому помощнику и оценить степень успешности атак. Расстояние образцов голоса от устройства также можно варьировать, чтобы оценить влияние расстояния на успешность атак.

В последние годы атаки с использованием подделок привлекли внимание как значительная угроза безопасности голосовых помощников.

Атаки повтора являются одной из распространенных методик тестирования, используемых для оценки устойчивости голосовых помощников к атакам подделки. При атаке повторного воспроизведения злоумышленники записывают голос жертвы и используют запись для выполнения мошеннических запросов к голосовому помощнику.

Другой методикой тестирования для оценки устойчивости голосовых помощников к атакам подделки является синтетическая голосовая атака. При атаке синтетическим голосом TTS-движки используются для создания голоса жертвы и выполнения мошеннических запросов к голосовому помощнику. Этот тип атаки может быть успешным, если синтетический голос достаточно естественен, чтобы обмануть голосового помощника.

Механизмы преобразования текста в речь (TTS) – это программы, которые преобразуют письменный текст в устную речь. Эти механизмы обычно используются в голосовых помощниках, поскольку они позволяют устройствам отвечать на команды пользователя, генерируя речь, которая звучит естественно и по-человечески. Однако TTS-движки также могут использоваться для проведения атак на голосовые помощники с использованием подделки.

При атаке с использованием синтетического голоса TTS-движки используются для создания синтетического голоса, имитирующего голос жертвы. Злоумышленники могут использовать этот синтетический голос для выполнения мошеннических запросов к голосовому помощнику, которые могут быть приняты за настоящие запросы жертвы. Успех атак с использованием синтетического голоса зависит от естественности синтетического голоса.

Чтобы оценить эффективность атак с использованием синтетического голоса, исследователи провели эксперименты, используя различные TTS-движки для создания синтетических голосов. Некоторые TTS-движки лучше других справляются с созданием естественных голосов, а качество синтетического голоса может варьироваться в зависимости от характеристик синтезируемого текста.

Злоумышленники также могут использовать TTS-движки для создания синтетических голосов, подражающих определенным знаменитостям или общественным деятелям. Этот тип атаки, известный как атака с подменой голоса, может использоваться для создания поддельных аудиозаписей, искажающих слова или действия целевого лица.

Для защиты от атак подделки голоса, использующих движки TTS, голосовые помощники могут быть запрограммированы на распознавание уникальных характеристик голоса жертвы, таких как высота тона, тембр и каденция. Это может

затруднить злоумышленникам создание синтетических голосов, достаточно убедительных для того, чтобы обмануть голосовой помощник.

В целом TTS-движки могут быть мощным инструментом для создания естественных голосов, но они также могут использоваться для атак на подставных лиц.

Таким образом, чтобы атаки с использованием подделок представляли собой незначительную угрозу для безопасности голосовых помощников, нужно оценить устойчивость этих систем к таким атакам. Для этого можно использовать различные методики тестирования, включая атаки воспроизведения и синтетические голосовые атаки.

В заключение следует отметить, что голосовые помощники стали важной частью нашей повседневной жизни, но они также уязвимы для атак в виде голосовых подделок. Эти атаки могут использоваться для обмана голосовых помощников и заставлять их выполнять непредусмотренные действия. Защита от подделки голоса требует сочетания технических и нетехнических мер, включая повышение точности алгоритмов распознавания голоса и информирование пользователей о рисках, связанных с этими атаками. Принимая эти меры, мы можем гарантировать, что голосовые помощники останутся безопасным и надежным инструментом для выполнения широкого круга задач.

Список литературы

1. Deep Learning for Voice Conversion: A Review by Tomoki Toda, Ling-Hui Chen, and Keiichi Tokuda (<https://ieeexplore.ieee.org/document/8462535>).
2. Deepfake Speech Detection Using Transfer Learning by Saurabh Kumar, Anurag Ranjan, and Shiv Ram Dubey (<https://ieeexplore.ieee.org/document/8821636>).
3. Deep Learning-Based Voice Conversion and Its Applications by Tomoki Toda and Keiichi Tokuda (<https://www.mdpi.com/2076-3417/9/20/4396>).
4. Deep Learning for Voice Spoofing Detection: A Review by Kailash Patidar, Saurabh Kumar, and Anurag Ranjan (<https://ieeexplore.ieee.org/document/9052338>).
5. Protecting Voice Assistants Against Deepfake Attacks by Yuxin Chen, Yulong Cao, and Jun Li (<https://ieeexplore.ieee.org/document/9089773>).
6. A Survey on Deep Learning Techniques for Voice Conversion by S. S. S. Sowmya, S. S. S. Sridhar, and V. S. K. Reddy (<https://ieeexplore.ieee.org/document/9122521>).
7. Detecting Deepfake Audio Using Convolutional Neural Networks by N. M. R. D. Bandara, M. A. M. F. F. Marikkar, and N. D. Kodikara (<https://ieeexplore.ieee.org/document/9501953>).
8. Deepfake Voice Recognition Using Convolutional Neural Networks by S. S. S. Sowmya, S. S. S. Sridhar, and V. S. K. Reddy (<https://ieeexplore.ieee.org/document/9461250>).
9. A Survey on Deepfake Detection Techniques for Voice and Speech by K. R. S. S. R. Kumar, S. S. S. Sridhar, and V. S. K. Reddy (<https://ieeexplore.ieee.org/document/9449459>).
10. Deepfake Detection in Voice and Speech: A Review by K. R. S. S. R. Kumar, S. S. S. Sridhar, and V. S. K. Reddy (<https://ieeexplore.ieee.org/document/9517208>).

Коломина А. С.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Полякова О. С.²,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

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

ДИПФЕЙКИ: ПОДДЕЛЬНОЕ ПРОШЛОЕ, НАСТОЯЩЕЕ И БУДУЩЕЕ

Deepfake – совокупность двух терминов: «глубокое обучение» и «подделка». Стоит отметить, что количество видеоподделок, циркулирующих только в Интернете, неуклонно удваивается каждые полгода. Общее их количество бесчисленно. По данным некоторых зарубежных экспертов, всего за два года благодаря инструменту *deepfake* было выявлено более 85 000 единиц только «очевидного» вредоносного видеоконтента. В то же время разумно предположить, что в любой момент времени в цифровом пространстве могут находиться сотни миллионов синтетического контента всех видов (видео, аудио, изображения, текст).

Чтобы ответить на вопрос, что такое дипфейк с технической точки зрения, давайте рассмотрим два наиболее распространенных типа: видео и аудио. Процесс создания фейкового видео основан на работе генеративной состязательной сети (GAN), в которой люди, а не машины анализируют огромные объемы данных, изучают мимику, черты и выражения лица «субъекта», а затем имитируют эти черты. Процесс имитации заключается в «погружении» двух изображений человека в алгоритм глубокого обучения, который обучается с помощью множества различных параметров, чтобы заменить одно лицо на другое как можно более естественно (используется метод отображения лица). Как правило, существует прямая зависимость: чем больше различных исходных видео анализируется, тем выше качество конечной подделки.

В случае аудиодипфейков процесс создания во многом похож. Требуется аудио, записанное в различных ситуациях, таких как интервью, речи, телефонные голосовые сообщения, бытовые разговоры и т. д. Все это разбивается на микро-

¹ © Коломина А. С., 2023.

² © Полякова О. С., 2023.

образцы и отправляется в алгоритмы глубокого обучения. В настоящее время для создания подделок среднего качества можно использовать 10–15 минут необработанных данных. Однако для создания синтетического голоса, который бы точно соответствовал «оригинальным» характеристикам, таким как акцент, паузы и междометия, требуется несколько часов записи различных голосов. В этом случае клонируется и синтезируется наиболее естественно звучащий голос. Без специального программного обеспечения или технологии, позволяющей распознавать подделки по незначительным отличиям в звучании, отличить их от настоящих практически невозможно.

Для большей ясности мы проанализировали несколько программ по созданию дипфейков, начнем с онлайн редактора для изменения голоса.

При изменении были получены два образца аудиозаписи. Далее был проведен анализ для проверки распознавания голосовых команд устройств «Яндекс-станции (Алиса)», Google-ассистент, Ассистент Siri (Apple), для исследования было взято несколько фраз от «Голоса пользователя» и «Аудиодипфейка». Результатом данной работы является понимание, насколько аудиодипфейки действительно хороши и могут обмануть систему.

Далее проанализируем создание видеодипфейка, для его создания будет использоваться программа DeepfakesWeb. Там мы регистрируемся, получаем советы по созданию и приступаем к работе. Изначально нам необходимо два видео (которое изменяем и еще то, которое накладываем), загружаем их и запускаем создание, соглашаясь при этом с условиями конфиденциальности. Создание происходит около 187 минут.

Для сравнения рассмотрим другую программу DeepfakeVFX.com. Проблемы могут возникнуть уже со стадии «скачивание», но эта программа того стоит. Функционал ее намного шире, и соответственно работа получается более качественной. После того, как мы поместили видеоматериалы (исходное и целевое видео), извлекаем их, далее идет обработка видеофайла, и для каждого кадра будет создан файл .png.

Переходим к обработке изображения и извлекаем лица, которые будут использоваться в нашей подделке, используем значение по умолчанию. Через несколько минут извлечение завершится и предоставит отчет о количестве найденных изображений и обнаруженных лиц. После просматриваем исходные и целевые наборы лиц с помощью файлов «просмотр выровненных результатов», можем даже удалить ненужные лица из проекта.

Начинаем обучение нашей модели deepfake. Используем настройки по умолчанию, программа загружает все наши файлы изображений и запускает первую итерацию обучения. Если оно выполнено успешно, то откроется окно предварительного просмотра обучения. В окне «Предварительного просмотра» вверху есть несколько клавиатурных команд. График показывает точность обучения и предварительный просмотр изображений моделей. Если обновить окно, то появится измененный график и изображения. Строки представляют значения потерь, которые со временем будут приближаться к нулю, поэтому, чем ниже строка, тем лучше будут результаты.

Предварительный просмотр изображения содержит несколько столбцов, показывающих обрабатываемые исходные и целевые изображения. Используется окно предварительного просмотра, чтобы решить, когда хотим завершить обучение. После завершения обучения объединяем лица и создаем окончательное видео с подделкой. В окне слияния видим карту команд клавиатуры. Если видим черный предварительный просмотр, то используем клавишу, чтобы перейти к первому кадру. Видим текущий номер кадра и настройки, отображаемые в окне командной строки. С помощью определенных клавиш можем менять значение маски и размытия для сужения границ вокруг лица или же для увеличения значения маски размытия.

Последняя часть этого процесса заключается в объединении новых кадров deerfake в видеофайл с целевым звуком. Дипфейк создается в новых файлах программы.

Сравнивая две программы, а именно DeepfakesWeb и DeepfakeVFX.com, обращая внимание, что в первой программе было больше количества признаков подделки, чем во второй программе, делаем умозаключение, что программа DeepfakeVFX.com справляется со своей задачей лучше. Из всей проделанной работы можем сделать вывод, что создание качественного дипфейка, пользуясь ПО, которое находится в свободном доступе – возможно.

Список литературы

1. Дипфейки: поддельное настоящее / сост. А. С. Рубцова. Новеллы Конституции Российской Федерации и задачи юридической науки, 2021. С. 109–112.
2. Дипфейки как угроза персональным данным / сост. Я. А. Масликова. Грядущим поколениям завещаем, 2021. С. 391–395.
3. Проблема этической верификации: от фейка к дипфейку / сост. Е. М. Гашкова. Коммуникативные стратегии информационного общества, 2021. С. 92–95.
4. Дипфейки и искусственный интеллект: вопросы правового регулирования / сост. Е. С. Гринь. Социально-экономическое развитие и качество правовой среды, 2021. С. 240–243.
5. Использование технологии дипфейка в преступных целях: криминалистические аспекты противодействия расследованию / сост. В. Н. Ситник. Традиции и новации в системе современного российского права, 2022. С. 209–213.

Лащенко П. М.¹,

*командир отделения факультета подготовки
специалистов 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*

РАЗВИТИЕ И ХАРАКТЕРИСТИКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

В настоящее время кибербезопасность становится все более актуальной проблемой, особенно с учетом быстрого развития технологий и увеличения количества угроз в интернете.

Искусственный интеллект (далее – ИИ) становится все более значимым и эффективным инструментом в борьбе с киберугрозами. Использование машинного обучения и нейронных сетей позволяет создавать инновационные системы, способные распознавать, анализировать и реагировать на угрозы в режиме реального времени.

Использование ИИ в кибербезопасности позволяет автоматизировать процессы обнаружения и предотвращения угроз, повышая эффективность и скорость реагирования на возможные угрозы.

Сегодня системы ИИ используются для распознавания аномального поведения в сетях, анализа логов, обнаружения уязвимостей в системах безопасности, предсказания и предотвращения кибератак и многого другого. Многие компании и организации используют ИИ для защиты своих сетей и данных, в том числе Google, Amazon, IBM, Microsoft и т. д. [2].

Таким образом развитие и совершенствование ИИ для кибербезопасности – это непрерывный процесс, в котором используются самые последние достижения в области машинного обучения и нейронных сетей. Кроме того, многие ученые и исследователи активно работают над созданием новых алгоритмов и методов для улучшения систем ИИ в кибербезопасности.

Однако, несмотря на все достижения, ИИ для кибербезопасности не является полностью идеальным. Некоторые угрозы еще остаются незамеченными, и некоторые атаки могут быть успешно проведены даже при наличии современных систем ИИ. Этими недоработками активно пользуются киберпреступники. Например, они могут использовать подобные системы для улучшения своих методов атаки и обхода существующих систем защиты.

¹ © Лащенко П. М., 2023.

Кроме того, возникает вопрос о конфиденциальности данных, собранных ИИ для кибербезопасности.

Так, например, по данным экспертов, эти данные могут содержать конфиденциальную информацию, которая может быть использована злоумышленниками для проведения атак.

Существует множество способов применения ИИ в кибербезопасности при получении конфиденциальной информации [3].

Некоторые из них включают:

1. Анализ поведения. Системы ИИ могут использоваться для анализа поведения пользователей в компьютерных сетях. Эти системы могут определять типичное поведение пользователей и выявлять необычные действия, которые могут указывать на попытку взлома или другую кибератаку.

2. Разведка данных. ИИ может использоваться для анализа больших объемов данных, что позволяет выявлять скрытые угрозы безопасности. Например, могут анализироваться данные об уязвимостях, которые могут быть использованы злоумышленниками для атаки.

3. Прогнозирование. ИИ может использоваться для прогнозирования возможных угроз безопасности. Например, могут анализировать данные о прошлых атаках, чтобы определить вероятность будущих атак.

4. Автоматическая защита. ИИ может использоваться для автоматической защиты компьютерных систем от кибератак. Например, он может использоваться для автоматического распознавания и блокирования вредоносных программ или для автоматической адаптации системы защиты к новым типам атак.

5. Машинное обучение. Машинное обучение – это один из ключевых компонентов ИИ в кибербезопасности. Системы машинного обучения могут использоваться для обнаружения угроз безопасности, автоматической классификации данных, анализа потенциальных уязвимостей и многого другого.

Применение ИИ в кибербезопасности имеет ряд преимуществ, но также сопряжено с некоторыми рисками.

Преимущества:

1. Способность быстро анализировать большие объемы данных. ИИ способен обрабатывать большие объемы данных и выявлять угрозы безопасности быстрее, чем это может сделать человек.

2. Повышенная эффективность. ИИ может работать круглосуточно, без перерывов на отдых или питание, и обрабатывать значительно больше информации, что позволяет повысить эффективность в обнаружении угроз безопасности.

3. Снижение затрат. Применение ИИ в кибербезопасности может снизить затраты на персонал и оборудование, которые требуются для обнаружения и предотвращения кибератак.

Риски:

1. Недостаточная точность. ИИ может допускать ошибки, что может привести к недостаточной точности в выявлении угроз безопасности.

2. Недостаточная прозрачность. ИИ может быть сложен для понимания, что может сделать его принятие решений непрозрачным.

3. Уязвимость к атакам. ИИ может стать объектом атак злоумышленников, которые могут попытаться изменить данные или повлиять на решения, принимаемые системой.

4. Ограниченность. ИИ может быть ограничен в способности адаптироваться к новым типам атак или воспринимать нестандартные ситуации.

Таким образом, развитие и применение ИИ в кибербезопасности имеют огромный потенциал для обнаружения и предотвращения кибератак. ИИ может быстро анализировать большие объемы данных, работать круглосуточно и повышать эффективность в обнаружении угроз безопасности.

Однако также важно учитывать потенциальные риски, связанные с применением ИИ, такие как недостаточная точность, недостаточная прозрачность, уязвимость к атакам и ограниченность в адаптации к новым типам атак.

Поэтому необходимо продолжать исследования в этой области и развивать новые методы и технологии, чтобы максимально эффективно использовать ИИ в кибербезопасности и минимизировать потенциальные риски.

В заключение необходимо отметить, что использование ИИ в кибербезопасности является необходимым шагом для защиты информации и повышения уровня безопасности в цифровой сфере.

Список литературы

1. Что такое ИИ? Подробнее об искусственном интеллекте. URL: <https://www.oracle.com/cis/artificial-intelligence/what-is-ai/>.
2. Google's AI-powered Cybersecurity Solution Is Now Generally Available. URL: <https://venturebeat.com/2021/07/29/googles-ai-powered-cybersecurity-solution-is-now-generally-available/>.
3. Искусственный интеллект в кибербезопасности. URL: <https://hashdork.com/ru/artificial-intelligence-in-cybersecurity/>.

Боровиков В. Б.¹,

профессор кафедры уголовного права

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

Боровикова В. В.²,

доцент кафедры уголовного права

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

О ПРОБЛЕМАХ ПРЕПОДАВАНИЯ РАЗДЕЛОВ КУРСА УГОЛОВНОГО ПРАВА ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Цифровизация общества существенным образом повлияла на все его сферы, в том числе и систему образования.

Можно по-разному относиться к этому процессу. Но реалии таковы, что информационные технологии³ есть, вложены огромные деньги в их производство, существует немало заинтересованных лиц, имеющих значительное влияние в государственных структурах и бизнесе.

Система образования одна из первых столкнулась с процессом цифровизации и определенным образом на это отреагировала. Особое значение проблема цифровизации приобрела в связи с распространением «COVIDA-19», когда учебные заведения страны были вынуждены использовать дистанционное обучение. Оно вызвало противоречивую реакцию в педагогическом сообществе, связанную с наличием ряда негативных последствий, указанного процесса. Вместе с тем, как мы уже писали, есть и активные сторонники внедрения названных выше технологий в образовательные учреждения Российской Федерации. Правда, в последнее время, на наш взгляд, стали появляться более аргументированные суждения, согласно которым надо избегать крайностей в деле цифровизации российского образования.

Особо выделим в связи с этим выступление Секретаря Совета безопасности РФ Н. П. Патрушева, в котором он подчеркивает, что именно советская школа образования исторически была самой передовой и прогрессивной в мире, и движение вперед должно осуществляться с учетом этого обстоятельства. «Нельзя делать ставку исключительно на цифровизацию образования, поскольку Интернет может быть не только источником энциклопедических сведений, но и политизированной дезинформацией».

¹ © Боровиков В. Б., 2023.

² © Боровикова В. В., 2023.

³ Данный термин для удобства мы будем преимущественно использовать в нашей публикации.

Итак, мы согласны с этим утверждением. Подчеркнем лишь, что никакие информационные технологии не заменят мастерство преподавателя, обладающего высокой общей и профессиональной культурой, который в яркой и доходчивой форме, умело используя разнообразные методики обучения, может вызвать интерес у обучающихся, создать атмосферу, благоприятную для усвоения и получения знаний.

Вместе с тем информационные технологии тоже могут приносить свою пользу, например, в части усиления наглядности обучения, расширения возможностей проведения консультационной и самостоятельной работы, педагогического промежуточного контроля.

Данные рассуждения имеют отношение к преподаванию курса уголовного права, в том числе и тем, где речь идет об ответственности за преступления, совершенные с использованием информационных технологий. При этом надо иметь в виду, что уголовный закон запрещает не только совершение деяний, указанных в гл. 28 УК РФ «Преступления в сфере компьютерной информации», но и другие формы общественно опасного поведения, названные в иных главах кодекса.

Об особенностях преподавания темы курса уголовного права «Преступления в сфере компьютерной информации».

Тема объективно сложная, т.к. она насыщена специальной терминологией. Поэтому в принципе для курсантов и слушателей полезно уже в процессе лекции по данной теме иметь раздаточный материал, содержащий основные термины, определения и понятия, относящиеся к гл. 28 УК РФ. Конечно, можно использовать и слайды для мультимедийного обеспечения. Но есть опасность, что только изучение и написание этих терминов «заберут» основное учебное время (на освещение других вопросов лекции останется мало времени).

В связи с чем, на наш взгляд, необходима подготовка словаря основных терминов, понятий, определений для изучения темы «Преступления в сфере компьютерной информации». Это будет полезным подспорьем в изучении ее положений.

Далее в процессе лекции целесообразно обратить внимание на специфику уголовно-правовой политики в области борьбы с преступлениями, совершаемыми с использованием информационных технологий. Это важно по ряду причин: активности применения данных технологий со стороны ряда недружественных к Российской Федерации стран, раскрытия реальной общественной опасности преступности в сфере компьютерной информации, освещения в краткой форме особенностей уголовной ответственности за анализируемые деяния за рубежом, показа вариантов совершенствования уголовного законодательства об ответственности за данные деяния.

И все равно остается проблема нахождения стимулов, способных вызвать интерес к изучению этой темы (отметим, что даже курсанты и слушатели, как показывает педагогическая практика, факультета подготовки специалистов в области информационной безопасности, проявляют больший интерес к другим темам, чем собственно к вопросам ответственности за компьютерные преступления).

Как изменить в лучшую сторону сложившуюся ситуацию?

Ответ — поиск нестандартных методик. Например, по нашему мнению, полезно использовать при изучении данной темы следующую методику. На прак-

тических занятиях, групповых упражнениях учебный коллектив разбивается на команды. Преподаватель, выступая в роли арбитра, задает вопросы (желательно небольшие, например, на знание предмета этих преступлений, отдельных элементов их составов). Команды в течение определенного периода времени дают ответы на поставленные вопросы (в этом данная методика чем-то напоминает известную телеигру «Что? Где? Когда?»); преподаватель их оценивает. По итогам группового упражнения в зависимости от количества набранных баллов объявляется команда победитель. Бесспорно, эта частная методика вызывает оживление в аудитории, интерес к учебной теме. Обучающиеся позитивно относятся к этой форме учебного занятия.

О других «находках». На факультете подготовки специалистов в области информационной безопасности авторы данной статьи используют и уголовно-правовые казусы в стихотворной форме (автор – В. Б. Боровиков). Естественно, использование поэзии не должно «вредить» общему делу. Это лишь дополнительный помощник преподавателя в достижении учебных целей. Но, как показывает педагогическая практика, курсанты и слушатели в целом положительно реагируют на такого рода «вкрапления» в учебные занятия.

Кстати, для более глубокого познания реалий темы «Преступления в сфере компьютерной информации», а также поддержания интереса на семинарских занятиях полезно заслушивание сообщений на тему «Уголовно-правовые проблемы борьбы с компьютерной преступностью в художественных произведениях Е. Замятина, С. Лема, О. Хаксли, Р. Шекли» (выбор авторов может меняться). Этот материал хорошо воспринимается на факультете подготовки специалистов в области информационной безопасности при условии, если заранее провести с будущими докладчиками соответствующую консультационную работу (к сожалению, наши курсанты и слушатели не отличаются особой тягой к чтению художественной литературы).

В ходе семинарских и практических занятий по данной теме, конечно, надо обращать внимание обучающихся на отдельные проблемы квалификации деяний, предусмотренные ст.ст. 272–274.1 УК РФ (в частности, имеются сложности с толкованием таких признаков составов преступлений, как «тяжкие последствия» (ч. 4 ст. 272, ч. 3 ст. 273, ч. 2 ст. 274, ч. 5 ст. 274.1 УК РФ); «причинение вреда критической информационной инфраструктуре Российской Федерации» (ч. 2, 3 ст. 274.1 УК РФ)). Для реальной оценки общественной опасности данных деяний целесообразно уделить место в ходе семинара рассмотрению вопроса о видах и размерах наказания, назначаемых за их совершение.

Кстати, изучение темы «Преступления в сфере компьютерной информации» помогает более глубоко подойти к исследованию и других тем курса уголовного права. Так, появление в июле 2022 г. в УК РФ ст. 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования» заставляет по-новому рассматривать и вопросы темы «Преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления». Дело в том,

что Примечание к ст. 274.2 УК РФ содержит определение должностного лица, противоречащее тому, которое дается в п. 1 примечания к ст. 285 УК РФ.

Естественно, такое положение не способствует уяснению смысла как вопросов применения норм, включенных в гл. 28 УК РФ, так и гл. 30 УК РФ. Следовательно, на законодательном уровне подобные противоречия должны быть устранены.

Вопросы ответственности за иные преступления, совершаемые с использованием информационных технологий, естественно, рассматриваются при анализе признаков основного и квалифицированного составов. В принципе, на наш взгляд, должны применяться те же подходы, о которых было сказано применительно к освещению преступлений, предусмотренных гл. 28 УК РФ (см., например, ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ч. 3 ст. 137, п. «в» ч. 2 ст. 151.2, п. «г» ч. 3 ст. 158, 159.6 УК РФ). Но основное внимание здесь уделяется информационным технологиям как к способу совершения тех или иных преступлений. Ставка в данных случаях делается не столько на раскрытие их собственного содержания, сколько на вопросы квалификации этих деяний, разграничение их со смежными преступлениями. Так, целесообразно значительное место при изучении учебного материала отводить разграничению преступлений, предусмотренных п. «г» ч. 3 ст. 158 УК РФ и ст. 159.3, ст. 159.6 УК РФ. В подобных случаях хорошо использовать и разъяснения Пленума Верховного Суда РФ, данные в соответствующих постановлениях, посвященных применению различных уголовно-правовых норм об ответственности за отдельные виды преступлений. Кроме того, надо рекомендовать курсантам и слушателям ряд работ, где специально анализируются аспекты квалификации преступлений с использованием информационных технологий (см., например, Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е. А. Русскевич. М. : Инфра-М, 2019 ; Юрченко И. А. Преступления против информационной безопасности : учебное пособие. М. : Проспект, 2021; Летелкин Н. В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) : монография / отв. ред. А. В. Петрянин. М. : Проспект, 2020).

Кроме того, в процессе практических занятий по названным выше темам не надо пренебрегать «Практикумом по уголовному праву. Общая и Особенная части». М. : Юрайт, 2022 (автор – Боровиков В. Б.).

Нелишне в ряде случаев для подготовки к практическим занятиям осуществлять подборку уголовно-правовых казусов в Интернете, системе ГАС «Правосудие», печатных СМИ для возможного использования их в процессе преподавания разделов курса уголовного права, в которых рассматриваются вопросы ответственности за совершение преступлений, совершенных с использованием информационных технологий.

Таким образом, цифровизация образования ставит перед профессорско-преподавательским составом, осуществляющим преподавание курса уголовного права вузов МВД России, ряд задач, связанных с повышением эффективности педагогического процесса. Информационные технологии должны найти здесь разумное применение без ущерба тому богатству, которое было накоплено лучшими представителями отечественной науки и педагогики в области уголовного права.

Баранов В. М.¹,

*доцент кафедры стратегического управления
института экономики и менеджмента
Белгородского государственного
технологического университета имени В.Г. Шухова,
кандидат педагогических наук, доцент*

Жукова П. Н.²,

*заместитель начальника кафедры высшей математики
и системного моделирования сложных процессов
Санкт-Петербургского университета ГПС МЧС России,
доктор физико-математических наук, доцент*

Прокопенко А. Н.³,

*профессор кафедры информационных технологий
учебно-научного комплекса автоматизированных систем
и информационных технологий
Академии ГПС МЧС России,
кандидат технических наук, доцент*

ЕДИНАЯ БИОМЕТРИЧЕСКАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ: ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ В ИНФРАСТРУКТУРЕ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

По мере развития систем видеоаналитики, включающей программное обеспечение для распознавания лиц, в России начал подниматься вопрос о необходимости создания единой системы, которая позволяла бы осуществлять идентификацию граждан по фотографии, видеоизображению или голосу. Изначально обсуждались варианты использования других видов биометрии для проведения идентификации, но поскольку аппаратура для распознавания отпечатков пальцев, сетчатки или радужной оболочки глаза не доступна в массовом количестве для российских граждан, то было принято решение использовать видеоизображение и голос. При этом вариант с использованием смартфонов, сканирующих отпечатки пальцев, был отвергнут в связи с их не унифицированной конструкцией, недостаточным качеством снимаемой информации и, самое главное, невозможностью обеспечить конфиденциальность этих персональных данных из-за программного обеспечения принадлежащего иностранным вендорам [1].

Создание системы было поручено Ростелекому и Центральному банку Российской Федерации. Всю техническую часть взял на себя Ростелеком, который инвестировал в создание системы почти 250 млн рублей. Правовым основанием созда-

¹ © Баранов В. М., 2023.

² © Жукова П. Н., 2023.

³ © Прокопенко А. Н., 2023.

ния Единой биометрической системы стал Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2], в который была введена статья 14.1, урегулировавшая отдельные вопросы использования биометрии для идентификации физических лиц [3].

Система была представлена Ростелекомом совместно с Почта Банком, под руководством Банка России на Международном финансовом конгрессе 7 июня 2018 г. [4]. Официальный запуск системы произошел несколько позже – 30 июня 2018 г. Поскольку проект курировался Центробанком, то удалось вовлечь в его реализацию существенное количество финансовых структур – сбором биометрических персональных данных захотели заняться 438 банков [5]. Оператором Единой биометрической системы был назначен разработчик системы «Ростелеком» [6].

В состав сведений, помещаемых в Единую биометрическую систему (ЕБС) включаются данные изображения лица человека, полученные с помощью фото-видео устройств и данные голоса человека, полученные с помощью звукозаписывающих устройств. Состав сведений и особенности их формирования, обработки, хранения и использования установлен в постановлении Правительства Российской Федерации от 30.06.2018 № 772 [7].

Однако по мере реализации проекта возникли трудности с подключением к системе небольших банков, и в результате в программе к началу 2020 г. участвовали только 233 банка, а сведений было собрано всего со 120 тысяч человек [8]. В целом можно указать на недостаточную популярность системы, непроработанность ее для граждан, наличие существенного количества технических проблем, в том числе недостаточная защищенность информации и возможность ее подделки. На этот факт указывал и Герман Греф, который считал, что поскольку система сырая, то банки не надо заставлять ее использовать и предоставлять через нее заранее утвержденный перечень услуг [9].

В 2020 г. было предложено разрешить гражданам самостоятельно регистрироваться в Единой биометрической системе и дистанционно вносить в нее свои биометрические персональные данные. Кроме того, изменения должны были значительно расширить функционал системы и передать ее в собственность государства, сделав соответственно государственной информационной системой. Указанные изменения, которые принципиально скорректировали назначение и функционирование системы были закреплены в Федеральном законе от 29.12.2020 № 479-ФЗ, который внес значительные корректировки в статью 14.1 ФЗ «Об информации...» [10].

В соответствии с изменениями, утвержденными Законом № 479-ФЗ, Единая биометрическая система получила статус государственной информационной системы. Все собранные банками сведения интегрируются в Единую систему идентификации и аутентификации портала Госуслуг, но Ростелеком пока был оставлен ее оператором. При этом использование биометрических персональных данных было распространено на оказание любых финансовых услуг, предоставления государственных услуг и функций, а также нотариальных и страховых услуг. Если изначально размещение сведений осуществлялось только банками, то

в настоящий момент такие права даны многофункциональным центрам и самим физическим лицам, которые могут для этого использовать специализированное мобильное приложение.

Таким образом, до 2022 г. Единая биометрическая система находилась на стадии формирования и позволяла гражданину проходить удаленную идентификацию по биометрическим образцам только для получения некоторых финансовых услуг [11]. После принятия 24.12.2021 Постановления Правительства РФ от № 2459 [12] Единая биометрическая система официально стала частью портала Госуслуги, войдя в состав единой системы идентификации и аутентификации. Интегрирование Единой биометрической системы в систему электронного правительства продолжилось после предоставления ей в июне 2022 г. постановлением Правительства Российской Федерации от 16.06.2022 № 1089 статуса государственной информационной системы [13]. Правила размещения гражданами своих видеозаписей, фотографий и записей голоса, а также контроля их соответствия утверждены Постановлением Правительства РФ от 15.06.2022 № 1066 [14]. В соответствии с указанными Правилами до 1 марта 2023 г. было разработано и внедрено специализированное мобильное приложение, которое позволяет физическим лицам самостоятельно предоставлять в Единую биометрическую систему свои биометрические сведения. Пересдача биометрических данных для их актуализации предусмотрена внепланово при критических травмах или планово с периодичностью один раз в три года [11].

В конце 2022 г. статья 14.1. ФЗ «Об информации...» была признана утратившей силу, а для правового регулирования функционирования Единой биометрической системы был принят новый Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» [15]. При этом принципиальных изменений правовое регулирование Единой биометрической системы не претерпело. Кроме того, в конце 2022 г. было принято решение о замене оператора Единой биометрической системы, функции которого от Ростелекома были переданы вновь созданному АО «Центр Биометрических Технологий» [16].

Для использования Единой биометрической системы к ней был организован доступ через портал bio.rt.ru, впоследствии добавилась возможность подключения к системе через портал Госуслуг gosuslugi.ru, а с 1 марта 2023 г. и через мобильное приложение «Госуслуги Биометрия». Для защиты соединений используется криптографическое шифрование. При этом право аутентификации граждан через ЕБС дано не только банкам, как ранее, но и государственным и муниципальным органам власти, нотариусам и вообще различным организациям, подключившимся к системе. Направления использования Единой биометрической системы были закреплены постановлением Правительства Российской Федерации от 15.06.2022 № 1067 и вступили в силу с 1 марта 2023 г. [17]. Они будут осуществляться посредством интеграции ЕБС с другими информационными системами и в дополнение к целям, упомянутым ранее, позволят:

- предоставлять дистанционные финансовые услуги, как это осуществлялось и до 2023 г., но не обладало существенной популярностью;
- осуществлять дополнительную аутентификацию физического лица при предоставлении очных финансовых услуг;
- предоставлять гражданам расширенный перечень государственных услуг и функций, которые ранее требовали личного присутствия, например, выдача карты болельщика;
- оплачивать мелкие покупки до 1 000 рублей без предъявления банковских карт или мобильных приложений только по лицу в коммерческих организациях, подключившихся к ЕБС;
- оплачивать проезд в общественном транспорте на первом этапе в метро города Москвы;
- заключать договора для оказания услуг, в том числе по подключению к мобильной связи и Интернет;
- использовать ЕБС для аутентификации обучающихся при сдаче вступительных испытаний, зачетов, экзаменов и защите дипломов;
- использовать ЕБС для аутентификации физических лиц для прохода на территорию граждан в детские сады, школы, колледжи, государственные и муниципальные органы и организации.

Резюмируя вышесказанное, необходимо отметить, что в России активно развивается направление сбора, обработки и использования биометрических персональных данных. Создание, помимо имеющихся в правоохранительных органах информационных систем биометрических персональных данных, общегосударственной Единой биометрической системы, является существенным шагом на пути цифровизации российской экономики и системы государственного управления.

Оценивая перспективы использования Единой биометрической системы, можно отметить, что за счет расширения ее функциональных возможностей количество собранных биометрических персональных данных должно возрасти, а популярность системы увеличиться. В настоящий же момент активность граждан в данной сфере невелика. В перспективе Единая биометрическая система должна стать системой аутентификации граждан всей страны, которая позволит не только получать финансовые услуги или проходить в метро, однозначно привязать человека к его учетной записи на портале Госуслуг, но и оплачивать покупки и получать услуги. За счет использования системы будет возможно ведение медицинской карты физического лица, организация удаленного голосования на выборах всех уровней, регистрация нотариальных действий и коммерческих сделок, а также другие функции [18]. Рассмотренная единая система идентификации физических лиц позволит не только облегчить и улучшить жизнь российских граждан, но и значительно снизит количество преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Список литературы

1. Сайт Единой биометрической системы. Раздел «Общие вопросы». URL: <https://bio.rt.ru/faq/project/>.

2. Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://www.pravo.gov.ru>.
3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. № 165. 2006.
4. Анна Еремина. ЦБ и «Ростелеком» показали, как будет работать Единая биометрическая система // «Ведомости». 2018. 07 июня.
5. В РФ с 1 июля запустят систему биометрической идентификации: Биометрия будет использоваться банками для удаленной идентификации клиентов при открытии счетов // «Интерфакс». 2018. 29 июня.
6. Распоряжение Правительства РФ от 22 февраля 2018 г. № 293-р (утратило силу) «О возложении на публичное акционерное общество междугородной и международной электрической связи «Ростелеком» функций оператора единой информационной системы персональных данных» // Собрание законодательства Российской Федерации. 2018. № 11. Ст. 1640.
7. Постановление Правительства РФ от 30 июня 2018 г. № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства Российской Федерации. 2018. № 28. Ст. 4234.
8. Вероника Горячева. У банков сдвигается биометрия: ЦБ готов пойти на встречу рынку при внедрении новой технологии // «Коммерсантъ». 2018. 19 октября.
9. Людмила Петухова. Почему забуксовал проект по оцифровке россиян и при чем тут ФСБ и Греф // «Forbes.ru». 2020. 27 марта.
10. Федеральный закон от 29 декабря 2020 г. № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.
11. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» / [Р. В. Амелин и др.]. Электронное издание. Специально для системы ГАРАНТ, 2020.
12. Постановление Правительства РФ от 24 декабря 2021 г. № 2459 «О внесении изменений в постановление Правительства Российской Федерации от 8 июня 2011 г. № 451» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.
13. Постановление Правительства РФ от 16 июня 2022 г. № 1089 «Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия

предоставленным биометрическим персональным данным физического лица» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.

14. Постановление Правительства РФ от 15 июня 2022 г. № 1066 «О размещении физическими лицами своих биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.

15. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.

16. Постановление Правительства РФ от 16 декабря 2022 г. № 2326 «О возложении на акционерное общество «Центр Биометрических Технологий» функций оператора единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также о признании утратившими силу распоряжения Правительства Российской Федерации от 22 февраля 2018 г. № 293-р и пункта 4 изменений, которые вносятся в акты Правительства Российской Федерации, утвержденных постановлением Правительства РФ от 24 июня 2021 г. № 982» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.

17. Постановление Правительства РФ от 15 июня 2022 г. № 1067 «О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.

18. Попов О. В., Прокопенко А. Н. Особенности правового регулирования использования биометрических персональных данных в системе государственного управления на современном этапе цифровой трансформации общества // Административное право и процесс. 2023. № 2. С. 22–24.

Рамаева К. В.¹,
инспектор
учебно-методического центра
ГУ МВД России по Московской области

ПОЗИТИВНЫЙ РЕЗУЛЬТАТ ОТ ВНЕДРЕНИЯ В ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В настоящее время преступность вышла на новый уровень реализации криминальных мотивов, что обуславливается техническим прогрессом и цифровизацией социального пространства. Гражданские отношения на данном этапе развития также подвержены трансформации, так как покупки, досуг, общение, работа чаще всего связаны с взаимодействием в информационном пространстве. Поэтому информационно-телекоммуникационные технологии стали неотъемлемой частью нашей повседневной жизни.

Такое развитие событий заставляет видоизменяться не только преступную среду. Процесс информатизации и цифровизации гражданского общества влияет на деятельность правоохранительных органов. Связано это с тем, что система ОВД должна разрабатывать и использовать новые методы защиты государства и общества от преступных посягательств.

Оптимизировать работу правоохранительных органов возможно посредством внедрения в деятельность ОВД информационно-телекоммуникационных систем, позволяющих структурировать данные, ускорять процесс взаимного обмена оперативнозначимой информацией, архивировать и хранить необходимые сведения, вести статистический учет, регулировать вопросы административно-распорядительного характера, реагировать на управленческие решения, контролировать аналитический процесс, повышать уровень безопасности для общества и государства.

Для нужд правоохранительных органов было принято воспользоваться решениями информационно-телекоммуникационных технологий.

Конечно, сотрудники ОВД уже давно пользуются продуктами цифровизации для выполнения возложенных на них обязанностей.

Таким образом, для документооборота используются программы «Microsoft Office», а именно: Access, Word, PowerPoint, Excel. Данные программы необходимы для работы с процессуальными документами, заполнения бланков следственных действий, направления запросов и поручений, составления фототаблиц, графиков и для решения других задач. Для внутреннего документооборота используются ресурсами СЭД.

Помимо вышеперечисленных программ, особую роль в деятельности ОВД играет использование различных информационно-справочных ресурсов, например, «Гарант», «КонсультантПлюс», «Кодекс».

¹ © Рамаева К. В., 2023.

Для работы с изображениями, схемами, таблицами или видеоматериалами может возникнуть потребность в использовании графических редакторов, например «Adobe Photoshop».

Кроме того, сотрудники ОВД, уполномоченные осуществлять оперативно-разыскные мероприятия, для контроля почтовых отправлений, телеграфных и иных сообщений, прослушивания телефонных переговоров, а также их контроль и запись, пользуются специальными техническими средствами с соответствующим программным обеспечением.

Применяются информационно-поисковые системы, например, «АБД-Центр», ИЦ, «Сфера», «Паутина», «ГЛОНАСС» для обнаружения лиц, подозреваемых в совершении преступления, поиска транспортного средства, трупа, похищенного имущества, огнестрельного оружия, а также средств и веществ, запрещенных в гражданском обороте.

Для судебных трасологических, баллистических, портретных, автотехнических и компьютерных экспертиз обращаются к автоматизированной информационной системе «Папилон», а для вопросов баллистики к системе «Арсенал».

Одним из ведущих направлений информатизации и оптимизации работы в ОВД является использование баз данных, которые содержат информацию, непосредственно относящуюся к лицам: подозреваемым в совершении преступления, свидетелям, потерпевшим, очевидцам, что позволяет установить круг общения, криминальные связи, взаимодействие с криминальными элементами. Кроме того, характеристику на то или иное лицо можно получить посредством анализа движения денежных средств искомого, его доходы и расходы, денежные переводы, использование электронных кошельков или крипто-кошельков.

Для хранения массива информации сотрудники правоохранительных органов активно пользуются ИСОД.

Для осуществления рабочего процесса каждый сотрудник снабжен АРМ, позволяющим пользоваться информационными ресурсами, базами данных, работать с документами, обмениваться файлами и информацией в цифровом пространстве.

Однако использование вышеперечисленных технологических решений не гарантирует повышения эффективности работы сотрудников ОВД.

На практике мы встречаемся с такими проблемами, как:

- 1) ограниченность кадрового ресурса;
- 2) отсутствие необходимых знаний у сотрудников для успешного использования продуктов информационно-телекоммуникационного свойства;
- 3) высокие финансовые затраты на соответствующее оборудование;
- 4) сложность в освоении нового программного обеспечения;
- 5) нехватка времени для понятия принципов работы продукта информационно-телекоммуникационных технологий;
- 6) быстроменяющееся оборудование;
- 7) небольшое количество сотрудников, готовых передать знания и привить навык работы с информационными системами.

Несмотря на то что проблем в реализации заявленного технического процесса много, есть и позитивная сторона рассматриваемого вопроса по внедрению информационно-телекоммуникационных технологий.

Так как проблемы выявлены и обозначены, то можно разработать методику по работе с личным составом ОВД. При приеме на работу уже многие сотрудники обладают цифровыми компетенциями и имеют базовые знания для работы с продуктами информатизации, что значительно облегчает выполнение возложенных на правоохранительные органы обязанностей.

В случае успешного преодоления трудностей, связанных с применением в деятельности ОВД информационно-телекоммуникационных технологий, эффективность рабочего процесса повысится и станет возможным решить следующее:

- задачу автоматизации основных видов деятельности подразделений МВД России;

- организовать централизованное хранение и обработку данных;

- повысить эффективность выполнения государственных функций;

- снизить срок предоставления государственных услуг и оптимизировать данный процесс;

- использовать единое пространство по предоставлению информации для сотрудников ОВД;

- облегчить доступ к информационным ресурсам, что позволит оперативно обрабатывать необходимую информацию и использовать в превенции преступных фактов;

- улучшить качество кадрового ресурса, так как сотрудники будут обладать способностью работы с информационно-телекоммуникационными технологиями без ущерба в продуктивности;

- достичь высокого уровня информационно-аналитического обеспечения;

- снизить финансовые затраты на техническое оборудование, его обслуживание и сопровождение;

- снизить трудозатратность на получение, обработку, хранение информации и доведение ее до пользователей.

Таким образом, можно отметить позитивную тенденцию внедрения в деятельность ОВД информационно-телекоммуникационных технологий. Использование продуктов цифровизации позволяет в короткий срок собрать необходимую информацию, обладающую оперативной значимостью, чтобы выявить преступные факты и разработать методику борьбы с ними. Плюрализм баз данных и программного обеспечения повышает динамику успешного расследования преступлений, исключает возможность привлечения к уголовной ответственности невиновных лиц, а также позволяет осуществлять превентивную функцию, так как позволяет выявить лиц, способных на совершение преступления, вычислить их круг общения и установить мониторинг за их деятельностью.

Главным достоинством применения информационно-телекоммуникационных технологий является помощь сотрудникам ОВД при работе с большим объемом информации и вводных данных, так как наибольшую сложность вызывает обработка неструктурированных данных, которые значительно повышают степень неопределенности и риска при принятии решений назначения экспертиз, следственных действий, оперативных мероприятий и других решений процессуального характера. Переработать такой объем данных возможно только за счет применения современных информационных технологий, основанных на перспектив-

ных методах анализа данных. Значительная роль в процессе принятия решений отводится системе информационно-аналитического обеспечения как одного из ключевых компонентов системы управления.

На данном этапе внедрения продуктов информатизации и цифровизации в деятельность ОВД существует еще много недоработок, далеко не все еще разработано и функционирует без изъянов, но, несмотря на все имеющиеся недостатки, более 90 % преступлений расследуются с использованием информационно-телекоммуникационных технологий.

Список литературы

1. Информационные технологии в управлении органами внутренних дел : учебник / В. В. Баранов и др. ; под ред. И. В. Горошко. М. : Академия управления МВД России, 2015.
2. Лукашов Н. В., Лебедев В. Н., Макаров В. Ф. Информатизация и информационная безопасность органов внутренних дел : курс лекций. М. : Академия управления МВД России, 2012.
3. Торопов Б. А., Апульцин В. А. Технологии многокритериального оценивания результатов деятельности территориальных органов МВД России на региональном уровне : учебное пособие. М. : Академия управления МВД России, 2016. Защита информации : учебник в двух томах.
4. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // Собрание законодательства Российской Федерации. 2011. № 7. Ст. 900.
5. Указ Президента РФ от 1 марта 2011 г. № 248 «Вопросы Министерства внутренних дел Российской Федерации» // Российская газета. 2011. 2 марта (№ 43).

Ситников А. А.¹,

слушатель факультета подготовки

специалистов в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Елин В. М.,

доцент кафедры информационной безопасности

Московского университета МВД России имени В.Я. Кикотя,

кандидат педагогических наук

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА АВТОМАТИЗИРОВАННОГО ПОИСКА ОПЕРАТИВНО ЗНАЧИМОЙ ИНФОРМАЦИИ В СИСТЕМАХ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ

Процесс коммуникации является основной частью социального взаимодействия, которое обеспечивает выживание и доминирование определенного вида. Также в работе «Концептуальные представления о структуре общения» доктор психологических наук О. В. Зациринская выделяет три основные составляющие структуры общения: помимо представленной выше коммуникативной (обмен информацией), перцептивная (взаимное восприятие), интерактивная (взаимодействие с использованием как познаний, так и отдельных действий [1].

Администрация СМОС Telegram по некоторым данным официально сотрудничает и предоставляет информацию правоохранительным органам Российской Федерации только в том случае, когда объектом преступного посягательства является общественная безопасность или нормальное функционирование органов власти. Учитывая данное обстоятельство, растущее количество пользователей сети, а также тот факт, что мессенджер имеет открытый исходный код программного интерфейса приложения и подробно описанную документацию по работе с API, актуальность данной темы заключается в оперативном сборе и обработке информации, находящейся и генерируемой пользователями в социальной сети.

Во всем мире насчитывается почти четыре миллиарда пользователей социальных сетей, что составляет практически 57 % всего мирового сообщества. Типичный пользователь активно посещает в среднем шесть различных платформ и проводит около двух часов в социальных сетях каждый день. Учитывая тот факт, что человеку свойственно находиться в состоянии сна от 7 до 8 часов в день, эти данные показывают, что примерно 15 % бодрствующей жизни составляет время, уделяемое социальным сетям.

Обмен мгновенными сообщениями – это форма онлайн-общения в режиме реального времени. История мгновенных сообщений (IM) восходит к 1960-м годам, но современные IM, какими мы их знаем в настоящее время, начались в середине 1990-х годов с очень популярных ICQ или AOL Instant Messenger. В настоящее

¹ © Ситников А. А., 2023.

время человеческое взаимодействие и общение все чаще происходят в цифровой сфере, а обмен мгновенными сообщениями представляет собой цифровую версию разговорного диалога.

Сегодня многие социальные сети также предоставляют ту или иную форму решения для обмена сообщениями. Пользователи в этом плане очень требовательны. Мессенджеры де-факто должны иметь как мобильный, так и веб-доступ, желательно в форме полноценных мобильных и десктопных приложений, а также более продвинутые возможности, нежели текстовые сообщения, например, мультимедиа, голос или обмен данными о местоположении. Стоит отметить, что массовое отслеживание действий, а также передача информации специальным службам, информация, поступившая от бывшего сотрудника АНБ Эдварда Сноудена, подстегнули спрос на безопасность и конфиденциальных сведений.

В условиях современного киберпространства раскрытие преступлений требует оперативного и эффективного поиска информации, сконцентрированной на криминогенных объектах сети. Такие объекты могут содержать следы противоправной деятельности, сообщения свидетелей или участников преступлений, а также ссылки на запрещенные материалы. Для получения нужной информации необходимо анализировать коммуникационные акты, которые могут быть осуществлены через различные каналы, включая закрытые и открытые чаты мессенджера Telegram, электронную почту, сеансы прямой связи или зашифрованные сообщения, размещенные на общедоступных сетевых информационных ресурсах с использованием стеганографии. Поэтому проведение оперативно-разыскных мероприятий в сети Интернет можно рассматривать как процесс оперативного поиска ценной информации на криминогенных объектах.

Для более эффективной и результативной работы была разработана интеллектуальная система автоматизированного поиска оперативно значимой информации.

В заключение отметим, что данное направление представляет собой одно из наиболее перспективных в сфере своевременного предупреждения преступности, а также поиска оперативно значимой информации для целей ОРД. Успешное испытание ИСАП «Волкон» показало свою работоспособность и актуальность на практике.

Список литературы

1. Защирина О.В. Концептуальные представления о структуре общения // Вестник Санкт-Петербургского университета. Серия 12.
2. DataReportal «отчет о цифровых трендах 2023 года» // URL: <https://datareportal.com/reports/digital-2023-russian-federation?rq=russia>.
3. Официальный интернет-портал правовой информации // URL: <http://publication.pravo.gov.ru/Document/View/0001202203040007?index=2&rangeSize=1>.
4. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // Собрание законодательства Российской Федерации. 2011. № 7. Ст. 900.
5. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

Фролкина А. М.¹,

слушатель факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Овчинский А. С.,

профессор кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

доктор технических наук, профессор, Академик РАЕН

МОДЕЛЬ ЦИФРОВОЙ ПЛАТФОРМЫ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ

Современная инфоцивилизация становится свидетелем поистине колоссальных изменений в сфере информационных технологий, которые непосредственно влияют на изменение геоэкономических, геополитических, а также геокультурных процессов современного мира. Одновременно с развитием цифровой индустрии и информационно-коммуникационных технологий происходят процессы криминализации, которые отражают развитие преступности, совершаемой с помощью цифровых технологий.

Профилактику преступных деяний в сфере информационных технологий можно классифицировать следующим образом:

- общесоциальная профилактика;
- криминологическая профилактика;
- оперативно-разыскная профилактика.

Общесоциальная профилактика направлена на предложение и реализацию мер, направленных на повышение уровня жизни и благополучия граждан.

Криминологическая профилактика основывается на накопленных ресурсах знаний о преступности в цифровом мире, законодательной базе и правоприменительной практике.

Оперативно-разыскная профилактика подразумевает под собой деятельность, направленную на информационно-аналитическое и информационно-психологическое сопровождение мероприятий по выявлению угроз общественной безопасности, оперативному реагированию, направленному на предупреждение, предотвращение и пресечение криминальной активности.

На сегодняшний день на законодательном уровне понятие цифровой платформы не закреплено, однако в научной литературе данный термин трактуется следующим образом: «Цифровая платформа – это открытая среда и экосистема с понятным набором смоделированных правил, вспомогательных руководств для пользователей, ресурсов и службы поддержки, которые стимулируют сотрудничество представителей всех референтных групп для создания не только обще-

¹ © Фролкина А. М., 2023.

ственной ценности, но и ценности для каждого участника в отдельности так, как он ее понимает».

В настоящее время цифровые платформы стали выполнять не только оптимизацию технологических решений, но и формировать социоинформационные пространства, которые обуславливают повышение производительности труда.

Принято выделять следующие виды цифровых платформ:

- инструментальные;
- инфраструктурные;
- прикладные.

Под инструментальными цифровыми платформами понимается совокупность программно-аппаратных продуктов, позволяющих ускорить разработку программных и программно-аппаратных решений для обработки информации с помощью предоставления шаблонных функций и типовых интерфейсов, рабочего инструментария для создания и отладки средств прикладного назначения.

Цифровые платформы, используемые в правоохранительной деятельности, непосредственно влияют на раскрытие и расследование преступлений, однако помимо всего прочего на показатели преступности прямо пропорционально влияют такие действия, как профилактика и предупреждение преступных деяний. Для создания цифровой платформы по профилактике преступлений необходимо уделить внимание трем направлениям:

- создание модели закрытой (административной) части цифровой платформы, т. е. функционал платформы, не видимый пользователем;
- создание модели открытой (пользовательской) цифровой платформы, т. е. функционал, доступный пользователю на web-сайте;
- создание модели программной оболочки мобильного приложения цифровой платформы, т. е. функционал, доступный пользователю при использовании мобильного приложения.

Требования к цифровой платформе: создавать учетную запись пользователя; редактировать личную информацию в учетной записи; оставлять сообщения модератору и исполнителям; отображать статус сообщения пользователя; просматривать новостную ленту; просмотр FAQ; предоставлять доступ к развлекательному модулю.

Данная подсистема должна содержать следующие модули:

- модуль авторизации пользователей в системе;
- модуль распределения прав доступа;
- модуль «Администрирование», включающий в себя создание учетных записей пользователей, ведение нормативно-справочной информации, формирование структур первоначальных сообщений с помощью конструктора первоначальных сообщений;
- модуль «Аналитическая справка», включающий в себя статистическую информацию о предоставлении юридической и психологической помощи гражданам;
- модуль «Модерация чатов», где будет происходить распределение потоков сообщений по направлениям юридической и психологической помощи, а также осуществляться контроль за формами сообщений;

– модуль «Оказание помощи», представленный в виде мессенджера, где граждане могут получать помощь специалистов.

Открытая часть цифровой платформы должна включать в себя следующие модули:

- модуль «Личный кабинет», где будет отражена информация о пользователе;
- модуль «Сообщения», представленный в виде чата, где граждане могут получить юридическую и психологическую помощь;
- модуль «Новости», где будут отражены положительные аспекты службы представителей органов внутренних дел;
- модуль «Развлечения», представленный в виде игр (визуальных новелл, викторин), направленных на повышение уровня осведомленности граждан в сфере преступности, а также на формирование высокого уровня доверия граждан к правоохранительным органам.

Создание цифровой платформы по профилактике преступлений в социально-информационных сферах позволит повысить уровень осведомленности о новейших способах совершения преступлений в информационной сфере, повысить степень доверия к правоохранительным органам со стороны граждан, помимо всего прочего отдельный блок цифровой платформы может выступать в роли помощника для граждан, нуждающихся в психологической поддержке или юридической консультации, при столкновении каким-либо образом с преступной средой, а в перспективе цифровая платформа позволит осуществлять целенаправленные информационно-психологические воздействия с целью помощи жертвам преступления, а также выявления преступных намерений у злоумышленников и предотвращения преступлений.

Список литературы

1. Гретченко А. А. Типы цифровых платформ и их содержание // Научная статья. 2020 // URL: <https://cyberleninka.ru/article/n/typy-tsifrovyyh-platform-i-ih-soderzhanie>. С. 1–3.
2. Симонова С. С. Теория и практика профилактики преступлений : учебное пособие. 2022. С. 54–68.
3. Путин В. В. Выступление Президента РФ на расширенном заседании коллегии МВД России // URL: <https://66.ru/news/society/261870>.
4. Фрумкин К. Г. Клиповое мышление и судьба линейного текста // Литературно-философский журнал Топос. 2010 // URL: <https://www.topos.ru/article/7371>.
5. Millard J. Open governance systems: Doing more with more // Government Information Quarterly. 2018.

Цыцурин С. Л.¹,

научный сотрудник

ФКУ НПО «Специальная техника и связь» МВД России

АВТОМАТИЗАЦИЯ ПОИСКА СВЕДЕНИЙ В ОТКРЫТЫХ ИСТОЧНИКАХ – ЭФФЕКТИВНОЕ СРЕДСТВО ПРОВЕДЕНИЯ ОПЕРАТИВНЫХ МЕРОПРИЯТИЙ

Российская Федерация на рынке разработки и внедрения информационно-аналитических систем предлагает одни из лучших в мире аппаратно-программные решения в области обеспечения информационной безопасности, легального контроля, мониторинга сети, аналитических комплексов и платформ.

Одним из них является программный комплекс «Виток-OSINT» (далее – Комплекс), обеспечивающий эффективный поиск сведений в открытых источниках информации и их последующий анализ.

Ручной поиск сведений в открытых источниках занимает много времени, его качество зависит от знаний, умений конкретного специалиста и требует большого количества аккаунтов для авторизации на различных ресурсах.

Для решения такого рода проблем находит свое применение рассматриваемый Комплекс, являясь эффективным средством автоматизации деятельности по поиску сведений в открытых источниках. Комплекс позволяет унифицировать процедуру поиска сведений, осуществляя ее быстро и эффективно.

Комплекс прошел апробацию в подразделении органа внутренних дел, где по объективным замерам показал сокращение времени поиска в десятки раз с существенным повышением его качества.

К основным решаемым задачам Комплекса относятся:

- поиск информационного следа объекта интереса по различным входным данным (IP-адрес, доменное имя, адрес электронной почты, номер телефона, ФИО, ИНН, биткоин-адрес, государственный номер автомобиля, идентификаторы в социальных сетях и другие). Поиск по одним данным приводит к нахождению других, таким образом, получается итерационное, комплексное изучение объекта интереса;

- изучение связей объекта интереса. Важнейшую роль здесь имеет как механизмы сбора сведений из социальных сетей (друзья, профили, оставляющие комментарии, лайки и т. д.), так и встроенные в Комплекс механизмы построения и кластеризации графов, позволяющих визуализировать данные, а также определять элементы с наиболее плотными связями (рис. 1);

- формирование статистики. Данный механизм позволяет решать самые разные задачи, начиная от удобной навигации по данным, заканчивая поиском мест притяжения объекта интереса, его потенциальной сферы деятельности (рис. 2).

¹ © Цыцурин С. Л., 2023.

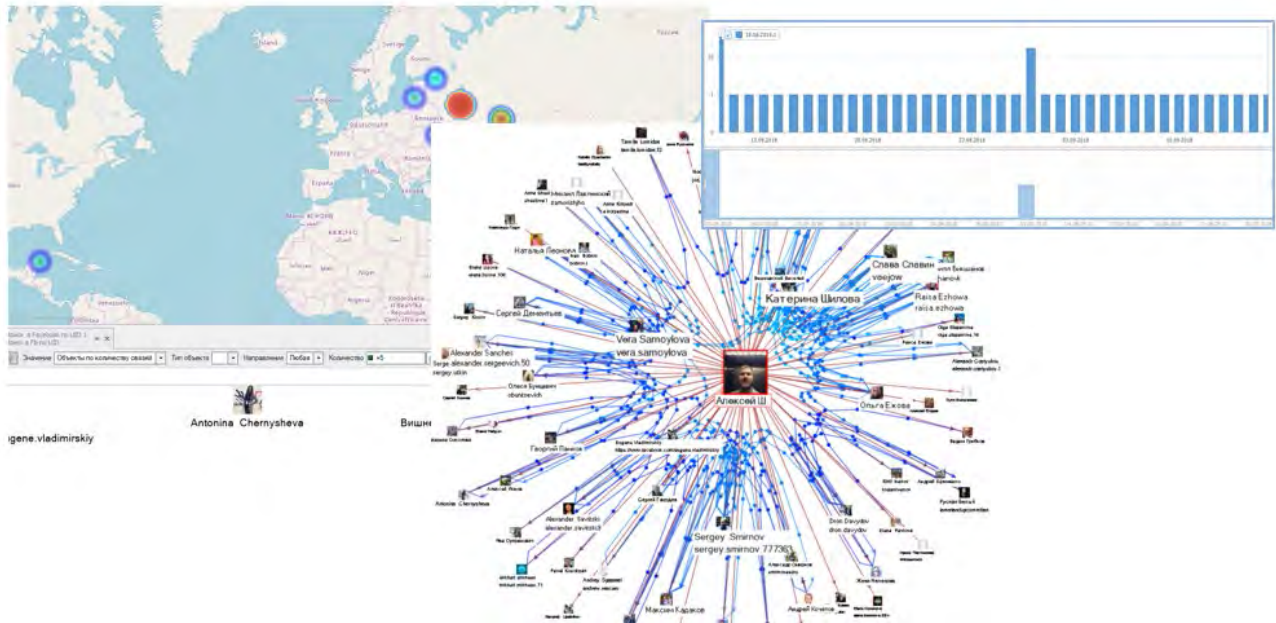


Рис. 1. Механизмы построения и кластеризации графов

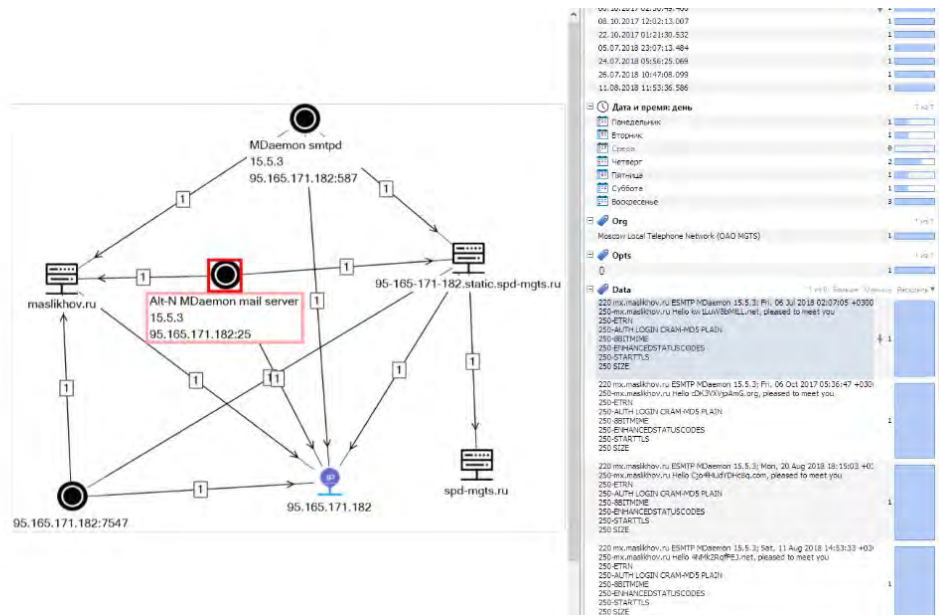


Рис. 2. Задачи комплекса

В Комплексе заложены следующие основные компоненты:

- среда бескомпроматного доступа. Отвечает за сокрытие источника запроса в открытые источники, а также за анонимную авторизацию на различных платформах (социальные сети, форумы, приложения и пр.);
- поисковые роботы. Отвечают за автоматические запросы к источникам данным. Комплекс содержит более 400 поисковых роботов, поддерживаемых в актуальном состоянии;
- аналитический интерфейс. Позволяет проанализировать выявленные сведения, построить взаимосвязи между объектами, сделать картографическую визуализацию данных и пр. В данном интерфейсе реализовано множество различных аналитических инструментов, накопленных по направлению прикладной работы и научных изысканий в области анализа больших массивов данных;

– вспомогательные подсистемы, предназначенные для регистрации профилей и обхода проверки со стороны сервисов. К ним можно отнести сервисы по решению капчи, приему СМС, регистраторы электронной почты и пр.

Источники Комплекса условно разделяются на несколько категорий:

- сервисы, предназначенные для поиска информации по автомобилю;
- поиск данных по географическим координатам;
- общедоступные государственные сервисы;
- сервисы, предназначенные для поиска информации по юридическим лицам;
- мессенджеры;
- сервисы, предназначенные для поиска информации по изображению;
- сервисы, предназначенные для анализа сетевой безопасности;
- социальные сети;
- приложения, порталы для занятия спортом;
- иные источники.

Список источников Комплекса регулярно пополняется. Разработчики постоянно проводят исследования новых источников информации и регулярно ведут работы по автоматизации взаимодействия с ними. Работа по изучению источников включает в себя и нахождение неявных механизмов поиска, скрытых от глаз пользователя, анализ исходного кода сервиса и передаваемого трафика.

Также стоит отметить, что пользователи Комплекса могут работать и с собственными локальными файлами, применяя к ним как возможности по аналитике данных, так и механизмы по обогащению данных. Создание коннекторов к новым источникам данных (как внешних, так и внутренних) имеет в Комплексе открытую документированную структуру, в связи с чем новые источники данных могут быть подключены как специалистами разработчика, так и пользователем.

Накопление полученных данных возможно и на сервере, установленного у пользователя Комплекса. Помимо этого, есть возможность сохранения полученных сведений в виде отдельной папки, с которой можно будет потом продолжить работу или экспортировать в отчет.

Для удобства пользователей организована техническая поддержка Комплекса, одной из особенностей которой является организация дежурной смены, контролирующей работоспособность источников данных и при необходимости вносящей своевременные корректировки в работу поисковых роботов. В самом же Комплексе встроен механизм оповещения пользователей о новых функциях и источниках данных.

Комплекс внесен в реестр отечественного программного обеспечения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Он зарекомендовал себя как надежное и эффективное средство для проведения оперативных работ по поиску информации в открытых источниках, что послужило основанием принятия его в 2021 г. на снабжение органов внутренних дел Российской Федерации.

Шайдаев М. Ш.¹,

*старший научный сотрудник
отдела координации и внедрения
научно-технической продукции Центра сопровождения
научно-исследовательских и опытно-конструкторских работ
в области информационных технологий
ФКУ НПО «Специальная техника и связь» МВД России,
кандидат юридических наук*

ВОЗМОЖНОСТИ ТЕХНОЛОГИЙ ИНТЕРНЕТА ВЕЩЕЙ В ОБЕСПЕЧЕНИИ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Информационные технологии уже давно вошли в повседневную практику и нашли применение во многих сферах общественной жизни и экономики. И с каждым годом ученые-специалисты и разработчики расширяют круг возможностей их использования.

1999 год отмечается появлением новой информационной технологии интернета вещей, который благодаря увеличению числа новых технологий, используемых в повседневной жизни, и количеству устройств, подключенных к интернету, к настоящему времени претерпел колоссальные изменения, превратившись в сложную систему элементов и взаимодействий.

Интернет вещей (Internet of Things, IoT) – это комплексное понятие, подразумевающее под собой экосистему устройств, подключенных к сети. Это могут быть представители любой привычной техники, которые выходят в Интернет и взаимодействуют друг с другом.

Для интернета вещей характерно три признака: наличие большого количества устройств, подключенных к сети Интернет, аккумулялирование данных об окружающем пространстве и обмен ими между соединенными устройствами, автоматическое (без участия людей) осуществление устройствами интернета вещей своих функций [1].

Технологии интернета вещей нашли применение в огромном количестве сфер, начиная от промышленности и заканчивая перспективным направлением развития как «умный город» и другие схожие проекты.

Принцип работы интернета вещей зависит от сферы применения и используемых устройств и в общем представляет собой систему, состоящую из устройств, взаимодействующих между собой и внешним миром посредством Интернета. Самый простой пример подобного интернета вещей – умный дом, так называемый консьюмерский вариант.

Другим видом, отличающимся намного большими масштабами применения, является индустриальный интернет вещей, в котором могут быть задействованы сотни и тысячи человек, например, умный город, интернет вещей

¹ © Шайдаев М. Ш., 2022.

в аграрном секторе, логистике, сфере ЖКХ, медицине, транспорте, сфере безопасности и др.

По прогнозам специалистов, интернет вещей будет только развиваться. Это связано как с ростом количества умных устройств, так и совершенствованием интернет-сетей, например создание сетей пятого поколения. Кроме того, развитию интернета вещей способствует ряд его преимуществ: освобождение специалистов от мониторинга различных показателей при экономии времени, иными словами, обеспечение эффективной работы без вмешательства человека, а также автономность систем.

Однако вместе с преимуществами интернета вещей следует отметить его недостатки как отсутствие в настоящее время законодательного регулирования его применения (на практике интернет вещей регулируется в связи с другими технологиями), так и недостаточной его безопасностью.

Угрозы безопасности связаны в основном с уязвимостями популярных устройств интернета вещей, так как больше 70 % этих устройств вообще не используют шифрование при передаче данных, а вся деятельность ведется в открытых каналах. Это открывает возможности злоумышленникам в любой момент получить контроль над чьим-нибудь домом или целым предприятием, или доступ к личным данным людей.

В России интернету вещей также уделяется особое внимание. Еще в 2017 году он был включен в список сквозных технологий программы «Цифровая экономика Российской Федерации», которые позже российское правительство трансформировало в высокотехнологичные направления (ВТН) и высокотехнологичные области (ВТО), к числу которых был отнесен и интернет вещей. В 2019 году интернет вещей вошел в перечень из восьми ВТО, которые правительство Российской Федерации развивает совместно с госкорпорациями. Затем была утверждена дорожная карта развития этой ВТО.

Одновременно с этим идет формирование и нормативной базы. В августе 2020 года Росстандарт утвердил серию предварительных национальных стандартов в области интернета вещей, сенсорных сетей и промышленного интернета вещей. А в феврале текущего года была утверждена вторая серия национальных стандартов.

С учетом реализации цифровых инициатив на государственном уровне участники и аналитики отечественного рынка интернета вещей предрекают ему устойчивый рост.

Перспективы развития интернет вещей в последние годы связывают с технологиями искусственного интеллекта, органичное вплетение которого в сети интернета вещей позволило объединить эти технологии под общим названием «искусственный интеллект вещей». Это не просто слияние двух технологий, а объединение их возможностей. По мнению специалистов, эти две технологии вместе позволят создать интеллектуальные связанные системы, в которых искусственному интеллекту отведена роль «мозга», а интернету вещей – «тела». Устройства интернета вещей, собирая данные от множества источников, передают ее искусственному интеллекту для поддержания процесса его обучения, в результате чего достигается осуществление требуемой автоматизации нужных процессов.

Искусственному интеллекту вещей предрекают применение практически во всех областях человеческой деятельности, благодаря его возможностям обеспечения анализа и реагирования в режиме реального времени, проведения долгосрочного анализа, позволяющего пользователям определять тенденции и закономерности на протяжении определенных периодов времени. Кроме того, одновременным использованием искусственного интеллекта и интернета вещей повышается скорость обработки данных.

Внедрение информационно-коммуникационных технологий в оперативно-служебную деятельность подразделений органов внутренних дел является одним из приоритетных направлений цифровой трансформации МВД России. В настоящее время перед ведомством стоит задача планомерного перехода от устаревших технологий к современным цифровым решениям.

В МВД России уже сейчас применяются информационные системы и программные комплексы с применением технологий машинного распознавания образов: лиц, находящихся в розыске, либо подозреваемых в совершении преступлений, похищенных или вызывающих подозрение транспортных средств. Разработана система биометрической идентификации, позволяющая производить поиск по массивам информации, содержащим фотоизображения лиц. Другое важное направление – развитие робототехники, в том числе систем управления наземными и воздушными робототехническими комплексами, средств противодействия беспилотным воздушным судам и т. д.

Одновременно с этим перспективные направления внедрения информационных технологий в практику правоохранительной деятельности связываются с развитием и расширением доступности технологий умного города, датчиков, интернета вещей. При этом искусственный интеллект представляет существенные возможности по оптимизации процессов извлечения ценной информации из неструктурированных данных, полученных от устройств интернета вещей.

В рамках информационных отношений интернет вещей может быть как объектом преступного посягательства, так и источником необходимой для расследования и раскрытия преступлений информации, а также средством для обеспечения правоохранительной деятельности.

Киберпреступность в сфере интернета вещей, хотя еще не имеет угрожающих размеров, но тем не менее последствия от вмешательства в него могут быть весьма серьезными. К примеру, внедрение различных вирусов в компьютерную систему центров опасных производств может внести изменения в технологический процесс и привести в дальнейшем к аварийным ситуациям. А если это произойдет на объектах атомной энергетики или химическом производстве, о последствиях нетрудно догадаться. В этой связи в качестве решения проблемы информационной безопасности предлагается обеспечение устройств четко регламентированными стандартами защиты информации, а также высокими требованиями для идентификации пользователей [1].

Как источник информации интернет вещей аккумулирует разного рода сведения, начиная от личной (персональной) и заканчивая внешней информацией. К таковой можно отнести: технологические данные (любая информация, собираемая датчиками и передаваемая по сети (информация об окружающей среде, дан-

ные счетчиков ЖКХ, контролеров станков или газовых турбин), коммерческая информация, персональные (личные) данные от носимых гаджетов.

В части, касающейся расследования и раскрытия преступлений, элементы интернета вещей могут рассматриваться как носители косвенных или прямых признаков преступлений, совершенных их владельцами. Так называемые следы электронного цифрового характера могут содержать как устройства (смартфоны, умные часы, иные устройства), так и центры управления, аккумулирующие информацию от этих устройств.

Как отмечают специалисты, из носимых гаджетов, фиксирующих физиологическое состояние их владельца, можно получить сведения о температуре его тела, частоте пульса, кровяном давлении, при наличии GPS модуля – местонахождение владельца. Эти данные, как правило, служат косвенной информацией, но при сопоставлении с другими имеющимися в распоряжении следователя сведениями могут свидетельствовать о причастности владельца гаджета к совершенному преступлению. Например, высокий пульс и высокое давление могут характеризовать эмоциональное или физическое напряжение, или волнение человека в определенный момент, а при наличии датчиков местоположения можно определить, находились ли в этот момент подозреваемый и потерпевший в одном месте, отследить их передвижение на предмет их встречи и ее продолжительности.

При расследовании дорожно-транспортных происшествий превышающие норму показатели пульса и давления могут свидетельствовать, например, о нахождении владельца носимого гаджета в состоянии алкогольного или наркотического опьянения.

При наличии в носимых гаджетах систем бесконтактных платежей цифровой след могут оставлять проведенные платежи, например лицу, подозреваемому в совершении преступления. Чем «продвинутей» гаджет, тем больше сведений можно получить от него: модуль GPS поможет отследить передвижение владельца в течение определенного времени, электронный секретарь может содержать запись о различных планируемых мероприятиях (встречах, посещениях каких-либо мест, покупках билетов для совершения поездок и т. д.), имеющийся диктофон может содержать различные аудиозаписи, в том числе и телефонных разговоров, при анализе памяти гаджета можно обнаружить интересующую фото-, видеоинформацию.

Источником информации могут служить и другие умные устройства и системы подвижного (умный автомобиль) или стационарного (умный дом) характера. Информация из различных датчиков и систем указанных устройств может восстановить все действия их владельцев, состояние в котором они находились, возможный круг их общения в интересующий момент времени.

Сопоставление этой информации и данных, имеющихся у следователя, может помочь при составлении картины преступления и установить причастность лиц к его совершению [2].

Должное обеспечение информационной безопасности интернета вещей может стать отправной точкой расширения сферы ее использования в правоохранительной деятельности.

По мнению специалистов, технологии интернета вещей имеют потенциал для преобразования пенитенциарных учреждений в интеллектуальные пенитенциарные учреждения «умная тюрьма», которая поможет создать более безопасную среду как для заключенных, так и для персонала. В основе «умной тюрьмы» лежит разработка универсальной платформы (программного обеспечения), которая будет соединять все компоненты экосистемы интернета вещей (различные виды датчиков: устройства позиционирования, видеокамеры, мониторы периметра, наручники или браслеты с метками и другие), позволяющие осуществлять полный контроль как над заключенными, так и безопасностью самой тюрьмы.

Установка устройств интернет-вещей непосредственно на заключенных (например, наручники или специальная униформа с метками) позволит администраторам «умных тюрем» контролировать и автоматически вести подсчет заключенных, контролировать передвижения и анализировать образцы поведения или заключенных, определять местонахождение заключенного в любое время. Кроме того, данные о физическом состоянии заключенных (температура, давление пульс и другие) позволят контролировать как их здоровье, так и следить за психоэмоциональным состоянием заключенных для принятия превентивных мер по предотвращению криминальных и суицидальных попыток со стороны заключенных.

Вторым важным составляющим «умной тюрьмы» является обеспечение безопасности. Возможность получения в режиме реального времени данных от камер наблюдения, различных датчиков, установленных на территории, объектах и внутри помещений, позволит недопустить нарушение границ тюрьмы, контролировать подозрительное поведение как на территории тюрьмы, так и в специальных помещениях с ограниченным доступом (секретные помещения, склад вооружения и боеприпасов др.). Кроме того, из анализа поступающих от датчиков данных можно судить о состоянии пожарной безопасности, безопасности электрических и гидравлических сетей и установок.

Еще одно направление внедрения технологий интернета вещей в правоохранительную деятельность можно рассмотреть на примере «умных отделов полиции», состоящего из центра управления (сервер), к которому подсоединены «умный транспорт полиции», мобильные и иные устройства (смартфоны, умные часы, светофоры видеокамеры). Кроме того, к «умному отделу полиции» могут быть подсоединены различные подсистемы: служебные (обеспечение контроля доступом на различные спецобъекты), обеспечивающие подсистемы (например, управление системой пожаротушения, вентиляцией, климатом, аварийного энергоснабжения и т. д.).

«Умный автотранспорт полиции» может с помощью данных ГЛОНАСС – или GPS-систем и сети Интернет оценивать загруженность и состояние дорог, наличие каких-либо препятствий для обеспечения наиболее удобного и быстрого маршрута автотранспорту полиции и иному спецтранспорту при чрезвычайных происшествиях (ДТП, пожар, технологические аварии и т. д.).

Умные устройства могут обмениваться с управляющим центром различной информацией как состоянием здоровья сотрудников полиции, так и состоянием общественного порядка на объектах и маршрутах патрулирования.

Быстрорастущий рынок интернета вещей требует своевременного реагирования правоохранительных органов, прежде всего, с точки зрения контроля и доступа к передаваемым абонентами интернета вещей данным. В связи с этим предлагается создать реестр идентификаторов интернета вещей, который обеспечит единую идентификацию пользователей данных сетей.

Создание единой системы уникальных идентификаторов направлено на решение задачи подключения сетей Интернета вещей, присоединенные к сетям связи общего пользования, к системе оперативно-разыскных мероприятий (СОРМ), обеспечивающей спецслужбам перехват данных от абонентов связи. Интерес для правоохранительных органов может представлять анализ не только по отдельным пользователям и их группам, но и комплексный анализ больших массивов данных для поиска различных корреляций, в том числе с учетом данных, получаемых из других источников.

Для эффективной работы СОРМ предполагается ограничить информационный обмен устройств интернета вещей таким образом, чтобы все передаваемые данные и факты о событиях могли быть структурированы и сохранены сервисной платформой интернета вещей. Будет организован пассивный съем информации, передаваемой по каналам связи между оконечными устройствами и сервисной платформой интернета вещей, и ее передача на технические средства СОРМ.

Таким образом, с развитием технологий интернета вещей сфера его внедрения будет иметь тенденцию к расширению. Следовательно, будут оставаться актуальными вопросы внедрения технологий интернет вещей в правоохранительную деятельность. Использование его потенциала, на наш взгляд, будет способствовать решению подразделениями МВД России как частных, так и общих оперативно-служебных задач.

Список литературы

1. Купцова А. С. Правовое регулирование использования интернета вещей // Образование и право. 2021 № 7. С. 225–230. URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-ispolzovaniya-interneta-veschey>.
2. Смушкин А. Б. Отдельные аспекты использования концепции интернета вещей в целях противодействия преступности // Всероссийский криминологический журнал. 2020. Т. 4. № 3. С. 453–460. URL: <https://cyberleninka.ru/article/n/otdelnye-aspekty-ispolzovaniya-kontseptsii-interneta-veschey-v-tselyah-protivodeystviya-prestupnosti>.

Черкесова Д. А.¹,

*слушатель факультета подготовки специалистов
в области информационной безопасности
Московского университета МВД России имени В.Я. Кикотя*

Научный руководитель:

Овчинский А. С.,

*профессор кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
доктор технических наук, профессор, Академик РАЕН*

ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОМ ОБЕСПЕЧЕНИИ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Для повышения эффективности профилактики раскрытия и расследования преступлений необходимо последовательно повышать уровень информационно-аналитического обеспечения оперативно-разыскной деятельности, развивать методы и средства аналитической обработки всей совокупности поступающих и накопленных данных. На сегодняшний день можно выделить такие виды аналитики, как: описательная, диагностическая, предписывающая, предиктивная, актуальная, инициативная и другие. Наибольшие перспективы среди них имеет предиктивная (предсказательная) аналитика. Она включает в себя большой спектр инструментов обработки данных, в числе которых: искусственный интеллект с технологиями машинного обучения, а также анализ больших данных. В целом развитие аналитических технологий позволяет обеспечивать динамику и придавать дополнительный импульс совершенствованию информационно-аналитического обеспечения оперативно-разыскной деятельности.

Под большими данными сегодня принято понимать не только огромные объемы сведений и данных, но и технологии их сбора, хранения и обработки. Такие технологии открывают возможности обнаружения скрытых зависимостей и выявления закономерностей на основе полномасштабного анализа структурированной и неструктурированной информации, поступающей из самых разнообразных источников. Анализ больших данных в совокупности с факторами, влияющими на оперативную обстановку, позволяет прогнозировать и оценивать варианты дальнейшего развития криминальной обстановки. Кроме того, использование предиктивной аналитики возможно и при построении стратегических планов как инструментов анализа и отражения оперативной обстановки в противодействии проявлениям активности организованных преступных формирований.

Согласно пункта 3.1 ГОСТ Р ИСО/МЭК 24668-2022 от 01.01.2023 «Информационные технологии. Искусственный интеллект. Структура управления процессами аналитики больших данных», подготовленного научно-образовательным

¹ © Черкесова Д. А., 2023.

центром компетенций в области цифровой экономики ФГБОУ высшего образования МГУ имени М.В. Ломоносова МГУ и автономной некоммерческой организацией «Институт развития информационного общества» (ИРИО), утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2022 г. № 1258-ст: Big Data – это большие массивы данных, отличающиеся главным образом такими характеристиками, как объем, разнообразие, скорость обработки и/или вариативность, которые требуют использования технологии масштабирования для эффективного хранения, обработки, управления и анализа.

Под технологией масштабирования обычно понимается система, способная при увеличении ресурсов или процессов увеличивать и свою производительность. На сегодняшний день выделяют два основных вида масштабируемости: вертикальное и горизонтальное масштабирование. Под вертикальным масштабированием подразумевается увеличение каждого отдельного компонента всей системы, а под горизонтальным – разбиение такой системы на более мелкие компоненты и (или) увеличение количества рабочих серверов, направленных на обработку одной определенной функции.

Принцип работы рассматриваемой технологии основывается на максимальном информировании пользователя по конкретному запросу о каких-либо явлениях и предметах. Это необходимо в первую очередь для постижения сути и прогнозирования будущего, ведь, обрабатывая огромные потоки информации с различных источников, можно предсказать многое, начиная от спроса на конкретную продукцию и заканчивая предотвращением техногенных катастроф специальными службами. К источникам больших данных обычно относятся: социальные сети, средства массовой информации, сайты и форумы, архивы и базы данных и т. д. Условно их можно разделить на:

- внутренние (базы данных, информация о транзакциях, архивы данных, данные сотовой связи, системы управления контролем доступа и т. д.);
- и внешние (информация, содержащаяся в социальных сетях, СМИ, форумы, сайты и т. д.).

В свою очередь, к основным методикам анализа и обработки больших массивов информации можно отнести: глубинный анализ (методика технологий работы со структурированной информацией), сплит-тестирование (сравнение элементов массива между собой «до» и «после» изменения, прогнозирование, машинное обучение (использование искусственного интеллекта), блокчейн (децентрализованная система транзакций) и т. д.

Большие данные позволяют решать следующие задачи:

- 1) первичная обработка и хранение огромных объемов постоянно обновляющихся данных;
- 2) структурирование разнородных данных для поиска связей;
- 3) анализ и прогнозирование.

Условно всю имеющуюся оперативно-разыскную информацию можно разделить на три категории, непосредственно пересекающимися и с категориями больших данных, которые были описаны ранее:

– реактивная оперативно-разыскная информация, т. е. информация, позволяющая адекватно реагировать на возникающие проблемы, связанные с криминальной обстановкой, своевременно раскрывать, предупреждать и пресекать преступления, а также намечать стратегические цели;

– ресурсная оперативно-разыскная информация, т. е. набор знаний и сведений, используемых при раскрытии и расследовании преступлений;

В настоящее время одним из условий совершенствования управления ОВД является широкое использование информационно-телекоммуникационных систем, технологий и компьютерной техники. Их внедрение в деятельность отдельных служб и подразделений ОВД позволит привести к качественным изменениям алгоритмов и методов управления. Значительная часть информации, обрабатываемая в ОВД, хранится в виде больших объемов неструктурированных или малоструктурированных данных, включающих изображения, тексты, видео и т. д. Одним из приоритетных направлений, позволяющих повысить эффективность информационно-аналитического обеспечения, является использование технологий искусственного интеллекта (ИИ) и больших данных.

Список литературы

1. ГОСТ Р ИСО/МЭК 24668-2022 «Информационные технологии. Искусственный интеллект. Структура управления процессами аналитики больших данных» (введен в действие с 1 января 2023 г.).
2. Оперативно-разыскная деятельность и современность : сборник научных трудов / под ред. д-ра юрид. наук В. С. Овчинского. М. : Инфра-М, 2022.
3. Актуальные проблемы оперативно-розыскной деятельности : сборник научных трудов / под общ. ред. К. К. Горяинова, В. С. Овчинского. М. : Инфра-М, 2017.
4. Минбалеев А. В. Понятие «Искусственный интеллект» в праве // Вестник Удмуртского университета. Серия «Экономика и право». 2022. № 6. URL: <https://cyberleninka.ru/article/n/ponyatie-iskusstvennyy-intellekt-v-prave>.
5. Саркисян Г. Г. Информационное обеспечение деятельности оперативных подразделений органов внутренних дел // Труды Академии управления МВД России. 2018. № 2 (46). URL: <https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-deyatelnosti-operativnyh-podrazdeleniy-organov-vnutrennih-del>.
6. Денисова О. Ю., Мухутдинов Э. А. Большие данные – это не только размер данных // Вестник Казанского технологического университета. 2015. № 4. URL: <https://cyberleninka.ru/article/n/bolshie-dannye-eto-ne-tolko-razmer-dannyh>.
7. Информационные технологии управления и организация защиты информации : курс лекций / В. А. Апульцин, Ш. Х. Гонов, В. Н. Лебедев, В. Ю. Петрова. М. : Академия управления МВД России, 2021.
8. Кулаичев А. П. Методы и средства комплексного анализа данных : учебное пособие / А. П. Кулаичев. М. : Форум, НИЦ Инфра-М, 2016.

Осипова А. А.¹,

слушатель факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Гончар В. В.,

начальник кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОТДЕЛЬНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПО РАСПОЗНАВАНИЮ ДИПФЕЙКОВ

В современном цифровом мире информационные технологии развиваются со стремительной скоростью, что приводит к появлению новых явлений и вызовов, таких как дипфейки.

Дипфейки (Deepfakes) – это поддельные видео, фото, аудио и тексты, созданные с помощью специальных технологий глубокого обучения, таких как искусственные нейронные сети (ANN), генеративно-состязательные сети (GAN) и другие. С помощью этих технологий можно создавать реалистичные подделки, которые трудно отличить от настоящих, что может привести к различным последствиям, включая манипуляцию общественным мнением, фальсификацию доказательств и другие.

Проблема дипфейков и их распространения в настоящее время активно изучается учеными в различных странах мира. Вот несколько примеров известных исследователей в этой области:

1. Нео Li – профессор научного центра Калифорнийского университета, известный эксперт в области компьютерного зрения, графики и видеоэффектов. Он работает над разработкой технологий распознавания и предотвращения deepfakes.

2. Нано Фарид – профессор информатики в Дартмутском колледже, который исследует проблему цифровой подделки, включая дипфейки, и разрабатывает методы и технологии для их выявления и борьбы с ними.

3. Исследователи из университета Оксфорда в Великобритании разработали инструменты и методы, позволяющие определять, является ли видео deepfake или нет. Этот инструмент был создан с помощью машинного обучения и большого количества образцов реальных и поддельных видео.

4. Ученые из Facebook также работают над разработкой инструментов и методов, которые могут автоматически определять дипфейки. Они используют нейронные сети и алгоритмы машинного обучения для анализа и сравнения видео и фотографий, что позволяет выявлять подделки.

¹ © Осипова А. А., 2023.

5. Компания Truepic разрабатывает технологию, позволяющую фотографам и журналистам подтверждать подлинность своих фотографий и видео, используя блокчейн и криптографические методы.

6. Российские ученые из Института радиотехники и электроники РАН разработали технологию распознавания deepfakes на основе анализа дыхания человека. В научной статье «Deep Breathing: Authentication of Deep Neural Networks via Breath Dynamics», которая была опубликована на конференции по компьютерному зрению и обработке изображений (Computer Vision and Pattern Recognition, CVPR) в 2020 г. описывается суть метода: при произнесении слов, которые не были изначально записаны голосом человека, человеческое дыхание меняется и это можно зафиксировать с помощью микрофона.

Ученые обучили искусственный интеллект распознавать эти изменения в дыхании и сравнивать их с реальным голосом человека. Эта технология может использоваться в качестве одного из методов борьбы с ними, так как с ее помощью можно определить, является ли запись настоящей или поддельной.

Виды дипфейков:

1. Видео дипфейки – поддельные видеозаписи, которые создаются с помощью технологий глубокого обучения. Наиболее известным примером такого видео является Deepfake порно, в котором использовались лица знаменитостей.

2. Фото дипфейки – фотографии, которые создаются с помощью тех же технологий, что и видео дипфейки. Например, могут быть созданы фото с изображением людей на сценах преступлений или фото с изображением политических деятелей в компрометирующих позах.

3. Аудио дипфейки – поддельные аудиозаписи, которые могут быть использованы для манипуляции общественным мнением. Например, можно создать поддельное звонкое сообщение от главы государства с призывом к конфликту с другими странами или к борьбе с определенной группой населения.

4. Дипфейки текстов – поддельные тексты, которые могут быть использованы для фальсификации доказательств или для манипуляции общественным мнением.

Для противодействия и предотвращения последствий вреда дипфейков необходимо их распознавать, что входит в компетенцию экспертов (специалистов) органов внутренних дел, которые проводят различные виды экспертиз, такие как видеотехнические, фототехнические, фонотехнические и т. д., где необходимы определенные специальные знания. Их значимость в распознавании дипфейков заключается в том, что они способны выявлять допущенные ошибки и манипуляции, которые используются для создания дипфейков, которые помогут доказать их поддельность.

В заключение дипфейки представляют серьезную угрозу для общества и государства, и борьба с ними является важной задачей. Распознавание дипфейков является важным компонентом этой борьбы и требует от экспертов органов внутренних дел специальных знаний и навыков. Различные методы и программы уже разработаны, но их усовершенствование и развитие продолжают. Научные разработки и проекты других организаций могут содействовать улучшению существующих методов и созданию новых для противодействия распро-

странению дипфейков. Правительства Российской Федерации и других стран разрабатывают новые методы для защиты общества от данной проблемы, а эксперты (специалисты) изучают и разрабатывают новые способы распознавания дипфейков.

Список литературы

1. Shruti Agarwal, Hany Farid, Yuming Gu, Mingming He, Koki Nagano, Hao Li Protecting World Leaders Against Deep Fakes // Conference on Computer Vision and Pattern Recognition (CVPR) Workshops. Proceedings of the IEEE/CVF, 2019. С. 38–45.
2. «What? So What? Now What?» Episode 3: A Video on Deepfakes featuring Prof. Hany Farid // CLTC URL: <https://cltc.berkeley.edu/publication/what-so-what-now-what-episode-3-a-video-on-deepfakes-featuring-prof-hany-farid/>.
3. Facebook develops new method to reverse-engineer deepfakes and track their source / The work could help future deepfake investigations // URL: <https://www.theverge.com/2021/6/16/22534690/facebook-deepfake-detection-reverse-engineer-ai-model-hyperparameters>.
4. New Standard Aims To Protect Against Deepfakes // URL: <https://truepic.com/news/new-standard-aims-to-protect-against-deepfakes/>.
5. Deepfakes и deep media: Новое поле битвы за безопасность // URL: <https://habr.com/ru/companies/Voximplant/articles/501068/>.
6. Голосовой DeepFake, или как работает технология клонирования голоса // URL: <https://proglib.io/p/golosovoy-deepfake-ili-kak-rabotaet-tehnologiya-klonirovaniya-golosa-2019-12-11>.
7. Ученые СПбГУ научили нейросеть распознавать оптическую иллюзию // Санкт-Петербургский государственный университет. URL: <https://spbu.ru/news-events/novosti/uchenye-spbgu-nauchili-neyroset-raspoznivat-opticheskuyu-illyuziyu>.
8. МВД занялось системой распознавания фейковых видео // URL: [https://www.tadviser.ru/index.php/Проект:Зеркало_\(Верблюды\)_-_система_МВД_для_распознавания_фейковых_видео](https://www.tadviser.ru/index.php/Проект:Зеркало_(Верблюды)_-_система_МВД_для_распознавания_фейковых_видео).

Пименова О. В.¹,

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

КОМПЛЕКС ПЕРВООЧЕРЕДНЫХ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ВНЕШНИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ МВД РОССИИ В СОВРЕМЕННЫХ УСЛОВИЯХ АКТИВИЗАЦИИ ЗАРУБЕЖНЫХ ХАКЕРСКИХ ГРУППИРОВОК

В 2022 г. Российская Федерация столкнулась с значительным ростом числа кибератак на информационные ресурсы. Так, представители МИД России отметили, что наибольшее число хакерских нападений направлено на государственный сектор. Заместитель главы ведомства Олег Сыромолотов в интервью «РИА Новости» сообщил, что на фоне проведения специальной военной операции наша страна столкнулась с беспрецедентной внешней агрессией в информационном пространстве. В 2022 г. количество кибератак на Россию увеличилось на 80 % [1].

Представители экспертного сообщества также отмечают рост количества атак на государственный сектор. Так, эксперты Positive Technologies отмечают, что в 2022 году внимание киберпреступников привлекали все ключевые отрасли экономики. Государственный сектор был целью номер один.

Кратный рост числа атак на госорганы с февраля 2022 г. подтверждают и представители иных крупных российских компаний в области информационной безопасности (Solar JSOC компании «РТК-Солар»). В связи с политической ситуацией к хакерам добавились так называемые хактивисты, которых массово вербовали в соцсетях и Telegram-каналах. Их активность была направлена в основном на госучреждения и значительно увеличила количество атак [3].

Основными векторами стали DDoS- и веб-атаки на публичные ресурсы госорганов. Целью злоумышленников, как правило, являлось создание дополнительной напряженности в обществе за счет дефейсов (подмены одной веб-страницы другой с публикацией сообщения от хакеров), недоступности значимых для населения ресурсов и утечек данных пользователей.

Такого же мнения придерживаются и представители государственных регуляторов. По словам заместителя директора созданного ФСБ России Национального координационного центра по компьютерным инцидентам Николая Мурашова, против России в информационном пространстве развернута «беспрецедентная по своим масштабам киберкомпания». Ее основными целями является выведение из строя информационной инфраструктуры, а также несанкционированный доступ к информационным системам организаций и предприятий.

¹ © Пименова О. В., 2023.

Хакеры через Telegram-каналы агитировали людей на совершение кибератак и распространяли необходимые инструменты и инструкции для этого. «Особенностью DDoS-атак последних месяцев стало по-настоящему большое количество их участников. В кратчайшие сроки были сформированы Telegram-каналы, в которых проводились агитация обычных людей, инструктажи участников, координация, цели, указания, а также распространялись элементы проведения атак».

Возможно, большой объем DDos-атак явился своего рода прикрытием для более серьезных воздействий. Немало компьютерных атак было направлено на проведение системы организаций с целью хищения информации и вывода из строя технологических процессов.

Кроме того, большое внимание хакеры уделяют атакам, которые могут иметь общественный резонанс. «Это всевозможные дефейсы информационных ресурсов, в результате которых на них размещаются антироссийские, антигосударственные материалы, а также фейковые новости», – пояснил замглавы центра [4].

В настоящее время ситуация кардинально не поменялась. В 2023 г. число кибератак на российские системы выросло на 65 %. Об этом сообщил вице-премьер РФ Дмитрий Чернышенко [5].

Наиболее активными хакерскими группировками, деятельность которых направлена против государственных учреждений различных государств, в том числе и Российской Федерации, согласно аналитическим исследованиям Positive Technologies, являются следующие [6]:

Таблица

Основные хакерские группировки

№ п/п	Название группировки	Атакуемые отрасли	Описание (характеристика) группировки
1	Calypso	Государственный сектор	Впервые активность группы Calypso была выявлена специалистами PT Expert Security Center в марте 2019 г. Основной целью группы является кража конфиденциальных данных, основные жертвы – государственные учреждения Бразилии, Индии, Казахстана, России, Таиланда, Турции
2	ChamelGang	Государственный сектор Финансовый сектор Энергетика Авиационно-космическая промышленность Телекоммуникации	Во втором квартале 2021 г. Экспертный центр безопасности Positive Technologies (PTESC) обнаружил деятельность неизвестной ранее группы. Группа была названа ChamelGang (от Chameleon) за умение эффективно маскировать свою деятельность и обходить средства защиты. Жертвы данной группы находятся по всему миру, в том числе и в России
3	Goblin Panda	Государственный сектор	Goblin Panda впервые обнаружена в 2013 г. исследователями из CrowdStrike и считается группой, действующей в интересах Китая. Группа сосредоточена на шпионаже и имеет в своем арсенале ВПО способное коммуницировать в закрытых сетях. В результате анализа ВПО было выявлено, что группа имеет пересечения с инструментами группы Calypso.

4	Higaisa	Государственный сектор	Кибершпионская группа Higaisa активна как минимум с 2009 г. Нацелена на государственные, общественные и торговые организации в Северной Корее. В списке атакованных стран также Китай, Польша, Россия, Япония
5	Lazarus	Государственный сектор Финансовый сектор Информационные технологии Авиационно-космическая промышленность Военно-промышленный комплекс Медиа Фармацевтика Здравоохранение Криптовалютные биржи	Lazarus – АРТ-группа, которую исследователи связывают с правительством Северной Кореи. Наиболее известна по шифровальщику WannaCry, от которого пострадали более 150 стран, и взлому Sony Pictures. Группа активна с 2009 г., организует широкомасштабные кампании кибершпионажа, операции с применением программ-шифровальщиков, а также атаки на криптовалютный рынок
6	RTM (Read The Manual)	Государственный сектор Финансовый сектор Энергетика Промышленный сектор Информационные технологии	Киберпреступная группа RTM начала свою активность в 2015 г. и атакует организации из различных отраслей с целью кражи денежных средств со счетов, кражи конфиденциальных документов, учетных записей. Группа использует вредоносное ПО (ВПО) собственной разработки. ВПО группы не имеет статического контрольного сервера: оно получает его через блокчейн
7	TA505	Финансовый сектор Государственный сектор Энергетика Авиационно-космическая промышленность Исследовательские компании	Одна из самых опасных и активных преступных кибергрупп, действующая более чем в 60 странах. Основная цель группы – кража или вымогательство денежных средств
8	TaskMasters	Государственный сектор Энергетика Промышленный сектор Транспортные компании	Кибершпионская группировка TaskMasters обнаружена в 2018 г. специалистами PT Expert Security Center. Группа активна с 2010 г. Среди атакуемых организаций – крупные промышленные и энергетические предприятия, государственные структуры, транспортные компании. Группировка атакует компании из разных стран, но большинство жертв находится в России и странах СНГ
9	Winnti	Государственный сектор Финансовый сектор Энергетика Игровая индустрия Разработка ПО Авиационно-космическая промышленность Телекоммуникации Строительство Образование Фармацевтика	Группа Winnti активна с 2012 г. Группа происходит из Китая и принадлежит к классу спонсируемых правительством. Ключевые интересы группы – это шпионаж и получение финансовой выгоды. Основной арсенал группы состоит из собственного разработанного ВПО. Winnti использует сложные методы атак в числе которых supply-chain и watering hole. Группа точно знает, кто их жертва, она очень осторожно развивает атаку и только после детального анализа зараженной системы загружает основной инструментарий. Группа атакует страны по всему миру

С учетом вышеизложенного трудно предположить, что информационные ресурсы МВД России остались без внимания хакерских группировок.

Наиболее часто атаки были направлены на внешние информационные ресурсы ведомства: аппаратно-программный комплекс «Интернет-сайт МВД России», сайт ГИБДД.МВД.РФ, информационный интернет-портал «МВД МЕДИА», официальные аккаунты территориальных органов МВД России в социальных сетях.

Официальный сайт МВД России неоднократно подвергался DDoS-атакам, в том числе высокой мощности (до 10 Гбит/с).

Например в Telegram канале от имени «Студенческий Комитет Кибербезопасности и Обороны Украины контакт studentcyberarmy@gmail.com», указанные в призыве IP-адрес и порт принадлежат сайту мвд.рф, март 2022 г.

Зафиксирован случай несанкционированной модификации кода виджета АИС «Мониторинг государственных сайтов» Минэкономразвития России, который используется на сайте «mvd.ru» и официальных сайтах иных ведомств для подсчета количества посетителей. В результате эксплуатации указанной уязвимости на главной странице сайтов, использующих виджет, отображалось изображение геополитического содержания.

В отдельных территориальных органах МВД России использовались IP-видеокамеры, подключенные к сети Интернет, с уязвимым программным обеспечением и стандартными учетными записями, в результате чего осуществлен их «взлом» и подмена транслируемого изображения на изображение противоправного содержания.

В целях противодействия указанным выше угрозам необходимо на постоянной основе обеспечить взаимодействие с НКЦКИ ФСБ России, ФСТЭК России и Минцифры России по вопросам обеспечения защиты «внешнего периметра» инфраструктуры, реализовать исполнение рекомендаций, поступающих от данных ведомств. В первоочередном порядке подлежат реализации следующие основные мероприятия:

1. Блокировка с применением сертифицированных средств защиты информации возможности доступа к внешним информационным ресурсам МВД России из недружественных стран, а также блокировка трафика, поступающего из «темного Интернета» и анонимных серверов.
2. Обеспечение доступа к внешним информационным ресурсам МВД России с использованием систем очистки трафика от DDoS-атак.
3. Исключение возможности удаленного управления и автоматического обновления телекоммуникационного оборудования иностранного производства.
4. Корректировка настроек используемых средств защиты информации с целью выявления и блокирования «фишинговых атак» и спам-рассылок на ведомственную электронную почту сотрудников.
5. Информирование сотрудников о необходимости соблюдения требований по защите информации.
6. Использование для администрирования официальных аккаунтов подразделений МВД России служебных средств вычислительной техники, методов двухфакторной аутентификации.

7. Своевременное обновление программного обеспечения IP-видеокамер и других служебных устройств, подключенных к сети Интернет, использование сложных паролей.

Реализация перечисленных выше мер позволит нивелировать риски успешных атак на внешние информационные ресурсы МВД России, обеспечить их бесперебойное функционирование, предотвратить имиджевые потери ведомства.

Список литературы

1. Олег Сыромолотов: Киев – плацдарм для испытания кибернаработок Запада // РИА Новости (сайт). URL: <https://ria.ru/20221228/syromolotov-1841757872.html>.
2. Актуальные киберугрозы: итоги 2022 года // Positive technologies (сайт). URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/>.
3. Хакеры атаковали госорганы в три раза чаще в 2022 году // Ведомости (сайт). URL: <https://www.vedomosti.ru/technology/articles/2023/01/16/959104-hakeri-atakovali-gosorgani-chasche>.
4. Центр кибербезопасности заявил о росте с начала СВО числа кибератак на инфраструктуру РФ // ТАСС (сайт). URL: <https://tass.ru/obschestvo/16980861>.
5. Число кибератак на информационные системы России выросло на 65 % // Ведомости (сайт). URL: <https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak>.
6. Хакерские группировки // Positive technologies (сайт). URL: <https://www.ptsecurity.com/ru-ru/research/hacker-groups/>.

Гавриленко А. А.¹,

заместитель командира взвода

факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Котов И. Д.²,

командир отделения взвода

факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель

Булгакова Е. В.,

доцент кафедры информационной безопасности

Московского университета МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

АНАЛИЗ ЗАЩИЩЕННОСТИ ИОТ-УСТРОЙСТВ С ГОЛОСОВЫМИ ПОМОЩНИКАМИ НА ПРЕДМЕТ ВМЕШАТЕЛЬСТВА ЗЛОУМЫШЛЕННИКОВ В УПРАВЛЕНИЕ С ИСПОЛЬЗОВАНИЕМ АУДИОДИПФЕЙКОВ

В настоящее время, Internet of Things (IoT, «интернет вещи») является одним из наиболее активно развивающихся направлений в технологической индустрии. С каждым днем все больше устройств подключается к Интернету, и все больше людей используют голосовые помощники, такие как Siri, Яндекс или Google Assistant для управления своими умными домами и другими IoT-устройствами.

Однако с увеличением количества подключенных устройств IoT также растет и количество уязвимостей, которые могут быть использованы злоумышленниками для вмешательства в управление устройствами и получения доступа к конфиденциальной информации. Один из таких методов атаки – использование аудиодипфейков, которые могут быть созданы с помощью глубокого обучения и использованы для подделки голосовых команд.

Таким образом, статья на тему «Анализ защищенности IoT-устройств с голосовыми помощниками на предмет вмешательства злоумышленников в управление с использованием аудиодипфейков» имеет следующую актуальность:

1. Существует растущее количество устройств IoT с голосовыми помощниками, которые используются в домашних и коммерческих условиях. Эти устройства могут быть уязвимы к вмешательству злоумышленников с использованием аудиодипфейков.

¹ © Гавриленко А. А., 2023.

² © Котов И. Д., 2023.

2. Злоумышленники могут использовать аудиодипфейки для манипулирования устройствами с голосовым управлением, что может привести к утечке конфиденциальной информации или физическому вреду.

3. Анализ защищенности IoT-устройств с голосовыми помощниками на предмет вмешательства злоумышленников в управление с использованием аудиодипфейков может помочь разработчикам и производителям устройств улучшить их безопасность и предотвратить возможные атаки.

Примеры исследований, проводимых в рамках данной научной статьи, могут включать анализ защищенности различных устройств IoT с голосовыми помощниками, проверку на уязвимости, связанные с использованием аудиодипфейков, и разработку методов защиты от таких атак. Также возможно проведение экспериментов, в которых злоумышленники будут использовать аудиодипфейки для вмешательства в управление устройствами с голосовым управлением, чтобы выявить уязвимости и придумать способы защиты.

Для выполнения анализа по выявлению уязвимостей в голосовых помощниках IoT-устройств применялась следующая модель исследования:

1. С помощью специализированного программного обеспечения был сгенерирован аудиодипфейк, имитирующий голосовые команды пользователя.

2. Был создан набор команд для теста, называемый «общим списком», куда вошли основные команды, такие как: «построй маршрут до дома», «включи мою музыку» и «включи свет дома».

3. Тестирования проводились на конкретных устройствах, с установленными голосовыми помощниками. При этом сперва отдавалась команда от настоящего пользователя, затем ТВ же команда, но уже от дипфейка.

4. Результат анализа вносился в таблицу.

Яндекс станция «Алиса»

Данная станция была разработана и представлена аудитории в 2018 году.

Первоначальными задачами для нее были возможность включать музыку, распознавать голос и отвечать на вопросы пользователя. Со временем данной станции добавили множество возможностей, в том числе подключили систему «умный дом», возможность управлять онлайн-кинотеатром и многое другое. Станция управляется посредством голосового помощника «Яндекса» «Алисы».

В новых версиях программно обеспечения голосовой помощник имеет возможность различать пользователей по их голосу. Так, к примеру, у разных людей есть возможность запускать собственные плейлисты с музыкой на одном устройстве, при условии, что ранее они прошли процесс авторизации на данном IoT-устройстве.

Несмотря на все плюсы данной станции, она очень плохо справляется с задачами защиты персональных данных. Несмотря на возможность «узнавать» пользователей, станция не проводит разграничение для выдачи ответа на команды из так называемого «общего списка». В проводимых тестах использовались такие команды, как «построй маршрут до дома», «включи мою музыку» и «включи свет дома».

Google-ассистент

Данный голосовой помощник был представлен публике в далеком 2016 году. Однако поддержку русского языка данная система получила только в 2019 году.

На данный момент система представлена не только на телефонах, но и в виде голосового помощника «умного дома», системой быстрого обмена сообщениями, а также в виде умных часов от компании Google.

Несмотря на огромное влияние на рынке, систем Google так и не смог решить проблемы по защите своего голосового помощника. Он также не может отличить голос пользователя от любого другого, и фактически любой человек может управлять им, что, в свою очередь, обеспечивает возможность для утечки пользовательских данных.

Ассистент Siri (Apple)

Первым моментом появления Siri на iOS-устройствах можно назвать 2010 год, когда она стала доступна в App Store. Дальнейшее ее развитие привело к тому, что на данный момент Siri является неотъемлемой частью всех устройств на ОС iOS.

Несмотря на все сложности, с которыми столкнулись производители по внедрению данного ассистента, они добились хорошего результата в сфере защиты персональных данных пользователя.

Только в 2016 году появилась поддержка русского языка у данного голосового помощника. Попытки научить Siri понимать и озвучивать русский язык были предприняты еще в 2014 году, но из-за трудностей в реализации конечный результат был представлен только через два года.

В отличие от предыдущих ассистентов Siri имеет гораздо больше возможностей. Она со временем подстраивается под предпочтения самого пользователя, что позволяет более конкретно и быстрее достигать результата.

Но самым главным новшеством является возможность Siri распознавать голос своего владельца. Это означает, что, если кто-либо посторонний попытается с помощью голосового помощника выполнить любую команду, ему будет отказано в этом.

Тестирование голосовых помощников

Для проверки данных голосовых помощников будем использовать программу Adobe audition, которая позволит нам создать голосовые аудиофайлы. Так как в нашем случае у нас будет использован наш, мужской голос, в программе создадим женский колос и роботизированный голос.

Одним из наиболее распространенных методов атаки является использование аудиодипфейков, которые могут быть созданы злоумышленниками, чтобы обмануть голосового помощника и выполнить команды на устройстве без разрешения пользователя. Аудиодипфейки могут быть созданы с использованием различных технологий, включая голосовое клонирование, синтез речи и акустический перехват.

Для анализа защищенности IoT-устройств с голосовыми помощниками на предмет вмешательства злоумышленников в управление с использованием аудиодипфейков было проведено исследование, в котором были проанализированы различные аспекты безопасности, включая возможности атаки, сценарии угроз и методы защиты.

В результате исследования было выявлено, что многие устройства IoT с голосовыми помощниками имеют уязвимости, которые могут быть использованы злоумышленниками для выполнения атак с использованием аудиодипфейков. Проведя тестирование и получив результаты, можно прийти к выводу, что наиболее защищенной в плане сохранения персональных данных будет голосовой помощник Siri на iOS устройствах. Два остальных помощника будут работать в обычном режиме вне зависимости от того, кто отдает им указания.

Список литературы

1. Безопасность умных колонок // TADVISER Государство. Бизнес. Технологии.
2. Безопасны ли умные колонки? // Kaspersky URL: <https://www.kaspersky.ru/resource-center/threats/how-to-improve-your-smart-speaker-privacy>.
3. Попов М. А. Обеспечение безопасности iot-устройств // решетневские чтения. – 2021: федеральное государственное бюджетное образовательное учреждение высшего образования «сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» (Красноярск), 2021.
4. Пиликина Е. А., Васяткин М. А., Белоус К. В. Технология «умный дом» // инновации. Наука. Образование. № 31. 2021.
5. Фризоргер Н. Г. Умные колонки // Актуальные проблемы авиации и космонавтики, сборник материалов VI международной научно-практической конференции, посвященной дню космонавтики. 2020: федеральное государственное бюджетное образовательное учреждение высшего образования «сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» (Красноярск), 2021.
6. Дмитриева Н. Н, Плотникова О. И., Романов М. А. Применение беспроводных технологий управления при строительстве «умного дома» // социально-экономическое управление: теория и практика. 2018. № 2 (33).

Рудковская Е. Р.¹,

курсант факультета подготовки специалистов

в области информационной безопасности

Московского университета МВД России имени В.Я. Кикотя

Научный руководитель:

Пименова О. В.,

доцент кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя,

кандидат технических наук

АНАЛИЗ РИСКОВ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Сотрудники патрульно-постовой службы, Госавтоинспекции в своей деятельности используют удаленный доступ к сервисам ИСОД МВД России с помощью мобильных устройств. Удаленный доступ к сервисам ИСОД МВД России подразумевает доступ к информации посредством веб-интерфейса сервисов ИСОД МВД России.

Вопросы безопасности при использовании мобильных устройств в ОВД являются серьезной проблемой. Угрозы могут быть вызваны как со стороны внутренних пользователей, так и со стороны внешних злоумышленников. Чтобы предотвратить риски и угрозы, необходимо разрабатывать комплекс мер по предотвращению и защите.

В целях обеспечения безопасности информации в мобильном сегменте ИСОД МВД России хранение информации не осуществляется.

Говоря о рисках и угрозах, которые направлены на повреждение информации при использовании мобильных устройств в ОВД, нужно иметь в виду, что вред будет причинен либо системе ОВД, либо государству в целом. Поэтому необходимо понимать, что представляет из себя информационная безопасность РФ.

Перечислим основные риски и угрозы, связанные с использованием мобильных устройств в работе правоохранительных органов:

1. Потеря или кража устройства.
2. В таком случае злоумышленник может завладеть всей информацией, в том числе конфиденциальной, хранящейся на устройстве.
3. Вирусы и вредоносные программы.
4. Мобильные устройства могут быть заражены различными вирусами, что в последствии может привести к утечки секретной информации и ослаблению безопасности передачи данных.
5. небезопасные подключения Wi-Fi.

¹ © Рудковская Е. Р., 2023.

6. Небезопасные сети могут быть использованы для атак на персональные устройства и перехват передаваемой информации, такой как логин и пароль.

7. Неавторизованные доступы.

8. Отсутствие паролей или PIN-кодов может привести к несанкционированному использованию информации, находящейся на устройстве.

9. Нарушение политики безопасности.

Для предотвращения рисков и угроз необходимо принимать меры по защите мобильных устройств в ОВД. К ним относят:

1. Шифрование данных. Это позволяет защитить информацию на мобильном устройстве, делая ее недоступной для посторонних лиц. Существуют различные методы шифрования, включая аппаратное и программное.

2. Необходимо проводить регулярную проверку мобильных устройств на наличие вирусов и других вредоносных программ.

3. Политики безопасности. Необходимо разработать и регулярно обновлять политики безопасности для использования мобильных устройств в органах внутренних дел, чтобы обеспечить единый подход к защите информации и уменьшить риски и угрозы.

4. Использование многофакторной аутентификации. Для повышения уровня безопасности можно использовать многофакторную аутентификацию, например, комбинацию пароля и отпечатка пальца.

5. Ограничение доступа к информации. Важно ограничивать доступ к конфиденциальной информации только тем сотрудникам, которые имеют необходимые права доступа.

6. Обучение сотрудников. Обучение сотрудников правилам информационной безопасности поможет снизить риски утечки и кражи конфиденциальной информации.

Организационные и технические меры защиты информации позволяют обеспечить конфиденциальность, доступность и целостность служебной информации.

Заключение. В настоящее время органы внутренних дел активно используют мобильные устройства для повышения эффективности работы и оперативности реагирования на происшествия. Однако такое использование устройств может быть небезопасным, так как они могут стать объектом взлома и утечки служебной информации.

Список литературы

1. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: <https://www.garant.ru/products/ipo/prime/doc/71456224/>.

2. Риски использования мобильных устройств / URL: <https://www.osp.ru/winitpro/2014/01/13039202>.

Акинъшин И. С.¹,

заместитель начальника

Московского университета МВД России имени В.Я. Кикотя,

кандидат экономических наук

ОСОБЕННОСТИ ИЗУЧЕНИЯ НЕКОТОРЫХ ВИДОВ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

На сегодняшний день существует множество решений для исследования мобильных устройств. Наиболее эффективные решения это Belkasoft Evidence Center, Cellebrite UFED, Oxygen Forensic Detective, Elcomsoft Mobile Forensic Bundle, Susteen Secure View, MOBILEdit Forensic Express и Micro Systemation XRY. К сожалению, не все из данных решений доступны сегодня из-за санкционной политики в отношении нашей страны.

Следует отметить, что при исследовании мобильных устройств, работающих под управлением перечисленных выше операционных систем (далее – мобильные устройства), судебные эксперты сталкиваются со следующими трудностями:

1. На сегодняшний день не создано программы для извлечения данных, поддерживающей все существующие на рынке мобильные устройства.

2. Не существует единого инструмента, способного извлекать и анализировать журналы работы программ, написанных под операционные системы Android и IOS, получение информации из которых представляет интерес для эксперта. Приходится использовать сразу несколько различных инструментов для изъятия информации с мобильного устройства.

3. В настоящее время для следствия недостаточно получения информации из телефонной книги, SMS-сообщений. Теперь необходимо изымать из устройства гораздо больший объем информации: историю посещенных сетевых ресурсов (данные веб-браузеров), историю обмена сообщениями в мессенджерах, удаленные данные (графические файлы, видеофайлы, SQLite базы данных и т. п.) и другую криминалистически значимую информацию.

4. Существующие программно-аппаратные комплексы, как правило, имеют высокую стоимость, что является препятствием для их приобретения судебными лабораториями и экспертными подразделениями.

5. Возможное повреждение устройства или потеря данных. Используя один из методов проведения экспертизы, подразумевающий получение прав суперпользователя, возможно необратимое повреждение устройства. Поэтому важно использовать гарантированно рабочими инструментами.

6. Постоянное развитие мобильных устройств, обновление программного обеспечения, развитие схем шифрования. Для получения доступа к системным файлам используются «уязвимости» устройств, которые могут быть устранены с обновлениями программного обеспечения. Поэтому некоторые решения, которые когда-то работали, могут потерять свою эффективность.

¹ © Акинъшин И. С., 2023.

7. Облачные извлечения и развитие контрэкспертизы. В то время как все больше и больше данных пользователей оказывается в облаке, компании продолжают защищать свои облачные сервисы от простых попыток их получения. Начиная с Android 9, Google начал шифровать резервные копии Android с помощью пароля устройства пользователя. В настоящее время никакие другие данные не шифруются, даже здоровье (Google Fit) или пароли.

Apple продолжает свои усилия по противодействию судебному доступу к частям своих облачных сервисов. Резервные копии iCloud, хотя и не зашифрованные с помощью учетных данных пользователя, становятся все более труднодоступными из-за использования учетных данных устройства в качестве необходимого предварительного условия для доступа к данным. Пароли пользователя (связка ключей iCloud), данные о состоянии здоровья и даже сообщения надежно шифруются с помощью пароля блокировки экрана пользователя или системного пароля.

Ввиду разнообразности устройств и их версий ОС зачастую трудность составляет именно выбор инструмента, поскольку не все они могут поддерживать исследуемое устройство.

Существующие на сегодняшний день инструменты используют один или несколько уровней извлечения данных с устройств. Каждый из этих уровней имеет свои особенности. Данные уровни представлены в виде пирамиды, где по мере приближения к вершине методы становятся более сложными с технической стороны, правильными с точки зрения криминалистики и наукоемкими.

1. Ручное извлечение: ручное извлечение включает в себя просмотр содержимого данных на телефоне непосредственно на его экране. Обнаруженная информация документируется вручную (обычно с помощью цифровой камеры). На этом уровне невозможно восстановить удаленную информацию. Были разработаны некоторые инструменты, которые помогают исследователю легко документировать ручное извлечение. Эти инструменты захватывают то, что показано на устройстве, затем в оцифрованном виде эта информация используется и хранится.

2. Логическое извлечение: данный уровень предполагает, что мобильное устройство подключается к персональному компьютеру эксперта с помощью USB-кабеля и беспроводным методом. Далее выполняется побитовое копирование файлов и каталогов, находящихся на логических дисках мобильного устройства. Для синхронизации персонального компьютера и мобильного устройства используется интерфейс программы. Но данный уровень не обеспечивает полный доступ к данным устройства и не позволяет произвести восстановление удаленной информации. Но данный способ позволяет восстановить записи баз данных SQLite, которые имеются в операционных системах IOS и Android, так как стертые записи данных баз помечаются как удаленные, а не перезаписываются сразу. Помимо этого, данный способ позволяет извлекать из кэш-директории миниатюрных эскизов всех просмотренных на устройстве графических и видео-файлов, даже если сами файлы были уже удалены.

3. Шестнадцатеричный дамп: шестнадцатеричный дамп, чаще называемый «физическим извлечением», предоставляет исследователю больше данных, чем

на предыдущих уровнях. На данном уровне снимается побитовая копия всей внутренней памяти мобильного устройства, что позволяет произвести восстановление удаленных файлов. Для извлечения необходимо подключить устройство к персональному компьютеру с помощью кабеля, после чего создать побитовую копию данного устройства с помощью программы. Но данный метод имеет некоторые нюансы, которые мешают его реализовать. Производители ограничивают возможность чтения информации с мобильных устройств с целью повышения безопасности. Именно для реализации данного метода используются утилиты, загрузчики, позволяющие получить доступ к памяти мобильного устройства, обойти ограничения производителей, а также пароли, установленные пользователем.

4. Chip-Off или Извлечение данных из интегральной схемы памяти: на данном уровне производится извлечение информации из микроэлектронного устройства (чипа памяти). Данная схема извлекается из мобильного устройства и монтируется в аналогичное мобильное устройство или в специальное для данного вида извлечения устройство. Нюансом использования данного метода является то, что в одних и тех же мобильных устройствах могут использоваться различные чипы. К положительной стороне данного метода можно отнести возможность снятия информации даже с неисправного мобильного устройства.

Отдельного внимания заслуживает метод извлечения данных из интегральной схемы памяти посредством отладочного интерфейса JTAG (Joint Test Action Group). Устройство подключается через порт тестирования (TAP), и его процессор получает команду на копирование данных, имеющихся на интегральной схеме памяти.

Объем необходимых следовательно знаний значительно увеличивается на этом уровне. Некоторые из аспектов, которые делают этот метод сложным, включают в себя широкое разнообразие используемых типов чипов и риск причинения физического повреждения чипу в процессе извлечения.

Рынок средств на сегодняшний день имеет несколько основных продуктов, которые используются большинством экспертных учреждений. Как правило, такие средства используют сразу несколько методов получения информации с устройства. Наиболее известными коммерческими компаниями, предлагающими подобные средства, являются: Cellebrite, Oxygen Forensic Detective и MSAB.

UFED (Universal Forensic Extraction Device (Cellebrite Mobile Synchronization Ltd.)) – программно-аппаратный комплекс, используемый для разблокировки устройств, выполнения расширенных разблокировок, выполнения логического/полного извлечения файловой системы/физического извлечения, а также выборочного извлечения данных приложений и облачных токенов.

Cellebrite UFED Touch 2 позволяет извлекать информацию с устройств в полевых условиях, UFED Physical Analyzer используется в лаборатории для анализа данных с устройства. На сегодняшний день в лабораториях используются такие программные решения, как UFED 4PC и UFED Physical Analyzer, установленные на персональный компьютер эксперта. База поддерживаемых данным комплексом устройств постоянно обновляется, что обеспечивает извлечение данных из большинства имеющихся на рынке мобильных устройств. Но стоит отметить, что

данные обновления являются платными. MSAB XRY / MSAB XRY Field от компании Micro Systemation является продуктом, аналогичным описанному выше. Упор данной компании сделан на продукты, реализуемые на стационарных компьютерах и ноутбуках. В комплекте с комплектом идет набор необходимых для подключения мобильных устройств кабелей и переходников, USB-хаб. Также, среди производимых компанией устройств можно выделить две более мобильные версии, выполненные в виде планшета и киоска – MSAB XRY Field и MSAB XRY Kiosk. Данные решения не распространены на территории России, как продукция от Cellebrite.

Еще одной организацией, которая производила аппаратные инструменты для извлечения данных, является Rusolut. Данный комплекс позволяет извлечь данные любых устройств, независимо от их состояния и наличия блокировки устройства. В набор также входит множество переходников и кабелей. Однако данное решение потеряло свою актуальность, так как все современные мобильные устройства шифруют хранимую на них информацию. Поэтому после извлечения данные будут в зашифрованном виде.

Одной из наиболее часто встречающихся программ для анализа данных, извлекаемых из мобильных устройств, является «Мобильный Криминалист». Помимо автоматического анализа данных программой, в ней интегрировано множество решений, позволяющих исследовать данные вручную [1, с. 176].

Множество современных программ включают в себя смешанный функционал, например производители, занимающиеся производством решений, ориентированных на исследование HDD, внедряют в свои инструменты функционал, направленный на исследование мобильных устройств и наоборот. Как итог, на рынке появляются так называемые «комбайны», способные выполнять широкий спектр функций по извлечению и анализу данных из различных источников.

Существует еще две популярные среди экспертов программы: Magnet AXIOM и Belkasoft Evidence Center. Возможно, данные программы по своей функциональности уступают описанным выше решениям, но они также хорошо справляются с анализом данных и могут использоваться для контроля полноты извлечения данных. Однако наиболее эффективно в настоящее время использовать решения от компании Elcomsoft, работающих на российском рынке.

Список литературы

1. Предварительное следствие в органах внутренних дел / [М. В. Мешков и др.]. М. : Московский университет МВД России, 2007.

Толстых М. Ю.¹,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий
Московского университета МВД России имени В.Я. Кикотя,
кандидат технических наук*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВЫХ ПРОДУКТОВ НА ВСЕХ ЭТАПАХ ИХ ЖИЗНЕННОГО ЦИКЛА

Цифровые продукты (программное обеспечение, оборудование, системы, модуль или сервис) создаются в очень сложной и быстроменяющейся среде. В настоящее время общество в лице разработчиков и пользователей сталкивается с быстрыми изменениями в технологиях, а также в потребностях и ожиданиях, которые напрямую влияют на ИТ-продукты, с учетом высокого уровня инновационности и конкурентоспособности, что делает весь жизненный цикл продукта еще более сложным. Уменьшение слабости в части противостояния угрозам информационной безопасности как характеристики цифровых продуктов может быть реализовано путем формирования концептуального, а также практического воплощения алгоритмов и протоколов, методик и техник повышения защищенности не только при их применении и использовании [1], но также и на стадии их проектирования (дизайна), в иные периоды их жизненного цикла.

В области информационно-коммуникационных технологий жизненный цикл продукта представляет собой временной интервал от разработки продукта и его вывода на рынок до снижения продаж или окончательного удаления с рынка. Подход используется разработчиками (вендорами) продуктов, менеджерами проектов и руководителями для управления присутствием продукта и его востребованностью на рынке.

Управление жизненным циклом гарантирует, что продукт проектируется и разрабатывается с учетом потребностей пользователя и продолжают удовлетворять эти потребности по мере их развития и с течением времени. Оно также способствует выявлению и снижению рисков, влияющих на востребованность и результативность продукта (технические проблемы или уязвимости в системе безопасности). Управление жизненным циклом помогает определить области для повышения производительности, такие как взаимодействие с пользователем, скорость или стабильность цифрового решения.

Одной из ключевых частей управления жизненным циклом при проектировании является масштабирование с помощью системного мышления. Тем более, что продукты управляются на протяжении протяженного временного интервала, дизайн может помочь командам разработчика гарантировать, что язык проектирования, его концепция соответствуют долгосрочной перспективе. Применение безопасности в дизайне требует эволюционного, гибкого подхода, который позво-

¹ © Толстых М. Ю., 2023.

ляет технологиям приспосабливаться к развивающимся процессам и расширяющемуся спектру опасностей за счет детекции и обработке новых уязвимостей.

Технологии интегрированы почти во все аспекты повседневной жизни. Системы с выходом в Интернет связаны с критически важными сегментами, которые напрямую влияют на наше экономическое процветание, материальные средства к существованию и физическое благополучие, начиная от управления персональной идентификацией и заканчивая медицинским обслуживанием.

Сейчас, как никогда, важно, чтобы производители технологий создавали безопасные по умолчанию цифровые решения, а ключевые точки проектирования продукта и процессов их разработки характеризовались среди прочего показателями киберзащищенности. Исторически сложилось так, что производители технологий полагались на исправление уязвимостей, обнаруженных после того, как потребители опробовали продукты, это требовало применения контрмер в части обеспечения информационной безопасности от пользователей.

Безопасное проектирование (дизайн), прежде всего, означает то, что технологические продукты созданы таким образом, чтобы разумно защитить себя и своих пользователей от злоумышленников, успешно получающих доступ к устройствам, данным и к подключенной инфраструктуре. Производители цифровых продуктов должны проводить оценку рисков с целью определения и предотвращения распространенных киберугроз (например, системам критической информационной инфраструктуры [2], что к данному моменту является законодательно установленным обязательством, а следовательно, определено в процессуальном аспекте нормативно).

Безопасные методы разработки информационных технологий и многоуровневая защита, известные как эшелонированная защита, также рекомендуются для предотвращения действий злоумышленников в части компрометации систем или получения несанкционированного доступа к конфиденциальным данным, актуальна в этой связи и разработка индивидуальной модели угроз во время создания каждого конкретного цифрового продукта. Безопасная конфигурация должна быть базовой линией по умолчанию, в которой продукты автоматически включают наиболее важные элементы управления безопасностью, необходимые для защиты от злоумышленников.

Вендорам необходимо применять целостный подход к обеспечению безопасности своих продуктов, решений и платформ, популярных экосистем. Интеграция безопасного проектирования требует значительных инвестиций, ресурсов производителей на каждом уровне проектирования и разработки, это процесс, который не может быть «запущен» позже. Важно сделать безопасность приоритетом работы организации, функционирования предприятия или бизнеса, а не просто технической функцией. Должны быть расставлены приоритеты в функциях, механизмах и реализации инструментов, которые преследуют цель защищать потребителей, а не функции продукта, кажущиеся привлекательными.

Не существует единого оптимального и универсального решения, чтобы положить конец постоянной угрозе со стороны злоумышленников, использующих технологические уязвимости, но цифровые продукты, которые «защищены по дизайну», будут очевидно в меньшей группе риска, если их разработчики раз-

работают дорожные карты для согласования характеристик информационной безопасности своего продукта, разработки портфолио с большим количеством практик и апробированных решений по защите информации.

В дополнение к тому, чтобы обеспечить безопасность продукта по умолчанию приоритетом в организации, ИТ-руководители должны сотрудничать со своими коллегами по отрасли, чтобы понять, какие продукты и услуги лучше всего воплощают отмеченные принципы проектирования. Лидеры должны согласовывать свои запросы, чтобы помочь производителям определить приоритеты своих предстоящих инициатив в области безопасности. Работая вместе, потребители могут помочь обеспечить значимый вклад для производителей в направлении создания для последних стимулов уделять первоочередное внимание безопасности.

При использовании интеграций и коллабораций организации должны убедиться, что они понимают общие модели ответственности с поставщиком технологий. Организации должны отдавать приоритет поставщикам услуг, которые прозрачны в отношении своей безопасности, реализуют открытый контроль своей деятельности, ее качества, демонтируют способность выполнять свои обязательства в соответствии с общими принятыми моделями обязательств и ответственности.

Безопасность цифрового продукта в век информатизации имеет первостепенное значение. Мало того, что угрозы и атаки становятся все более изощренными в своей реализации, потребители также ищут продукты с высокими рейтингами безопасности, что трансформирует безопасность продукта из относительно малоизвестного процесса, осуществляемого на стороне разработчиков, в функцию, занимающую центральное место в умах людей, критерий выбора приобретения того или иного цифрового решения на рынке.

Кибербезопасность не может быть второстепенной задачей, потребители заслуживают продуктов и решений, которые безопасны с самого начала. Активное и постоянное взаимодействие между государством, промышленностью и общественностью жизненно важно для того, чтобы поставить информационную безопасность в центр процесса разработки технологий.

Список литературы

1. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности : ГОСТ Р ИСО/МЭК 27002-2021. URL: <https://docs.cntd.ru>.
2. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26.07.2017 № 187-ФЗ. URL: <https://docs.cntd.ru>.

Турсунов У. Н.¹,

слушатель факультета подготовки

иностранных специалистов

Московского университета МВД России имени В.Я. Кикотя

Галиев Д. В.²,

старший преподаватель кафедры

информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета МВД России имени В.Я. Кикотя

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ПОМОЩИ BROWSER FINGERPRINT

В современном мире, когда люди проводят столько времени в Интернете, защита личной информации становится все более и более актуальной темой. Идентификация пользователей при помощи browser fingerprint, или отпечатка браузера, становится все более популярным методом определения пользователя в сети Интернет. Этот метод основывается на том, что каждый браузер, а также операционная система, на которой он установлен, имеет уникальный набор свойств и настроек, с помощью которых можно определить конкретного пользователя.

Browser fingerprint может включать в себя различные параметры, такие как версия операционной системы, разрешение экрана, установленные шрифты, языковые настройки и другие. Комбинация всех этих параметров позволяет нам создать уникальный отпечаток браузера. В отличие от классической идентификации по логину и паролю браузерный отпечаток учитывает данные о компьютере пользователя, на котором запущен браузер.

Более того, browser fingerprint может быть использован для идентификации пользователя, даже если он использует VPN или анонимайзер. В таком случае использование browser fingerprint для определения пользователя становится еще более удобным и эффективным.

Существует несколько инструментов, которые могут помочь узнать браузерный отпечаток своего устройства, например, Panopticlick, BrowserSpy и AmIBlockedOrNot. Некоторые компании и сайты используют эти инструменты для сбора информации о пользователях, чтобы создать более точную связную базу данных для идентификации пользователей и проведения мониторинга в Интернете.

Но чтобы снизить риск, связанный с использованием browser fingerprint, используя сервисы, собирающие информацию о системе, можно получить свой «отпечаток»:

Принцип работы браузерного отпечатка (browser fingerprint) заключается в том, что при посещении сайта веб-браузер не только передает информацию

¹ © Турсунов У. Н., 2023.

² © Галиев Д. В., 2023.

о запрашиваемой странице, но и передает информацию о браузере и устройстве пользователя, используемых для доступа к сайту. Эта информация необходима для корректного отображения страницы, а также глобальной аналитики. Комбинация данных параметров и составляет браузерный отпечаток, который уникален для каждого устройства и может использоваться для идентификации пользователя при повторных посещениях сайта. Существует несколько способов создания отпечатков браузеров. Некоторые сайты используют JavaScript для сбора информации об устройстве и браузере пользователя, в то время как другие используют специальные плагины, расширения для браузера или специальное программное обеспечение. После сбора этой информации она отправляется на сервер, где производится ее анализ для идентификации пользователя.

Интересной особенностью является то, что browser fingerprinting может быть использован для выявления мошенников, которые используют несколько аккаунтов для своих преступных целей. В частности, имеется несколько способов использования browser fingerprinting для этой цели:

1. Сравнение отпечатков. Если имеется информация, что несколько аккаунтов похожи друг на друга (например, они используют один и тот же IP-адрес, браузер и операционную систему), то можно сравнить их отпечатки, чтобы убедиться, что это действительно один и тот же пользователь. Так, например, в случае если злоумышленник использует данное устройство для личных нужд, может сложиться ситуация, при которой сессия с официальной учетной записи в сервисах, обязывающих предоставлять персональные данные, будет иметь тот же отпечаток, что и сессия, с которой производились противоправные действия.

2. Анализ пользовательского поведения. Браузерный отпечаток также может содержать информацию о том, как пользователь взаимодействует с сайтом, например, какие элементы пользователь нажимает, какие страницы он посещает и какие запросы делает. Анализ этой информации может помочь выявить мошенников, которые используют несколько аккаунтов для мошеннических целей.

Однако следует понимать, что browser fingerprinting не всегда является достоверным инструментом выявления мошенников, поскольку он может быть обманут внедрением ложной информации о браузере и операционной системе.

Почему бы для этой цели не использовать Cookie?

Потому что у Cookie есть несколько минусов:

1. Cookie можно очистить.
2. Режим incognito (в этом режиме cookie не будет работать).
3. Плагины не дают сохранять cookie.
4. Практически все сайты в настоящее время уведомляют об использовании cookie и позволяют не передавать их серверу.

Отличие cookie от Fingerprint. Cookies – это небольшие файлы, хранящие информацию на компьютере пользователя, которые используются веб-сайтами для сохранения сеансовых данных или предпочтений пользователя. Они содержат информацию о действиях пользователя на сайте, такие как предпочтения в покупках или вход в систему, чтобы при следующем посещении сайта эти данные могли быть быстро получены. Cookies могут быть использованы для отслеживания пользовательских действий на веб-сайтах, включая корзину покупок,

просмотренные страницы и рекламные предпочтения. Основным преимуществом cookies является повышение удобства использования Интернета. Если пользователь часто посещает сайт, то ему не нужно будет каждый раз вводить данные о себе. Кроме того, cookies помогают владельцам сайтов оптимизировать свои ресурсы и сделать их проще в использовании. Например, службы рекламы используют cookies, чтобы определить, какие объявления пользователь уже увидел и какие ему еще нужно показать, экономя время и ресурсы.

Основное отличие между Fingerprint и Cookies заключается в том, что Fingerprint не требует согласия пользователя и не может быть удален или изменен пользователем без использования специализированного ПО. Cookies, с другой стороны, могут быть заблокированы или удалены пользователем, а также требуют согласия пользователя на их использование для некоторых видов данных, в соответствии с действующим законодательством.

Существует несколько способов, которые могут использовать злоумышленник, чтобы защищать себя от browser fingerprinting:

1. Использование расширений, предназначенных для приватности. Наиболее популярные из них – это Privacy Badger, AdBlock Plus или uBlock Origin. Эти расширения блокируют сторонние скрипты, которые могут собирать информацию о пользователе.

2. Изменение настроек браузера. Отключение JavaScript и Cookies может помочь снизить вероятность отслеживания пользователей.

3. Использование инструментов для маскировки Fingerprints. Существует множество приложений и расширений, которые предназначены для того, чтобы сделать браузерный отпечаток менее уникальным.

4. Установка Tor Browser. Этот браузер позволяет обезопасить себя в сети Интернет, скрыв свой IP-адрес и многие другие данные, которые могут быть использованы для идентификации пользователя.

5. Ограничение использования браузера. Использование разных браузеров в разное время может изменять браузерные отпечатки.

Следует учитывать, что ни один из этих способов не обеспечивает полной защиты, но комбинация этих методов может помочь минимизировать риски идентификации браузерного отпечатка.

Шикалова В. М.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

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ КАК СОЦИОЛОГИЧЕСКАЯ КАТЕГОРИЯ

Компьютерная преступность – это одна из ключевых проблем современного общества, связанных с использованием информационных сетей, компьютерных технологий и интернета. Она может включать в себя кражу личных данных, кибершпионаж, распространение вредоносных программ, фишинг, кибербуллинг, кибертерроризм и другие противоправные действия.

Киберпреступники могут использовать различные методы и техники, чтобы получить доступ к чужой информации или нанести вред компьютерным системам и сетям. Например, для получения доступа к компьютеру жертвы они могут использовать вредоносные программы, такие как вирусы, трояны и шпионское ПО [1]. Они также могут использовать социальную инженерию, чтобы обмануть пользователей и получить доступ к их личной информации.

Социологическая составляющая компьютерной преступности заключается в том, что она может нанести ущерб не только индивидуальным пользователям и организациям, но и всему обществу в целом, будучи способной вызвать серьезные социальные последствия, такие как потеря доверия в интернете, ухудшение качества жизни, нарушение прав и свобод граждан, нарушение конституционных прав, утечку личных данных, финансовые потери, нарушение конфиденциальности, угрозы безопасности и даже физическое насилие и т. д.

Кроме того, компьютерная преступность может привести к разрушению международных отношений и угрожать национальной безопасности. Например, кибершпионаж может быть использован для получения секретной информации о других странах, а кибертерроризм – для атак на критическую инфраструктуру, такую как электростанции, государственные системы связи и транспортные сети.

Современное состояние компьютерной преступности характеризуется увеличением количества угроз информационной безопасности и развитием методов и средств защиты информации [2]. Однако несмотря на это, компьютерная преступность остается одной из наиболее сложных проблем в области информационных технологий.

¹ © Шикалова В. М., 2023.

В социологическом аспекте компьютерная преступность может быть изучена с помощью различных методов и подходов. Например, можно рассмотреть компьютерную преступность как социальное явление, которое связано с изменением социальных отношений и структур в обществе. Компьютерная преступность может быть связана с проблемами социализации, адаптации к новым условиям жизни, конфликтами внутри общества и т. д. [3].

Кроме того, компьютерная преступность может быть изучена с точки зрения социальных неравенств и дискриминации. Например, люди, которые имеют доступ к компьютерам и интернету, могут быть более склонны к совершению компьютерной преступности, чем те, кто не имеют такого доступа. Кроме того, компьютерная преступность может быть связана с гендерными и расовыми проблемами.

Перспективы изучения компьютерной преступности в социологическом аспекте связаны с использованием новых методов и подходов [4]. Например, можно использовать методы качественного и количественного анализа для изучения социальных факторов, влияющих на компьютерную преступность и уязвимость информационных систем. Кроме того, можно использовать сетевой анализ для изучения социальных отношений внутри сообществ, связанных с компьютерной преступностью [5].

Таким образом, компьютерная преступность является важной социологической категорией, которая требует комплексного исследования. Компьютерная преступность может быть изучена путем анализа социальных отношений и неравенств. Кроме того, для дальнейшего изучения компьютерной преступности необходимо использовать новые методы и подходы, которые позволят лучше понять причины и последствия этой проблемы.

Список литературы

1. Рааб М. Защита сетей: наконец-то в центре внимания / М. Рааб. М. : Просвещение, 1994.
2. Векслер Д. Наконец-то надежно обеспечена защита данных в радиосетях / Д. Векслер. М. : Знания, 1996. С. 13–14.
3. Сухова С. В. Система безопасности NetWare / С. В. Сухова. М. : Сети, 1995. С. 68.
4. Беляев В. Безопасность в распределительных системах [Текст] / В. Беляев. М. : Мысль, 1997. С. 36–40.
5. Ведеев Д. Защита данных в компьютерных сетях / Д. Ведеев. М. : Просвещение, 1995.

Шикалова В. М.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

ПРОБЛЕМА ОРГАНИЗАЦИИ ЗАЩИТЫ ЛИЧНОЙ ИНФОРМАЦИИ СОТРУДНИКОВ ОВД

В настоящее время защита личных данных является одной из важнейших задач в различных сферах деятельности, включая работу органов внутренних дел (ОВД) [1]. Сотрудники ОВД обрабатывают большое количество личной информации, которая может быть использована в корыстных целях. Поэтому защита личной информации сотрудников ОВД является важной задачей, которая требует серьезного внимания.

В настоящее время существует проблема организации защиты личной информации сотрудников органов внутренних дел [2]. Для того чтобы найти способы решения этой проблемы, нами была проанализирована деятельность сотрудников ОВД, проведен анализ научно-исследовательских работ, НПА, монографий, докладов и других источников, посвященных проблеме защиты личной информации и предложены рекомендации по ее решению.

В результате исследования были выявлены такие проблемы организации защиты личной информации сотрудников ОВД, как:

1. Недостаточная осведомленность сотрудников ОВД о принципах защиты персональных данных и правилах обработки такой информации.
2. Несоблюдение правил обработки персональных данных сотрудниками ОВД, которое зачастую обусловлено субъективным фактором.
3. Отсутствие должного контроля за доступом к персональной информации, что влечет за собой ее утечку.
4. Недостаточная защита информационных систем, используемых для обработки персональных данных, которая не гарантирует отсутствия возможности доступа к ней иных лиц.
5. Неэффективность механизмов ответственности за нарушение правил обработки персональных данных [3].

Для решения проблемы организации защиты личной информации сотрудников ОВД мы считаем необходимым организовать:

1. Обучение сотрудников ОВД правилам обработки персональных данных и принципам защиты конфиденциальности.

¹ © Шикалова В. М., 2023.

2. Разработку и внедрение правил обработки и хранения персональных данных сотрудников ОВД.

3. Внедрение системы контроля за доступом к персональной информации сотрудников ОВД.

4. Проведение регулярных проверок и аудитов, чтобы гарантировать соблюдение правил обработки персональных данных и защиты конфиденциальности.

5. Регулярное обновление систем защиты информации и контроля доступа к ней, чтобы обеспечить максимальную безопасность персональных данных сотрудников ОВД.

6. Сотрудничество с другими службами и организациями, которые занимаются защитой персональных данных, для обмена информацией и опытом в этой области [4].

Таким образом, защита личной информации сотрудников ОВД является важной задачей, требующей серьезного внимания [5]. Решение этой проблемы возможно путем обучения сотрудников ОВД правилам обработки персональных данных, внедрения системы контроля за доступом к персональной информации, проведения регулярных проверок и аудитов, а также обновления систем защиты информации и сотрудничества с другими службами и организациями, которые занимаются защитой персональных данных.

Список литературы

1. Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Аверченков В. И., Рытов М. Ю. Организационная защита информации: учебное пособие для вузов. Брянск : Издательство БГТУ, 2005.

3. Барсуков В. В., Водолазкий В. В. Современные технологии безопасности. Интегральный подход. М. : Нолидж, 2000.

4. Введение в защиту информации : учебное пособие. М. : Инфра-М, 2004.

5. Гринберг А. С. Защита информационных ресурсов государственного управления : учебное пособие для вузов. М. : ЮНИТИ-ДАНА, 2003.

Шульга Д. С.¹,

слушатель факультета подготовки специалистов

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

ПОНЯТИЕ И ВИДЫ ДИСТАНЦИОННЫХ МОШЕННИЧЕСТВ

В современном мире основным компонентом развития общества. Особенно это заметно в настоящее время, когда наше общество стало информационным. И вместе с развитием информационных технологий возрастает необходимость противодействия дистанционным мошенничествам. Данному виду преступлений свойственны значительное разнообразие, быстрая приспособляемость, динамика и способность меняться с учетом сферы применения.

Дистанционным мошенничеством является вид мошенничества, осуществляемого преступником дистанционно, по большей части используя телефонные либо компьютерные сети, через которые он путем обмана воздействует на потерпевшего и убеждает его передать свое имущество удаленным способом. Совершаются подобные преступления следующим образом. Преступник, не вступая в непосредственный контакт с жертвой, обманным путем получает от нее ее данные и далее доступ к счету банковской карты или мобильного телефона, с которого и совершается хищение денежных средств. В некоторых случаях обманутые потерпевшие самостоятельно переводят деньги. Кроме того, как показывает практика, нередко таким образом мошенники получают не только денежные средства потерпевших, но и оформляют на их имя кредиты, либо вводя их в заблуждение, либо получив доступ к их идентификационным данным. Денежные средства, выданные банком по кредиту, при этом поступают мошенникам.

Совершение преступлений с применением ИТ – это отдельный вид общественно опасной и противоправной деятельности, который на сегодняшний день встречается все чаще как в мировом масштабе, так и в конкретных странах, в том числе и в Российской Федерации. Быстроувеличивающаяся «популярность» в криминальной среде этой разновидности преступлений обуславливается наличием у нее таких свойств, как большая степень латентности, обуславливаемая всеобщей компьютеризацией общественной и личной жизни, а также трансграничным характером преступлений и связанной с ним неуловимостью компьютерных преступников, и вместе с тем относительная легкость совершения преступлений [3].

¹ © Шульга Д. С., 2023.

В то же время важно различать исследуемый вид преступлений от похожих, определяемых Уголовным кодексом как кража (ст. 158 УК РФ). При этом, согласно п. 17 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [4], кражей является хищение преступником денежных средств безналично, посредством предварительного получения доступа к личным данным владельца банковской карты (например, персональные данные владельца, данные платежной карты, контрольная информация), которые потерпевший, будучи введенным в заблуждение, самостоятельно передает преступнику.

К дистанционному мошенничеству относятся [5]:

1. Фишинг – это вид мошенничества, при котором злоумышленники пытаются получить доступ к личным данным пользователей, таким как пароли, номера кредитных карт и другие конфиденциальные данные. Они делают это, выдавая себя за доверенное лицо, например, банк или интернет-магазин. Чаще всего фишинг происходит через электронную почту или социальные сети.

2. Спам – это нежелательные сообщения, которые приходят на электронную почту или мобильный телефон. Они могут содержать рекламу, вирусы или ссылки на фишинговые сайты. Спам может быть отправлен массово или персонально, и его целью является заставить пользователей перейти на определенный сайт или купить определенный товар.

3. Вирусы – это программы, которые могут нанести вред компьютеру или мобильному устройству. Они могут быть распространены через электронную почту, социальные сети или загрузки из интернета. Вирусы могут украсть личные данные, заблокировать компьютер или использовать его для атак на другие устройства.

4. Социальный инжиниринг – это метод мошенничества, при котором злоумышленники используют психологические методы, чтобы убедить людей сделать то, что они хотят. Например, они могут позвонить вам и выдать себя за представителя банка, чтобы получить доступ к вашим личным данным. Или они могут отправить вам электронное письмо, в котором будут просить вас перейти на определенный сайт и ввести свои данные.

5. Кибершантаж – это вид мошенничества, при котором злоумышленники угрожают жертве опубликовать ее личные данные или компрометирующие материалы, если она не заплатит им деньги. Кибершантаж может происходить через электронную почту, социальные сети или мессенджеры.

6. Фейковые сайты – это сайты, которые выглядят как настоящие, но на самом деле созданы злоумышленниками для того, чтобы получить доступ к личным данным пользователей. Они могут быть созданы для фишинга, кибершантажа или распространения вирусов.

7. Кража личных данных – это преступление, при котором злоумышленники получают доступ к личным данным пользователей, таким как номера кредитных карт, адреса и телефоны. Они могут использовать эти данные для финансовых мошенничеств или продажи на черном рынке.

8. Криптовалютные мошенничества – это преступления, связанные с криптовалютами, такими как Биткоин. Злоумышленники могут создавать фейковые

криптовалютные биржи или кошельки, чтобы получить доступ к личным данным пользователей или украсть их криптовалюты.

В заключение дистанционные мошенничества могут принимать различные формы и направлены на получение выгоды за счет обмана других людей. Чтобы защитить себя от таких преступлений, необходимо быть осторожным при общении в интернете, не доверять незнакомым людям и не раскрывать свои личные данные.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 27.04.2023). URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.
2. Рагулина А. В. Компьютерное мошенничество // Пробелы в российском законодательстве. 2016. № 5. С. 41–49.
3. Егерова О. А. Некоторые вопросы методики расследования киберпреступлений / О. А. Егерова, В. В. Коломинов, М. С. Сизова // Сибирские уголовно-процессуальные и криминалистические чтения. 2018. № 4 (22). С. 24–32.
4. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // СПС «КонсультантПлюс».
5. Протасевич А. А. Борьба с киберпреступностью как актуальная задача современной науки / А. А. Протасевич, Л. П. Зверьянская // Криминологический журнал Байкальского государственного университета экономики и права. 2011. № 3. С. 28–33.