

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

**Международная научно-практическая конференция
(18 апреля 2024 г.)**

Сборник научных трудов

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

Научное электронное издание

Москва
Московский университет
МВД России имени В.Я. Кикотя

2024

© Московский университет МВД России
имени В.Я. Кикотя, 2024
ISBN 978-5-9694-1544-7

УДК 004.9
ББК 16.3
И74

Рецензенты:

заместитель начальника Департамента информационных технологий,
связи и защиты информации МВД России **М. В. Казаков**;
начальник кафедры информационных технологий
Академии управления МВД России **А. В. Бецков**

Составитель *И. С. Мельцева*

И74 Информационные технологии в деятельности органов внутренних дел : Международная научно-практическая конференция, 18 апреля 2024 г. : сборник научных трудов / [сост. И. С. Мельцева]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2024. – 375 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 978-5-9694-1544-7

В сборнике представлены научные труды участников Международной научно-практической конференции, состоявшейся 18 апреля 2024 г. в Московском университете МВД России имени В.Я. Кикотя в рамках Международного форума «Цифропол-2024». На конференции обсуждались вопросы обеспечения информационной безопасности государства, применения искусственного интеллекта при противодействии преступлениям, особенности проведения компьютерных и радиотехнических экспертиз, а также возможности использования беспилотных летательных аппаратов в деятельности органов внутренних дел.

Издание адресовано преподавателям, адъюнктам, курсантам и слушателям образовательных организаций МВД России, а также практическим работникам правоохранительных органов.

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, 2024

Издание подготовлено
с помощью программного обеспечения Microsoft Word

В авторской редакции

Компьютерная верстка *Табунова Е. А.*

Подписано к изданию 30.07.2024
Объем издания: 7 039 Кб
1 электронный оптический диск (CD-R)

ISBN 978-5-9694-1544-7



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

СОДЕРЖАНИЕ

Приветственные слова

<i>Чернышенко Дмитрий Николаевич</i>	<i>11</i>
<i>Шулика Виталий Дмитриевич</i>	<i>12</i>
<i>Войнов Юрий Витальевич</i>	<i>13</i>
<i>Калиниченко Игорь Александрович</i>	<i>15</i>

Аветисян Б. Р., Пивоваров Г. В.

Контроль и верификация декларируемых доходов в рамках налогообложения цифровых валют на этапе майнинга	18

Аветисян К. Р.

Противоборство легализации рекламы онлайн-казино и уклонению от уплаты налогов	22

Агафонов М. А.

Проблемы развития понятийного аппарата международного сотрудничества по делам о преступлениях в сфере информационных технологий	25

Андреев И. В.

Вопросы использования технологии виртуальной реальности в деятельности органов внутренних дел	30

Апарцев М. А.

Цифровой многоканальный комплекс автономной регистрирующей аппаратуры «Хронос».	
Тактико-технические характеристики и возможности применения	33

Батоев В. Б.

К вопросу о противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий	36

Баторов Б. О.

О некоторых вопросах применения технологий искусственного интеллекта в деятельности МВД России для анализа и обработки информации, содержащейся в аудио- и видеоматериалах	39

Богачева М. В.

Осуществление информационного взаимодействия МВД России и министерств внутренних дел государств – участников Содружества Независимых Государств	45

Брысин Н. Н.

Аутентификация физических лиц с использованием биометрических персональных данных при доступе к информационным системам	51

Бурмистров Е. С., Захаров Д. С.

Искусственный интеллект в жизни юриста	54

<i>Васильева Д. В.</i>	
Искусственный интеллект как новый тип криминального мышления.....	56
<i>Васильчикова А. А.</i>	
Каналы управления беспилотными летательными аппаратами	59
<i>Власюк Н. А., Толстых М. Ю.</i>	
Разработка адаптивных мер защиты электронной почты на базе технологий искусственного интеллекта	61
<i>Гермогенова Е. С.</i>	
Правовые аспекты определения имущественного ущерба при расследовании преступлений в сфере компьютерной информации.....	64
<i>Гончар В. В.</i>	
О формировании комплекса мер по противодействию преступлениям в сфере информационных технологий	67
<i>Горичева С. Д.</i>	
Аварийные регистраторы событий как объект экспертного исследования	71
<i>Григорусь Л. Н., Тутова О. В.</i>	
NFT как средство легализации (отмывания) доходов, полученных преступным путем	75
<i>Давыдов А. Д.</i>	
Безопасное использование общественных Wi-Fi.....	79
<i>Данилова А. О.</i>	
О проблемах доказывания обстоятельств преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации	81
<i>Дворцова А. А.</i>	
Использование технологий искусственного интеллекта в борьбе с преступностью	84
<i>Дудникова Е. В.</i>	
О некоторых вопросах развития интегрированных банков данных оперативно-справочных, криминалистических, розыскных и статистических учетов, формируемых на базе органов внутренних дел Российской Федерации.....	89
<i>Емельянова О. В., Диденко З. И.</i>	
Защита персональных данных в условиях применения цифровых технологий	93
<i>Жандров В. Ю.</i>	
Электронное наблюдение в механизме выявления и документирования незаконного оборота наркотиков	95

<i>Захарова А. М.</i> Анализ судебной практики по делам, связанным с незаконными организацией и проведением азартных игр	99
<i>Захарова С. Е.</i> Профайлинг как способ расследования преступлений	104
<i>Ивлева Е. А., Воробьева Т. И.</i> Роль электронных носителей в деятельности правоохранительных органов	107
<i>Игнашева В. С.</i> Оптимизация разведки по открытым источникам	109
<i>Калашникова А. А., Мишина А. А.</i> Проблемы использования алгоритмов искусственного интеллекта в правоохранительной деятельности.....	112
<i>Каримов А. К.</i> Риски информационной безопасности организаций	116
<i>Киселева С. М.</i> Использование искусственного интеллекта для обеспечения информационной безопасности	119
<i>Кравченко В. И.</i> Применение коллективного искусственного интеллекта в государственном управлении.....	123
<i>Крутинская С. Р.</i> Концепция распределенной информационной системы экспертно-криминалистического подразделения МВД России	126
<i>Кубасов И. А.</i> Перспективные направления применения технологий искусственного интеллекта и больших данных в деятельности органов внутренних дел.....	130
<i>Кузьминых А. В., Задохина Н. В.</i> Связь между трансформацией права и изменением правосознания в условиях цифровизации общественных отношений	135
<i>Куриленко Ю. А.</i> Актуальные вопросы взаимодействия государств – членов Организации Договора о коллективной безопасности в решении задач информационной безопасности	137
<i>Кутергина Е. М., Дядык Е. С.</i> Возможность автоматизации расчетов при производстве портретной экспертизы.....	140
<i>Линев Н. В.</i> Исследование эффективности пассивных методов подавления побочного электромагнитного излучения технических средств.....	143

Лустин В. И.

Особенности взаимной связи цифровой экономики
и киберпреступности..... 149

Максимова Е. А., Худяков В. В.

Судебная компьютерно-техническая экспертиза – инструмент
неотвратимости правосудия 152

Маликов С. А.

Актуальные вопросы применения беспилотных воздушных средств
в реалиях современной России 154

Маслов Н. В.

Фундаментальные и прикладные направления развития
естественнонаучных знаний в цифровой трансформации
правоохранительных органов, в том числе при подготовке
к производству судебно-биологических экспертиз и исследований 158

Меняйло Д. В., Дрога А. А., Назаренко И. С.

О некоторых особенностях мониторинга противоправного контента
в сети Интернет..... 162

Минаев В. А.

Полиция и криминогенная обстановка в России: цифровые тенденции,
методы, средства, системы анализа и управления..... 168

Минетулина А. Р.

Биометрические технологии в криминалистике:
инновационные подходы и перспективы для правоохранительных органов
в цифровую эпоху..... 182

Миронова Е. Ю.

К вопросу о категории справедливости в аспекте перспективы применения
искусственного интеллекта в уголовном судопроизводстве 185

Молодых В. А., Подружкина Т. А.

Использование технологий больших данных в расследовании
преступлений, связанных с теневой экономической активностью..... 190

Нурматов Н.

К вопросу применения специальных знаний при расследовании
преступлений в IT-сфере 194

Овчинский А. С.

Борьба с деструктивными сетевыми сообществами при обеспечении
информационной безопасности в условиях гибридной войны
против России 198

Орлов И. С., Харламова И. Ю.

Деятельность правоохранительных органов в процессе реагирования
на кибератаки..... 202

Панасюк А. В.

Использование технологий искусственного интеллекта
в борьбе с преступностью..... 204

Переходченко К. В.

Практические аспекты применения специальных знаний
специалистами следственно-оперативной группы
при расследовании преступлений в сфере
информационно-телекоммуникационных технологий 206

Пименова О. В., Клочкова Е. Н.

Перспективы использования искусственного интеллекта для обеспечения
кибербезопасности информационных ресурсов и систем на примере
технологий машинного обучения (ML-технологий) 210

Плотников Г. Г.

О модели оценки противодействия беспилотным системам..... 214

Поликарпов Е. С., Маяков Д. В.

Этапы создания и обучения языковой модели детектирования
компьютерных атак на основе аугментации данных..... 216

Полянская Е. П.

Правовые аспекты использования метода OSINT
в правоохранительной деятельности..... 222

Помещиков С. Е.

Применение технологий анализа больших данных и SIEM-систем
для выявления тенденций и паттернов в сфере
противодействия киберпреступлениям..... 225

Рожков Н. И.

Развитие методов и технологий квантовой криптографии
для обеспечения безопасности передачи данных
и защиты конфиденциальной информации 229

Роздорский Н. С.

Особенности идентификации граждан при прохождении
через контрольно-пропускные пункты МВД России 232

Рудометов Д. Р.

Идентификация лица, совершившего уголовное преступление
или административное правонарушение в сети Интернет 236

Рябинкина С. М., Александров Ю. Н.

Проблемы внедрения технологии 3D-сканирования
в экспертную деятельность 239

Сакулина Л. Л.

Проблемы регулирования искусственного интеллекта
в правовом пространстве Российской Федерации 242

Сапелкина А. В.

Методы регулирования криптовалютных операций в России 247

<i>Симакова М. А.</i>	
Роль международных организаций в борьбе с киберпреступлениями.....	249
<i>Симонова В. Д., Дубинина Н. М.</i>	
Информационные войны: история и современность.....	252
<i>Смирнов В. М.</i>	
Навигационно-мониторинговые системы в деятельности органов внутренних дел.....	254
<i>Страхов А. А., Жукова П. Н., Прокопенко А. Н.</i>	
Искусственный интеллект как глобальная угроза безопасности	257
<i>Сумина А. В.</i>	
Внедрение информационных технологий в правоохранительную деятельность: возможности искусственного интеллекта в раскрытии, расследовании и предупреждении преступлений	266
<i>Трофимов Е. А.</i>	
К вопросу правового регулирования цифровизации договорных отношений в гражданско-правовой сфере	269
<i>Трубачев Н. А.</i>	
Перспективы внедрения искусственного интеллекта в российский уголовный процесс	272
<i>Удалова Д. А.</i>	
Практические аспекты применения тактических приемов при расследовании преступлений в сфере информационно-телекоммуникационных технологий	276
<i>Филимонов А. А.</i>	
Система контроля версий Git как объект криминалистического исследования.....	280
<i>Харламов И. С.</i>	
Обзор современных операционных систем и перспективы их использования в информационном обеспечении МВД России	288
<i>Хатова Ж. М.</i>	
О цифровой гигиене студентов юридических вузов	295
<i>Ходусов А. А.</i>	
Цифровизация в криминалистике: современные вызовы	297
<i>Хорзов Д. С.</i>	
Анализ журналов работы беспилотных летательных аппаратов марки DJI в экспертно-криминалистических целях	303
<i>Хорошко А. А.</i>	
Борьба с киберпреступностью как специфическая функция органов внутренних дел Российской Федерации в условиях цифровизации общественных отношений	307

<i>Хотамов М. М.</i>	
Информационное воздействие на сознание человека	310
<i>Цимбал В. Н.</i>	
Актуальные вопросы применения технологий нейронных сетей при совершении противоправных деяний	313
<i>Чеканов И. Р., Краев И. В., Молоканова Б. Б.</i>	
Использование графовых структур для визуализации законодательства в области информационной безопасности.....	319
<i>Чубанова Е. И.</i>	
Перспективы использования искусственного интеллекта в деятельности органов внутренних дел.....	325
<i>Чурин Р. А.</i>	
Особенности исследования новейших беспилотных летательных аппаратов	329
<i>Чурина С. Р.</i>	
Применение норм контроля к беспилотным летательным аппаратам	335
<i>Шайдаев М. Ш.</i>	
Две стороны использования искусственного интеллекта в сфере противодействия терроризму и экстремизму	339
<i>Шапкин С. В.</i>	
Перспективы развития криптовалют и их влияние на информационную безопасность.....	347
<i>Шарай А. Е.</i>	
Оценка уровня экономической безопасности в сфере оборота децентрализованных финансовых активов.....	350
<i>Швырев Б. А., Ромашкин Т. Р., Антонов А. С.</i>	
Модель канала утечки речевой информации за счет использования Wi-Fi	352
<i>Шикалова В. М.</i>	
Внедрение технологии блокчейн в правоохранительную деятельность для обеспечения прозрачности и целостности данных	357
<i>Шубина К. С.</i>	
Электронные средства связи, используемые в деятельности правоохранительных органов и судов	359
<i>Эрдниева А. С.</i>	
Особенности подготовки специалистов в области информационной безопасности в современных условиях.....	365
<i>Яковлева К. Ю.</i>	
Применение электронной (компьютерной) модели в следственных действиях, проверке и оценке доказательств	369
<i>Ярмак К. В.</i>	
Об опыте проведения олимпиады школьников «Университет цифровой полиции» по информационной безопасности	372



Чернышенко Дмитрий Николаевич,
заместитель Председателя Правительства
Российской Федерации

**Участникам
Международного форума
«Цифропол-2024»**

Дорогие друзья!

Приветствую Вас на ежегодном Международном форуме «Цифропол-2024»! Символично, что он проходит на базе Московского университета МВД России имени В.Я. Кикотя – одного из сильнейших профильных вузов страны, где готовят специалистов в области информационной безопасности.

Президент Российской Федерации Владимир Владимирович Путин определил цифровую трансформацию национальной целью развития до 2030 г. Сегодня перед Россией стоят масштабные технологические вызовы и задачи, успешное выполнение которых невозможно без создания надежной системы кибербезопасности.

Только за прошлый год в нашей стране объем утечек конфиденциальной информации увеличился более чем в 100 раз по сравнению с 2015 г., особенно сильным кибератакам подвергаются государственные органы и объекты критической инфраструктуры. ИБ-специалисты также противодействуют новыми угрозам с применением технологий искусственного интеллекта – дипфейкам и нарушением частной жизни людей.

Россия должна быть готова к отражению информационных атак: ведется большая работа по обеспечению кибербезопасности граждан и бизнеса, активно развиваются собственные цифровые решения и разработки, способные гарантировать неприкосновенность данных. Так, в прошлом году доля отечественных средств защиты информации в закупках ПО для государственных и муниципальных нужд составила около 90 %.

Уверен, участники форума «Цифропол-2024» внесут вклад в разработку перспективных идей и решений, связанных с информационной безопасностью.

Желаю вам конструктивного диалога!



Шулика Виталий Дмитриевич,
заместитель Министра внутренних дел
Российской Федерации

Уважаемые коллеги!

Сегодня на площадке Московского университета МВД России имени В.Я. Кикотя мы проводим Международный форум «Цифропол-2024».

Это мероприятие становится все более популярным. В стенах Университета собралось 250 участников и более 100 человек виртуальных гостей.

В расширенном составе мы собираемся впервые, но, надеюсь, что такие встречи станут нашей доброй традицией.

Рад приветствовать представителей силовых ведомств стран – участников Содружества Независимых Государств: Азербайджана, Армении, Беларуси, Киргизии, Таджикистана и Узбекистана.

Приятно видеть в числе почетных гостей и участников форума представителей высших органов власти, научного и бизнес-сообществ, ведущих специалистов в области информационных технологий и искусственного интеллекта, а также коллег из силовых ведомств.

На фоне сложной геополитической обстановки наша совместная работа будет способствовать обеспечению безопасности граждан.

Поэтому цель нашей встречи – это организация обмена опытом по выявлению, предупреждению, пресечению и раскрытию преступлений, а также демонстрация новейших отечественных разработок специальной техники и ИТ-решений.

Помимо выступлений и докладов развернута выставочная экспозиция, организовано проведение практических мастер-классов, демонстрация возможностей искусственного интеллекта.

Высокая скорость обработки данных, автоматизация рутинных задач, помощь в принятии решений, получение новых знаний – выгода от использования новейших технологий очевидна.

Поэтому тематика основной секции форума определена как «Перспективы применения технологий и систем искусственного интеллекта в деятельности органов внутренних дел Российской Федерации».

Желаю всем участникам форума продуктивной работы, полезного обмена мнениями и опытом.



Войнов Юрий Витальевич,
начальник Департамента информационных
технологий, связи и защиты информации
МВД России,
кандидат технических наук

Уважаемые коллеги!

Вот уже шестой раз (начиная с 2018 г.) на площадке Московского университета МВД России имени В.Я. Кикотя обсуждаются актуальные вопросы применения информационных технологий в деятельности органов внутренних дел.

Цифровую основу деятельности МВД России составляет Единая система информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России). Она состоит из 40 сервисов повседневной и оперативно-служебной деятельности. В нее входит облачная платформа, единая система управления доступом к сервисам, подсистема обеспечения информационной безопасности, платформа для разработки и развертывания сервисов, базовые сервисы.

Особый интерес вызывают возможности предиктивной аналитики, способной выявить скрытые закономерности, тенденции, получить новые знания. В МВД России уже функционирует система Центров обработки данных. В настоящий момент проводится строительство нового федерального центра обработки информации, осуществляется создание «аналитической песочницы».

Указом Президента Российской Федерации от 15 февраля 2024 г. обновлена Национальная стратегия развития искусственного интеллекта, внесен ряд существенных изменений, конкретизированы цели, расширен список задач. Доверенные технологии искусственного интеллекта должны в том числе обеспечивать национальную безопасность и защиту правопорядка. Смысл их внедрения заключается в обеспечении соблюдения принципов объективности, исключения нарушений прав и свобод человека, недопустимости нанесения ущерба интересам общества и государства. Данная формула – основа работы сотрудников органов внутренних дел.

Важную роль в развитии искусственного интеллекта играет международное сотрудничество. МВД России поддержана инициатива института системного программирования Российской академии наук по созданию хранилища наборов данных, а также программных решений в области искусственного интеллекта, в том числе на международном уровне. Вместе с тем стандарты иностранных поисковых систем не в полной мере учитывают особенности и реалии национальной системы государственного управления. МВД России нацелено на использование отечественных решений.

С каждым годом растет количество программных решений, используемых в деятельности органов внутренних дел, в которых применяются и технологии

компьютерного зрения, и обработка естественного языка, и распознавание речи. С 2020 г. идентификация и поиск лиц по оперативным учетам успешно решаются при помощи биометрических алгоритмов.

К перспективному направлению развития искусственного интеллекта в МВД России можно отнести задачу (в настоящее время находится в разработке) по созданию интеллектуальной системы поддержки принятия решений при возникновении чрезвычайных ситуаций.

МВД России, со своей стороны, также участвует в научно-исследовательской деятельности в сфере искусственного интеллекта.

По данной тематике проведено шесть научно-исследовательских работ (изучены вопросы ДНК-фенотипирования, поиска серийности, анализа информации с комплексов видеорегистрации, выявления дипфейков, обнаружения и классификации татуировок), работа над двумя исследованиями продолжается (по изучению нейронных языковых моделей и формирования требований в подготовке датасетов).

Все чаще МВД России взаимодействует с научно-исследовательскими институтами, участвует в апробации инновационных разработок. Ярким примером взаимодействия является совместная работа с Фондом перспективных исследований. Один из проектов предназначен для определения вероятности внесения модификаций в аудио- и видеоконтент. Другой позволяет в автоматическом режиме создавать нейросетевые модели для решения задач «компьютерного зрения».

Расширение сферы применения технологий искусственного интеллекта предполагает значительные временные, материально-технические и организационные затраты. К примеру, для обучения нейросетевых моделей требуются подготовленные и размеченные датасеты. Однако специфика деятельности полиции накладывает ограничения на обработку соответствующей информации. Для проведения исследований в области развития искусственного интеллекта, а также формирования датасетов МВД России задействуются преимущественно ведомственные кадровые ресурсы: научно-производственное объединение «Специальная техника и связь» и образовательные организации МВД России.

Значительное внимание МВД России уделяет формированию кадрового потенциала, в том числе в области информационных технологий. Специалистов ИТ-сферы готовят на базе четырех ведомственных образовательных организаций высшего образования, в том числе в стенах Московского университета МВД России имени В.Я. Кикотя, гостеприимно предоставившего площадку для проведения Международного форума «Цифропол-2024». Технический и творческий потенциал курсантов раскрывается при участии в хакатонах по тематике «Искусственный интеллект для анализа больших данных».



Калиниченко Игорь Александрович,
начальник Московского университета
МВД России имени В.Я. Кикотя,
кандидат педагогических наук

Уважаемый Виталий Дмитриевич!
Уважаемые участники Международного форума «Цифропол-2024»!

Прежде всего позвольте поприветствовать вас – участников Форума и Международной научно-практической конференции. Впервые мы проводим научно-представительское мероприятие в новом формате, когда соорганизатором выступает один из наших главных заказчиков – Департамент информационных технологий, связи и защиты информации МВД России.

Наше сотрудничество с Департаментом при поддержке руководства МВД России позволило перевести на новый уровень процесс обучения будущих квалифицированных сотрудников по специальности «Информационная безопасность». Вместе с тем практико-ориентированная подготовка – динамичный процесс, требующий постоянного развития.

С учетом современной геополитической обстановки Университетом определены приоритетные направления развития, к которым относятся: методы использования и противодействия БВС, применение современных средств навигации и связи в особых условиях; внедрение технологии искусственного интеллекта в деятельность органов внутренних дел; противодействие преступлениям, совершаемым в сфере информационных технологий.

В рамках реализации приоритетных направлений решается комплекс задач. Так, в текущем году завершается работа по оснащению лабораторно-полигонной базы типовым комплектом технических средств обучения операторов БВС. Спроектирован и планируется к введению в эксплуатацию киберполигон SOC (Security Operation Center), позволяющий формировать навыки по выявлению компьютерных атак и расследованию инцидентов информационной безопасности. Для совершенствования подготовки специалистов по компьютерной и радиотехнической экспертизе России разработаны и согласованы с ЭКЦ МВД проекты учебных стендов и лабораторных комплексов. С целью совершенствования информационно-аналитического обеспечения служебной деятельности разработан концепт учебного полигона для решения следующих задач: распознавания и классификации объектов с помощью сверточных нейронных сетей, визуальной обработки и управления движением с помощью искусственного интеллекта, предиктивной аналитики для правоохранительных органов.

Новое материально-техническое обеспечение требует качественного научно-методического сопровождения. В 2023 г. авторским коллективом Университета

разработано первое учебное пособие «Противодействие преступлениям, совершаемым в сфере информационных технологий». В текущем году планируется разработка учебно-методических материалов по использованию типового комплекса БВС в учебном процессе.

Важнейшей задачей Московского университета МВД России имени В.Я. Кикотя является совершенствование подготовки кадров для органов внутренних дел, которое невозможно представить без внедрения в образовательный процесс современных информационных технологий. Сегодняшний формат взаимодействия – яркий пример научного подхода к интеграции прогрессивных информационных систем и программно-аппаратных комплексов в образовательное пространство.

Мы уверены в том, что результаты работы Форума не только позволят расширить представления о подходах и практиках внедрения информационных технологий в деятельность органов внутренних дел, но и раскроют новые горизонты для ведомственной системы подготовки кадров.

В работе Форума принимают участие:

- Виталий Дмитриевич Шулика, заместитель Министра внутренних дел Российской Федерации;
- Артем Геннадьевич Шейкин, сенатор Совета Федерации Федерального Собрания Российской Федерации;
- руководители Администрации Президента Российской Федерации;
- руководители Аппарата Правительства Российской Федерации;
- представители Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории стран – участников СНГ: МВД России, МВД Таджикистана, МВД Азербайджана, МВД Киргизии, МВД Узбекистана, полиции Армении, МВД Беларуси;
- офицеры связи правоохранительных органов, аккредитованных при посольствах зарубежных государств в г. Москве: МОБ Вьетнама, МВД Египта, Сил охраны правопорядка Ирана, МОБ Китая; представители Посольства Китая, Министерства юстиции и внутренних дел Монголии, МВД Объединенных Арабских Эмиратов, представители Посольства Турции, МВД Кубы, МВД Беларуси, МВД Киргизии;
- представители органов государственной власти Российской Федерации;
- представители и руководители образовательных организаций высшего образования, осуществляющих подготовку специалистов в сфере информационных технологий;
- руководители и сотрудники подразделений центрального аппарата МВД России;
- профессорско-преподавательский состав образовательных организаций МВД России.

Отдельного упоминания заслуживают наши партнеры, согласившиеся не только принять участие в научных изысканиях, но и продемонстрировать технические достижения, активно используемые в повседневной деятельности, в том числе и для выполнения государственных задач.

Мы уверены в том, что сегодняшнее мероприятие позволит участникам как найти пути решения повседневных задач, так и определить перспективные векторы для саморазвития.

В завершение своего приветствия позвольте поблагодарить вас за участие в нашем научно-представительском мероприятии, пожелать продуктивной работы в целях выработки совместной стратегической мысли по внедрению инновационных технологий в деятельность органов внутренних дел.

Благодарю за внимание!

Аветисян Б. Р.¹,
главный научный сотрудник
Научно-исследовательского института
образования и науки

Пивоваров Г. В.²,
сотрудник Межрегиональной инспекции
по крупнейшим налогоплательщикам
Федеральной налоговой службы

КОНТРОЛЬ И ВЕРИФИКАЦИЯ ДЕКЛАРИРУЕМЫХ ДОХОДОВ В РАМКАХ НАЛОГООБЛОЖЕНИЯ ЦИФРОВЫХ ВАЛЮТ НА ЭТАПЕ МАЙНИНГА

Следует понимать, какие принципиально важные особенности есть у цифровых валют. Условная анонимность сферы деятельности, следует использовать термин «квази-анонимность», поскольку пользователи могут раскрывать свои персональные данные в зависимости от канала коммуникации в рамках взаимодействия с другими участниками сети по поводу операций, связанных с цифровыми валютами.

Децентрализованность, воплощенная в технологии распределенных реестров, на которой строится система обращения цифровых валют. В основе технологии лежит идея, согласно которой контроль за деятельностью субъектов осуществляется всеми пользователями данных. Верификация содержащихся в системе данных происходит коллективным образом в сравнении с централизованным аналогом. По причине того, что в системе отсутствуют лица с «расширенными правами», взаимодействие пользователей трудно обезопасить, если только речь не идет о более привычных способах обмена активами друг с другом. В остальных случаях необходимо понимать, что границы цифровой юрисдикции строго не определены, а участники сети действуют в рамках единого цифрового пространства, не разделенного по региональному признаку.

В соответствии с Докладом для общественных консультаций Банка России «Криптовалюты: тренды, риски, меры» от 2022 г., регулятор выделяет следующие ключевые риски:

- угрозы для благосостояния граждан;
- угрозы для финансовой стабильности системы;
- угрозы, связанные с развитием нелегальной деятельности в России.

В целях обеспечения долгосрочного развития сегмента цифровых активов в рамках реализации политики всестороннего экономического развития, деятельность регулятора направлена на борьбу с обозначенными угрозами. В рамках Концепции законодательного регламентирования механизмов организации оборота цифровых активов, определены ключевые направления развития регулирования сферы обращения цифровых валют. Основными направлениями развития рынка цифровых активов в России выступают:

¹ © Аветисян Б. Р., 2024.

² © Пивоваров Г. В., 2024.

– регулирование (лицензирование) непосредственно самих участников рынка цифровых активов, оформление соответствующего порядка налогообложения цифровых валют;

– комплексная легализация криптовалют в том числе для осуществления международных операций (в рамках экспериментальных правовых режимов).

Связанный с Концепцией законопроект № 237585-8 о внесении изменений в Федеральный закон «О цифровых финансовых активах, цифровой валюте» предусматривает требования к осуществлению деятельности физическими и юридическими лицами, занимающимися майнингом цифровой валюты, включая участников майнинг-пула. Сформулированы требования к гибкости и масштабируемости, которые определили приоритетную задачу по обеспечению безопасности элементов критической информационной инфраструктуры Российской Федерации, в особенности, в отношении распределенных высокопроизводительных кластеров обработки Больших Данных (BIG DATA) и интеграции технологий виртуализации для предоставления облачных сервисов (Cloud Bursting).

Международная практика налогообложения цифровых валют устанавливает следующие ключевые налогооблагаемые события - создание в различных формах, в том числе первичное размещение монет, эйрдроп и майнинг; обмен, который может производиться на фиатную валюту, иной цифровой актив или использоваться в качестве средства платежа для приобретения товара или услуги на соответствующих цифровых площадках.

Налогообложение майнинга представлено в двух вариациях. Первая предусматривает возникновение налоговой обязанности в момент реализации «добытой» валюты. Вторая – в момент добычи цифровой валюты. Однако для эффективного применения каждого сценария у регулятора должна быть возможность верифицировать или устанавливать достоверность сведений о доходах и расходах, которые отражаются в декларации налогоплательщика.

Возможность верификации сведений усложняется используемыми каналами конвертации цифровых активов, которые в большей степени носят латентный характер, усложняя контролируемому органу механизм исполнения контрольно-надзорных и учетных функций.

Следует отметить, что при конвертировании цифровых активов в рубли и перечислении их на счета российских банков, процедура отслеживания соответствующих операций – реализуема.

К числу часто используемых каналов конвертации или обмена цифровых валют относятся централизованные и децентрализованные биржи, криптообменники, P2P площадки и иные сервисы, многие из которых позволяют использовать цифровые валюты в качестве платежного средства.

От используемого механизма обмена цифровых валют зависит порядок регулирования обозначенных рисков. Так, в целях верификации декларируемых доходов, получаемых в форме цифровых активов при реализации механизма консенсуса «Proof of Work», предлагается комплексное решение верификации майнинга, включающее:

- формирование древа сети или ее иерархическое представление - визуализация компонентов источника и адреса назначения;
- отображение элементов потока данных с визуализацией маршрутов «движения» используемых сетевых узлов;
- установление идентификаторов анализируемых узлов до web-ресурсов, к которым обращается «оператор» (mac-адрес узла и его IP адрес(а), mac-адрес точки доступа и ее IP адрес(а), а также сетевые протоколы, используемые порты и конечные URL-адреса).

Последовательный анализ цифрового контура исследуемого объекта с целью выявления вычислительных мощностей, используемых для майнинга цифровых активов, представляет:

- сканирование сети и дальнейшее выведения всех устройств на интерфейс пользователя (проверяющего лица, подключенного к сети объекта информатизации);
- перераспределение сетевого трафика, исследуемого в рамках объекта информатизации через проверяющего устройств. Проверяющий приобретает статус «координатора», осуществляющего контроль всего сетевого трафика;
- анализ сетевого трафика, проходящего через «координатора».

Развитие методологии и инструментария регулирования рынка цифровых валют повышает безопасность их использования, развития высокотехнологичной отрасли, в соответствии со стратегическим планированием и реализацией национальных интересов Российской Федерации.

Список литературы

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_216363/.
2. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_208191/.
3. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_389271/.
4. Распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р «Об утверждении программы “Цифровая экономика Российской Федерации”» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_221756/.
5. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10148/.

6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.

7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.

8. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_32834/.

9. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_358753/.

10. Письмо ФНС России от 4 июня 2018 г. № БС-4-11/10685@ «О порядке налогообложения доходов физических лиц» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_299587/.

Аветисян К. Р.¹,
доцент кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

ПРОТИВОБОРСТВО ЛЕГАЛИЗАЦИИ РЕКЛАМЫ ОНЛАЙН-КАЗИНО И УКЛОНЕНИЮ ОТ УПЛАТЫ НАЛОГОВ

Применение технологий нейронных сетей, обученных методами машинного обучения, с алгоритмами системного дообогащения обучающих выборок (дата-сетов), в целях выявления признаков уклонения от уплаты налогов, а также противодействия поддержанию теневой экономики через децентрализованные цифровые платформы, по типу онлайн-казино – выступает одной из наиболее ключевых и приоритетных задач на государственном уровне.

Алгоритм противодействия включает:

I. Выявление цифровых платформ (web-ресурсов), а также интегрированных в структуре реализации решения в древе иерархии всех групп социальных сетей, мессенджеров и их администраторов.

II. Ранжирование платформ по анализу активности и предметности исследуемого контента как на самих цифровых платформах, так и активности пользователей на них, включая типы интеграции, в том числе выступающие признаками к актуальности исследования объектов (каналов «лидеров мнений») на предмет получения оперативно-значимой информации с ресурсов.

III. Установление атрибутов онлайн-казино, идентификаторов хоста, его владельца. Специализированные карты имеют встроенные средства для проставления временных меток, аппаратной фильтрации, снятия заголовков низкоуровневых протоколов, балансировки нагрузки между процессорами на многопроцессорных компьютерах с учетом IP-потоков, выявления ошибочных и дублирующихся пакетов. Анализ трафика реализуется посредством контроля ключевых узлов и компонентов сетевой инфраструктуры: сетевые шлюзы, маршрутизаторы, коммутаторы (src-dst порты), и иные устройства с установлением их идентификаторов.

При трансляции сетевых пакетов по глобальной сети, в заголовок добавляется служебная информация, в которой содержатся логические адреса источника и получателя, а также всех иных транзитирующих сегментов данных участвующих в логистическом процессе. По установлению физических адресов – осуществляется процедура сопоставления физических и логических идентификаторов сети, установление стека сетевых узлов, их активности за исследуемый период времени. Далее произведение процедуры сопоставления физических адресов - асимметричный анализ трафика по глобальным и локальным идентификаторам, устанавливая перечень устройств и их роли (ретрансляция, хранение, обработка, др.), в рамках которых реализована или реализуется активность в цепи узлов исследуемых объектов по событию.

¹ © Аветисян К. Р., 2024.

После верификации исследуемого объекта целесообразно применение методов классификации на основе сигнатур и шаблонов, связанных с известными протоколами и приложениями, а также эвристических методов поведенческого анализа:

- определение реферальных источников трафика, количества участников сети и стека используемых протоколов;
- извлечение метаданных из пакетов: IP-адреса источника и назначения, номера портов, размеры пакетов, временные метки;
- проверка полезной нагрузки пакетов: URL-адреса, исследование ключевых блоков;
- исследование кэшированного содержимого на серверах, анализ сжатого/шифрованного трафика (распределение нагрузки посредством протокола ICAP).

Дополнительная обработка полученного массива данных зависит от решаемой задачи и может включать в себя следующие алгоритмы действий:

- разбор полей протокола (protocol parsing);
- сборка сессии с установлением соединения;
- извлечение данных приложения (content extraction) – страниц сайтов (HTML), файлов различных типов (исполняемых файлов, документов, др.);
- анализ приложений (application content parsing);
- исследование дейтаграмм, анализ трафика (потока пакетов – srcIP, srcPort, dstIP, dstPort, protocol) межсетевого взаимодействия исследуемых узлов/хостов реализуемый посредством декапсуляции;
- анализ пакетов (Packet Based No State, PBNS), сообщений (Message Based Per Flow State, MBFS), сборка IP-фрагментов в IP-пакеты (IP-нормализация), сборка TCP-сегментов в TCP-сеансы (TCP нормализация).

IV. В случае хостинга платформы вне контролируемой регулятором и государственными органами инфраструктуры необходимо установить все возможные ЦОДы ретранслирующие данные от источника (актуальна к созданию базы данных с визуализацией на интерфейс пользователя в целях последующего отслеживания и анализа активности объекта и всех «контрольных сетевых точек» предоставляющие функции подмены IP-адресов, VPN, а также аналогичных технологий маскирования верифицирующих пользователя данных, с сохранением высокой скорости передачи данных).

Список литературы

1. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Информационно-правовой портал «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/71570570/>.
2. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_208191/.

3. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_389271/.
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/.
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.
6. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_32834/.
7. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_358753/.
8. Письмо ФНС России от 4 июня 2018 г. № БС-4-11/10685@ «О порядке налогообложения доходов физических лиц» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_299587/.
9. Аветисян Б. Р. Эффективность механизма противодействия незаконной организации и проведению азартных игр на Deep-Web платформах // Ученые труды Российской адвокатуры и нотариата. 2023. № 3 (70). С. 24–30.
10. Свидетельство о государственной программе для ЭВМ «Интеллектуальная система по выявлению инцидентов несанкционированного использования вычислительных мощностей [Нейросетевой классификатор]».
11. Свидетельство о государственной программе для ЭВМ «Интеллектуальная система анализа крипто транзакций на Deep-Web платформах».

Агафонов М. А.¹,

бакалавр права, магистрант

факультета подготовки криминалистов

Московской академии Следственного комитета

Российской Федерации имени А.Я. Сухарева

Научный руководитель: Хатов Э. Б.,

заведующий кафедрой информационных технологий

и организации расследования киберпреступлений

Московской академии Следственного комитета

Российской Федерации имени А.Я. Сухарева,

кандидат юридических наук, доцент

ПРОБЛЕМЫ РАЗВИТИЯ ПОНЯТИЙНОГО АППАРАТА МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ожидается, что всестороннее развитие современного общества способствует увеличению числа преступлений, совершаемых с использованием информационных технологий. Этот вид преступлений является самым «популярным» в 20-е гг. нашего столетия, поскольку обычно оно не требует больших материальных, технических и человеческих затрат. Напротив, смартфона с доступом в Интернет может быть достаточно для совершения этих преступлений. Зачастую лица, совершающие эти преступления и каким-либо образом связанные с ними, находятся за пределами государства, на территории которого проводится расследование, и поэтому расследование этих преступлений представляет наибольшие трудности для правоохранительных органов. По этой причине развитие быстрого и эффективного международного сотрудничества в расследовании преступлений, совершенных с использованием информационных технологий, является важным не только для Российской Федерации, но и для всего мирового сообщества.

Всестороннее развитие современного общества ожидаемо способствует увеличению количества преступлений, совершаемых с использованием информационных технологий. Данный вид преступлений является самым «популярным» в 20-е гг. нашего века, так как они по большей степени не требуют больших материальных, технических и людских затрат. Напротив, для совершения данных деликтов может хватить и одного смартфона с выходом в сеть Интернет. Зачастую те лица, совершающие эти преступления и каким-либо образом связанные с ними, находятся за пределами государства, на территории которого проходит расследование, в связи с чем расследование данных преступлений вызывает у правоохранительных органов наибольшие сложности. По причине чего разви-

¹ © Агафонов М. А., 2024.

тие оперативного и эффективного международного сотрудничества по расследованию преступлений, совершенных с использованием информационных технологий является актуальным вопросом не только для Российской Федерации, но и для остальных развитых государств.

Актуальной проблемой международного сотрудничества по делам о преступлениях в сфере информационных технологий является отсутствие единого нормативного закрепления термина «киберпреступление» как во внутригосударственном уровне, так и на мировой арене.

Многие российские правоведы по-разному интерпретируют понятие «киберпреступление». Д. Н. Карпова рассматривает «киберпреступление» как «акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет» [7, с. 47]. Согласно мнению С. И. Буз, под киберпреступлением понимается «любое преступление, совершенное с помощью информационных технологий, либо в информационном пространстве» [6, с. 78]. Считаем, что наиболее полно понятие «киберпреступление» охарактеризовал И. В. Романов: «общественно опасное деяние, совершаемое в киберпространстве, и посягающее, с одной стороны, на общественную безопасность, собственность, права человека, другие охраняемые законом отношения, а с другой – необходимый элемент механизма подготовки, совершения и сокрытия преступления, отражением которого является компьютерная информация, выступающая в роли предмета или средства совершенного преступления» [8, с. 4].

В российском законодательстве термин «киберпреступление» не находит свое отражение в нормативных правовых актах. Вместо него используются такие понятия, как «преступления в сфере компьютерной информации», «преступления, совершенные с использованием (применением) информационно-телекоммуникационных технологий», «информационные преступления».

В гл. 28 Уголовного кодекса Российской Федерации (УК РФ) употребляется термин «преступления в сфере компьютерной информации». Данная глава содержит в себе пять составов преступления, таких как: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации; 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 [1, с. 1]. Проанализировав диспозиции норм, находящихся в гл. 28 УК РФ, можно сделать вывод о том, что данные преступления посягают на общественные отношения в сфере охраны компьютерной информации, точнее на процессы изготовления, использования, распространения и ее защиту. Ю. В. Белевитина утверждает, что «Соотнося тер-

мины “киберпреступность” и “преступления в сфере компьютерной информации”, представляется, что первое выходит далеко за пределы преступлений в сфере компьютерной информации и охватывает большее количество составов преступлений» [5, с. 56]. Согласимся с данным мнением и полагаем, что понятие «киберпреступления» шире и может посягать не только на общественные отношения по защите компьютерной информации. Если целью совершения преступлений в сфере компьютерной информацией является посягательство на общественную безопасность и общественный порядок, то единственную цель «киберпреступлений» выявить не представляется возможным: она достаточно разнообразна и варьируется в зависимости от интересов преступника.

Продолжая анализировать российское законодательство, обратимся к Указанию Генпрокуратуры России № 401/11, МВД России от 19 июня 2023 г. № 2 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности», где существует перечень № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации [2, с. 1]. Данный перечень выделяет множество способов совершения таких преступлений:

- посредством использования, создания и распространения вредоносных компьютерных программ;
- с использованием средств мгновенного обмена сообщениями (интернет-мессенджеров) и т. д.

По-нашему мнению, данный перечень не является исчерпывающим, так как существуют и другие составы преступлений, где, так называемое, «киберпространство» может являться местом совершения преступления. В качестве примера можем рассмотреть объективную сторону ст. 135 УК РФ. Нельзя не согласиться с мнением О. В. Скворцовой и Д. Д. Макаренко, которые пишут: «На сегодняшний день злоумышленники чаще всего используют для бесконтактного развращения подростков такие каналы передачи электронной информации как: социальные сети, электронная почта, мобильные приложения типа WhatsApp или Viber, сайты знакомств, форумы и чаты» [9, с. 147]. Исходя из вышеизложенного, можно сделать вывод о том, что киберпространство будет являться именно местом совершения данного преступления.

В законодательстве США киберпреступления рассматриваются как любая деятельность, нарушающая законы и связанная с использованием электронных устройств и компьютерных сетей. Это включает в себя преступления, где электронное устройство является целью нападения (например, хакерские атаки), преступления, где электронное устройство используется как инструмент для совершения преступления (например, мошенничество или кража личных данных), а также преступления, где электронные устройства используются для хранения значимой информации (например, кража конфиденциальных данных или нарушение авторских прав). Это широкий спектр деяний, которые регулируются соответствующими законами в США [10, с. 1].

В международных нормативных актах понятия «киберперступление» и преступления в сфере информационных технологий трактуются по-разному, или же отсутствуют вовсе.

В единственной на сегодняшний день Конвенции о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) [4, с. 1], являющейся глобальным международным договором, осуществляющим деятельность по противодействию киберпреступлениям, находит свое место только лишь определение «компьютерная система». Тем самым, можем сделать вывод о том, что даже этот международный правовой акт не может в полной мере охватить все преступления, которые можно совершить с каким-либо использованием информационных технологий. Поскольку, как уже было сказано выше: компьютерная система не является единственной системой, в которой можно совершить преступление.

Вступившая в силу 16 января 2023 г. «Директива (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого уровня кибербезопасности на территории Союза, вносящая поправки в Регламент (ЕС) № 910/2014 и Директиву (ЕС) 2018/1972 и отменяющая Директиву (ЕС) 2016/1148 (Директива NIS 2)» имеет в своем содержании ст. 6 «Определения». В данной статье содержится большое количество терминов из сферы технического оснащения кибербезопасности: «Уязвимость», «Система доменных имен», «Техническая спецификация» и т. д. Несмотря на обилие нормативной базы, данный нормативный правовой акт так и не содержит определения «киберпреступление».

Ратифицированное Российской Федерацией «Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» [3, с.1], которое было принято в целях обеспечения эффективной борьбы с преступлениями в сфере информационных технологий, содержит в себе определение «информационная система», под которой подразумевается «организационно упорядоченная совокупность средств, реализующих определенные технологические действия посредством информационных процессов, предназначенных для решения конкретных функциональных задач». Полагаем, что данная интерпретация наиболее полно охватывает ту среду, в которой может быть совершено так называемое «киберпреступление».

Исходя из вышесказанного, можем сделать вывод, что одной из актуальных и острых проблем в современном международном сотрудничестве по делам о преступлениях, совершенных с использованием информационных технологий является различная трактовка понятий «преступления в сфере компьютерной информации», «преступления, совершенные с использованием (применением) информационно-телекоммуникационных технологий», «киберпреступления» на внутригосударственном уровне. Отсюда вытекает другая проблема – отсутствие единого международного нормативного правового акта, который бы полностью аккумулировал термин «киберпреступление» и стал бы единым для использования его всеми странами мирового сообщества.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.
2. Указание Генпрокуратуры России № 401/11, МВД России от 19 июня 2023 г. № 2 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/documentcons_doc_LAW_451498/.
3. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru>.
4. Конвенция Совета Европы о противодействии киберпреступлениям // Совет Европы : официальный сайт. URL: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.
5. Белевитина Ю. В. О соотношении понятий «киберпреступность» и «преступления в сфере компьютерной информации» // Инновационная наука. 2023. № 1-2.
6. Буз С. И. Киберпреступления: понятие, сущность и общая характеристика // ЮП. 2019. № 4 (91).
7. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8.
8. Романов И. В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13).
9. Скворцова О. В., Макаренко Д. Д. Развратные действия с использованием сети Интернет // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2021. № 1.
10. Evans L. E. Internet Overview. New York : 63 TEX. B.J., 2000. P. 23.

Андреев И. В.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*

ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В настоящее время наблюдается тенденция развития технологии виртуальной реальности (далее – VR) в использовании ее в процессе обычной деятельности человека. Наряду с крупными IT компаниями, владеющими монополией внедрения инновационных технологий в массы, возникают краудфандинговые сборы, которые ставят перед собой задачу внедрения доступного оборудования для технологий VR, а также адаптацию этого оборудования для повседневной жизни.

Одним из потенциальных направлений внедрения технологий искусственной реальности является правоохранительная сфера, в частности, Министерство внутренних дел Российской Федерации (МВД России). В современную эпоху подразумевается повсеместное развитие и совершенствование сотрудников МВД России, а также полноразмерное использование компетенций, приобретенных в процессе служебной деятельности. VR может предложить сотруднику обширный функционал, который способствует в эффективном совершенствовании различных сторон сотрудника и повышает результативность его служебной деятельности. Из-за этого МВД России занимается вопросом внедрения данных технологий в органы внутренних дел (ОВД) на территории всего государства. Технологии VR имеют ряд положительных качеств, которые способствуют внедрению в служебную деятельность сотрудников ОВД [1].

Основополагающее направление для использования гаджетов VR является обучение сотрудников, в том числе отработка навыков в форме активного обучения. Виртуальная реальность может предложить вариативные условия, приближенные к реалистичным или мало отличимых от них, для тренировки, которые способствуют повышению профессиональных качеств сотрудников. Данный тренинг позволяет погрузиться в различные сценарии и отработать действия по преодолению нештатных ситуаций. Легкая конфигурация сценариев предполагает отработку большинства ситуаций, с которыми сотрудник может столкнуться в ходе своей служебной деятельности. Наряду с этим использование

¹ © Андреев И. В., 2024.

ВР технологий позволит сократить расходы на профессиональную подготовку сотрудников, оптимизировать бюджет на расходные материалы и подготовку специальных тренировочных полигонов. В данный момент сотрудники тратят достаточно много времени на организационные мероприятия.

Помимо тренировочного аспекта использования ВР можно предположить вариант использования данной технологии для расследования преступления. При помощи 3D-моделирования криминалисты могут воссоздавать место происшествия, учитывая все особенности сохранения мелких деталей, которые могут быть важны для расследования преступления [2]. Данную 3D-модель можно легко передавать в различные подразделения, в которых сотрудники могут лично ознакомиться с местом происшествия и оставленными на нем доказательствами. На основании исследования виртуальных моделей сотрудник может реконструировать событие в полном размере, которое может дать след на предполагаемого правонарушителя. Тем самым технологии ВР могут повысить эффективность в расследовании преступлений, расширить базу доказательств, которые имеют значение для раскрытия лица, совершившего преступление, а также оптимизирует работу сотрудников ОВД, сокращением выездов на место преступления и проведением дополнительных проверочных мероприятий. Одна созданная 3D-модель может легко дать ответ на вопрос кто и как совершил правонарушение.

Технологии ВР получают опыт использования в психологической области. Посредством ВР оборудования можно создать различные условия, при помощи которых можно определить психологические проблемы. Так как виртуальная реальность обладает таким качеством как иммерсивность, технология полного или частичного погружения в виртуальный мир, данная характеристика может способствовать эффективному лечению психологических расстройств. Фобии и посттравматическое стрессовое расстройство можно будет лечить или сводить из влияние на человека к минимуму с помощью аппаратуры ВР, человека помещают в среду с травмирующими воспоминаниями или стрессовую обстановку, в которой ему надо преодолеть свои страхи и тем самым бороться со своими психологическими проблемами.

Однако для полноценного внедрения технологии ВР в МВД России существуют ряд проблем и вопросов, связанных с данной технологией. Стоимость оборудования достаточно высокая для повсеместного внедрения данной технологии во все структурные подразделения ОВД на территории Российской Федерации. Многие отделы не имеют достаточного финансового и материального обеспечения, поэтому проблема стандартизации и унификации стоит основной перед МВД России. Следующая проблема – техническая сложность использования ВР, для того чтобы эффективно пользоваться оборудованием виртуальной реальности ряд сотрудников должны обладать специфическими умениями и навыками, которыми надо владеть на обыденном уровне, т. е. без использование посторонней помощи. Также виртуальная реальность подвержена кибератакам и уязвимостям, которые выражаются в потенциальной утечке конфиденциальной информации и нарушении работоспособности смежных систем, которые используются в профессиональной деятельности сотрудников. К тому же надо учитывать политические особенности в нашей стране, так 18 января 2023 г. был

издан приказ Минцифры России № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации». Он предполагает переход на использование российского программного обеспечения [3, ст. 1]. А на данный момент все оборудование ВР комплектуется зарубежным программным обеспечением, что согласно действующему законодательству неприемлемо использование данных технологий в МВД России. Потенциальная разработка отечественного аналога может занять некоторое время и потребуются использования достаточных средств бюджета.

Внедрение виртуальной реальности в МВД России имеет большой потенциал для развития правоохранительной сферы нашего государства и повышения защиты граждан от преступных посягательств. Однако для полноценного внедрения данной технологии надо решить ряд вопросов, которые затрагивают различные аспекты: правовой, технический, финансовый. При организованном и системном внедрении технологии ВР в систему МВД России может стать ключевой особенностью для реформирования, улучшения работы сотрудников и выполнения всех поставленных задач.

Список литературы

1. В МВД предложили ввести регулирование виртуальной реальности // ТАСС. URL: <https://tass.ru/obschestvo/16387883>.
2. В Тюмени открылся первый в стране VR-полигон для обучения криминалистов // RBC. URL: <https://t.rbc.ru/tyumen/09/02/2024/65c5dc719a7947e10271b333>.
3. Приказ Минцифры России от 18 января 2023 № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации» // Информационно-правовой портал «Гарант». URL: <https://www.garant.ru>.

Апарцев М. А.¹,
генеральный директор ООО «НПП “Магма”»

ЦИФРОВОЙ МНОГОКАНАЛЬНЫЙ КОМПЛЕКС АВТОНОМНОЙ РЕГИСТРИРУЮЩЕЙ АППАРАТУРЫ «ХРОНОС». ТАКТИКО-ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ

Повышение автоматизации, информатизации и цифровизации деятельности министерств, ведомств и служб на сегодняшний день остается актуальной задачей.

Цифровой многоканальный комплекс автономной регистрирующей аппаратуры «Хронос» (далее – цифровой многоканальный магнитофон или ЦММ «Хронос») – цифровой комплекс автономной аппаратуры регистрации речевой (служебной) информации и автоматизированного оповещения, выполненный в виде однокорпусного аппаратно-программного модуля на базе специализированных кодеков и микроконтроллеров и сочетающий в себе бесфайловую последовательную структуру записи принимаемых и передаваемых речевых сообщений на жесткий диск (HDD) с возможностью удаленной компьютерной обработки информации и работы под управлением персонального компьютера (ПК) в составе локальных сетей.

Назначение ЦММ «Хронос»: регистрация в автономном режиме речевых сообщений, передаваемых и принимаемых по проводным и радиоканалам, используемым диспетчерскими, оперативными, специальными и техническими службами, а также юридическими и физическими лицами в составе корпоративных и бизнес-сетей.

Особенность, выгодно отличающая ЦММ «Хронос» от других существующих систем (средств) контроля и записи речевой информации – является комплексом автономной звукозаписывающей аппаратуры 6-го поколения (по иерархии соответствующих систем, средств и технологий), совмещающим преимущества автономных магнитофонов с бесфайловым способом записи информации на накопительный жесткий магнитный диск с достоинствами цифровых регистраторов на базе персонального компьютера с файловым интерфейсом пользователя.

Основные параметры:

- 1) непрерывная (24x7) запись речевых переговоров в цифровом формате по 1-4 (1-8, 1-16, 1-32) каналам – до 200 суток;
- 2) оповещение по 1-4 каналам одновременно (предварительная запись – до 10 сценариев);
- 3) возможность подключения электропитания от сети переменного тока – 220В, постоянного тока – 12В, 24В, 27В, 48В;
- 4) коэффициент сжатия при необходимом качестве разборчивости и узнаваемости речи – до 8;
- 5) наличие симметричного гальванически развязанного линейного входа;

¹ © Апарцев М. А., 2024.

- 6) возможность переноса записей без прерывания процесса регистрации;
- 7) быстрый поиск записи по признакам (дата, время, № абонента);
- 8) наличие АОН;
- 9) защита от НСД;
- 10) возможность одновременной записи и воспроизведения информации;
- 11) автоматическое выравнивание уровня усиления абонентов при записи;
- 12) автоматическое усиление удаленного абонента при воспроизведении;
- 13) автоматическое сохранение ранее записанной информации при полном отказе (отключении) электропитания;
- 14) возможность удаленного доступа и работы под управлением ПК;
- 15) автоматический контроль исправности линии и система диагностики неисправностей;
- 16) возможность индивидуальной настройки каждого канала под параметры различных линий связи;
- 17) возможность интеграции с различными системами и средствами получения (съема) речевой информации;
- 18) возможность настройки включения записи по состоянию (превышение порогового уровня звукового сигнала, снятие трубки, включение тангенты радиостанции, задействованный номер абонента, текущее время и т. д.).

Преимущества ЦММ «Хронос»:

- 1) высокая функциональность – за счет совмещения достоинств автономной аппаратуры с возможностями стандартных информационных технологий на базе компьютерных средств;
- 2) наращивание оперативных возможностей контроля – за счет увеличения количества контролируемых каналов путем реализации блочно-модульного принципа построения аппаратуры и использования алгоритмически и технологически завершенных компонентов и блоков;
- 3) компактность аппаратуры – за счет реализации однокорпусного конструктива (габариты 16-канального ЦММ – 367x250x54 мм);
- 4) высокая эксплуатационная надежность – за счет использования специализированных кодеков с лицензированным алгоритмом сжатия речи, высокопроизводительных микроконтроллеров, интуитивно понятного пользовательского интерфейса и применения бесфайлового принципа записи на HDD;
- 5) большое время непрерывной записи – за счет применения современных методов сжатия речи и индивидуальной настройки параметров включения записи;
- 6) многоуровневая защита от НСД – за счет разграничения прав доступа и использования специального программного обеспечения сохранности и неизменяемости записей.

ЦММ «Хронос» разработан и выпускается серийно. В различных вариантах канальности ЦММ «Хронос» хорошо зарекомендовал себя и активно используется в структурах МВД России, МЧС России, Следственного комитета Российской Федерации и ФСИН России, ряде хозяйствующих структур – РЖД, Метрополитене, Управлении воздушным движением. Современные образцы аппаратуры «Хронос» обеспечивают весь спектр задач по регистрации речевой информации и автоматизированному оповещению.

В интересах силовых, специальных и технических служб функционал ЦММ «Хронос», в совокупности с другими техническими системами и средствами, может быть использован для обеспечения выполнения следующих, в том числе, оперативно-технических задач:

- определения каналов утечки конфиденциальной информации в процессе анализа контрольных записей речевых сообщений;
- регистрации телефонных и радио-переговоров подконтрольных лиц и структур в процессе проведения оперативно-технических мероприятий;
- контроля обмена речевыми сообщениями и регистрации речевой информации в процессе осуществления повседневной деятельности;
- оповещения о текущей обстановке, изменении степени готовности подразделений к выполнению боевых и специальных задач, чрезвычайных происшествиях и т. п.;
- контроля доведения речевой информации (распоряжений, докладов и т. д.) и информационного обмена в процессе повседневной деятельности;
- обеспечения аудиозаписи в процессе контроля радиоэфира;
- анализа эффективности использования систем и средств связи, а также качества передаваемой/принимаемой информации;
- контроля телефонных (в том числе, через операторов сотовой связи) переговоров в интересах антикоррупционной и иной противоправной деятельности;
- регистрации аудиоинформации в процессе совещаний, обсуждений, прений и т. д.

По необходимости и при наличии согласованных тактико-технических требований ЦММ «Хронос» может быть доработан до возможности регистрации видеоинформации.

Батоев В. Б.¹,

старший научный сотрудник

НПО «Специальная техника и связь» МВД России,

кандидат юридических наук, доцент

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В условиях продолжающейся цифровизации общественных отношений и технологического совершенствования вопросов организации общественных процессов ситуация в сфере противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий (ИТТ) продолжает оставаться напряженной.

Изучение практики показывает о совершенствовании форм и методов совершения противоправных деяний с использованием ИТТ, продолжающейся тенденции сращивания традиционных форм организации преступной деятельности с киберпространством и современными технологиями.

В данной работе предлагается тезисно рассмотреть современное состояние преступности в сфере ИТТ.

Традиционно, как показывает изучение официальных статистических данных Главного информационно-аналитического центра МВД России, в 2023 г. наблюдался существенный рост числа зарегистрированных преступлений, совершенных с использованием ИТТ (табл. 1).

Таблица 1

**Сведения о преступлениях,
совершенных с использованием ИТТ в 2023 г.**

№ п/п	Федеральный округ	Количество зарегистрированных преступлений
1	ЦФО	159 866
2	СЗФО	75 619
3	СКФО	21 053
4	ЮФО	72 623
5	ПФО	147 442
6	УрФО	64 420
7	СФО	89 108
8	ДФО	38 995
<i>Всего</i>		<i>676 951</i>

По данным таблицы можно заключить, что самые большие показатели совершенных киберпреступлений приходятся на Центральный и Приволжский федеральные округа, которые в совокупности составляют практически половину всех зарегистрированных киберпреступлений.

¹ © Батоев В. Б., 2024.

О степени и масштабах угроз от киберпреступлений могут свидетельствовать размеры причиненного материального ущерба (табл. 2).

Таблица 2

**Сведения о материальном ущербе, причиненного в 2023 г.
в результате совершения киберпреступлений**

№ п/п	Федеральный округ	Сумма причиненного ущерба (в тыс. руб.)
1	ЦФО	61 016 150
2	СЗФО	20 632 653
3	СКФО	2 239 448
4	ЮФО	12 212 355
5	ПФО	23 402 811
6	УрФО	9 847 227
7	СФО	15 316 768
8	ДФО	8 731 164
<i>Всего</i>		<i>156 470 763</i>

Изучение данных статистики показывает, что размеры причиненного ущерба от совершения киберпреступлений также подверглись значительному росту, которые в совокупности составили практически более четверти (26,6 %) от суммы причиненного материального ущерба, причиненного в результате совершения всех преступлений в целом.

В видовом разрезе преступления, совершенные с использованием ИТТ можно представить следующим образом.

Основная масса киберпреступлений в 2023 г. была совершена транснациональными преступными группами в форме краж и мошенничеств (табл. 3).

Таблица 3

**Сведения о зарегистрированных кражах и мошенничествах,
совершенных с использованием ИТТ в 2023 г.**

№ п/п	Федеральный округ	Пункт «г» ч. 3 ст. 158 УК РФ	Статья 159 УК РФ
1	ЦФО	27 626	92 651
2	СЗФО	13 164	4 175
3	СКФО	2 766	10 704
4	ЮФО	10 806	40 671
5	ПФО	26 010	70 638
6	УрФО	9 922	28 639
7	СФО	18 211	45 593
8	ДФО	8 602	21 537
<i>Всего</i>		<i>117 442</i>	<i>353 201</i>

Изучение приведенных данных позволяет отметить, что по кражам, совершенным с использованием ИТТ лидирующие позиции занимают Центральный

и Приволжский федеральные округа. Фактически более половины и числа всех преступлений, совершенных с использованием ИТТ приходится на долю мошенничеств. Мошенническими действиями традиционно характерно их совершение организованным преступными группировками с территории Украины.

Таблица 4

Сведения о материальном ущербе, причиненного в 2023 г. в результате совершения краж и мошенничеств

№ п/п	Федеральный округ	Сумма причиненного ущерба (в тыс. руб.)	
		Пункт «г» ч. 3, ч. 4 ст. 158 УК РФ	Статья 159 УК РФ
1	ЦФО	3 016 916	49 803 415
2	СЗФО	1 178 440	19 355 819
3	СКФО	210 897	4 350 611
4	ЮФО	853 247	11 200 811
5	ПФО	2 417 737	20 603 853
6	УрФО	768 779	9 012 785
7	СФО	1 593 828	13 509 041
8	ДФО	941 229	7 683 332
<i>Всего</i>		<i>10 991 238</i>	<i>135 649 971</i>

Данные таблицы указывают на увеличение размера ущерба, причиненного в результате совершения киберпреступлений в 2023 г. В целом общий размер причиненного ущерба составил 156 470 763 тыс. руб., что фактически составляет более четверти (27 %) от общего размера материального ущерба, причиненного в результате совершения всех зарегистрированных преступлений.

В заключении отметим, что современное состояние противодействия преступлениям, совершаемым с использованием ИТТ можно охарактеризовать как достаточно напряженное со следующими наблюдаемыми тенденциями:

- транснациональный характер организации преступной деятельности;
- высокий уровень латентности преступности и виктимного поведения потерпевших;
- продолжающийся рост киберпреступлений в целом, краж и мошенничеств в частности;
- совершенствование форм и методов преступной деятельности на фоне постоянного развития и доступности инновационных ИТ-технологий.

Баторов Б. О.¹,

*главный эксперт-специалист отдела
внедрения инновационных технологий
и искусственного интеллекта
Управления информационных технологий
Департамента информационных технологий,
связи и защиты информации МВД России,
кандидат технических наук*

О НЕКОТОРЫХ ВОПРОСАХ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ МВД РОССИИ ДЛЯ АНАЛИЗА И ОБРАБОТКИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В АУДИО- И ВИДЕОМАТЕРИАЛАХ

В последние годы технологии искусственного интеллекта стали широко использоваться в различных сферах жизни, включая обработку и анализ аудио- и видеоматериалов. Особенно важную роль эти технологии играют в работе правоохранительных органов, таких как МВД России. Данная научная статья посвящена изучению актуальных вопросов применения искусственного интеллекта для работы с аудио- и видеоданными в деятельности МВД России.

В рамках исследования рассмотрены различные методы и подходы к автоматической обработке звукового и видео контента с применением современных алгоритмов искусственного интеллекта, таких как машинное обучение, нейронные сети и другие технологии. Приведены успешные примеры использования AI в анализе аудио- и видеоданных и представлены ретроспективные и перспективные взгляды на применение этих технологий в деятельности МВД России.

Приведенное исследование поможет получить полное представление о возможностях, преимуществах и вызовах, связанных с применением искусственного интеллекта для анализа информации в аудио- и видеоматериалах образующихся в ходе деятельности МВД России.

Существующие методы и подходы анализа и обработки звукового и видеоконтента

Сегодня действительно наблюдается рост интереса к автоматической обработке аудио- и видеоматериалов с использованием передовых технологий искусственного интеллекта, таких как машинное обучение и нейронные сети. Эти методы открывают новые горизонты для создания инновационных продуктов и сервисов в различных областях, включая в правоохранительную сферу [1, с. 371].

В настоящее время на рынке программного обеспечения наблюдается увеличение спроса на инновационные решения, которые используются для автоматической обработки звукового и видео контента с помощью искусственного интеллекта. Различные компании, занимающиеся разработкой программного обеспечения, стремятся внедрять передовые методы и технологии, чтобы улучшить процессы обработки данных и создать более удобные и интеллектуальные решения для своих клиентов.

¹ © Баторов Б. О., 2024.

Проведенный анализ показывает, что наиболее эффективное применение комплекса моделей для обработки видеофайлов направлено на решение нескольких ключевых задач: детекции языка речи, распознавания речи и ее транскрибация в текстовое сообщение, перевода текста, классификации объектов и распознавания лиц на видеофрагментах [3, с. 1516]. Например, для детекции языка речи широко используются модели, основанные на методах машинного обучения, включающие в себя комбинацию сверточных и остаточных блоков. Извлечение векторных представлений речи осуществляется с использованием статистического объединения, а соотнесение о принадлежности производится на основе косинусного расстояния между представлениями.

Для задачи распознавания речи и перевода текста исследование показало успешное применение комплекса моделей, включающих глубокие нейронные сети и статистические методы. Модели, такие как RCTM, RNNEncdec/Seq2Seq, Transformers-модель Whisper и другие, успешно используются для транскрибации и перевода речевой информации. Для выявления именованных сущностей в текстах применяется модель RuBERT.

В процессе классификации объектов на изображениях успешно используются модификации сверточных нейронных сетей (CNN) и архитектуры Transformer, обученные на распознавание заданных классов. Различные архитектуры, включая модификации MobileNet, позволяют эффективно классифицировать объекты на видеофрагментах.

Для распознавания лиц на видеофрагментах применяются модификации сверточных нейронных сетей (CNN), а также архитектуры Transformer, включая разнообразные модификации MobileNet. Другими популярными моделями для поиска лиц являются MTCNN (Многомасштабный каскадный сверточный нейронный сетевой метод), модель – BlazeFace, RetinaFace основанные на сверточной нейронной сети CNN и архитектуре ResNet50 соответственно.

Детекция объектов на изображениях прямоугольниками могут осуществляться в том числе (CNN) YOLO, а задачи классификации изображений с помощью моделей EfficientNet, в том числе в ансамбле с выше перечисленными моделями.

Перспективы применения технологий искусственного интеллекта для анализа и обработки звукового и видеоконтента в МВД России

В целях изучения передовых технологий, разработанных и представленных на рынке отечественного ПО Департаментом информационных технологий, связи и защиты информации МВД России в инфраструктуре ведомственного Центра обработки данных (на стенде Главного конструктора ИСОД МВД России) развернута Интеллектуальная модель анализа и обработки аудио- и видеоматериалов «Медиа-Портал».

Специально разработанная интеллектуальная модель предназначена для анализа и обработки содержащейся в аудио- и видеоресурсах информации, поступающей из различных источников, включая технические средства видеонаблюдения и мобильные видеорегистраторы. Ее функциональность опирается на передовые

методы искусственного интеллекта, в том числе применение глубоких нейронных сетей для выявления акустических сигналов в аудиовизуальных материалах и их последующего преобразования в текст [2, с. 28].

Неоспоримым преимуществом «Медиа-Портала» является дифференциация событий в видеопотоке согласно заранее определенным характеристикам, ассоциированным с временными таймингами. Обеспечивает эффективную идентификацию разнообразных ситуаций и происшествий, таких как: проверка документов, противодействие законным требованиям, фиксация административных правонарушений, алкогольное тестирование, задержание протестующих лиц, сценарии погонь на автопатруле, отслеживание коррупционных действий и прочее.

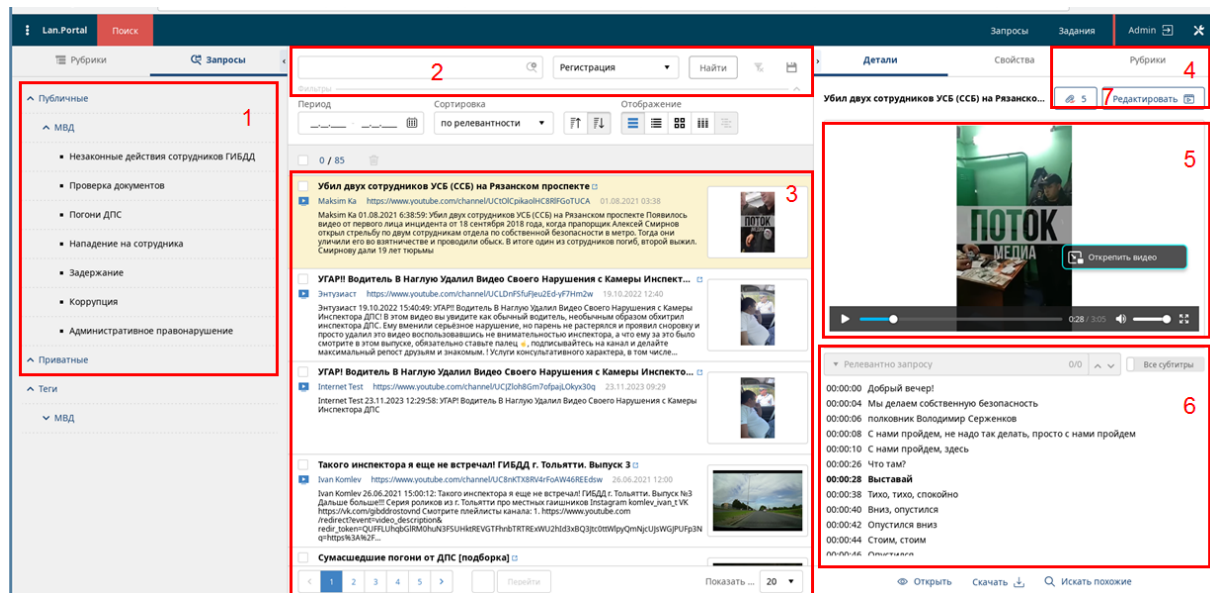


Рис. 1. Фрагмент рабочего интерфейса: 1 – классификация по маркерам (настраиваемый); 2 – фильтры создания маркеров; 3 – видеоматериалы; 4 – редактор медиа; 5 – видеопоток по тайм-кодам; 6 – транскрибированный текст по таймингу; 7 – медиа-редактор, распознавание лиц, оружия, военной техники и др. объектов на видео

Важно отметить, что «Медиа-Портал» обладает способностью к индивидуальной настройке классификационных фильтров без необходимости в программировании. Этот гибкий инструмент позволяет пользователям оперативно создавать необходимые категоризаторы.

С применением технологий искусственного интеллекта «Медиа-Портал» успешно решает задачи идентификации инцидентов на видеопотоке, включая распознавание оружия, лиц, военной техники, а также обнаружение правонарушений, таких как саботаж устройства записи, отклонения от заранее определенного маршрута патрулирования, массовые беспорядки и прочее.

Интеллектуальная модель анализа и обработки аудио- и видеоматериалов «Медиа-Портал» включает в себя следующие модули: загрузка видеоматериалов, обработка, распознавание аудио- и видеоданных, классификация и хранение данных (в базе данных).

Модуль хранения данных реализован в масштабируемой нереляционной (noSQL) базе данных Elasticsearch.

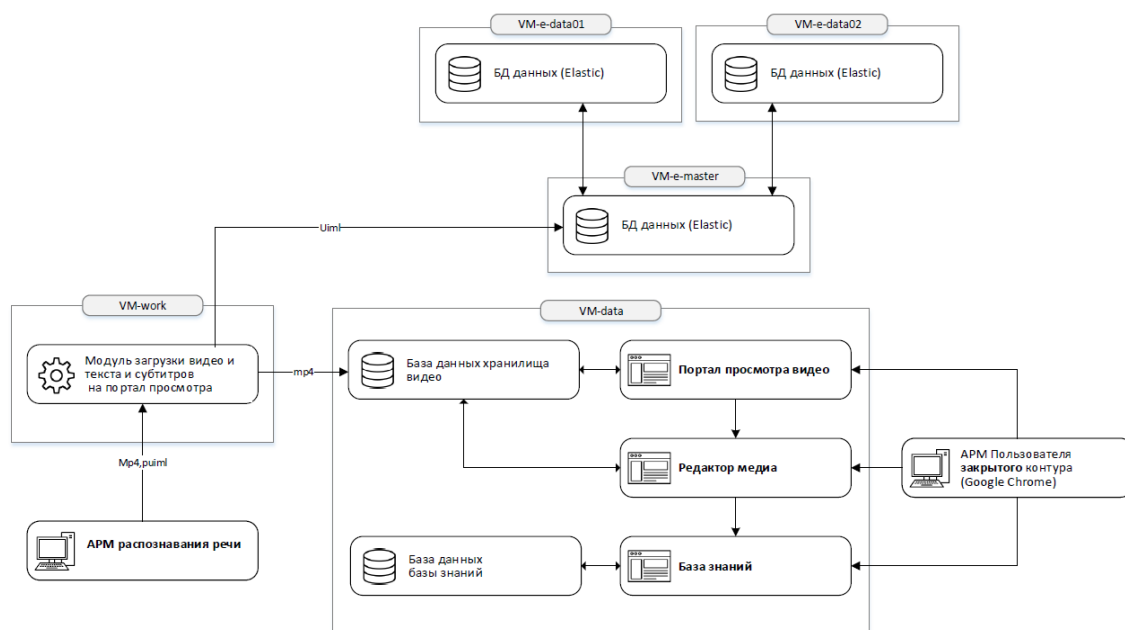


Рис. 2. Структурная схема интеллектуальной модели «Медиа-Портал»

Сценарий применения интеллектуальной модели анализа и обработки аудио- и видеоматериалов в подразделениях МВД России

Применение интеллектуальной модели для анализа и обработки аудио- и видеоматериалов образующиеся в деятельности МВД России может охватить механизмы контроля за исполнением служебных обязанностей сотрудниками, экипажами и нарядами многочисленных структурных подразделений, включая Патрульно-постовую службу, территориальные подразделения ИВС, Госавтоинспекцию, дорожно-патрульные наряды, регистрационные подразделения и подразделения, проводящие квалификационные экзамены по выдаче водительских удостоверений, службы технического надзора, отделы по пропаганде и связям с общественными организациями, а также дорожного надзора.

Кроме того, в соответствии с приказом МВД России от 28 июня 2021 г. № 49, принципы организации служебной деятельности строевых подразделений патрульно-постовой службы территориальных органов МВД России предусматривают системный контроль за организацией и исполнением служебных обязанностей нарядами ППС с использованием передовых технологических решений.

На практике для минимизации возможных нарушений и повышения эффективности работы предусмотрены оперативные расследования, основанные на анализе аудио- и видеоданных, полученных с использованием вышеупомянутых технических устройств, включая аудио- и видеорегистраторы. Проведение таких мер позволяет контролировать действия сотрудников и обеспечивать деятельность в рамках правового поля.

Для эффективного документирования различных юридических событий, включая противоправные действия, административные нарушения и происшествия, а также для контроля за действиями сотрудников, на патрульные автомобили устанавливаются специализированные устройства визуального и звукового

наблюдения. Данные системы записи, присутствующие как в салоне автомобиля так и в специальных отсеках для задержанных лиц, гарантируют объективное фиксирование происходящего и обеспечивают необходимый правовой анализ.

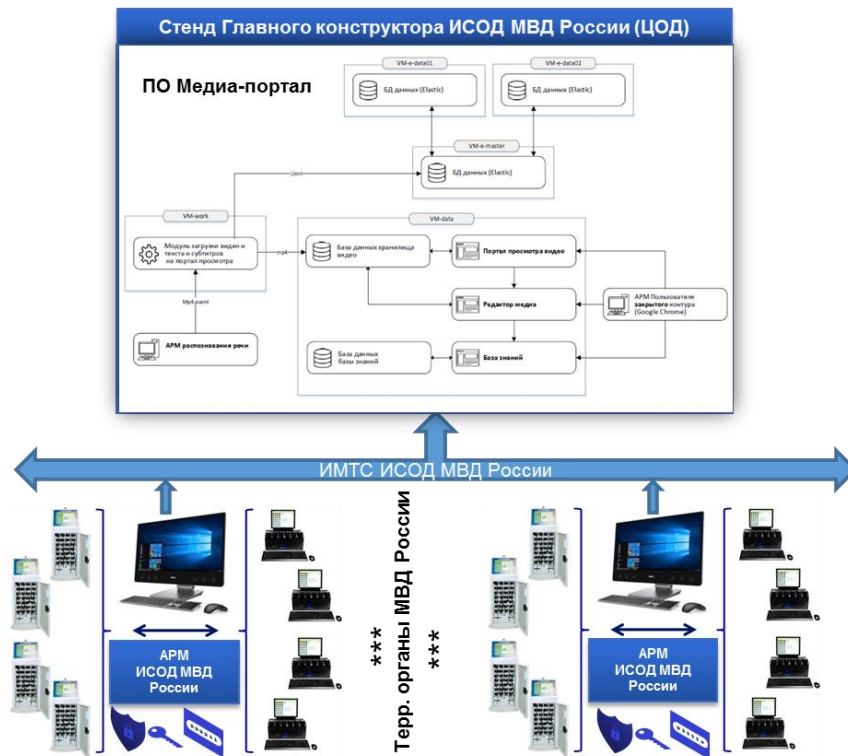


Рис. 3. Целевая схема организационно-технического сценария применения интеллектуальной модели анализа и обработки аудио- и видеоматериалов в МВД России

Внедрение технологий искусственного интеллекта в деятельность МВД России с целью анализа и обработки информации, содержащейся в аудио- и видеоматериалах представляет собой перспективное направление развития.

Для достижения данной цели, рекомендуется инициировать проведение научно-исследовательских и опытно-конструкторских работ с целью разработки прототипа программного комплекса способного осуществлять сбор, анализ, хранение и дальнейшее использование информации, получаемой из аудио- и видеоматериалов, собираемых с помощью технических средств видеонаблюдения, а также мобильных и переносимых комплексов видеорегистрации с применением методов искусственного интеллекта.

Автор предлагает следующие требования к научно-исследовательским работам по созданию интеллектуальной системы для нужд МВД России:

- разработка технологии и алгоритмов сбора аудио- и видеоматериалов с технических средств видеонаблюдения, а также мобильных и носимых комплексов видеорегистрации;
- разработка технологии и алгоритмов обработки и автоматического выявления типовых контрольных ситуаций на основе анализа результатов автоматического транскрибирования речи, получаемой с технических средств видеонаблюдения;

- разработка технологии и алгоритмов обработки и автоматического выявления типовых контрольных ситуаций на основе анализа содержания изображений видеоматериалов, получаемой с технических средств видеонаблюдения;
- разработка технологии и алгоритмов автоматической детекции и идентификации лиц видеоматериалов, получаемой с технических средств видеонаблюдения, с интеграцией с автоматизированной системой разыскиваемых лиц;
- разработка технологии и алгоритмов накопления, поиска и анализа записей видеоматериалов по месту, времени, субъекту формирования и ситуации в распределенной информационной системе;
- разработка технологии и алгоритмов визуализации местоположения видеорегистраторов на геоподоснове.
- разработка технологии и алгоритмов редактирования видеоматериалов в части создания сводных видеоматериалов из значимых фрагментов различных видеоматериалов;
- разработка технологии и алгоритмов автоматизированного формирования отчетов по результатам обработки и анализа видеоматериалов;
- разработка технологии и алгоритмов настройки правил анализа содержания видеоматериалов для выявления новых контрольных ситуаций с использованием правил на специальном языке или обучении на примерах;
- разработка программного комплекса экспериментального образца с применением готовых программных решений для обработки и анализа аудио- и видеоматериалов.

Список литературы

1. Осокин А. Г., Баторов Б. О. Использование больших данных в деятельности органов внутренних дел // Уголовная политика России на современном этапе: состояние, тенденции, перспективы : сборник научных трудов. М. : Академия управления МВД России, 2022. С. 369–374.
2. Баторов Б. О. Применение нейросети в интересах оценки эффективности социотехнических систем // Искусственный интеллект (большие данные) на службе полиции : сборник научных трудов. М. : Академия управления МВД России, 2020. С. 27–31.
3. Горошко И. В., Бондаренко Ю. В. Современные вызовы информатизации и правоохранительная деятельность // XIII Всероссийское совещание по проблемам управления ВСПУ-2019 : сборник трудов. М. : Институт проблем управления имени В.А. Трапезникова РАН, 2019. С. 1516–1519.

Богачева М. В.¹,
старший преподаватель кафедры
административно-правовых дисциплин
Белгородского юридического института
МВД России имени И.Д. Путилина

ОСУЩЕСТВЛЕНИЕ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МВД РОССИИ И МИНИСТЕРСТВ ВНУТРЕННИХ ДЕЛ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

МВД России в рамках своей информационной деятельности активно взаимодействует с министерствами внутренних дел других стран, а также с иными правоохранительными министерствами и ведомствами зарубежных государств. К основным направлениям взаимодействия относятся учет и регистрация преступлений, раскрытие актов терроризма и других особо тяжких преступлений, обмен информацией по поиску похищенных транспортных средств, распространению наркотиков, деятельности организованной преступности.

Наиболее тесное взаимодействие осуществляется между министерствами стран Содружества Независимых Государств (СНГ), поскольку до 1991 г. они входили в единую структуру МВД СССР. МВД России не только стал правопреемником союзного министерства, осуществляет ведение межгосударственного информационного банка (далее – МИБ), но и координирует взаимодействие коллег по многим направлениям деятельности.

3 августа 1992 г. в Киргизии, в городе Чолпон-Ата было заключено Соглашение МВД государств – участников СНГ [1], в соответствии с которым ГИАЦ МВД России не только формирует и ведет межгосударственный банк данных, но и предоставляет собираемую информацию по запросам правоохранительных органов Российской Федерации и стран СНГ. Осуществляется обмен информацией, накапливаемой в информационных базах и банках данных, архивах, а также в розыскных², справочных и криминалистических учетах.

Необходимо отметить существенный объем информации, предоставляемый в МИБ, который можно считать сопоставимым с объемом информации, предоставляемым региональными информационными центрами в ГИАЦ МВД России. Так, собирается информация о предметах ставших целью преступлений, украденных и изъятых вещах, нераскрытых преступлениях, а также о подучетных лицах. Собирается информация о большом количестве различных категорий лиц, к которым относятся осужденные лица, лица, освобожденные из мест лишения свободы, лица скрывающиеся от следствия или суда, иные разыскиваемые лица. Особое внимание уделено сбору информации о категориях преступников, несущих угрозу всем участникам СНГ. К ним относятся рецидивисты, лица, совершившие преступления с культурными ценностями, наркотиками или с особой

¹ © Богачева М. В., 2024.

² Здесь и далее написание слова *розыскной* приводится в соответствии с нормами русского языка, за исключением употребления в нормативных правовых актах.

жестокостью, гастролеры, лица, относящиеся к организованной преступности. Учитываются такие вещи, которые имеют некоторые отличительные особенности, номера и ценность. К ним относятся автомобили, электронные устройства, оружие, антиквариат, ценные бумаги.

Наибольшее внимание при учете нераскрытых преступлений уделено особо тяжким и тяжким преступлениям, преимущественно против личности: убийствам, похищениям людей, разбоям, половым преступлениям, вымогательствам и другим преступлениям совершенным с применением оружия и насилия. Вторым направлением особого внимания министерств внутренних дел стран СНГ являются крупные финансовые преступления, в том числе на бирже, подделка денег и ценных бумаг, фальшивомонетничество, хищения антиквариата и автотранспорта, незаконный оборот оружия и наркотических веществ.

Соглашение, подписанное в 1992 г. было модернизировано в 2009 г. в г. Астана 22 мая 2009 г. подписанием нового Соглашения об обмене информацией в сфере борьбы с преступностью [2]. Новым документом был существенно расширен перечень информации, которая предоставляется государствами-участниками в МИБ. Помимо вышеперечисленных подучетных лиц, информация стала собираться о лицах, занимающихся возбуждением межконфессиональной и межнациональной вражды, а также участвующих в деятельности террористических организаций, членов экстремистских сообществ. Также в Банк предоставляется информация о лицах, совершивших преступления в сфере миграции, экономические преступления, связанные с пересечением границ стран СНГ, в том числе контрабанда. Кроме того, добавилась информация о преступлениях, совершаемых в Интернет, в том числе легализации доходов, полученных преступным путем, распространении наркотиков, подделка ценных бумаг или средств платежа, распространение детской порнографии. Особое внимание в МИБ в настоящий момент уделяется экстремистским и террористическим нераскрытым преступлениям, выявлению и пресечению торговли людьми и органами человека.

Кроме накопления информации о преступности в межгосударственном информационном банке МВД стран СНГ осуществляют совместный поиск преступников. Для этого между ними подписан в г. Москве 10 декабря 2010 г. Договор о межгосударственном розыске лиц. В указанном Договоре участвуют уже не все государства СНГ, поскольку его не подписали Грузия, Украина и Туркмения [3]. Договор предполагает участие министерств в выявлении, задержании и последующей выдаче лиц, которые скрываются от уголовного преследования, отбывания наказания, следствия и суда в других странах. Для этого предполагается, что органы внутренних дел государств должны устанавливать места нахождения таких лиц и предоставлять информацию обо всех категориях разыскиваемых лиц. Отдельным направлением является установление личности неопознанных трупов, поиск без вести пропавших и иных устанавливаемых лиц.

В настоящий момент межгосударственный розыск осуществляется в соответствии с Регламентом, утвержденным Решением Совета глав правительств СНГ 30 октября 2015 г. в г. Душанбе [4]. Взаимодействие министерств по вопросам проведения межгосударственного розыска осуществляется на уровне регионов с помощью Бюро по координации борьбы с организованной преступностью

и иными опасными видами преступлений на территории государств – участников СНГ. Для осуществления поиска помимо МИБ могут создаваться специализированные информационные системы, использоваться базы и банки данных органов внутренних дел и других государственных и правоохранительных органов.

Объявление лиц в межгосударственный розыск осуществляется главными информационными центрами стран СНГ. При этом сбор данной информации, помещение ее в МИБ и дальнейший информационный обмен в электронном виде ведет ГИАЦ МВД России. В межгосударственном розыске лиц, на основании Указа Президента Российской Федерации от 13 июля 2016 г. № 332, участвует не только МВД России, но и все правоохранительные органы нашей страны [5].

По наиболее важным направления деятельности между министерствами государств – участников СНГ осуществляется более плотное сотрудничество. Оно регулируется отдельными соглашениями и договорами, а по отдельным направлениям созданы специализированные организации или координационные органы.

Для противодействия организованной преступности 24 сентября 1993 г. было создано Бюро по координации борьбы с организованной преступностью, которое действует на основании Положения [6]. Его работой руководит Совет министров внутренних дел государств, а одной из задач является информационно-аналитическое сотрудничество в указанной сфере.

Антитеррористическое сотрудничество является одним из основных направлений взаимодействия МВД государств и основано на Договоре о сотрудничестве государств – участников СНГ в борьбе с терроризмом, который подписан 4 июня 1999 г. в г. Минске [7]. Для осуществления информационного взаимодействия по вопросам борьбы с терроризмом, создан Антитеррористический центр государств – участников СНГ на основании Решения Совета глав государств СНГ [8]. Министерства внутренних дел принимают участие в противодействии терроризму, выявлении террористических ячеек, антитеррористической пропаганде вместе с органами безопасности стран СНГ.

Соглашение о сотрудничестве министерств внутренних дел (полиции) государств – участников СНГ в борьбе с торговлей людьми подписанное 17 сентября 2010 г. в г. Санкт-Петербурге предусматривает информационное сотрудничество органов внутренних дел, в том числе создание совместного банка данных о транснациональных преступных группах [9]. Данный банк данных содержит информацию не только о лицах, которые возможно причастны к торговле людьми, но и вероятных жертвах.

По вопросам противодействия налоговым и финансовым преступлениям 30 ноября 2000 г. создан Координационный совет руководителей органов налоговых (финансовых) расследований стран СНГ, действующий на основании Положения, утвержденного 31 мая 2013 г. решением Совета глав правительств СНГ [10]. Поскольку вопросы противодействия налоговым преступлениям после объединения ФСКН России с МВД России, относятся к компетенции полиции, то информационное взаимодействие в сфере финансовых преступлений осуществляется не только ФНС России и Росфинмониторингом, но и МВД России.

По вопросам противодействия преступлениям с использованием информационно-телекоммуникационных технологий осуществляется информационное взаимодействие на основании Соглашения о сотрудничестве стран СНГ в борьбе с преступлениями в сфере информационных технологий, принятого 28 сентября 2018 г. в г. Душанбе [11]. В частности осуществляется обмен информацией о совершенных и готовящихся преступлениях в ИТ-сфере, способах их совершения, и лицах их совершивших. Также осуществляется информационный обмен программными продуктами и решениями, применяемыми для противодействия преступности в ИТ-сфере, исполнение запросов о помощи в противодействии деятельности хакерских группировок.

Кроме вышеперечисленных отдельно выделенных направлений, осуществляется информационное взаимодействие в сферах обучения сотрудников, их пенсионного и социального обеспечения, обмена информации о мигрантах, обмена статистической информацией, сведениями о судимости и др.

Поводя итог рассмотрению информационного взаимодействия МВД России и МВД стран СНГ можно констатировать, что оно осуществляется очень активно по многим направлениям деятельности. Основным из них является формирование и ведение межгосударственного информационного банка в котором сосредоточена информация о лицах, совершивших преступления, нераскрытых преступлениях, предметах преступного посягательства и иных вещах. Наибольшее внимание в настоящее время уделяется преступлениям в ИТ-сфере, террористическим и экстремистским посягательствам, противодействию организованной преступности и торговле наркотиками. Отдельным направлением является выявление финансовых и налоговых преступлений, противодействие легализации преступных доходов.

Для информационного взаимодействия используются структуры Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории стран СНГ, Антитеррористический центр стран СНГ, Координационный совет руководителей органов налоговых (финансовых) расследований стран СНГ и другие координационные и совещательные органы. Для информационного взаимодействия по линиям противодействия торговле людьми и органами, преступлениям в ИТ-сфере и другим направлениям приняты дополнительные соглашения.

При этом основная часть информационного взаимодействия осуществляется в электронном виде через МИБ, который формируется и ведется ГИАЦ МВД России, что определяет особое координирующее положение МВД России среди министерств стран СНГ. Все вышеперечисленные Соглашения указывают, что массив централизованных учетов, статистической и архивной информации сосредоточивается в МИБ, который также является основой для межгосударственного поиска лиц. С 2018 г. лицо, поданное в федеральный розыск на территории России по преступлениям средней тяжести, тяжким и особо тяжким преступлениям автоматически подается в межгосударственный розыск на территории стран СНГ. Таким образом, именно МВД России осуществляет организацию розыска лиц, скрывающихся от органов дознания, следствия и суда на всей территории СНГ.

Список литературы

1. Соглашение о взаимоотношениях министерств внутренних дел в сфере обмена информацией (вместе с «Перечнем информации, предоставляемой в межгосударственный информационный банк») : заключено в г. Чолпон-Ате 3 августа 1992 г. // Правовые основы деятельности системы МВД России. М. : Инфра-М, 1996.
2. Соглашение об обмене информацией в сфере борьбы с преступностью (вместе с «Перечнем информации, предоставляемой в Межгосударственный информационный банк») : заключено в г. Астане 22 мая 2009 г. // Бюллетень международных договоров. 2011. № 1. С. 8–13.
3. Договор государств – участников Содружества Независимых Государств о межгосударственном розыске лиц : подписан в г. Москве 10 декабря 2010 г. // Собрание законодательства Российской Федерации. 2016. № 39. Ст. 5619.
4. Решение Совета глав правительств Содружества Независимых Государств «О Регламенте компетентных органов по осуществлению межгосударственного розыска лиц» : принято в г. Душанбе 30 октября 2015 г. // НПП «Гарант-сервис». URL: <https://base.garant.ru/71569602/>.
5. Указ Президента Российской Федерации от 13 июля 2016 г. № 332 «О компетентных органах Российской Федерации, осуществляющих сотрудничество в рамках Договора государств – участников Содружества Независимых Государств о межгосударственном розыске лиц» // Собрание законодательства Российской Федерации. 2016. № 29. Ст. 4798.
6. Решение Совета глав правительств Содружества Независимых Государств «О внесении изменений в Положение о Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников Содружества Независимых Государств» : принято в г. Казани 26 мая 2017 г. // Единый реестр правовых актов и других документов Содружества Независимых Государств. URL: <http://cis.minsk.by/>.
7. Решение Совета глав государств Содружества Независимых Государств «О создании Антитеррористического центра государств – участников Содружества Независимых Государств (вместе с “Положением об Антитеррористическом центре...”» : принято в г. Москве 21 июня 2000 г. // Содружество. Информационный вестник Совета глав государств и Совета глав правительств Содружества Независимых Государств. № 2 (35). С. 128–130.
8. Договор о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с терроризмом : подписан в г. Минске 4 июня 1999 г. // Собрание законодательства Российской Федерации. 2006. № 22. Ст. 2291.
9. Соглашение о сотрудничестве министерств внутренних дел (полиции) государств – участников Содружества Независимых Государств в борьбе с торговлей людьми (вместе с «Перечнем центральных подразделений...») : заключено в г. Санкт-Петербурге 17 сентября 2010 г. / Документ вступил в силу для России 9 марта 2011 г. // МИД России. URL: <http://www.mid.ru>.
10. Решение Совета глав правительств Содружества Независимых Государств «Об утверждении новой редакции Положения о Координационном совете

руководителей органов налоговых (финансовых) расследований государств – участников Содружества Независимых Государств» : принято в г. Минске 31 мая 2013 г. // НПП«Гарант-сервис». URL: <https://base.garant.ru/>.

11. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий : заключено в г. Душанбе 28 сентября 2018 г. // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>.

Брысин Н. Н.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*

АУТЕНТИФИКАЦИЯ ФИЗИЧЕСКИХ ЛИЦ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ДОСТУПЕ К ИНФОРМАЦИОННЫМ СИСТЕМАМ

Биометрия (биометрическое распознавание) – это процесс измерения и анализа уникальных физических и поведенческих характеристик людей. Она применяется для проверки и подтверждения личности человека. Основная идея заключается в том, что каждый человек может быть точно идентифицирован на основе его уникальных физических или поведенческих особенностей. Биометрическая информация, такая как отпечатки пальцев, голос, лицо или сетчатка глаза, используется для создания уникального идентификатора, который невозможно подделать или скопировать. Это позволяет обеспечить высокую степень безопасности и точности в процессе проверки личности человека. Биометрия находит применение в различных отраслях, включая государственные учреждения [1], финансовые организации, объекты транспорта и многие другие. В настоящее время эта технология продолжает активно развиваться и совершенствоваться, предлагая все более надежные и эффективные методы идентификации личности.

Биометрическая аутентификация – это метод аутентификации, основанный на распознавании уникальных биологических характеристик человека. Эти характеристики используются для проверки, является ли пользователь действительно тем, кем он себя представляет. Для этого биометрические данные человека сохраняются в базе данных в качестве эталонов. При биометрической аутентификации предъявляемые пользователем биометрические характеристики сравниваются с данными, хранящимися в базе. Если данные совпадают, то аутентификация считается успешной. Такой подход обеспечивает высокую степень безопасности и исключает возможность подделки или мошенничества.

Биометрия часто используется в качестве второго фактора аутентификации в различных областях.

Банки используют отпечатки пальцев или изображение лица, для проведения безопасных транзакций.

¹ © Брысин Н. Н., 2024.

В мобильных устройствах биометрия широко применяется в качестве дополнительной защиты и быстрого доступа к данным.

Биометрическая аутентификация уже давно используется в системах контроля и управления доступом.

Учитывая, что в МВД России эксплуатируется множество информационных систем, обрабатывающих довольно «чувствительную» информацию, доступ к которой ограничен федеральными законами, использование биометрии в качестве второго фактора аутентификации при доступе к данным, могло бы повысить уровень защищенности обрабатываемой информации и предотвратить несанкционированный доступ к ней.

Ниже рассмотрим различные технологии [2], которые могут быть использованы для организации двухфакторной аутентификации при доступе к информационным системам:

1. Распознавание по лицу.

Данная технология позволяет установить и подтвердить личность человека по его лицу. Система распознавания лиц может быть описана как процесс сопоставления лиц, попавших в объектив камеры, с базой данных ранее сохраненных и идентифицированных изображений лиц-эталонов. Однако, несмотря на все преимущества, использование биометрии по лицу имеет свои ограничения, например, системы распознавания лиц могут быть обмануты с помощью фотографий или масок, которые могут созданы с помощью различных программ.

2. Распознавание по голосу.

Данная технология позволяет идентифицировать человека на основе уникальных характеристик голоса, таких как тембр, высота тона, интонация, акцент. Одним из первых кто начал использовать «голос», как дополнительную аутентификацию, стал голландский банк ING. Была реализована возможность осуществлять мобильные платежи, с помощью активации голосом. Данное решение помогло упростить и обезопасить совершение платежей, через мобильные устройства. Но данная технология не является абсолютно точной, так как голос человека может изменяться.

3. Распознавание по отпечатку пальца.

Суть данного метода заключается в сканировании уникальных папиллярных узоров, которые присутствуют у каждого человека. Путем анализа определенных точек и рисунков на пальце создается уникальная модель. Основные преимущества использования аутентификации по отпечаткам пальцев включает простату в использовании, высокую скорость процесса аутентификации и надежность. Биометрические системы, использующие сканирование отпечатка пальца, легко подстраиваются под человека, например эти системы позволяют различить отпечатки пальцев при старении кожи или порезов.

Использование биометрии в качестве второго (дополнительного) фактора аутентификации при предоставлении доступа к банкам данных значительно снижает вероятность неправомерного доступа к информации. Биометрические данные неотчуждаемы. Их невозможно потерять (как например токен) или забыть (пароль). Биометрическая аутентификация является не только надежным, но

и удобным для пользователей способом доступа к данным, наши индивидуальные характеристики «всегда с собой». Учитывая огромный опыт МВД России в работе с дактилоскопической информацией, относительную простоту построения математических моделей отпечатков пальцев, а также распространенность технологии дактилоскопических сканеров использование отпечатка пальца в качестве второго фактора при предоставлении доступа к информационным системам ведомства видится наиболее перспективным направлением для дальнейшей проработки и внедрения. В свою очередь выбор конкретной из вышеперечисленных технологии для организации доступа должен определяться совокупной стоимостью.

Список литературы

1. Постановление Правительства Российской Федерации от 31 мая 2023 г. № 883 «Об утверждении Положения о единой биометрической системе, в том числе о ее региональных сегментах, и о признании утратившим силу постановления Правительства Российской Федерации от 16 июня 2022 г. N 1089» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_80481/.
2. Биометрическая аутентификация // Solar. URL: <https://rt-solar.ru/events/blog/3616/?ysclid=lvaxkmj682569904450>.

Бурмистров Е. С.¹,

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

Захаров Д. С.²,

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

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ЖИЗНИ ЮРИСТА

Мы находимся во время активного развития информационных технологий. У всех на слуху понятие «искусственный интеллект» (ИИ). Он стал надежным помощником во многих сферах нашей жизни: на работе, образовании и даже в быту.

ИИ имеет множество определений, его считают и наукой, систематизирующей знания по математике, кибернетике, психологии, биологии, физике. Со стороны технологического процесса ИИ – это способность компьютера «обучаться», он использует алгоритмы, анализирующие огромные объемы информации, и делает выводы, позволяющие принимать решения или предсказывать события. Иными словами, делать все то, чем занимается человек при работе с информацией.

Данная отрасль компьютерной техники развивается огромными темпами. Можно с уверенностью сказать, что XXI в. стал временем информационных технологий и в обозримом будущем машины смогут решать за человека многие задачи.

Компания «Гарант» представляет сервис Legal Tech – автоматизация правовых задач. Применение высоких технологий в модернизации и автоматизации текущих бизнес-процессов. Сервис позволяет каждому специалисту воспользоваться индивидуальным набором, который интегрирован в систему «Гарант».

Аналитическая система «Сутяжник» – упрощает подготовку к судебному процессу, сокращает время поиска нужной информации. Самообучаемый ИИ занимается систематизацией и подбором судебной практики, анализирует правовые нормы. Необходимо описать правовую ситуацию в поисковом окне и программа все сделает за вас [1].

«Гарант Коннект» – позволяет готовить юридические документы в современном виде со ссылками на действующие правовые нормы, а также поддерживать в актуальном виде документы, используемые в компании и на сайте. Сервис автоматизирует функции по использованию нормативных актов и подготовке текстов. Применяя возможности системы «Гарант» по поиску и обновлению документов в своем программном обеспечении, сервис следит за применением только

¹ © Бурмистров Е. С., 2024.

² © Захаров Д. С., 2024.

актуальных правовых норм на сайтах компании или на внутреннем ПО. Сервис справляется с расстановкой ссылок на законодательство в загруженном тексте.

Конструктор правовых документов – автоматизирует процесс заполнения документов быстро и правильно, сохраняя шаблоны для дальнейшего их использования. Сервис позволяет создавать юридически грамотные формы документов. Встроенная память позволяет запоминать все с чем работал сотрудник. С помощью всплывающих подсказок система объясняет, как заполнить форму, подсчитывает все, что нужно, используя калькуляторы, и решает проблемы с форматированием.

«Гарант диск» – приводит к единообразию и каталогизирует все внутренние документы компании, а также открывает к ним доступ для всех сотрудников. Сервис создает облачную базу внутренних корпоративных документов, доступных сотрудникам организации, что позволяет существенно упростить работу. Служащий в свободном доступе может найти и скачать нужные ему файлы, например, форму работы с клиентами или заявление на отпуск [2].

«Экспресс согласование» – сокращает время согласования документов между подразделениями, делает процесс более понятным и контролируемым. Система автоматизирует визирование документов, создавая маршрут движения файла с нужной информацией между отделами организации, позволяет обмениваться замечаниями и вносить правки, а также возвращать для доработки. Сервис дает возможность отследить на какой стадии идет согласование [3].

«Экспресс проверка контрагентов» – минимизирует риски при заключении договоров с новыми контрагентами, быстро выдает всю информацию. Имея только реквизит организации, сотрудник получает полный набор связанной с ним доступной информации – сведения о структуре и связях, бухгалтерских отчетах, выданных отчетах, арбитражной практике, вхождении в специальные списки, исполнительных производствах и многое другое [4].

Высокотехнологичный сервисы – это недалекая перспектива, заоблачные цены или самый сложный процесс внедрения и обучения. Это реальные инструменты, которыми любой желающий может воспользоваться уже сегодня. Автоматизация большинства процессов в работе – это современный взгляд на ведение бизнеса, экономия времени и средств организации.

Список литературы

1. Аналитическая система «Сутяжник». URL: <https://sutyazhnik.ru>.
2. Гарант диск. URL <https://lt.garant.ru/gar-disk>.
3. Экспресс согласование. URL: <https://visa.gardoc.ru/user/sign-in>.
4. Экспресс проверка. URL: https://www.garantexpress.ru/services/express_check/.

Васильева Д. В.¹,

*курсант Института-факультета подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

*Научный руководитель: **Страхов А. А.**,
доцент кафедры информатики и математики
Московского университета
МВД России имени В.Я. Кикотя*

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК НОВЫЙ ТИП КРИМИНАЛЬНОГО МЫШЛЕНИЯ

Мир не стоит на месте, человечество постоянно развивается и эволюционирует. По мере развития общества расширяется сфера человеческих потребностей. Для удовлетворения растущих потребностей во всех отраслях жизнедеятельности необходимо непрерывно внедрять новые технологии, создавать «умные» машины. Согласно данным аналитиков, одним из главных трендов IT-индустрии на данный момент является совокупность информационных технологий под общим названием искусственный интеллект (ИИ).

Современный ИИ, благодаря продвинутым алгоритмам машинного обучения на основе нейронных сетей, обретает всю большую степень автономии. Все чаще на разумных электронных помощников возлагается самостоятельное решение сложнейших и объемных задач, а также принятие ответственных решений в условиях минимальной определенности и ограничения по времени.

Идея создания машинного мышления возникла довольно давно, но сам термин «искусственный интеллект» возник с появлением цифровых программируемых вычислительных машин. Впервые его употребил американский специалист в области компьютерных технологий и когнитивистики Джон Маккарти в 1956 г. на научном семинаре в Дартмутском колледже.

Современный межгосударственный стандарт в области информационных технологий (ГОСТ 33707–2016, ISO/IEC 2382:2015) определяет ИИ (англ. AI – Artificial Intelligence) как «способность функционального блока выполнять функции, обычно ассоциирующиеся с интеллектом человека такие, как, например, рассуждения и обучение».

ИИ представляет собой технологию, способную изменить мир и может влиять на все аспекты нашей жизни. Умные машины способны логически мыслить и уже сейчас решают многие задачи не хуже большинства людей. Интеллектуальные киберсистемы применяются в медицине, экономике, военной и транспортной сфере, логистике, промышленности, торговле, образовании и т. п. По мнению профессора Макса Тегмарка, ИИ в совокупности с человеческим интеллектом может помочь цивилизации перейти на более высокий уровень технологического развития.

¹ © Васильева Д. В., 2024.

Однако наряду со множеством преимуществ повсеместное внедрение ИИ несет определенные риски и в ряде случаев порождает серьезные проблемы. Это связано с тем, что когнитивный потенциал ИИ не ограничивается безусловным решением полезных обществу задач. Билл Гейтс, Илон Маск, Стив Возняк и множество других лидеров IT-индустрии обеспокоены возможностями стихийного развития ИИ и расширения сферы его автономного применения.

С другой стороны, цифровизация повседневной жизни стимулирует рост высокотехнологичной киберпреступности. С развитием систем ИИ также увеличивается количество попыток использовать эти информационные технологии для противоправной деятельности. Киберсистемы, наделенные ИИ, предоставляют для криминальной среды новые, ранее недостижимые возможности.

С каждым годом статистика совершения преступлений с использованием ИИ возрастает, что приводит к беспокойству правоохранительных органов. Действующие меры профилактики и пресечения киберпреступлений не всегда соответствуют способам совершения этих деяний.

В исследовании, недавно опубликованном Центром Дауэса по борьбе с преступностью будущего при Калифорнийском университете, определены следующие направления криминального ИИ:

1) очень серьезные угрозы безопасности:

- высококачественные аудио- видеоподделки (для мошенничества, вымогательства, нанесения ущерба репутации или нарушения безопасности);
- беспилотный транспорт как оружие;
- целенаправленный фишинг (эксплуатация доверительных отношений с использованием очень личных данных);
- нарушение работоспособности Интернета вещей и промышленных систем управления (продовольственная логистика, коммунальные услуги, управление дорожным движением);
- широкомасштабный шантаж (создание и распространение порочащих фактов во многих источниках);
- фейковые новости (либо основанные на реальных событиях, либо полностью сфабрикованные);

2) угрозы безопасности среднего уровня:

- нецелевое применение боевых роботов;
- ненадежное шифрование (snake oil или «змеиное масло» – мошеннические услуги под видом машинного обучения);
- искажение обучающих наборов данных (data poisoning или «отравление данных» для неправильного машинного обучения);
- умные кибератаки (атаки с использованием больших данных и машинного обучения);
- управление ударными дронами (по отдельности или группами, с блокировкой человеческого контроля);
- онлайн-выселение (блокирование онлайн доступа к информационным ресурсам, например, банковским счетам, кредитным картам, коммунальным платежам);

- обман систем распознавания лиц (либо для того, чтобы избежать обнаружения, либо для поражения систем безопасности);
- рыночная бомбардировка (манипулирование финансовыми или фондовыми рынками);

3) угрозы безопасности низкого уровня:

- боты-взломщики (небольшие автономные роботы, доставляемые в помещения через небольшие точки доступа для получения ключей или открытия дверей для грабителей);
- манипулирование общественным мнением (поддельный контент, онлайн-рейтинги, аналитические обзоры или массовый размещение негативных комментариев);
- скрытие цифровых следов (методы предотвращения обнаружения доказательств незаконной деятельности);
- наблюдение за жертвой (отслеживание сообщений, действий, связей, перемещений методами интернет-разведки по открытым источникам OSINT);
- подделка ценных цифровых активов (музыкальных или художественных произведений).

Данная классификация группирует угрозы безопасности по следующим критериям (в порядке убывания значимости):

- степень ущерба, государству, обществу, личности;
- потенциальная преступная выгода;
- насколько легко преступление может быть совершено;
- насколько трудно будет нейтрализовать преступление.

В заключении следует отметить, что цифровой ИИ – это не друг, и не враг, а программные коды, стремящиеся к самосовершенству. Это инструмент, способный эффективно решать поставленные задачи с учетом приобретаемого опыта, имеющий собственное мнение, но при этом не ограниченный человеческой духовностью. В ИИ нет эмоций, совести, преступных пороков, он не создает заведомо вредоносные сценарии. Машина стремится решать поставленные задачи как можно лучше, но без контроля со стороны законопослушного человека ее оставлять нельзя.

Список литературы

1. ГОСТ 33707–2016 (ISO/IEC 2382:2015). Межгосударственный стандарт. Информационные технологии : словарь : введен в действие Приказом Росстандарта от 22 сентября 2016 г. № 1189-ст.
2. Страхов А. А., Прокопенко А. Н. Криминальный потенциал искусственного интеллекта // Проблемы информационного обеспечения деятельности правоохранительных органов : сборник статей. Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. С. 164–172.
3. Страхов А. А., Прокопенко А. Н. Эволюция искусственного интеллекта и его место в современном информационном обществе // Проблемы информационного обеспечения деятельности правоохранительных органов : сборник статей. Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2021. С. 161–182.

Васильчикова А. А.¹,

*курсант факультета подготовки специалистов
в области информационной безопасности
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*

КАНАЛЫ УПРАВЛЕНИЯ БЕСПИЛОТНЫМИ ЛЕТАТЕЛЬНЫМИ АППАРАТАМИ

Настоящее время можно справедливо охарактеризовать стремительным развитием технологий беспилотных летательных аппаратов (БПЛА), которые проникают в различные сферы жизнедеятельности человека. Как и другие технологии, БПЛА в первую очередь нашли свое применение в военной сфере, однако с уменьшением стоимости комплектующих, а также появлением инноваций в области летательных аппаратов, БПЛА стали также доступны для применения в гражданских и коммерческих целях, например для транспортировки грузов, в спасательных и поисковых операциях. С увеличением разнообразия беспилотных систем становится все более актуальным изучение каналов связи и систем навигации, которые обеспечивают эффективное функционирование и управление этими аппаратами.

Управление беспилотными системами может осуществляться как в ручном режиме, когда оператор при помощи пульта управления отправляет команды на БПЛА, так и в автономном режиме с использованием навигационных систем. Независимо от режима управления любое устройство должно обладать каналом передачи данных телеметрии, при ручном управлении выделяется дополнительный канал управления, который обеспечивает передачу команд от оператора к БПЛА.

Можно выделить следующие виды связи, используемые в каналах управления БПЛА:

Конвенциональная радиосвязь. Наиболее распространенный канал управления позволяет оператору управлять БПЛА на относительно небольших расстояниях, обеспечивая надежную и быструю передачу команд. Самая популярная частота, используемая современной аппаратурой радиоуправления – это 2,4 ГГц.

Спутниковая связь. Этот тип канала управления обычно используется для работы на больших расстояниях, а также в удаленных или труднодоступных районах, где может быть недоступна надежная наземная связь. Частоты работы спутникового канала управления могут различаться в зависимости от используемой

¹ © Васильчикова А. А., 2024.

спутниковой системы. Посредством технологий спутниковой связи также осуществляется передача эфемерид и сигналов точного времени систем глобального позиционирования.

Сотовая связь. В данном канале управление осуществляется через инфраструктуру мобильной связи, что может быть эффективно в городских или плотно населенных районах. На основании данных от элементов структуры сотовой связи также можно получить необходимую навигационную информацию. Это позволяет считать этот вид связи столь же эффективным, как и спутниковую связь, а с учетом значительно более низких технических показателей, еще и наиболее дешевым. При этом стоит понимать, что используемая структура сотовой связи представляет частную собственность, что может потребовать дополнительных действий по инициализации в системе с одной стороны, а с другой не гарантирует устойчивость связи в изменяющихся условиях оперативной обстановки.

Таким образом, существует значительное разнообразие доступных технологий управления и навигации БПЛА, каждая из которых имеет свои преимущества и применимость в различных условиях эксплуатации. Дальнейшее изучение и развитие этих методов может привести к улучшению эффективности, надежности и безопасности операций с беспилотными летательными аппаратами.

Список литературы

1. Бороздина В. Н., Плотников Г. Г. Сравнение систем конвенциональной и сотовой связи в решении задач правоохранительной системы // Информационные технологии в деятельности органов внутренних дел : сборник научных статей. М., 2021. С. 99–102.
2. Плотников Г. Г. О надежности систем передачи извещений // Информационные технологии в деятельности органов внутренних дел : сборник научных трудов. М., 2022. С. 297–299.

Власюк Н. А.¹,

студент института информационных наук

Московского государственного лингвистического университета

Толстых М. Ю.²,

*доцент кафедры международной информационной безопасности
института информационных наук*

Московского государственного лингвистического университета,

*доцент кафедры специальных информационных технологий
учебно-научного комплекса информационных технологий*

Московского университета

МВД России имени В.Я. Кикотя,

кандидат технических наук

РАЗРАБОТКА АДАПТИВНЫХ МЕР ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ НА БАЗЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Активное развитие искусственного интеллекта (ИИ) и его применение в различных сферах открывает новые возможности для улучшения систем безопасности и создания эффективных инструментов защиты информации (ЗИ) от актуальных угроз, в перечень которых входит спам.

В соответствии с Указом Президента Российской Федерации [1] и Национальным проектом [2] акцентируется внимание на разработке и внедрении передовых технологий, включая глубокое обучение и обработку естественного языка для повышения уровня информационной безопасности (ИБ). В данном контексте, разработка системы фильтрации спама, основанной на методах ИИ, является актуальной задачей. Подобные системы позволяют не только снижать риски ИБ, но и способствуют оптимизации процессов обработки данных, улучшают пользовательский опыт и эффективность коммуникаций.

Классификация сообщений на спам и не спам представляет собой основу для разработки и апробации алгоритмов, направленных на фильтрацию нежелательной информации. В процессе выполнения исследования по заявленной тематике были использованы различные методы предобработки текста, включая токенизацию и векторизацию, что позволило преобразовать текстовые данные в формат, пригодный для обучения нейронных сетей.

Разработанная модель машинного обучения основывается на принципах глубокого обучения и включает в себя несколько слоев обработки данных, что обеспечивает высокую точность классификации.

Архитектура нейронной сети и краткое описание модели приведены в графической (рис. 1) и табличной (табл.) форме соответственно.

¹ © Власюк Н. А., 2024.

² © Толстых М. Ю., 2024.

Модель была обучена на наборе данных, разделенном на обучающую и валидационную выборки, с последующей оценкой ее производительности по точности и потерям на обоих наборах данных. Результаты представлены графически (рис. 2).

Model: "sequential_1"

Layer (type)	Output Shape	Param #
embedding (Embedding)	(None, 309, 100)	2925800
conv1d (Conv1D)	(None, 305, 128)	64128
global_max_pooling1d (GlobalMaxPooling1D)	(None, 128)	0
dense (Dense)	(None, 64)	8256
dropout (Dropout)	(None, 64)	0
dense_1 (Dense)	(None, 1)	65

=====
 Total params: 2,998,249
 Trainable params: 2,998,249
 Non-trainable params: 0

Рис. 1. Архитектура нейронной сети

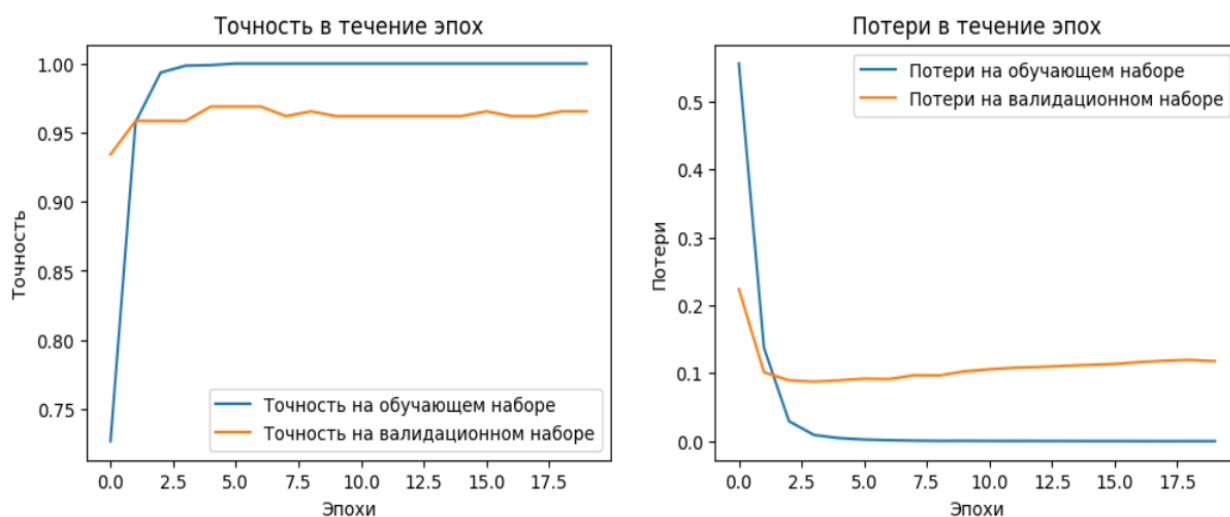


Рис. 2. График изменения точности и потерь во время обучения

Преимущество предложенного подхода заключается в его изначальной простоте и модульности, что делает модель легко адаптируемой к специфическим требованиям пользователей (потребителей/заказчиков в лице различных компаний и организаций). Благодаря этому, система может быть эффективно интегрирована в существующий информационный ландшафт для исключения нежелательного контента в автоматическом режиме, что существенно повысит качество обработки данных и обеспечит более высокий уровень ИБ.

Описание архитектуры модели

Слой	Особенности
Встраивающий слой (Embedding)	Преобразует индексированные слова в плотные векторы фиксированной размерности, облегчая модели выявление связей между словами
Сверточный слой (Conv1D)	Использует 128 фильтров с размером ядра 5 для выявления важных последовательностей слов в тексте, способствуя эффективному извлечению признаков
Слой глобального максимального объединения (GlobalMax Pooling1D)	Уменьшает размерность данных, выделяя наиболее значимые признаки из каждого сверточного фильтра, что способствует уменьшению риска переобучения
Полносвязный слой (Dense)	Состоит из 64 нейронов с функцией активации «relu», обеспечивает дальнейшую обработку выделенных признаков для формирования вывода модели
Слой исключения (Dropout)	С вероятностью 0,5 исключает часть нейронных связей на каждом шаге обучения, что помогает снизить риск переобучения за счет увеличения обобщающей способности модели
Выходной слой	Однонейронный слой с функцией активации «sigmoid», преобразует выходные данные модели в вероятность принадлежности сообщения к классу спам

В дальнейшем для улучшения результатов функционирования разработанной системы целесообразна фокусировка на последующем ее масштабировании и диверсификации обучающей выборки, а также на экспериментах с архитектурой нейронной сети и параметрами обучения, что позволит адаптировать систему под конкретные потребности пользователей и сделает ее еще более эффективной в борьбе с распространением спама и других угроз безопасности информации.

Список литературы

1. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (с изменениями и дополнениями) // НПП «Гарант-сервис». URL: <https://base.garant.ru/72838946/>.
2. Минцифры России: статья «В России появится новый нацпроект – «Экономика данных». URL: <https://digital.gov.ru/ru/events/45686/>.
3. Козин И. С., Рошин А. А. Метод обеспечения безопасности информации при ее обработке в информационной системе на основе машинного обучения // Техника средств связи. 2019. № 4 (148). С. 70–82.
4. Разработка методики внедрения машинного обучения для повышения информационной безопасности web-приложения / [М. М. Ковцур и др.] // Техника средств связи. 2020. № 4 (152). С. 74–86.

Гермогенова Е. С.¹,

*курсант Института-факультета подготовки сотрудников
для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель: Стащенко С. П.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ПРАВОВЫЕ АСПЕКТЫ ОПРЕДЕЛЕНИЯ ИМУЩЕСТВЕННОГО УЩЕРБА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Определение имущественного ущерба в рамках расследования преступлений в сфере компьютерной информации имеет свои особенности и требует учета различных правовых аспектов. Следует отметить, что преступления, предусмотренные гл. 28 Уголовного кодекса Российской Федерации (УК РФ), посягают в первую очередь на компьютерную информацию, то есть на сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. По своей сути, такая информация является собственностью гражданина, наравне с предметами материального мира, но все же обладает спецификой своего существования в виртуальном, эфемерном мире – в сети. Такую информацию нельзя потрогать, перенести или совершить иные действия с ней в реальном мире, поэтому компьютерную информацию можно поставить на одну ступень с интеллектуальной собственностью человека – результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации предпринимателей и юридических лиц, товаров, работ, услуг и предприятий, которые охраняются законом и чаще всего воспринимается как совокупность прав человека позволяющих распоряжаться этими нематериальными объектами, запрещать и разрешать их использование третьим лицам. Поэтому компьютерную информацию, по-моему, мнению можно воспринимать такой же точки зрения – как совокупность прав автора, создателя или правообладателя, которые позволяют выполнять те или иные действия с такой информацией. С другой стороны, так как компьютерная информация находится в нематериальном, материальном мире, то все имеющиеся сведения можно назвать виртуальным имуществом.

Так же, компьютерная информация представлена в разных видах. Ей могут являться самые простые текстовые документы, таблицы и наравне с тем программные обеспечения и различные кодированные разработки. Отсюда вытекает глав-

¹ © Гермогенова Е. С., 2024.

ная проблема – как оценивать такой вид информации, особенно при расследовании преступлений. По сути, сам по себе текстовый документ не имеет никакой ценности. Это просто набор электронных знаков, и, например, при хищении такого документа с компьютерного устройства, в первую очередь нарушаются права человека и гражданина на защищенность и конфиденциальность своей информации. Но с другой стороны важно содержание такого документа. Например, если документ содержит в себе информацию о банковских счетах человека, логины и пароли от личного кабинета банка, и в следствии хищения причиняется материальный ущерб путем списания денежных средств на таких счетах, то уже можно говорить об определенной оценке такой информации. В п. 2 примечания к ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» говорится о том, что крупным ущербом в статьях гл. 28 УК РФ признается ущерб, сумма которого превышает один миллион рублей. Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» не дает никаких пояснений к оценке причиненного ущерба преступлением в сфере компьютерной информации, однако, данный вопрос был освещен В. К. Барчуковым, который предложил под виртуальным имуществом предлагает понимать «совокупность объектов виртуального мира, имеющих реальное стоимостное выражение, которые находятся в собственности какого-либо лица, а также права имущественного характера на данное имущество». Необходимо отметить, что компьютерная информация, будучи объектом преступления, может быть подвергнута различным видам ущерба:

- уничтожение данных или искажение информации (преступник может удалить, исказить или повредить ценные данные, что может привести к потере информации и нанести значительный ущерб пострадавшей стороне. В таких случаях оценка ущерба может основываться на стоимости восстановления данных или на потерянной ценности информации);
- потеря доступа к системам (преступник может блокировать доступ к компьютерным системам или шифровать данные, требуя выкуп для их разблокировки. В этом случае ущерб может быть определен как сумма выкупа или затраты на восстановление доступа к системам);
- неправомерное использование информации (если преступник получает доступ к конфиденциальной информации и злоупотребляет ею, например, продавая ее третьим лицам или используя для совершения мошенничества, ущерб может быть определен как потеря прибыли, которую пострадавшая сторона могла бы получить от использования этой информац Оценка имущественного ущерба в расследовании преступлений в сфере компьютерной информации может быть сложной задачей, требующей участия специалистов по информационной безопасности и экспертов. Они проводят анализ систем, данных и последствий преступления для определения объема, и стоимости ущерба).

Таким образом, определение имущественного ущерба при расследовании преступлений в сфере компьютерной информации требует комплексного подхода, экспертных знаний и анализа последствий преступления для пострадавшей стороны.

На мой взгляд, не указание законодателем таких факторов, как стоимость восстановления или воспроизведения компьютерной информации, затраты на меры по защите и восстановлению системы, а также возможные потери, связанные с прекращением работы или утратой бизнес-возможностей в роли обязательного элемента рассмотрения при определении размера ущерба, является важным упущением, которое в дальнейшем только осложнит работу органов предварительного расследования и суда.

Список литературы

1. Еремченко В. И., Сафронкина О. В. Проблемные вопросы определения суммы материального ущерба и пути их решения при расследовании мошенничества в сфере компьютерной информации в области индустрии компьютерных игр // Общество и право. 2019. № 4. С. 70.
2. Попов А. Б. Проблемы квалификации преступлений в сфере компьютерной информации // Вестник ТГУ. 2008. № 10. С. 339–340.
3. Баркалова Е. В. К вопросу об определении вреда при расследовании преступлений против собственности // Криминалисть. 2013. № 1 (12). С. 67–71.
4. Федосеева Е. Л., Воропаев С. А., Кузнецов Р. Н. Особенности квалификации и расследования преступлений, связанных с причинением имущественного ущерба правообладателям и потребителям цифрового контента : учебно-методическое пособие . Екатеринбург : Уральский юридический институт МВД России, 2020. С. 50.
5. Алексеева Е. А. Состояние преступлений в сфере компьютерной информации: проблемы и перспективы // Национальные экосистемы : сборник научных трудов.

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*

О ФОРМИРОВАНИИ КОМПЛЕКСА МЕР ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Активное развитие экономики, технологий и информатизация многих сфер жизни привели к значительному изменению структуры преступности. Количество преступлений в сфере информационных технологий с 2019 по 2023 г. увеличилось более чем в два раза с 294 тыс. до 677 тыс. в 2023 г., а доля в общей структуре преступности увеличилась с 14 % до 34 %.

Основной массив зарегистрированных преступлений – «дистанционные» хищения, среди которых преобладают мошенничества.

Говоря о мерах по противодействию данной преступности, следует отметить, что они должны иметь комплексный характер.

В основе данных мер, будут профилактические мероприятия. На постоянной основе органами внутренних дел осуществляются информирование граждан о видах мошенничества, проводятся разъяснительные мероприятия по повышению финансовой грамотности населения, что усиливает готовность граждан к возможным противоправным действиям в отношении них и затрудняет достижение преступниками своих целей.

Также на официальном интернет-сайте МВД России создана рубрика «Профилактика мошенничества». В разделе «Новости» размещено несколько сотен информационных сообщения. В частности, о проведении профилактических акций: «Стоп мошенники», «Осторожно: мошенники», «Защитим наших родителей», «Пожилой человек», «Участок». В ходе систематических акций сотрудники полиции проводят разъяснительные беседы о том, как не стать жертвой мошенников.

На официальных страницах ведомства в социальных сетях в рубрике «Твоя безопасность» регулярно публикуются новостные и мультимедийные тематические материалы.

Тема финансовой грамотности населения систематически публикуется в СМИ. Опубликовано более пятидесяти тысяч публикаций на данную тематику.

На общедоступном официальном канале «Вестник киберполиции России» в мессенджере «Телеграм» ежедневно размещаются новостные и профилактические текстовые, фото- и видеоматериалы, в том числе предупреждающие граждан о самых новых способах мошенничества.

¹ © Гончар В. В., 2024.

Систематически подготавливаются и направляются информационные письма об организации взаимодействия по профилактике дистанционных хищений в Минцифры России, кредитно-финансовые учреждения (Банк ВТБ (ПАО), ПАО Сбербанк), Пенсионный фонд Российской Федерации, интернет-ресурс «Циан», Банк России, операторам связи (ПАО «Мегафон», ПАО «Вымпелком», ООО «Т2 Мобайл»), Министерство транспорта Российской Федерации, Министерство культуры Российской Федерации, а также в адрес СМИ (ИА «Интерфакс», АО «Аргументы и факты»).

Периодически проводятся рабочие встречи с представителями бизнес-сообщества.

Органами внутренних дел совместно с Минцифры России на портале «Госуслуги» создан раздел «Кибербезопасность – это просто», на котором размещена гиперссылка на электронную форму заявления о преступлении на официальном сайте МВД России. Оказано содействие в съемках документального сериала «Цифровая броня».

При информационной поддержке пресс-центра МВД России и Следственного департамента МВД России снят художественный фильм «Цифровой код», направленный на профилактику преступлений в сфере информационных технологий.

Сотрудниками Следственного департамента МВД России также принято участие в проведении различных форумов, на которых бизнес-сообществу рекомендовано решать задачи по предоставлению безопасных услуг и повышению цифровой грамотности населения. Необходимо научить клиента не только приобретать услуги и отдавать за это денежные средства, но и безопасно пользоваться сферой предоставления услуг и не терять свои деньги. А бизнесу, активно продвигающими свои услуги в онлайн и повышающими из-за этого прибыль необходимо обеспечить безопасность данных каналов передачи данных, в том числе от применения приемов социальной инженерии.

Комплекс профилактических мероприятий очень широк и проводится в основном для лиц из особых групп риска, а это школьники/студенты и лица пенсионного возраста. Начинаться профилактика преступлений совершенных с использованием ИТТ, должна именно со школьной скамьи, причем основные правила безопасного поведения должны быть заложены в программу предмета «Основы безопасности и защиты Родины», а с начальных классов эти темы необходимо обсуждать в уроки, посвященные разговорам о важном.

Следующим элементом формируемого комплекса являются мероприятия организационного характера. В 2022 г. в МВД России создано специализированное оперативное подразделение – Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий и его региональные подразделения.

В Следственном департаменте МВД России также создан и функционирует отдел по организации расследования дистанционных хищений, который тесно взаимодействует с оперативными подразделениями по борьбе с киберпреступ-

лениями, иными правоохранительными и федеральными органами государственной власти, что позволяет решать совместными усилиями многогранные задачи.

В Следственном комитете Российской Федерации создан и функционирует аналогичный отдел.

Следующим элементом формируемого комплекса следует признать необходимость изменения действующего законодательства.

Например, отсутствие уголовно-правового запрета на передачу третьим лицам электронных средств платежа позволяет злоумышленникам для вывода похищенных денежных средств использовать банковские карты, оформленные на различных граждан.

Хищение денежных средств граждан с использованием методов социальной инженерии, а далее перевод похищенных денежных средств осуществляется в короткий промежуток времени в связи с чем необходимо принимать незамедлительные меры к прекращению расходных операций по счетам, управление которыми осуществляют злоумышленники. В целях принятия своевременных мер к возмещению ущерба потерпевшим в МВД России подготовлена законодательная инициатива по внесению изменений в Уголовно-процессуальный кодекс Российской Федерации. Предлагается установить сроки исполнения операторами по переводу денежных средств, операторами связи запросов сотрудников правоохранительных органов, наделить следователя и дознавателя правом приостановления расходных операций с денежными средствами, электронными денежными средствами, авансовыми платежами по счетам, использовавшимся в преступной деятельности, получения сведений о соединениях между абонентами и (или) абонентскими устройствами на основании постановления следователя без судебного решения в случаях, не терпящих отлагательств.

Для сокращения сроков получения требуемых сведений территориальными органами МВД России также заключены соглашения об электронном документообороте с рядом кредитных организаций и операторов связи.

В этих же целях между МВД России и Банком России организован информационный обмен на базе платформы ФинЦЕРТ. Сотрудникам органов внутренних дел предоставлена возможность оперативного получения сведений об использованных в операциях, совершенных без согласия клиента, счетах, их владельцах, остатке денежных средств. Необходимо отметить, что Банком России проводится большая работа по расширению имеющегося в их распоряжении функционала, совершенствованию аналитической составляющей при оперировании базами данных.

В заключении следует отметить, что в настоящее время еще не сформирован действенный комплекс мер по противодействию преступлениям в сфере информационных технологий. Ежегодный рост числа зарегистрированных преступлений подтверждает этот факт. В то же время во всех ключевых правоохранительных органах созданы специализированные подразделения, которые совместно с представителями иных государственных органов и бизнес-сообществом показывают определенные позитивные результаты. Сегодняшний этап становления комплекса мер по противодействию преступлениям в сфере информационных

технологий можно охарактеризовать так: предприняты необходимые шаги, но их очевидно не достаточно!

Список литературы

1. Информационно-аналитические материалы Следственного департамента МВД России.
2. Состояние преступности, информация МВД России // Официальный сайт Министерства внутренних дел Российской Федерации. URL: <https://мвд.рф/folder/101762>.

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

Научный руководитель: **Чурин Р. А.,**
главный эксперт отдела компьютерных
и радиотехнических экспертиз
управления экспертиз цифровой и речевой информации
Экспертно-криминалистического центра МВД России,
преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

АВАРИЙНЫЕ РЕГИСТРАТОРЫ СОБЫТИЙ КАК ОБЪЕКТ ЭКСПЕРТНОГО ИССЛЕДОВАНИЯ

Преступления против безопасности движения и эксплуатации транспорта на сегодняшний день отличаются своей распространенностью и высокой общественной опасностью. Расследование преступлений против безопасности дорожного движения в настоящее время связано с применением новых научных методов и технических средств обнаружения, фиксации, изъятия и исследования доказательств. Для доказывания по делам указанной категории необходимо получение объективных данных о скорости, траектории движения, расположении участников дорожно-транспортного происшествия и другие данные [2, с. 79].

В уголовном судопроизводстве требуются специальные знания и активное участие экспертов и специалистов. Воссоздание произошедших событий позволяет сведущим лицам создать модель дорожно-транспортного происшествия, которая позволяет представить произошедшее и провести анализ события с разных ракурсов.

Одним из перспективных путей решения данной проблемы является исследование аварийного регистратора событий или EDR (Event Data Recorder – регистратор данных о событиях). Аварийный регистратор событий предназначен, прежде всего, для регистрации и воспроизведения данных, связанных с дорожно-транспортными происшествиями или ситуациями, близкими к аварийным, например, при срабатывании подушек безопасности. Как правило EDR интегрированы в электронные блоки управления системами пассивной безопасности (SRS), но встречаются и исключения, например, когда «черный ящик» фиксирует параметры в системах предотвращения наезда на пешехода, управления двигателем или вспомогательных системах.

EDR непрерывно отслеживает различные параметры автомобиля:

¹ © Горичева С. Д., 2024.

- скорость движения транспортного средства;
- частота вращения коленчатого вала;
- положение педали тормоза;
- цикл зажигания;
- присутствие пассажира;
- статус срабатывания подушек безопасности;
- статус антиблокировочной системы;
- нагрузка на двигатель;
- параметры активации систем безопасности;
- состояние замка ремня безопасности и многое др.

Эти данные сохраняются в постоянно запоминающем устройстве (ПЗУ) и могут быть извлечены для проведения экспертного исследования после дорожно-транспортного происшествия [4, с. 110].

Структура EDR включает в себя микроконтроллер, который управляет сбором данных и их хранением. Данные также могут быть зашифрованы для защиты конфиденциальности и предотвращения несанкционированного доступа к ним.

Получение криминалистически важной информации из EDR может быть осуществлено при производстве радиотехнических экспертиз. Как правило, перед экспертом ставится единственный вопрос: «Имеется ли в представленном блоке (в блоках представленного автомобиля) информация о параметрах движения автомобиля (указывается марка, модель, государственный регистрационный знак) непосредственно перед дорожно-транспортным происшествием (указывается место и дата ДТП)?». Также могут вноситься дополнительные вопросы, которые интересуют следствие.

В настоящее время для получения информации из EDR применяется оборудование Bosch Crash Data Retrieval, что позволяет сформировать отчет с необходимыми исходными данными. Структура отчета включает в себя:

- информацию о событии, где содержатся данные об импортированном файле, VIN-номере автомобиля, дата и время сохранения, информация об оборудовании и типе приспособления EDR, последние события и другие, не менее, важные детали;
- словарь специализированных терминов, ограничения сохраненной информации в регистраторе данных события и описание информации о данных и параметрах;
- выходные параметры систем безопасности автомобиля, изложенных в таблицах (рис.).

Анализ полученного отчета показал, что в таблице (рис.) содержатся данные о скорости автомобиля за последние пять секунд до происшествия, угол поворота руля, нажатии педали тормоза (в процентах), обороты двигателя, давление тормозной жидкости в тормозной системе, величина ускорения и замедления.

Эти данные являются максимально объективными, при этом для некоторых измерений погрешность данных в EDR не превышает 1 %.

Определение параметров движения автомобиля в момент аварии вызывает затруднения из-за отсутствия специального оборудования во многих экспертных

подразделений, небольшого практического опыта и отсутствия методики по исследованию объектов радиотехнических экспертиз.

Pre-Crash Data -5 to 0 Seconds (Most Recent Event, TRG 12) - Table 1 of 4

Time (sec)	Vehicle Speed (MPH [km/h])	Accelerator Pedal, % Full (%)	Percentage of Engine Throttle (%)	Fuel Injection Quantity (mm ³ /st)	Engine RPM (RPM)	Motor RPM (RPM)	Service Brake, ON/OFF
-4.65	104.4 [168]	57.5	59.5	Invalid	3,500	Invalid	OFF
-4.15	104.4 [168]	57.5	63.0	Invalid	3,500	Invalid	OFF
-3.65	104.4 [168]	1.5	19.5	Invalid	3,500	Invalid	OFF
-3.15	101.9 [164]	0.0	0.0	Invalid	3,490	Invalid	OFF
-2.65	93.8 [151]	37.5	6.5	Invalid	3,500	Invalid	ON
-2.15	78.3 [126]	75.5	15.5	Invalid	3,400	Invalid	ON
-1.65	51.6 [83]	3.0	13.0	Invalid	2,500	Invalid	ON
-1.15	31.1 [50]	67.5	9.5	Invalid	1,700	Invalid	ON
-0.65	24.2 [39]	0.0	0.0	Invalid	600	Invalid	OFF
-0.15	11.2 [18]	0.0	0.0	Invalid	100	Invalid	OFF
TRG(0)	8.7 [14]	0.0	0.0	Invalid	100	Invalid	OFF

Pre-Crash Data -5 to 0 Seconds (Most Recent Event, TRG 12) - Table 2 of 4

Time (sec)	ABS Control Status	BOS Control Status	Brake Oil Pressure (Mpa)	Longitudinal Acceleration, VSC Sensor (m/s ²)	Yaw Rate (deg/s)	Steering Input (degrees)	Shift Position
-4.65	OFF	OFF	0.00	0.790	-0.49	0.0	D
-4.15	OFF	OFF	0.00	0.431	-0.98	-1.5	D
-3.65	OFF	OFF	0.00	0.215	2.93	22.5	D
-3.15	OFF	OFF	0.00	-1.436	19.52	6.0	D
-2.65	OFF	OFF	1.73	-2.871	23.42	-55.5	D
-2.15	ON	ON	11.23	-3.517	36.60	-109.5	D
-1.65	ON	OFF	9.89	-3.517	18.06	-99.0	D
-1.15	ON	OFF	10.42	-7.537	61.00	-94.5	D
-0.65	ON	OFF	0.00	0.861	13.66	52.5	D
-0.15	ON	OFF	0.00	-5.384	61.00	-39.0	D
TRG(0)	ON	OFF	0.14	-6.973	61.00	-34.5	D

Pre-Crash Data -5 to 0 Seconds (Most Recent Event, TRG 12) - Table 3 of 4

Time (sec)	Sequential Shift Range	Cruise Control Status	VSC Control Status	READY Signal	Drive Mode, Power Train	Drive Mode, Snow	Drive Mode, EV
-4.65	Undetermined	OFF	ON (enable)	Invalid	Normal	OFF	Invalid
-4.15	Undetermined	OFF	ON (enable)	Invalid	Normal	OFF	Invalid
-3.65	5	OFF	ON (enable)	Invalid	Normal	OFF	Invalid
-3.15	5	OFF	ON (enable)	Invalid	Normal	OFF	Invalid
-2.65	5	OFF	Engaged	Invalid	Normal	OFF	Invalid
-2.15	5	OFF	Engaged	Invalid	Normal	OFF	Invalid
-1.65	5	OFF	Engaged	Invalid	Normal	OFF	Invalid
-1.15	5	OFF	Engaged	Invalid	Normal	OFF	Invalid
-0.65	5	OFF	Engaged	Invalid	Normal	OFF	Invalid
-0.15	5	OFF	ON (enable)	Invalid	Normal	OFF	Invalid
TRG(0)	5	OFF	ON (enable)	Invalid	Normal	OFF	Invalid

Рис. Фрагмент отчета о зафиксированных сведениях состояния электронных систем транспортного средства на момент аварийного события

Таким образом, данные, зафиксированные аварийными регистраторами событий, позволяют более объективно раскрывать и расследовать преступления и правонарушения, связанные с использованием автотранспорта. При этом необходимо сформировать типовое методическое обеспечение, а также продолжить анализ предоставления EDR в качестве объектов криминалистических экспертиз.

Список литературы

1. Родионова Н. С., Шишкова Е. В. Автомобильные Черные ящики: анализ возможностей и ограничений. 2018.
2. Герасимова С. А., Еликеева Н. А. Экспертно-криминалистическое исследование данных автомобильных аварийных регистраторов // Вестник ВГУ. Серия: Юриспруденция. 2017. № 3. С. 79–83.
3. Деменков А. В. Экспертное исследование аварийных регистраторов данных транспортных средств : учебное пособие. М. : Юрайт, 2020.

4. Головчанский А. В. Использование данных электронных систем безопасности и управления транспортного средства при расследовании дорожно-транспортных преступлений // Вестник Воронежского института МВД России. 2014. № 3. С. 165–170.

5. Изосимов А. Ю., Вострокнутов А. М. Судебно-экспертное исследование данных аварийных регистраторов // Вестник Академии прокуратуры Российской Федерации. 2019. № 4. С. 107–112.

6. Головчанский А. В. Установление скорости движения транспортного средства на момент дорожно-транспортного происшествия // Научный портал МВД России. 2014. № 1. С. 32–39.

7. Методика исследования объектов радиотехнической экспертизы : методика / [В. М. Щербак и др.]. М. : Экспертно-криминалистический центр МВД России, 2019.

Григорусь Л. Н.¹,

*старший преподаватель кафедры гуманитарных
и социально-экономических дисциплин*

Крымского филиала

Краснодарского университета МВД России

Тутова О. В.²,

*старший преподаватель кафедры гуманитарных
и социально-экономических дисциплин*

Крымского филиала

Краснодарского университета МВД России,

кандидат педагогических наук, доцент

NFT КАК СРЕДСТВО ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЯ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ

Приблизительно с 2021 г. NFT (Non-fungible tokens) стали темой обсуждения различных криптовалютных бирж и произвели фурор в криптовалютной индустрии. В данные токены начались активные инвестиции сотен тысяч долларов не только мировых звезд, предпринимателей, брокеров, но и некоторых стран мира. NFT – это уникальные по своей природе, не идентичные между собой и невзаимозаменяемые цифровые объекты на основе блокчейн технологии – в отличие от обычных криптовалют, таких как Bitcoin, Ethereum, чьи единицы (токены) являются взаимозаменяемыми. Non-fungible tokens может хранить свои данные в системах блокчейна. Так, большинство NFT-проектов построены на таких блокчейн-системах, как Ethereum и Solana, и данные, которые там хранятся, могут быть связаны с различными изображениями, видеофайлами, аудиофайлами, цифровыми активами. На сегодняшний день популярно NFT-цифровое изображение искусства, так как многие известные художники (Джастин Блау, Mad Dog Jones и др.) перешли в цифровой мир.

2021 г. ознаменовался достаточно впечатляющими темпами роста оборота NFT. В 2021 г. объем проведенных сделок с невзаимозаменяемыми токенами вырос до \$13 млрд по сравнению с \$33 млн в 2020 г. Резкий скачок связан с расширившейся сферой внедрения токенов: NFT стали предметами искусства, карточками спортивных клубов и основой для модели play-to-earn в виртуальных играх. Кроме того, появились маркетплейсы NFT, которые активно поспособствовали их распространению: специализированные площадки, крупные криптобиржи (Coinbase, Huobi, Binance) [1].

В начале 2022 г. этот рынок был относительно устойчивым. Как отмечает ресурс NonFungible, в середине января 2022 г. число продаж NFT приблизительно было равно 164 000 сделкам. Однако чуть позже рынок NFT пошел на спад, как и основной рынок криптовалют [1].

¹ © Григорусь Л. Н., 2024.

² © Тутова О. В., 2024.

С марта 2022 г. еженедельные продажи NFT начали сокращаться, приблизительно до \$230 млн. Тогда большинство аналитиков связало сокращение продаж с начавшейся специальной военной операцией России на Украине, что повлекло закономерный отток спекулянтов из этой отрасли. Портал Be(In)Crypto опубликовал информацию о том, что во всем мире в феврале продажи NFT составили \$2,92 млрд, а март ознаменовался сокращением продаж до \$2,3 млрд.

В конце марта активность на рынке продаж NFT начала возрастать и объёмы еженедельных торгов в данной сфере возросли до \$469 млн, однако продлилось это недолго. Согласно данным аналитики Chainalysis в 2023 г. на адреса незаконных криптовалютных кошельков поступило криптовалют на сумму не менее \$24,2 млрд. Сюда относятся адреса, которые были идентифицированы как связанные с финансированием терроризма, мошенничеством, а также адреса, попавшие под санкции.

В отчете показано, что в 2023 г. на долю организаций и юрисдикций, попавших под санкции, пришелся совокупный объем незаконных транзакций на сумму \$14,9 млрд, что составляет 61,5 % от всего объема незаконных транзакций за год. Большая часть этой суммы поступила от криптосервисов, которые попали под санкции США или расположены в США.

Такие качели являются типичными для крипторынка и падение цен тех или иных токенов далеко не всегда связано с утратой интереса к ним [1]

Это говорит о резкой популярности данного уникального токена. Отчет Chainalysis также показывает, что цифра в \$24,2 млрд почти наверняка занижена и будет расти по мере выявления большего количества незаконных адресов, так же как уже был удвоен оценочный показатель по 2022 г. с \$20,6 млрд до \$39,6 млрд.

Однако, как и любые ноу-хау и уникальные технологии, NFT создают новые возможности для злоупотребления и совершения преступных деяний. Огромные обороты денежных средств в этой сфере делают её привлекательной для преступников, желающих легализовать доход, полученный преступным путем, что связано в первую очередь:

1) с анонимностью криптовалютных трансфертов и отсутствием каких-либо проблем с транспортировкой токенов (нет необходимости хранить их на физическом носителе);

2) минимальными требованиями к KYC (системе верификации пользователя) на платформах, ориентированных на NFT, или отсутствие верификации вообще;

3) сегментом невзаимозаменяемых токенов, которая остается «Серой зоной» для правоохранительных органов, что создает возможность для легализации активов, полученных преступным путем;

4) отсутствием законодательной базы, регулирующей финансовые операции, осуществляемые блокчейн – системами, а в частности, транзакций в адрес NFT – проектов.

В данной статье рассмотрим две формы незаконной деятельности, наблюдаемые на рынках NFT:

- совершение фиктивной торговли для искусственного повышения стоимости невзаимозаменяемого токена с целью дальнейшего отмыwania преступных денежных средств;
- совершение действий, направленных на отмывание (легализацию) доходов, полученных в результате совершения преступления лицом или третьими лицами.

Фиктивная торговля представляет собой деятельность, направленную на совершение сделок, по обе стороны которых находится один и тот же продавец с целью завышения стоимости и придания ликвидности активу. В случае с уникальным токеном, целью фиктивной торговли является искусственное завышение («накачка») стоимости невзаимозаменяемого токена путем совершения его фиктивной продажи вновь созданному кошельку, однако, контролируемому тем же лицом. Ончейн-анализ продаж NFT адресам, финансируемым из того же источника, показывает, что некоторые продавцы NFT выполняют сотни фиктивных сделок с принадлежащими им токенами для искусственного повышения стоимости невзаимозаменяемого токена.

В данном случае указанные манипуляции способствуют завышению стоимости цифрового актива и создают благоприятные условия для дальнейшего отмыwania денежных средств в любой валюте, полученных в результате совершения преступных деяний. Кроме того, это также подрывает доверие к экосистемам NFT-маркетплейсов и препятствует их дальнейшему росту. С целью противодействия указанным процессам маркетплейсам необходимо максимально препятствовать такой деятельности, систематически выявлять сомнительные операции и транзакции в адрес NFT – платформ и блокировать пользователей, действия которых направлены на искусственную «накачку» стоимости уникального токена.

Отмывание преступных активов давно уже стало проблемой в мире, в том числе и в сфере изобразительного искусства. Например, произведения искусства (картины) легко перемещать. Они, как правило, оцениваются согласно субъективному мнению коллекционеров, которые могут предлагать определенные налоговые преимущества держателям данных картин. Все это обуславливает привлекательность NFT-цифрового изобразительного искусства для совершения действий, направленных на легализацию преступных доходов.

Эксперт аналитической компании Quantexa Мэтью Лонг отметил привлекательность NFT для субъектов отмыwania денег, по его словам «за фасадом скупающих богачей, покупающих цифровые произведения искусства по безумно высоким ценам, скрывается зловещая и изощренная схема отмыwania денег ультрабогатой криптоэлитой, которая стремится придать незаконным доходам законный вид».

Конкретные примеры покупки NFT преступниками из различных категорий можно увидеть на графе транзакций (рис.).

Здесь мы можем наблюдать адреса, ассоциируемые с несколькими киберпреступниками из различных категорий – включая операторов вредоносных программ, мошенников и Chatex, – отправляющие средства на популярный NFT-маркетплейс.

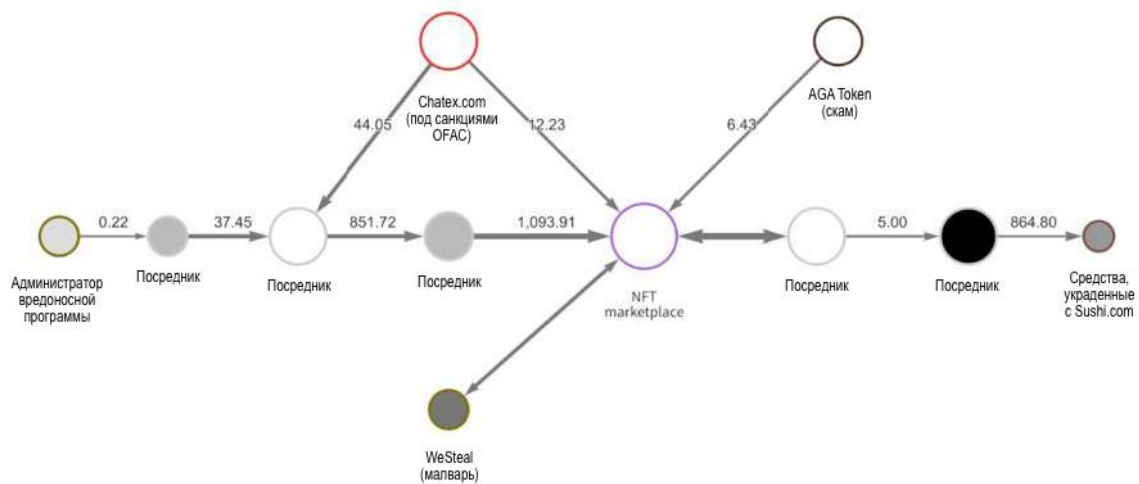


Рис. Графа транзакций

Таким образом, подводя итог вышесказанному стоит отметить, что на сегодняшний день преступники нашли новые способы совершения действий, направленных на отмыwanie доходов, полученных преступным путем, в частности, путем использования NFT-маркетплейсов, что позволяет это делать практически анонимно и в больших объемах, при этом не попадая в поле зрения правоохранительных органов. Тем не менее отмыwanie денег и, в частности, незаконные переводы, представляют собой большой риск для экономики страны и мировой экономики в целом и должны тщательнее контролироваться торговыми площадками, регуляторами и правоохранительными органами.

Список литературы

1. URL: <https://secretmag.ru/technologies/nft-obozvali-sduvshimsya-puzyryom-tak-li-eto-i-mozhno-li-eshyo-investirovat-v-kartinki-na-blokcheine.htm>.
2. Могильный Н. К. Актуальные вызовы мировой экономики в борьбе с легализацией преступных доходов и финансированием терроризма // Евразийский юридический журнал. 2018. № 5. С. 398–400.

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

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

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ОБЩЕСТВЕННЫХ WI-FI

Безопасное использование общественного Wi-Fi с каждым днем становится все более актуальной проблемой для людей. Сети Wi-Fi, к которым подключаются пользователи имеют низкий уровень защиты, что может способствовать утечки их личных данных, паролей, банковских карт и других важных сведений.

Для данной проблемы существуют два нормативных правовых акта, которые регулируют общественные Wi-Fi. Один из них – Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Он контролирует использование сетей в общественных местах. В нем можно выделить несколько норм, направленных на обеспечение защиты пользователя.

Например, операторы сетей Wi-Fi, согласно законодательству Российской Федерации, обязаны соблюдать конфиденциальность и защиту персональных данных пользователя. Они должны обеспечивать пользователям регулирование и фильтрацию информации. Чтобы предотвратить все возможные утечки данных, операторы обязаны обеспечивать такой защитой, при которой невозможен несанкционированный доступ.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» также содержит нормы, направленные на обеспечение безопасности использования общественных Wi-Fi сетей. Рекомендуются использовать средства, которые предотвращают утечки данных. Пользователи общественного Wi-Fi обязаны знать о возможной потере данных при подключении к незащищенным сетям.

Чтобы прерывать атаки злоумышленников, существуют различные методы защиты.

Один из самых распространенных – аутентификация. Протокол WEP, самый первый открыл начало в попытке защитить общественные сети в 1997 г., но через время он стал более уязвимым, и ему на смену пришли улучшенные версии протоколов. С помощью протокола шифрования WPA и его улучшенной версии WPA2 обеспечивается полная защита, используя ключи шифрования.

Нельзя не упомянуть защиту данных путем шифрования. С помощью стандартов AES (Advanced Encryption Standard) и TKIP (Temporal Key Integrity

¹ © Давыдов А. Д., 2024.

Protocol) также применяются для защиты данных по сети Wi-Fi. Второй стандарт более устаревший и имеет уязвимости на сегодняшнее время, так как он разрабатывался для улучшения протокола WEP. Поэтому рекомендуется использовать именно стандарт AES. У него высокий уровень обеспечения безопасности.

Киберпреступники каждый день придумывают различные подходы к получению информации, используя общественные Wi-Fi сети и технику манипуляции. Подделка точки доступа или же «Fake Wi-Fi» – самая частая проблема пользователей, подключающихся к ним. Этот метод очень эффективный, особенно в отелях или других местах, где возможен большой трафик людей. В заведении, может быть, несколько официальных сетей, но кто мешает злоумышленникам добавить еще одну. Преступники этим способом могут получить большое количество информации на телефоне потерпевшего. Это могут быть пароли, данные банковских карт, фотографии и другие данные. Чтобы обезопасить себя от потери данных, можно использовать проверенный VPN – виртуальная частная сеть, которая с помощью интернета создает подключение между устройствами. Маскируя IP-адрес от злоумышленников, она обеспечивает полную безопасность важной информации. Но следует учесть, что не все VPN могут быть безопасными, поэтому пользоваться такими частными сетями нужно у достоверных источников.

Общественные сети Wi-Fi иногда бывают необходимой мерой в внезапных ситуациях. При подключении к все доступным сетям следует не вводить важные персональные данные, использовать только проверенные точки доступа и соблюдать все меры предосторожности при подключении к ним.

Список литературы

1. Брэгг Р., Родс-Оусли М., Страссберг К. Безопасность сетей : полное руководство. М. : Эком, 2020.
2. Мерритт М. Безопасность беспроводных сетей. М. : Книга по требованию, 2021.
3. Радке Хорст-Дитер, Радке Йеремиас. Все о беспроводных сетях. М. : НТ Пресс, 2023.

Данилова А. О.¹,

*курсант Института-факультета подготовки сотрудников
для органов предварительного расследования*

Московского университета

МВД России имени В.Я. Кикотя

Научный руководитель: Страхов А. А.,

доцент кафедры информатики и математики

Московского университета

МВД России имени В.Я. Кикотя

О ПРОБЛЕМАХ ДОКАЗЫВАНИЯ ОБСТОЯТЕЛЬСТВ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ (ПРИМЕНЕНИЕМ) ИНФОРМАЦИОННО- ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Следы остаются при совершении любого преступления, но характерной особенностью киберпреступлений является то, что эти следы представлены в цифровом виде. С целью изучения вопросов выявления и раскрытия преступлений в сфере компьютерной информации, а также разработки методов и средств поиска, получения, исследования и консолидации цифровых доказательств в криминалистике сформировалось отдельное прикладное направление – криминалистическая экспертиза или форензика.

Существуют два типа следов: материальные, которые возникают после взаимодействия субъекта с материальными объектами (к примеру, отпечатки кожных покровов частей тела человека, гильзы, оставленные на месте преступления) и идеальные, которые отражают объективную реальность, связанную с преступлением в памяти человека в виде образов, формирующихся в процессе восприятия событий.

При раскрытии и расследования преступлений в сфере информационно-телекоммуникационных и компьютерных технологий цифровые следы могут быть выделены в отдельную категорию. В свою очередь цифровые носители, такие как оптические, магнитные, электронные диски или флэш-карты, являются материальными объектами (носителями следов) с определенными физическими свойствами и методами представления информации. Цифровая информация, находящаяся на этих носителях, представляет собой результат психической деятельности человека, и ее можно обнаружить только с помощью специального технического оборудования и соответствующих знаний [2].

Цифровые следы могут быть обнаружены на компьютерах злоумышленника, жертвы и третьих лиц, а также на удаленных информационных ресурсах в сети Интернет. Довольно часто возникают ситуации, когда одни и те же следы обнаруживаются одновременно в различных местах.

¹ © Данилова А. О., 2024.

Подтверждение надежности найденной цифровой информации и ее связи с конкретным преступлением является сложной и комплексной задачей. Однако, можно рассмотреть варианты решения этой проблемы, ссылаясь на международный опыт. Например, первичная регистрация в социальных сетях Китая требует подтверждения личности другим зарегистрированным пользователем. Это позволяет администрации сети в случае совершения противоправных действий идентифицировать злоумышленника, связавшись с его поручителем. Дополнительно администрация сайта при регистрации может подтвердить личность пользователя фотографией с целью применения интеллектуального поиска с помощью систем габитоскопической идентификации.

Сложность получения цифровых следов для установления личности преступника обусловлена анонимностью Интернета. Инкриминирующие действия в этой области требуют специальных знаний, навыков и практического опыта, которых часто не хватает сотрудникам правоохранительных органов. Чтобы преодолеть эти проблемы в борьбе с преступлениями в сфере компьютерной информации, правоохранительные органы обращаются к специализированным экспертам по кибербезопасности из ведущих IT-компаний. Например, эксперты «Лаборатории Касперского» или международной компании Group-IB уже много лет сотрудничают с правоохранительными органами, участвуя в оперативно-разыскных¹ мероприятиях, следственных действиях по сбору цифровых следов и получению доказательств, а также в судебных процессах.

В эпоху всеобщей цифровизации компьютерная информация становится полноценным доказательством в уголовно-процессуальной практике. Следует отметить, что содержание термина «цифровые доказательства» не зафиксировано в каком-либо нормативном правовом акте, но в соответствии с действующим уголовно-процессуальным законодательством цифровые следы могут быть материальными доказательствами или документированной информацией [3].

Исходя из положений теории уголовного права и уголовного процесса, цифровое доказательство – это единство информации и ее материального носителя. В соответствии со ст. 84 Уголовно-процессуального кодекса Российской Федерации (УПК РФ), документы могут содержать информацию, собранную как в письменной, так и в иной форме. К ним могут относиться текстовые, фото-, аудио- и видеоматериалы, полученные, запрошенные или представленные в порядке, установленном ст. 86 УПК РФ. Документы, имеющие признаки, указанные в ч. 1 ст. 81, признаются вещественными доказательствами в соответствии с ч. 4 ст. 84 УПК РФ [1].

В сфере компьютерной информации термины «документ», «вещественное доказательство» и «другой документ» могут использоваться в разных значениях. В классическом понимании документом, как вещественным доказательством, является материальный объект, который содержит следы преступной деятельности. Другой документ должен содержать информацию о юридически значимых фактах на материальном носителе [5]. В криминалистической терминологии

¹ Здесь и далее написание слова *разыскных* приводится в соответствии с нормами русского языка, за исключением употребления в нормативных правовых актах.

цифровая информация относится к данным, собранным компьютерной системой на цифровых носителях, связанным с совершением действий в цифровом пространстве. Термин «цифровые доказательства» относится к документу в формате, который может быть просмотрен с использованием электронных технологий, передан по информационным сетям и обработан в информационных системах.

Процессуальными действиями для получения цифровых доказательств являются обыск, изъятие или следственный осмотр, а также оперативно-разыскные мероприятия. Важно учитывать, что информация становится доказательством только в том случае, если она получена и обработана в соответствии с требованиями УПК РФ. Цифровые следы легче подделать или уничтожить, чем вещественные, а это может привести к ошибочным выводам при установлении обстоятельств дела и подорвать доверие ко всей доказательной базе.

В заключении следует отметить, что цифровизация общества породила киберпреступность, борьба с которой требует новых решений в области права, криминалистики, уголовного судопроизводства, технического обеспечения оперативно-служебной деятельности. Эффективность профилактических мер, выявления, раскрытия и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в значительной степени зависит от профессионализма сотрудников органов внутренних дел. Особое внимание следует уделить совершенствованию нормативной правовой базы, разработке методов и инструментов для выявления, фиксации и анализа цифровых следов, юридического закрепления полученной информации в виде цифровых доказательств в уголовных делах. Грамотные действия по сбору цифровых доказательств позволят оперативно не только установить истинные обстоятельства преступлений, мотивы и роли всех причастных лиц, но и минимизировать нанесенный ущерб.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 25.12.2023) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/.
2. Цифровые следы преступлений : учебное пособие / [А. М. Багмет и др.]. М. : Проспект, 2020.
3. Ростовцев А. В. Особенности судебно-экспертного исследования «Цифровых следов» // Академическая мысль. 2019. № 3.
4. Чернятин Г. Л. Интернет для Интернета вещей // Студенческий вестник. 2019. № 25-3 (75). С. 81–82.
5. Глотина И. М., Шевчук И. С. Киберпреступность – проблема без границ // Экономика АПК Предуралья. 2019. № 1. С. 30–33.

*Дворцова А. А.¹,
студент Высшей школы права
Российского экономического университета
имени Г.В. Плеханова*

*Научный руководитель: Григорьев Д. А.,
доцент кафедры государственно-правовых
и уголовно-правовых дисциплин
Российского экономического университета
имени Г.В. Плеханова,
кандидат юридических наук*

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Технологии искусственного интеллекта активно развиваются и находят применение в самых необычных сферах общественной жизни. Нейронные сети применяются для распознавания объектов, написания текстов на основе анализа и накопления информационных баз данных, генерирования совершенно новой информации и в десятках других областей. В рамках криминалистики искусственный интеллект используется для выявления следов преступлений по фото- и видеоматериалам, анализа ДНК, распознавания лиц, предоставления рекомендаций по ведению дел. Сфера использования технологий нейронных сетей в борьбе с преступностью весьма обширна и многогранна.

Согласно Указу Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» [7] под искусственным интеллектом понимается комплекс технологических решений, который способен имитировать когнитивные функции человека, например, поиск решений без установленного алгоритма, и получать результаты при выполнении определенных задач, которые возможно сопоставить с интеллектуальной деятельностью человека или с информацией, превосходящей данную человеческую деятельность.

Существует несколько способов использования искусственного интеллекта преступниками. Первый из них – фишинг. Он представляет собой интернет-мошенничество, используемое для получения конфиденциальных данных пользователя [2, с. 753–766]. К числу данных, получаемых преступниками, могут относиться логины и пароли от приложений банков, личных кабинетов, государственных сайтов. Также используются рассылки от имени официальных источников. Открыв такое письмо, к примеру, на электронной почте, можно неосознанно предоставить злоумышленникам всю личную информацию, хранящуюся на вашем личном компьютере или телефоне. Обычно ссылка в сообщении ведет на сайт, почти на сто процентов схожий с сайтом банка, интернет-магазина или другого источника, но вводя пароль на таком поддельном сайте, вы переда-

¹ © Дворцова А. А., 2024.

ете данные преступникам. Более серьезные преступления с использованием искусственного интеллекта прослеживаются на государственном и даже мировом уровнях. Злоумышленники могут использовать технологии нейронных сетей, программируя дронов. Такие дроны способны практически полностью автономно выявлять необходимые цели и выполнять поставленные задачи, к примеру, участвуя в организации терактов или иных преступлений, связанных с покушением на жизнь и здоровье людей. Дроны также используются для незаконной доставки товаров, в том числе наркотических веществ, в том числе в масштабах межгосударственной перевозки.

Злоумышленники приспособились к современным реалиям и могут использовать искусственный интеллект для реализации практически любого преступления. Для государств это создает необходимость в создании и развитии новых способов борьбы с преступлениями, совершенными при помощи искусственного интеллекта. Например, по информации МВД России с использованием информационно-телекоммуникационных технологий (далее – ИТТ) совершается каждое третье преступление. В 2023 г. в этой сфере зарегистрировано на 29,2 % преступлений больше, чем в январе-сентябре 2022 г. [3]. Более 677 тыс. преступлений, с использованием ИТТ, было зарегистрировано в Российской Федерации за 2023 г. Для сравнения, в 2022 г. таких преступлений было 522,1 тыс. За 11 лет число преступлений данной сферы выросло в 62 раза [5].

В Российской Федерации активно разрабатываются технологии, при помощи искусственного интеллекта помогающие в борьбе с преступностью. Так, существует система под названием «Криминалист». Эта система анализирует базы данных, в том числе информационные ресурсы ФНС России, ФСБ России, МВД России и других государственных органов. Система «Криминалист» позволяет обнаружить предполагаемых преступников или точки совершения преступлений, кроме того, она может предложить эффективные решения для правоохранительных органов.

Во всем мире используется система Predictive Policing. Она генерирует прогнозы совершения преступных деяний в конкретных местах и в конкретное время. Это происходит благодаря анализу ранее совершенных преступлений. Еще одна система называется Correctional Offender Management Profiling for Alternative Sanctions, сокращенно – COMPAS. Данный алгоритм способен оценить вероятность рецидива у осужденных. Программа ShotSpotter способна уловить звуки выстрелов из огнестрельного оружия и определить, где произошел выстрел или серия выстрелов. После обнаружения информация с данными незамедлительно передается правоохранительным органам для эффективного реагирования государственных служб.

В г. Москве активно внедряются системы видеонаблюдения с использованием искусственного интеллекта. Данная технология позволяет распознавать лица людей и их деятельность, которая может нарушать законодательство. За 2023 г. в городе около 70 % преступлений в парках, скверах и других уличных пространствах были раскрыты с помощью уличного видеонаблюдения [4]. Система видеонаблюдения с использованием искусственного интеллекта позволяет

не только повысить уровень раскрываемости преступлений, но и снизить их количество. Люди менее охотно идут на преступный умысел при наличии информации о том, что их обнаружат и осудят с помощью камер на улицах города. При этом местоположение многих точек наблюдения сокрыто от граждан.

Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» определяет одной из задач осуществления национальной безопасности страны предупреждение преступной деятельности, совершаемой при помощи технологий искусственного интеллекта или информационно-телекоммуникационных технологий [8]. Это является еще одним доказательством актуальности проблемы на общегосударственном уровне.

Президент Российской Федерации В. В. Путин поручил до 1 июня 2024 г. провести анализ искусственного интеллекта в расследовании преступлений. Данным вопросом будут заниматься Верховный Суд Российской Федерации, Генеральная прокуратура Российской Федерации, Минюст России, МВД России и СКР России. Поручение было утверждено после проведения заседания Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека, проходившее 4 декабря 2023 г. [6]. Это говорит о том, что совершенствование технологий искусственного интеллекта и его применение в сфере расследования преступлений становится одним из приоритетных направлений развития государства.

На том же заседании, Совета по развитию гражданского общества и правам человека при Президенте Российской Федерации, Е. Меркачева обратила внимание всех присутствующих на вопиющий факт. Уголовное дело было возбуждено в отношении ученого А. Цветкова. Искусственный интеллект счел, что, лицо ученого на 55 % совпадает с фотороботом убийцы, составленный в 2003 г. Кроме того, еще одним основанием стало показания рецидивиста, который в ходе допроса указал на Цветкова как на соучастника убийств. По мнению специалистов в области искусственного интеллекта оценка 55 % считается очень низкой для правильного ответа.

Данный пример показывает, что нельзя «слепо верить» результатам применения искусственного интеллекта. Все доказательства должны оцениваться в купе с другими доказательствами, тем более коллеги Цветкова подтверждали его алиби. Они указывали на то, что в момент совершения преступлений он находился в научной экспедиции. Позднее, уголовное преследование в отношении Цветкова было прекращено и прокуратура Москвы принесла официальное извинение «за моральный вред, связанный с необоснованным привлечением к уголовной ответственности».

Особенность преступлений с использованием искусственного интеллекта заключается в реализации деятельности одновременно в информационном и реальном пространствах [1, с. 82–87]. Этому способствуют следующие особенности рассматриваемых преступлений и причины их активного распространения:

- повсеместность использования информационно-телекоммуникационных систем;
- распространение общедоступности системы Интернет;

- анонимность в сети Интернет;
- трансграничность;
- распространение электронных платежей.

Очевидно, что борьба с преступностью в виртуальном мире должна происходить иначе, чем в виртуальном. Стремительное развитие технологий привело к тому, что правоохранители оказались совершенно не готовы к резкому скачку количества преступлений в глобальной сети. В данный момент во всем мире разрабатываются и внедряются технологии, помогающие в борьбе с преступностью при помощи искусственного интеллекта. Однако, существуют сферы деятельности, на которые, по мнению автора, стоит обратить особое внимание, в частности, на территории Российской Федерации.

Во-первых, необходимо оптимизировать взаимодействие финансовых организаций с правоохранительными органами. Создание системы обмена информацией позволит своевременно бороться с преступлениями, связанными с деятельностью в рамках платежных систем и финансовыми махинациями. По информационным каналам правоохранителям может быть незамедлительно передана информация о подозрительных транзакциях, попытках взлома системы финансовых организаций. Кроме того, следует снизить уровень анонимности финансовых операций и предоставить доступ к такой закрытой информации ограниченному кругу государственных органов, в том числе – правоохранительным.

Во-вторых, следует создать единую систему борьбы с преступностью, объединяющую базу данных различных правоохранительных органов по всей территории страны. Оптимизировать поиск и анализ информации вышеуказанной системы поможет внедрение искусственного интеллекта, создающего условия для сокращения затрат времени правоохранителей на раскрытие преступлений. Кроме того, к функционалу искусственного интеллекта можно отнести определение цифровых устройств по заданным параметрам и поиск цифровых следов, что позволит идентифицировать личность преступника.

Таким образом, перспектива применения искусственного интеллекта в борьбе с преступностью обширна. Нейросети активно развиваются и позволяют не только повысить количество преступлений с их использованием, но и предоставляют возможность оптимизировать правоохранительную деятельность. Уже сейчас искусственный интеллект функционирует на благо закона и справедливости: позволяет оперативно анализировать информацию, распознает лица преступников и передает информацию в правоохранительные органы, обнаруживает возможные места преступлений. Однако стоит и дальше развивать схожие системы и повсеместно внедрять их для борьбы не только с реальной преступностью, но и с виртуальной.

Список литературы

1. Васюков В. Ф., Шеметов А. К. Возможности использования искусственного интеллекта в раскрытии преступлений // Вестник Московской академии Следственного комитета Российской Федерации. 2022. № 1.

2. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12. № 6.
3. Министерство внутренних дел Российской Федерации. URL: <https://мвд.рф/news/item/42987324/>.
4. Информационный портал газеты Известия: Нейронное дело: как ИИ помогает в борьбе с преступностью. URL: <https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu>.
5. Информационный портал газеты Известия: В России за год совершено почти 680 тыс. IT-преступлений. URL: <https://iz.ru/1654427/2024-02-22/v-rossii-zagod-soversheno-pochti-680-tys-it-prestuplenii>.
6. Официальные сетевые ресурсы Президента России. URL: <http://kremlin.ru/acts/assignments/orders/73277>.
7. Указ Президента Российской Федерации от 10 октября 2019 г. N 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.
8. Указ Президента Российской Федерации от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2021. № 27 (ч. II). Ст. 5351.

Дудникова Е. В.¹,

*научный сотрудник отдела координации
и внедрения научно-технической продукции*

*Центра сопровождения научно-исследовательских
и опытно-конструкторских работ*

в области информационных технологий

Научно-исследовательского института специальной техники

НПО «Специальная техника и связь» МВД России

О НЕКОТОРЫХ ВОПРОСАХ РАЗВИТИЯ ИНТЕГРИРОВАННЫХ БАНКОВ ДАННЫХ ОПЕРАТИВНО-СПРАВОЧНЫХ, КРИМИНАЛИСТИЧЕСКИХ, РАЗЫСКНЫХ И СТАТИСТИЧЕСКИХ УЧЕТОВ, ФОРМИРУЕМЫХ НА БАЗЕ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

В современном мире информационные технологии стремительно развиваются. Одним из приоритетных направлений правоохранительной деятельности является развитие имеющихся программно-технических комплексов и систем, а также создание новых сервисов, удовлетворяющих потребностям сотрудников правоохранительных органов.

Для раскрытия и предотвращения преступности сотрудникам правоохранительных органов необходима современная информационная поддержка, с различными базами данных.

Так, одним из основных информационных ресурсов, необходимых для раскрытия и предотвращения преступлений являются оперативно-справочные, розыскные и криминалистические учеты, формируемые органами внутренних дел Российской Федерации (ОВД) [1].

За время своего существования учеты ОВД превратились в крупнейшие региональные (Информационные центры МВД России (ИЦ) и федеральный (ФКУ «ГИАЦ МВД России») базы данных, обеспечивающие информационную поддержку деятельности правоохранительных органов.

В настоящее время функционирует интегрированный банк данных оперативно-справочных, криминалистических, розыскных и статистических учетов, формируемых на базе ОВД (далее – ИБД-Ф).

В настоящее время ПТК ИБД-Ф состоит из различных подсистем:

– «Административная практика» (учет сведений об административных правонарушениях, в том числе совершенных иностранными гражданами и лицами без гражданства, в отношении которых принято решение о выдворении, депортации (реадмиссии);

– «АБД-Центр» (система данных о преступлениях и лицах, подозреваемых, обвиняемых в их совершении);

¹ © Дудникова Е. В., 2024.

- «Номерные вещи» (учет похищенных и изъятых номерных вещей и документов);
- «ФР-Оповещение» (учет лиц, объявленных в федеральный и межгосударственный розыск);
- «Оружие» (учет утраченного и выявленного оружия и иного вооружения);
- «Автопоиск» (учет разыскиваемых транспортных средств);
- «Антиквариат» (учет похищенных предметов, имеющих культурную (историческую, научную, художественную) ценность);
- «Криминал-И» (подсистема данных о преступлениях, совершенных иностранными гражданами, лицами без гражданства, а также о преступлениях, совершенных в отношении их);
- «Оперативно-справочная картотека» (учет сведений о судимости и привлечении к уголовной ответственности);
- «Номерные вещи» (учет похищенных и изъятых номерных предметов и документов, а также предметов, имеющих культурную (историческую, научную, художественную) ценность) и др.

Стоит отметить, что в случае необходимости сотрудники информационных центров могут разрабатывать и вводить в эксплуатацию необходимые подсистемы. Так, для организации учета служебных командировок, была разработана подсистема автоматизированного учета командировок (программное обеспечение «САУК»).

Таким образом ПТК «ИБД-Ф» обеспечивает информационную поддержку деятельности правоохранительных органов.

Основным минусом в настоящее время является то, что ПТК работает на иностранном программном обеспечении. Осложняет оперативность и тот факт, что сопряжение с другими сервисами невозможно.

Одним из важных направлений в повышении полноты, достоверности и эффективности использования учетов, а также в целях соблюдения требований постановления Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» необходимо перевести уже эксплуатируемые базы данных на современную российскую программно-техническую платформу.

Для улучшения деятельности подразделений необходимо создать новый сервис, который будет располагаться в Единой системе информационно-аналитического обеспечения деятельности (ИСОД) МВД России, а также иметь возможность взаимодействовать с другими сервисами.

В настоящее время идет подготовка к выполнению опытно-конструкторской работы по разработке программного обеспечения (сервиса) мастер-сервиса интегрированных данных оперативно-справочных, криминалистических, розыскных и статистических учетов, формируемых на базе органов внутренних дел Российской Федерации.

Целью работы является создание программного обеспечения сервиса интегрированных данных оперативно-справочных, криминалистических, розыскных, статистических и иных учетов, формируемых на базе ОВД, на основе применения современных информационных технологий и обеспечения качественной, своевременной и комплексной обработки данных.

Создание программного обеспечения нового сервиса предназначено для увеличения эффективности использования, формирования и ведения интегрированных банков данных оперативно-справочных, криминалистических, розыскных, статистических и иных учетов, формируемых на базе ОВД, повышения качества предоставления государственных услуг по линии информационно-справочной работы, улучшения межведомственного информационного обмена в электронном виде.

При создании сервиса будет создана новая структура, которая позволит как актуализировать старые подсистемы, так и сохранить имеющиеся, а также создать новые подсистемы, отвечающие современным требованиям.

Рассмотрим основные новшества, запланированные в сервисе.

Так, планируется создание сервиса поиска, который будет предназначен для обеспечения поиска информации в подсистемах сервиса как своего сервиса, так и в других сервисах ИСОД МВД России.

Планируется создание подсистемы, организующей взаимодействие с правоохранительными органами государств – участников СНГ.

Также планируется создание подсистемы, которая предназначена для решения задач выявления признаков серийности (сходства) преступлений с использованием методов машинного обучения и семантического анализа данных и должна обладать возможностью распределенной обработки данных при выполнении вычислительных процедур поисковых запросов.

Планируется создание подсистемы учета похищенных и изъятых номерных предметов и документов, а также предметов, имеющих культурную (историческую, научную, художественную) ценность. Из новых требований к подсистеме является то, что она должна обеспечить возможность поиска предметов по фотоизображению в открытых источниках сети Интернет.

Внедрение результатов позволит:

- сократить временные затраты граждан, необходимые для получения справок в рамках оказания информационными центрами территориальных органов МВД России на региональном уровне государственных услуг;
- обеспечить ведение статистического учета как путем ручного ввода, так и загрузки информации правовой статистики;
- организовать обмен данными с сервисами;
- обеспечить единую точку доступа пользователей в пределах предоставленных привилегий к получению полной информации на запрашиваемый объект учета.

Подводя итог сказанному, можно сказать, что создание нового сервиса направлено на повышение уровня информатизации деятельности сотрудников МВД России как центрального аппарата, так и территориальных подразделений ОВД, улучшение информационно-аналитического обеспечения деятельности

ОВД в целом, увеличение эффективности использования, формирования и ведения интегрированных банков данных оперативно-справочных, криминалистических, розыскных и статистических учетов, формируемых на базе ОВД, а также повышение качества предоставления государственных услуг по линии информационно-справочной работы, улучшение межведомственного информационного обмена в электронном виде.

Список литературы

1. Рябев И. В., Дудникова Е. В. О некоторых вопросах при конвертации баз данных на примере оперативно-справочной картотеки // Научно-технический портал МВД России. 2022. № 1 (41).
2. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.
3. Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_189116/.
4. Концепция научно-технической политики Министерства внутренних дел Российской Федерации до 2030 года : одобрена Научно-техническим советом МВД России (п. 1.1 протокола от 27 августа 2019 г. № 1).
5. План внедрения искусственного интеллекта в деятельность МВД России на 2021 г. и плановый период 2022 и 2023 гг.

Емельянова О. В.¹,

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

Диденко З. И.²,

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

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

В представленной статье рассмотрены основные проблемы, связанные с использованием данных о гражданах, среди которых стоит обратить внимание на главные трудности, влияющие на эффективную работу органов внутренних дел, связанные с эксплуатацией информации.

Одним из наиболее важных аспектов данной проблемы является утечка данных и нарушение конфиденциальности. В рамках, например, проверки сообщения о преступлении или предварительного расследования, сотрудник получает и документирует различные данные. Причинами утечек могут быть хакерские атаки, халатное выполнение должностных обязанностей, превышение должностных полномочий из корыстных побуждений [1].

Для предотвращения этой проблемы необходимо принять ряд мер, которые значительно повысят уровень защиты данных и будут способствовать сохранности конфиденциальности данных:

- обеспечить строгий контроль доступа к конфиденциальной информации граждан;
- обеспечить регулярное обновление систем безопасности и шифрования;
- обеспечить постоянную работу по мониторингу доступа к информации;
- обеспечить разработку строгих правил и процедур по обработке и хранению информации.

Другой немаловажной проблемой является низкий уровень киберзащищенности. Отсутствие строгой политики паролей, двухфакторной аутентификации, регулярного обновления и усовершенствования программного обеспечения создает для злоумышленников приятную среду. Преступники используют слабые места в системе благодаря чему могут манипулировать информацией или даже блокировать работу систем, исказить уже имеющиеся данные, тем самым нарушать деятельность правоохранительных органов.

¹ © Емельянова О. В., 2024.

² © Диденко З. И., 2024.

Одной из немаловажных проблем также является недостаточный уровень подготовки персонала правоохранительных органов по вопросам конфиденциальности и защиты данных. Получая доступ к закрытым базам данным, сотрудник обязан понимать степень ответственности. Следует обратить внимание на методическую выработку профессионального правосознания у сотрудников, с целью предупреждения превышения должностных полномочий, а также обучения этики использования данных.

Конфиденциальность информации напрямую зависит от проблемы законодательного регулирования. При слишком размытом трактовании нормы права либо же должностного регламента, сотрудник может получать доступ к информации, не входящей в его компетенции или не относящейся к материалам расследуемого им дела. Более четкая формулировка норм права, а также ужесточение предоставления доступа к банкам данных, также может стать фактором улучшения сохранности информации [2].

С появлением технологий и современного аппаратно-программного обеспечения в правоохранительных органах, масса возложенных обязанностей были автоматизированы либо значительно упрощены, но внедрение чего-либо нового всегда представляет собой ряд проблем. При комплексном подходе проблеме конфиденциальности и защиты информации можно будет значительно снизить с вектором направления стремящемся к нулю, но при условии, что всегда будут проводиться улучшения технологий, правил пользования и предоставления доступа к банкам данных и, что немало важно, комплексные повышения нравственных принципов и квалификации сотрудников правоохранительных органов, которые также включают в себя обмен опытом другими структурными подразделениями и органами государственной власти, которые сталкиваются с использованием информации о гражданах.

Список литературы

1. Демина Р. Е. Совершенствование организации и использования криминалистических учетов МВД России для успешного раскрытия преступлений // Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 2.
2. Малюгина А. В., Ануфриева А. Н. Возможности оптимизации и совершенствования деятельности полиции России, связанные с применением технологических инноваций (анализ зарубежного опыта) // European Journal of Natural History. 2020. № 4.

Жандров В. Ю.¹,
*доцент кафедры оперативно-разыскной деятельности
и специальной техники
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ЭЛЕКТРОННОЕ НАБЛЮДЕНИЕ В МЕХАНИЗМЕ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЯ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ

Развитие информационно-телекоммуникационных технологий (далее – ИТК) повлекло расширение возможностей их использования криминалитетом для повышения анонимности коммуникации и дистанционного совершения преступлений. Примечательно, что именно наркоторговля стала пионером использования инновационных ИТ-решений, которые начали апробироваться вовлеченными лицами уже в 2000 гг. В сфере незаконного оборота наркотиков (НОН) произошла трансформация способов сбыта запрещенных веществ, вследствие которой в их структуре стало преобладать бесконтактное проведение преступных сделок. Новый способ сбыта наркотиков исключил прямое физическое взаимодействие между покупателями и продавцами, поскольку оказался способен опираться на анонимные каналы связи, поддерживаемые новыми платформами обмена сообщениями, а также на использование цифровых валют для осуществления транзакций.

На фоне произошедших изменений практика документирования преступной деятельности фигурантов сформировала очевидный запрос на поиск новой тактики проведения оперативно-разыскных² мероприятий (ОРМ), методы которой соответствовали бы новым криминальным реалиям. Закономерным шагом на пути поиска новых подходов выявления и документирования НОН стало обращение внимания теории оперативно-разыскной деятельности (ОРД) к такому специальному методу расследования как электронное наблюдение.

Появление термина «электронное наблюдение» связывают с периодом действия «сухого закона» в США (1920–1930-е гг.), когда впервые в правоприменительной практике для борьбы с подпольным производством и торговлей алкоголем было использовано мероприятие «подслушивание телефонных переговоров» [7]. С течением времени появление разнообразных способов передачи информации сопровождало использование и новых негласных способов ее перехвата – «слухового контроля переговоров» и «видеоконтроля помещений и местности», которые также рассматривались в качестве способов электронного наблюдения.

Нормативное закрепление термина «электронное наблюдение» связывают с принятием Закона США 1978 г. «О контроле за внешней разведкой» [3],

¹ © Жандров В. Ю., 2024.

² Здесь и далее написание слова *разыскной* приводится в соответствии с нормами русского языка, за исключением употребления в нормативных правовых актах.

и последующим его распространением на расследование обычных преступлений Законом США 1986 г. «О конфиденциальности электронных коммуникаций (ЕСР) [4].

В международном праве термин «электронное наблюдение» впервые был использован ст. 20 Конвенции ООН против транснациональной организованной преступности (принята Резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 г.) [1], а затем воспринят и ст. 50 Конвенции ООН против коррупции (принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003) [2]. В обоих документах электронное наблюдение определено в качестве специального метода расследования по уголовным делам.

Именно в таком значении электронное наблюдение нашло свое отражение в актуализированном Управлением ООН по наркотикам и преступности в 2022 г. Модельном законе о взаимной правовой помощи по уголовным делам 2007 г. (в ред. 2022 г.) при формулировании положений об электронных доказательствах [5]. Определение упомянутого закона раскрывает «электронное наблюдение» через два вида мониторинга [6]:

- мониторинг, перехват, копирование или манипулирование сообщениями, данными или сигналами, которые хранятся, передаются или находятся в процессе передачи электронными средствами;
- мониторинг или запись деятельности с помощью электронных средств, а также любое скрытое участие в электронной связи с подозреваемыми, связанная с проведением агентурных мероприятий.

Обращение к международному опыту, практике законодательного регулирования зарубежных стран, а также возможностям современных информационно-телекоммуникационных технологий полагаем возможным в самом первом приближении очертить рамки электронного наблюдения следующими мерами:

- электронный мониторинг местоположения мобильного объекта;
- прослушивание телефонных переговоров;
- перехват актов коммуникации и мониторинг преступной активности в режиме online посредством удаленной активации камер и микрофонов электронных мобильных устройств;
- мониторинг социальных сетей, получение доступа к аккаунтам, подключение к наркорентированным онлайн-сообществам;
- получение и анализ данных из открытых электронных источников;
- получение контроля над ЭМУ для ознакомления с текстами сообщений и внутренней информацией устройства;
- зашифрованное участие в электронном общении с подозреваемым в совершении преступления с целью сбора доказательств или проверки оперативной информации.

Некоторые из перечисленным мер очевидно перекрываются положениями Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», который в ст. 6 закрепляет прослушивание телефонных переговоров, снятие информации с технических каналов связи и получение компьютерной информации в числе ОРМ. Безусловно, возможно расширительно трактовать

содержание регулируемых законом мероприятий, однако в реалиях неоднозначности соблюдения конституционных прав человека в цифровой среде этот подход может оказаться не вполне удачным и привести к их нарушению в рамках ОРД.

Различие между традиционным сбором цифровых данных в ходе уголовного судопроизводства и получением доказательств в Интернет заключается в методах и инструментах, используемых для проверки и аутентификации, в соответствии с требованием действующего законодательства. При этом простого создания снимков экрана или использования изображений с цифровой камер уже недостаточно для документирования преступлений в информационно-телекоммуникационной среде. В связи с чем встает проблема аутентификации (англ. *authentication* – «реальный, подлинный» – процедура проверки подлинности), которую необходимо решить в ходе проведения оперативно-розыскных мероприятий, чтобы обеспечить допустимость информации, хранящейся в электронном виде, для целей уголовного судопроизводства. Конечной точкой здесь будет являться надлежащее получение и процессуальное закрепление интернет-данных, выраженных в цифровой форме, хранящиеся на каком-то устройстве.

Вышеизложенное позволяет сформулировать ряд положений, имеющих значение для совершенствования механизма выявления и документирования незаконного оборота наркотиков:

1. В условиях цифровизации и стремительного развития ИТК неминуемой становится трансформация ОРД по противодействию НОН, осуществляемому бесконтактным способом. Данный процесс должен сопровождаться пересмотром тактики проведения ОРМ за счет расширения приемов и способов сбора электронных доказательств.

Поскольку действующее оперативно-розыскное законодательство не охватывает всех тех возможностей, которые предоставляют современные ИТК, постольку совершенствования механизма выявления и документирования НОН в современных условиях возможно достичь за счет развития теоретических и законодательных положений об электронном наблюдении как относительно самостоятельном методе ОРД, включающем перечень специальных мер по слежению, контролю и фиксации действий фигурантов с помощью современных ИТК.

2. Включение электронного наблюдения в российскую практику ОРД по противодействию НОН отвечает как новым вызовам в этой сфере, так и современной конфигурации правового обеспечения этой деятельности. Во-первых, расширение перечня специальных методов расследования за счет включения мероприятий, имеющих специфические функции, отражает объективно сложившуюся потребность правоохранительных органов в фиксации картины произошедших преступных событий в Интернет и смежной с ней цифровой среде. Во-вторых, Российская Федерация является участником ряда международных конвенций, предусматривающих электронное наблюдение в качестве специального метода расследования, в связи с чем в соответствии с принципами отечественной правовой системы и в пределах своих возможностей принимает необходимые меры для реализации положений ратифицированных документов, направленных на обеспечение надлежащего процесса сбора доказательств, в том числе электронных.

Список литературы

1. Конвенция Организации Объединенных Наций против транснациональной организованной преступности : принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 г. URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml.
2. Конвенция Организации Объединенных Наций против коррупции : принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003 г. URL: https://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml.
3. 50 Кодекс США, глава 36 «Надзор внешней разведки». URL: <https://www.law.cornell.edu/uscode/text/50/chapter-36>.
4. Electronic Communications Privacy Act of 1986 (ECPA). URL: <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285>.
5. Model Law on Mutual Assistance in Criminal Matters. URL: https://sherloc.unodc.org/cld/uploads/pdf/EI%20Evidence%20Hub/Model_Law_on_MLA_2007.pdf.
6. Типовой закон о взаимной помощи по уголовным делам (2007 г.), с поправками, включающими положения об электронных доказательствах и применение специальных методов расследования (2022 г.) (п. 7 р. 27 ч. 4). URL: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_31/CRP/E_CN15_2022_CRP6_e_V2202980.pdf.
7. Самохин Б. М., Князев В. В. Зарубежный опыт оперативно-розыскной деятельности в борьбе с преступностью : научный обзор. М.: ВНИИ МВД СССР, 1991.

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

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

АНАЛИЗ СУДЕБНОЙ ПРАКТИКИ ПО ДЕЛАМ, СВЯЗАННЫМ С НЕЗАКОННЫМИ ОРГАНИЗАЦИЕЙ И ПРОВЕДЕНИЕМ АЗАРТНЫХ ИГР

В современном обществе дела, связанные с незаконной организацией и проведением азартных игр, остаются актуальными и вызывают серьезные обсуждения в различных сферах. Правовые нормы стремятся эффективно бороться с подобными преступными явлениями, однако сложность их регулирования и непрерывно изменяющаяся природа преступлений создают вызовы для правоохранительных органов.

Анализ судебной практики в данной области является ключевым инструментом в понимании динамики преступлений, законодательных требований и эффективности принимаемых мер по предотвращению и пресечению незаконной азартной деятельности. В данной статье проведем обзор судебной практики, связанной с делами о незаконной организации и проведении азартных игр, с целью выявления основных тенденций, проблем и перспектив в этой области.

По законодательству существует легальное определение понятия «азартная игра» – основанное на риске соглашение о выигрыше, заключенное двумя или несколькими участниками такого соглашения между собой либо с организатором азартной игры по правилам, установленным организатором азартной игры [2, с. 4].

Судебная практика по ст. 171.2 УК РФ, касающейся незаконной организации и проведения азартных игр, демонстрирует важные тренды в динамике применения правовых норм.

Так, в 2021 г. прокуратурой г. Москвы было утверждено обвинительное заключение по уголовному делу в отношении 25 человек, обвиняемых в организации и проведении незаконных азартных игр. По результатам расследования установлено, что под видом лицензии на букмекерскую деятельность действовала организованная преступная группа из сотрудников крупной букмекерской конторы. В помещениях, где осуществлялась так называемая букмекерская деятельность, посетителям предоставлялась возможность делать ставки, указывать

¹ © Захарова А. М., 2024.

сумму ставки и, в случае выигрыша, участвовать в дополнительных играх через программу «Lotobet (Vloto)». Интерфейс данной программы типичен для игровых автоматов, таких как «Игрософт» и «Гаминатор». Сервер, с которого загружались азартные игры, находился на территории иностранного государства. Пять организаторов уголовной деятельности, включая генерального директора и четырех технических специалистов, а также управляющего игровым залом и 19 операторов игровых автоматов, привлечены к уголовной ответственности. Сторона защиты утверждает, что организация имеет лицензию на букмекерскую деятельность, и ставки принимаются только на реальные спортивные события. При этом статистика игр взята у иностранной компании, с которой имеется соответствующий договор [7].

На основе собранных данных был составлен график (рис. 1), который отображает количество осужденных по данной статье в течение последних пяти лет.

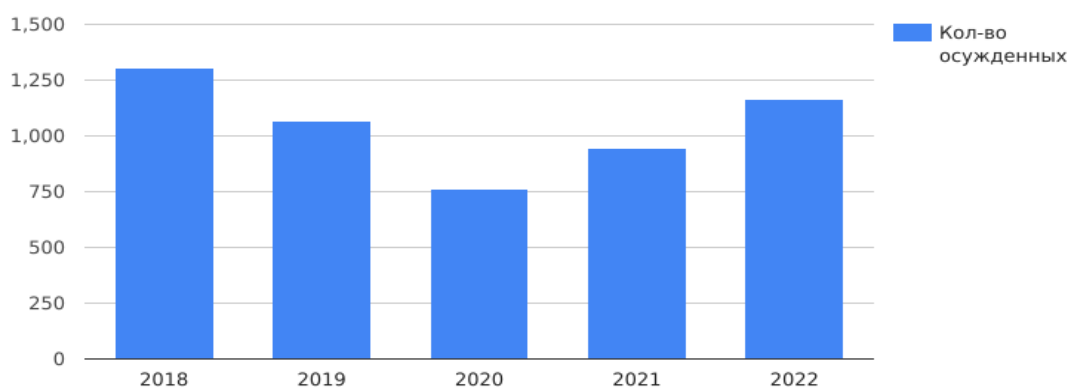


Рис. 1. График количества осужденных за период 2018–2022 гг.

Рассмотрим изменения в количестве осужденных и попытаемся выявить потенциальные причины и следствия этих изменений.

В 2018 г. был наивысший показатель в рассматриваемом периоде – 1306 осужденных. Это может быть связано с активизацией правоохранительных органов и ужесточением надзора за азартными играми, что привело к увеличению числа выявленных и дошедших до суда дел. В 2019 г. количество осужденных снизилось до 1067 человек. Понижение на 18 % по сравнению с предыдущим годом может быть обусловлено различными факторами, включая возможное улучшение законодательной базы, уменьшение числа незаконных игорных заведений в результате предыдущих мер применения правовых норм или же изменения в политике судов по отношению к таким преступлениям. А вот в 2020 г. снижение числа осужденных дошло до 762, что может быть связано с пандемией COVID-19, ограничениями на движение и сокращением социальной активности, в том числе и в сфере нелегальных азартных игр. В 2021 г. рост числа осужденных поднялся до 946 человек. Возможно, после снятия ограничений, связанных с пандемией, активность нелегальных игорных заведений возросла, что привело к увеличению количества преступлений. Ну и в 2022 г. количество осужденных

увеличилось до 1164 человек, что может указывать на возобновление тенденции роста активности в сфере нелегальных азартных игр или на повышенную эффективность правоохранительных органов в выявлении и пресечении таких преступлений [3; 4].

Из этого анализа видно, что количество осужденных по ст. 171.2 УК РФ колеблется от года к году, что может быть обусловлено как внешними факторами, так и изменениями в практике применения норм права. Это подчеркивает необходимость постоянного мониторинга ситуации и адаптации мер правового и оперативного воздействия для борьбы с нелегальными азартными играми.

Второй график (рис. 2) иллюстрирует региональные особенности пресечения деятельности по незаконной организации азартных игр.

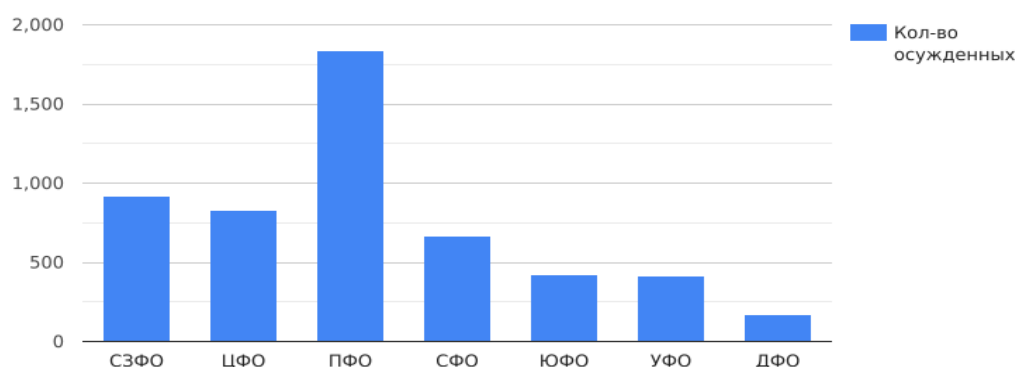


Рис. 2. График количества осужденных по федеральным округам за период 2018–2022 гг.

Из представленных данных можно провести общий анализ по количеству осужденных по ст. 171.2 УК РФ в различных федеральных округах России, что поможет оценить региональные различия в активности и эффективности пресечения незаконной организации и проведения азартных игр.

Приволжский федеральный округ (ПФО) выделяется среди других округов с наибольшим количеством осужденных – 1 834 человека. Это может указывать на высокую распространенность незаконных азартных игр в данном регионе или на повышенную активность деятельности правоохранительных органов.

Северо-Западный федеральный округ (СЗФО) и Центральный федеральный округ (ЦФО) также имеют высокие показатели – 917 и 829 осужденных соответственно. Эти данные могут отражать значительное внимание к проблеме азартных игр в экономически развитых и густонаселенных регионах.

Сибирский федеральный округ (СФО), Южный федеральный округ (ЮФО) и Уральский федеральный округ (УФО) имеют средние показатели – 669, 421 и 418 осужденных соответственно, что может свидетельствовать о меньшей распространенности проблемы или о различиях в методах борьбы с незаконной деятельностью.

Дальневосточный федеральный округ (ДФО) с 167 осужденными находится на нижней ступени данной статистики. В данном случае это может быть связано

с меньшим населением и удаленностью региона, что затрудняет организацию крупномасштабных незаконных игорных операций [3; 4].

Общий анализ показывает, что активность в сфере незаконных азартных игр и эффективность правоохранительных мер значительно варьируются в зависимости от региона. Это требует регионально адаптированных подходов в применении правовых норм и возможно, дополнительных ресурсов в более проблемных округах для усиления контроля и превентивных мер.

При изучении судебной практики по делам, связанным с незаконной организацией и проведением азартных игр, важно обратить внимание на роль программного обеспечения. Несмотря на строгость законов, появляются новые технические методы и средства, направленные на обход законодательства и проведение незаконных азартных игр. Популярностью особенно начинают пользоваться биржевые терминалы, которые используются в качестве игровых аппаратов или компьютеров с установленным на них специальным программным обеспечением для организации азартных игр. Рассмотрим несколько примеров программ и комплексов, упоминаемых в судебной практике по ст. 171.2 УК РФ:

1. Программное обеспечение «Лотос» - это клиентская программа, предоставляющая доступ к внутренним функциям, позволяющая выбрать анимацию и загрузить программное обеспечение, которое внешне аналогично игровому автомату типа «Игрософт» [5, с. 14].

2. Программное обеспечение «Мой вексель – вексельная система» сосредоточено на азартных играх, а не на торговле векселями. Взаимодействие пользователя с анимацией через интерфейс программы соответствует стандартному интерфейсу игровых автоматов типа «Игрософт». Возможность размещения ставок на различное количество линий, наличие таблицы с объяснением значений элементов анимации и возможность выбора размера ставки – все это присутствует как в программном обеспечении, так и в функциональности игровых автоматов «Игрософт» [5, с. 17].

3. Программный комплекс «MultiGame 2014» – это программное обеспечение, представляющее собой прикладную программу, которая дает доступ к функциям внутренних программ игровых автоматов «Новоматик». Интерфейс с анимацией, взаимодействие с которым осуществляется через кнопки программного обеспечения «MultiGame 2014», аналогичен интерфейсу игровых автоматов «Новоматик». Возможность делать ставки на количество линий, таблица с объяснением значений анимации и указание размера ставки делают программу идентичной программному обеспечению игровых автоматов «Новоматик» [6, с. 26].

4. Программный комплекс «StavkaBet» – прикладное программное обеспечение, обеспечивающее функции ставок на различные события и участие в азартных играх, которое состоит из клиентской части клиент-серверной системы. Клиентское приложение «StavkaBet» включает в себя программные модули и исполняемый файл «StavkaBet.exe», реализующие функции ставок и организации игр, а также возможность делать ставки на разное количество линий и задавать размер ставки [6, с. 28].

5. Программно-аппаратная платформа «Lotobet (Vloto)» – это программное обеспечение, которое предоставляет доступ к так называемой лотерейной платформе «Vloto». Эта платформа предоставляет пользователю возможности делать ставки на различные лотереи, с использованием анимации, схожей с той, что используется в игровых автоматах типа «Игрософт», «Гаминатор» [6, с. 30].

6. Программный комплекс «РАВК» (также известный как «Meteo Life») представляет собой игровое программное обеспечение, специализированное на организации и проведении азартных игр. Оно является клиентским приложением в рамках клиент-серверной системы «Meteo Life». Клиентская часть «РАВК (Meteo Life)» содержит программные модули, предназначенные для ставок на основе координат воздушных судов и метеорологических данных. Эти модули выполняют функции, характерные для игровых автоматов от «Игрософт» и «Новоматик» [6, с. 32].

Проанализировав судебную практику по ст. 171.2 УК РФ, можно сделать выводы о том, какие факторы влияют на динамику и эффективность борьбы с незаконной организацией азартных игр. Различия в применении правовых норм по регионам, влияние технологического прогресса, а также особенности и специфика организации азартных игр с использованием современных технологий требуют адаптации подходов и методов работы правоохранительных органов. Такой анализ способствует формированию целостного взгляда на проблему и разработке мер, направленных на улучшение ситуации в будущем.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.
2. Федеральный закон от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_64924/.
3. Судебные и нормативные акты Российской Федерации «СудАкт». URL: <https://sudact.ru/>.
4. Судебная статистика Российской Федерации. URL: <https://судебнаястатистика.рф/stats/ug/t/14/s/17>.
5. Методы идентификации программно-аппаратных средств организации и проведения азартных игр в Российской Федерации / [Л. В. Астахова и др.] // Наука, техника и образование. 2020. № 2 (55). С. 10–19.
6. Волков А. В., Лужнов В. С., Валяев Е. А. Методики исследования программно-аппаратных средств организации и проведения азартных игр в Российской Федерации // Наука, техника и образование. 2021. № 5 (69). С. 26–34.
7. Артемов А. Уголовная ответственность за незаконную игорную деятельность // Zakon.ru. 2020. 30 марта. URL: https://zakon.ru/blog/2020/3/30/ugolovnaya_otvetstvennost_za_nezakonnuyu_igornuyu_deyatelnost.

Захарова С. Е.¹,

*курсант Института-факультета подготовки сотрудников
для органов предварительного расследования*

Московского университета

МВД России имени В.Я. Кикотя

Научный руководитель: Стащенко С. П.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий*

Московского университета

МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ПРОФАЙЛИНГ КАК СПОСОБ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Наверное, каждый современный человек слышал термин «профайлинг»: при устройстве на работу, при просмотре социальных сетей или кабельного телевидения, но не все задумываются о значении данного термина. Дословно, в переводе с английского языка слово «profile» означает профиль, в широком же смысле это понятие, обозначающее совокупность психологических методов и методик оценки и прогнозирования поведения человека на основе анализа наиболее информативных частных признаков, характеристик внешности, невербального и вербального поведения. Другими словами, профайлинг – это составление психологического портрета человека. В правоохранительной деятельности составление психологического портрета преступника является неотъемлемой частью всего производства, и носит название психолого-криминалистический портрет. Широкий вклад в развитие данной области уголовно-правовых наук внес Ганс Гросс, основатель криминалистики, который предложил рассматривать личность преступника через призму совершенного им правонарушения. То есть, необходимо изучать способ совершения преступления для правильной характеристики личности преступника.

Так, доктор Пол Л. Кирк утверждал, что криминалистическое профилирование – естественный результат оценки материальных доказательств [2]. Часто встречается понятие «почерк преступника», которое как раз и обозначает способ совершения преступлений. Иными словами, изначально характеризуют способ совершения преступления, через который в последствии дают оценку личность самого преступника. Связано это с тем, что субъекту, ведущему расследование, изначально известно лишь о самом преступлении, без лица, логично что и оценка начинается с самого преступления: места, времени, обстоятельствах и способах его совершения, потерпевшего и следов преступления, и лишь потом, при обнаружении и задержании преступника начинается оценка его самого.

¹ © Захарова С. Е., 2024.

Несмотря на то, что термин «профайлинг» употребляется достаточно давно, в Российской Федерации до сих пор не создано никаких методологических и правовых основ его применения. В научной литературе часто встречается мнение о том, что «профайлинг» – слово иностранное, не совсем понятное и приятного для русского ума, поэтому его необходимо заменить более подходящим термином. Например, «психологическое профилирование». По моему мнению, это ошибочные суждения, так как самым важным в профайлинге, отличающим его от психолого-криминалистического портрета преступника, является то, что оценка преступника происходит без длительного и детального изучения личности, почти сразу. В данном случае имеет место известная пословица «Встречают по одежке...».

Закономерности запечатления внешнего облика человека, а также методы по собиранию, исследования и использования данных о внешнем облике человека изучает такой раздел науки криминалистики как габитоскопия. Из вышесказанного логично, что для собирания и изучения таких сведений необходимо время, что прямо противоречит сущности профайлинга, целью которого, в первую очередь является в определении экспрессивных выражений поведения, которые проявляются здесь и сейчас, в настоящий момент. Логическим выводом является то, что профайлинг в правоохранительной деятельности – это воссоздание мысленной модели преступника.

Учитывая современные тенденции развития общества, а именно цифровизацию, а в соответствии с этим размножения преступлений с использованием информационно-телекоммуникационных технологий, целесообразно использовать профайлинг при их расследовании.

Например, часто встречается ситуации, когда в социальных сетях создают страницу несуществующего человека и занимаются мошеннической деятельностью (продают какие-либо вещи, проводят конкурсы, предлагают работу и так далее). При одном взгляде на такую страницу становится ясно, что она является подставной. Во-первых, это можно понять по фотографиям, а если быть точнее – по их количеству, давности публикации и смысловой нагрузки, заключенной в них. Очень часто на таких страницах мало фотографий, они опубликованы недавно и на них либо не изображены люди, либо изображены, но это фотографии, взятые с других интернет-ресурсов. Информация на такой странице тоже представлена в ограниченном формате или ее вообще нет. Другими словами, оценивать при расследовании такого преступления необходимо страницу в социальной сети или на другой виртуальной площадке. Но информационный мир настолько плотно сосуществует с реальным, что представляется логичным в качестве объекта профайлинга использовать, например, профиль в социальной сети «ВКонтакте». Страницы в социальных сетях также можно использовать в качестве предмета изучения профайлина, при проведении проверочных, оперативно-розыскных и иных мероприятий предварительного расследования. Иногда, люди не понимают, как много информации хранят в своих профилях. Подписки, например, могут помочь узнать увлечения преступника или места наиболее частого посещения, так же, как и иные пользователи, которые взаимодействуют с изучаемым профилем.

Профайлинг в качестве метода изучения личности, можно использовать при проведении отдельных следственных действий. Например, при осмотре мобильного телефона, компьютера, планшета или иного устройства, имеющего «выход» в Интернет. Наиболее часто посещаемые сайты, приложения, точки вызова такси, фотографии, используемые программы могут оказаться необходимыми доказательствами по уголовному делу или следами совершения преступления.

Таким образом, профайлинг можно использовать не только при оценке человека вживую, но и удаленно, посредством изучения его активности в социальных сетях и используемых технических средств.

Список литературы

1. Gross H. Criminal Investigation. L., 1924.
2. Kirk P., 1953. Crime Investigation. Interscience, New York, NY. McNamara, J., Morton, 2007. Cracking the BTK Case. The RCMP Gazette 69.
3. Канузель А. Е. Криминальный профайлинг как способ составления и анализа личности преступника // Искусство правоведения. The art of law. 2023. № 2 (6). С. 55–59.
4. Психологические аспекты изучения личности преступника при расследовании преступлений / [А. В. Довгушева и др.] // Образование и право. 2023. № 7. С. 467–470.
5. Истомина А. С. Криминологический профайлинг: понятие и содержательные черты // Молодежь, наука и цивилизация. 2022. С. 484–486.

Ивлева Е. А.¹,

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

Воробьева Т. И.²,

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

РОЛЬ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

В век информационных технологий, когда цифровизация стала глобальным процессом, все большее значение приобретают электронные носители. Согласно ГОСТ 2.051–2013 [1], под электронным носителем понимается: «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники». К ним относятся: жесткие диски (HDD), твердотельные накопители (SSD), флеш-накопители, CD-ROM, DVD-ROM и т. д.

Современные средства хранения данных прочно вошли в сферу правоохранительной деятельности. Можно выделить следующие направления использования электронных носителей информации в деятельности органов внутренних дел:

- применение в качестве вещественных доказательств;
- хранение информации;
- работа с ИСОД МВД России.

Рассмотрим каждое из этих направлений подробнее.

Применение в качестве вещественных доказательств

Согласно ч. 7 ст. 185 УПК РФ [2], электронные носители информации могут быть осмотрены и подвержены изъятию в качестве вещественных доказательств, если есть основание полагать, что в них содержатся данные, имеющие значение для уголовного дела. Они всегда прилагаются к протоколу следственного действия.

Как показывает практика, электронные носители информации служат средствами совершения преступления и сохраняют в себе следы преступления (так называемые, цифровые следы). Поэтому, электронно-цифровой след используется для обнаружения преступления и установления обстоятельств уголовного дела [3]. Злоумышленник может оставить после себя историю посещения веб-сайтов, отправленные электронные письма, «засветиться» на камере видеонаблюдения. Чтобы достичь оперативного раскрытия преступления, правонарушения, сотрудники правоохранительных органов уделяют должное внимание электронным носителям информации. Так, при осмотре места происшествия

¹ © Ивлева Е. А., 2024.

² © Воробьева Т. И., 2024.

специалисты копируют или изымают данные, хранящиеся на электронных носителях, с мобильных телефонов, ноутбуков, видеорегистраторов и других электронных устройств. Это позволяет воссоздать наиболее полную картину совершенного правонарушения.

Хранение информации

Электронные носители информации являются удобным местом хранения данных. Современные носители информации обладают большим объемом памяти и позволяют хранить доказательства в различных видах (текст, фотографии, видео-, аудиозаписи и др.). Наиболее часто используются цифровые фотоизображения с места преступления.

В настоящее время правоохранительные органы применяют для раскрытия преступлений большое количество разнообразных банков данных, для хранения которых, также используются электронные носители на серверах. Такой способ хранения данных позволяет обеспечить сотрудников правоохранительных органов оперативным доступом к информации, а также оперативно обмениваться информацией между подразделениями и службами, что повышает эффективность их работы.

На съемных электронных носителях сохраняются и передаются материалы дела для производства экспертизы или направляются в суд материалы уголовного дела. Во время заседания суда составляется протокол, который может храниться на компьютере для удобства его дальнейшего использования.

Работа с ИСОД МВД России

Съемный электронный носитель (рутокен) используется для безопасного хранения сертификата и ключа электронной подписи для организации безопасного доступа к сервисам ИСОД МВД России без дополнительного ввода логина и пароля.

Таким образом, электронные носители информации используются на всех этапах расследования от обнаружения следов, до передачи документов дела в суд, а также при обеспечении информационной безопасности, что говорит об их важности в деятельности правоохранительных органов.

Список литературы

1. ГОСТ 2.053–2013 «ЕСКД. Электронная структура изделия. Общие положения» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/>.
2. Уголовно-процессуальный кодекс Российской Федерации от 18 января 2001 г. № 174-ФЗ (ред. от 01.04.2024) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/.
3. Льянов М. М. Понятие «электронные носители информации» применительно к расследованию преступлений // Юридическая наука и правоохранительная практика. 2023. № 3 (65). С. 74–81.

Игнашева В. 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*

ОПТИМИЗАЦИЯ РАЗВЕДКИ ПО ОТКРЫТЫМ ИСТОЧНИКАМ

В настоящее время реальный мир все больше и быстрее переходит в виртуальный. Люди делятся фотографиями с отдыха, работы, ставят друг другу «реакции» и выражают свое мнение в комментариях. В связи с этим появляется огромное количество не только информации, которая занимает весь Интернет, но и цифровых следов, помогающих в раскрытии преступлений. С каждым годом преступность в сети Интернет набирает обороты, появляются новые способы совершения преступлений, с которыми нужно бороться соответствующими методами. Один из таких методов – компьютерная разведка, она делится:

- на разведку в сети Интернет;
- разведку в сети передачи данных;
- разведку в защищенных компьютерных сетях.

Подтверждая вышеизложенные доводы, приведем в пример отчет Digital 2023 Global Overview Report: на начало 2023 г. в России насчитывалось 127,6 млн интернет-пользователей, проникновение Интернета составило 88,2 %. Пользователей социальных сетей в январе 2023 г. было 106 млн – это 73,3 % об всей численности населения.

Интересно также знать, что по данным «ТАСС» (российское государственное федеральное информационное агентство) сфера данных к 2025 г. достигнет объема данных в 175 зеттабайт (зеттабайт составляет 1 млрд терабайт).

Рассмотрим подробнее разведку в сети Интернет, или OSINT (Open Source Intelligence). Само понятие включает в себя информацию, которая распространяется узкой аудитории для решения конкретных задач. В контексте разведки в Интернете OSINT включает в себя получение и обработку информации разными методами. Источниками OSINT являются:

- поисковые службы (Яндекс, Google и др.);
- Web-сайты;
- социальные сети;
- доски с объявлениями торговых площадок (Avito, Юла и др.);

¹ © Игнашева В. С., 2024.

- Telegram-боты;
- специализированные программы поиска и анализа (Maltego, WireShark и др.);
- утекшие БД;
- теневой Интернет;
- специализированные поисковые службы.

OSINT также имеет некоторые преимущества перед другими видами разведки:

1. *Исследования и аналитика.* OSINT предоставляет доступ к широкому спектру информации, которая может быть использована для анализа рынка, конкурентной разведки, оценки общественного мнения и других исследовательских задач.

2. *Безопасность.* OSINT может использоваться для мониторинга и анализа угроз безопасности, включая отслеживание активности преступников, оценку потенциальных уязвимостей в системах и выявление потенциальных угроз.

3. *Разведка.* Для государственных и коммерческих организаций OSINT является важным инструментом для сбора информации о конкурентах, потенциальных партнерах или клиентах, а также о политических и социальных событиях.

4. *Проверка достоверности информации.* В эпоху фейковых новостей и дезинформации OSINT может служить инструментом для проверки достоверности информации, анализа источников и выявления манипуляций.

Важно заметить, что OSINT не является гарантом качественной разведки, так как имеет ряд недостатков:

1. *Неполнота данных.* OSINT может быть ограниченным или неполным из-за ограниченного доступа к информации. Некоторые данные могут быть защищены законом или ограничены правами доступа, что делает невозможным получение полной картины.

2. *Недостоверность информации.* Информация, полученная из открытых источников, может быть неточной или искаженной. Это может произойти из-за ошибок, умышленной дезинформации или простого недостатка проверки фактов.

3. *Отсутствие контекста.* Иногда данные из открытых источников могут быть представлены без контекста, что затрудняет их интерпретацию и анализ.

4. *Ограниченные методы сбора.* Осинт часто ограничен теми методами сбора информации, которые доступны публично. Некоторые важные данные могут быть недоступны или труднодоступны из-за технических или правовых причин.

5. *Недостаточная актуальность.* Информация из открытых источников может быть устаревшей из-за задержек в ее публикации или обновлении. В быстро меняющемся мире это может снижать актуальность и полезность данных.

6. *Потребление времени и ресурсов.* Сбор и анализ данных из различных открытых источников может потреблять много времени и ресурсов. Это может быть особенно проблематичным при работе с большими объемами информации.

В силу невозможности установления четких рамок исследуемого понятия возможно считать инструментами даже поисковые системы браузеров, однако существуют узкоспециализированные OSINT-сервисы. Приведем ниже группировку сервисов по объекту поиска:

- поиск по мобильному номеру телефона и imei (Kode.su, Spravportal, imei.info);
- поиск по ФИО (Foma.one, Milliard-Iudei);
- поиск по фотографии (search4faces, Metadata2go.com, Camgirlfinder.net, Maps&Directions, GeoTree);
- поиск по Интернету, ip, mac, доменам и поддоменам (AllDataFeeds.com, WHOIS, ip2geolocation, 2ip.ru);
- поиск по vin и регистрационному знаку автомобилей (VINformer, ФРИ, Автокод, ГИБДД.РФ, ФНП);
- телеграм-боты (@Vin01bot, Quick OSINT, Cerberus, Telescan).

Приведенные выше сервисы являются общедоступными для каждого пользователя и позволяют получить информацию бесплатно и быстро.

Например, создание агрегатора с такими сервисами поможет экономить время для поиска нужной информации, так как не придется искать подходящий сайт или телеграм-бот для поиска более полных и достоверных данных.

Таким образом, оставляя в Интернете цифровые следы, обычные пользователи и преступники открывают друг для друга, а также для сотрудников правоохранительных органов широкие возможности по поиску открытой информации. При этом необходимо четкое понимание о получаемых материалах из любого источника, так как неумение разграничивать объемы и достоверность данных не приведут к выполнению цели и получению желаемого результата.

Список литературы

1. Дворянкин О. А. Osint, pentest, нетсталкинг-информационные технологии интернета // НАУ. 2022.
2. Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Уральский юридический институт МВД России. 2023.
3. OSINT или разведка по открытым источникам. URL: <https://habr.com/ru/companies/deiteriylab/articles/595801/>.
4. OSINT: в чем опасность и как защититься. URL: <https://www.kaspersky.ru/blog/osint-open-source-intelligence/35955/>.

Калашникова А. А.¹,

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

Мишина А. А.²,

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

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

В последние годы наблюдается рост уровня преступности в Российской Федерации, что требует от сотрудников МВД России разрабатывать новые и эффективные методы борьбы с ней. В первую очередь правоохранительные органы применяют возможности инновационных информационных технологий, которые по своей сути направлены на выявление, предупреждение и пресечение противоправных действий. Отметим, что в современном мире преступники активно стали использовать новые технологии и преступные схемы в глобальной сети Интернет для совершения преступлений. Поэтому, проводимые сотрудниками мероприятия, должны соответствовать этим изменениям и обеспечивать эффективное получение информации о преступлениях и их участниках, где использование систем искусственного интеллекта (ИИ) позволяет решить данные проблемы.

Далее следует дать определение понятию «искусственный интеллект», под которым, по мнению Д. А. Степаненко следует понимать создаваемое с помощью группы смежных технологий программное обеспечение, функционирующее нелинейно, способное к обучению, ограниченному пониманию причинности и выполнению задач интеллектуального, эвристического характера с возможностью обучения, корректировки и уточнения за счет опыта принимаемых решений [1, с. 207–208]. Рассматривая использование существующих алгоритмов искусственного интеллекта для деятельности МВД России при выявлении преступлений, следует понимать, что под данным положением следует понимать комплекс мер по формированию, ведению, использованию и совершенствованию информационных систем при помощи технологий ИИ, который ориентирован на обеспечение сотрудников МВД России значимыми сведениями в виде систематизированной информации, необходимой им для осуществления возложенных на них задач. Исходя из данной трактовки, следует отметить, что основная сущность

¹ © Калашникова А. А., 2024.

² © Мишина А. А., 2024.

использования систем ИИ в правоохранительной сфере заключается в том, что благодаря накопленному ранее опыту информационная система создает новые и эффективные методы выполнения задач по выявлению преступлений.

Сущность использования ИИ в деятельности сотрудников МВД России заключается в том, что оно является неотъемлемой частью современного информационного обеспечения: позволяет сотрудникам, осуществляющих деятельность по выявлению преступлений, получить необходимую информацию для реализации целей, представленных на рис.

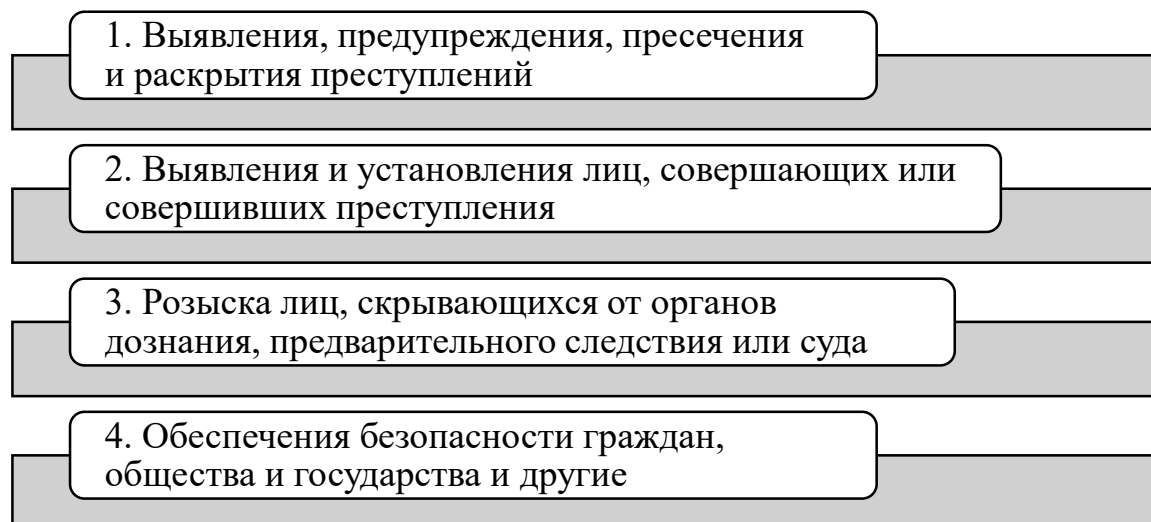


Рис. Цели использования ИИ в деятельности сотрудников МВД России

Далее отметим, что с развитием информационных технологий, увеличением пользователей, а также переходом нашей повседневной жизни в виртуальную реальность возникло множество проблем, связанных с желанием преступников воспользоваться современными информационными возможностями и технологиями для целей личного обогащения, появились новые преступные схемы и многие преступления стали совершаться с использованием информационных технологий. Все вышеперечисленное привело к необходимости создания новых методов и средств противодействия преступлениям и выявлению современных возможностей использования ИИ в деятельности сотрудников МВД России.

К сожалению, информационные системы использующие ИИ или программное обеспечение позволяющее обратиться к технологии ИИ в настоящее время имеют ряд сложностей, среди которых, на основании анализа имеющихся данных, выделим следующие:

1. Огромный объем информации, циркулирующей в сети Интернет и постоянное обновление такой информации.

Данное положение, безусловно позволяет сотрудникам получать необходимую информацию об преступлениях оперативно, но оно также затрудняет процесс выявления и сбора информации об преступлениях. Причина в том, что сеть Интернет является огромным информационным пространством, в котором ежедневно генерируется огромное количество данных, новостных блогов, комментариев, высказываний, которые необходимо вносить в информационную базу ИИ, обновлять такую информацию и анализировать, отсеивать лишнюю информацию, а это в свою очередь не только временные затраты, но и финансовые

(обеспечение финансирования соответствующего технологического и программного обеспечения) [3].

2. Проблема недостаточной точности модели ИИ.

Структура и сама система ИИ направлена на использование опыта прошлых лет, а также современных методик, но современные преступления обладают отдельными характеристиками и особенностями, которые могут завести ИИ в заблуждение, а это приведёт к неправильной оценке деятельности физического или юридического лица (ложное срабатывание системы).

3. Настройка соответствия гласных и негласных систем ИИ.

Так в деятельности МВД России при выявлении преступлений используются оперативно-разыскные¹ мероприятия, собирается секретная информация, анализируется информация, полученная от агентов и многое другое, что требует от существующих алгоритмов ИИ соблюдать режим секретности. К сожалению, в современности ИИ не предусматривает функции по работе с материалами ограниченного доступа, что создаёт вероятность распространения таких материалов на платформы открытого доступа.

Выделенные проблемы, по нашему мнению, являются основными, без решения которых невозможно эффективно использовать алгоритмов искусственного интеллекта в деятельности МВД России при выявлении преступлений. Неразрешённость данных проблем приведет как к техническим проблемам: выхода из строя ИИ или использование устаревших методик анализа преступной деятельности, так и к правовым: нарушению прав граждан, нарушению режима секретности, раскрытию конфиденциальных сотрудников и многому другому.

В качестве решения могут быть предложены следующие мероприятия, по устранению упомянутых проблем.

Для решения первой проблемы предлагается создать аналитическую базу, основанную на современных, высокоточных и высококачественных технологиях анализа огромных данных. В данной аналитической базе должны быть заложены определённые источники получения «свежей» информации о происходящих событиях в мире, а полученные аналитические данные и выбранные методики выявления преступности системой искусственного интеллекта, должны быть проверены специалистами в данной области. Каждое предположение и методика, выбранные ИИ должны пройти контрольное тестирование, как в процессе создания, так и в процессе функционирования.

В целях решения второй проблемы, предлагается разработать и внедрить определенные аналитические модели анализа деятельности ИИ. А именно следует собрать ряд специалистов данной области и разработать методы повышения точности модели ИИ, где рассматриваемые факторы и методы оценки должны быть проверены и иметь научное обоснование. Также следует использовать более сложные алгоритмы обучения системы ИИ, что достигается посредством применения методов машинного обучения, которые легли в основу создания ИИ.

Заключительная проблема требует особого внимания, так как имеет множественные способы решения, оценить эффективность которых, к сожалению, невозможно без тестирования. Первый способ решения проблемы заключается

¹ Слово *разыскные* приводится в соответствии с нормами русского языка.

в создании гласной системы ИИ и негласной системы ИИ. Такие системы следует разделить и дать доступ негласной системы к получению информации из гласной системы ИИ, а в обратном порядке запретить такой доступ в целях сохранения режима ограниченного доступа. Негласная система ИИ должна быть изолирована от других систем, но иметь доступ к получению данных из открытых систем, что позволит обновлять информационную базу такой системы. Она должна быть разработана так, чтобы исключить возможность распространения материалов ограниченного доступа на открытые платформы, но иметь возможность получать информацию из открытых источников. Данный способ требует значительных финансовых затрат.

Второй способ заключается в внедрении (или создании) такого программного обеспечения, которое позволит системе ИИ анализировать, обрабатывать, хранить и отправлять информацию с секретными материалами. Такие функции должны обеспечивать физическую и логическую изоляцию секретных данных от открытых данных, но такая программа будет доступна в одной информационной базе. Взлом такой базы будет доступнее по сравнению с первым способом, но и финансовые затраты будут значительно ниже.

Третий способ – отказ от работы с материалами ограниченного доступа в системе ИИ. Данный способ носит организационный характер и направлен на запрет сотрудникам МВД России работать с секретными данными в системах ИИ, нарушение чего повлечет наступление соответствующей ответственности. Дополнительно, в целях контроля процесса работы с подобного рода материалами следует создать соответствующую систему контроля деятельности сотрудников МВД России. Такая система контроля должна включать в себя процедуры согласования доступа к данным ограниченного доступа, а также механизмы отчетности о использовании этих данных, где будет устанавливаться контролер использования ИИ при работе с информацией.

В заключение следует отметить, что стремительное развитие информационных технологий обуславливает появление новых возможностей и способов подготовки и совершения преступлений, поэтому вопросы, связанные с информационным обеспечением и внедрением ИИ в деятельность МВД России, являются одними из ключевых и требуют особого внимания как со стороны руководства ОВД, так и руководства Российской Федерации.

Список литературы

1. Степаненко Д. А., Бахтеев Д. В., Евстратова Ю. А. Использование систем искусственного интеллекта в правоохранительной деятельности // Всероссийский криминологический журнал. 2020. № 2. С. 206–214.
2. Судебная статистика Российской Федерации. URL: <https://stat.xn----7sbqk8achja.xn--p1ai/>.
3. Таран А. Н., Огрыза А. В., Таран К. А. Кибермошенничество как источник теневой экономики и главная угроза 21 века // Евразийский юридический журнал. 2021. № 10 (161). С. 418–420.

Каримов А. К.¹,

старший преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета

МВД России имени В.Я. Кикотя

РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

Эффективная система защиты информационной среды – одна из важнейших задач, стоящих перед любой организацией. Данные используются для принятия различных решений, и от их достоверности и актуальности может зависеть дальнейшая судьба организации. Определение рисков информационной безопасности является основой в разработке эффективных систем защиты и методических рекомендаций по информационной безопасности для организаций.

Риски информационной безопасности можно объединить по каким-либо определенным критериям или характеристикам, зависящим от индивидуальных потребностей и требований каждой организации.

На сегодняшний день можно выделить основные риски информационной безопасности по следующим критериям:

1. Вероятность возникновения угрозы информационной безопасности – классификация возможных угроз, их источников, характеристик и вероятных последствий.

2. Характеристики ресурсов, связанных с информационной безопасностью – классификация ресурсов, определение важности ресурсов и защитных мер по их обеспечению.

3. Степень ущерба от реализации угроз – общая величина ущерба, категории ущерба, методы определения величины ущерба для каждой категории.

4. Уязвимости информационной безопасности – виды уязвимостей информационной безопасности, принадлежность к категориям уязвимостей.

5. Меры обеспечения информационной безопасности – определение мер защиты информационной безопасности по типу, виду, применяемым технологиям, применению.

Риск нарушения доступности зависит от надежности аппаратных и программных средств, используемых в работе информационных систем. Причиной возникновения нарушений является несоблюдение требований стандартов при создании и эксплуатации различных систем.

Нарушение целостности определяется вероятностью отказа оборудования и программного обеспечения, надёжностью алгоритмов аутентификации пользователей, которые имеют право на редактирование данных.

Риск нарушения конфиденциальности зависит от надежности алгоритмов аутентификации пользователей, соблюдения требований стандартов, эффективности организационной структуры.

По времени возникновения информационные риски можно разделить:

– на ретроспективные;

¹ © Каримов А. К., 2024.

- текущие;
- перспективные.

Ретроспективные риски – это риски, возникшие в прошлом, до реализации тех или иных управленческих решений.

Текущие риски характеризуются деятельностью компании в данный период времени.

Перспективные риски могут возникнуть в обозримом будущем в связи с реализацией будущих проектов компании. Анализируя риски, имевшие место в прошлом, их природу и меры по снижению, можно намного точнее прогнозировать текущие и перспективные риски.

В зависимости от среды, в которой возникают риски, их можно разделить:

- на внешние;
- внутренние.

Внешние риски – это те риски, которые не зависят от внутренних составляющих предприятия и не связаны напрямую с его деятельностью. Их уровень зависит от политической ситуации, состояния рыночной экономики, социального уровня населения.

Внутренние риски – это риски, зависящие непосредственно от персонала и деятельности организации.

По характеру угрозы риски могут быть:

- организационные;
- технические;
- природные.

Организационные риски связаны с деятельностью персонала, правилами работы (внутренняя организация работы).

Технические риски связаны с оборудованием, программным обеспечением, способами проектирования, разработки и эксплуатации информационных систем.

Природные – риски, не зависящие от деятельности человека и связаны в основном с активностью природных явлений (землетрясения, наводнения, бури и ураганы).

Учитывая последствия наступления рисков, можно выделить:

- допустимые;
- критические;
- катастрофические.

При этом допустимым будет риск, наступление которого принесет организации убытки, не превышающие ожидаемую прибыль, и деятельность предприятия будет продолжена.

При критическом риске организации грозят потери, превышающие ее прибыль, которые могут привести к потере всех средств, вложенных в реализацию проекта.

Катастрофический риск наносит предприятию ущерб, превышающий прибыль от деятельности организации. Кроме того, нанесенный ущерб превышает имущественное положение предприятия. К катастрофическим также относятся

риски, связанные с опасностью для жизни и здоровья человека или возникновением экологической катастрофы.

Основная цель подробного рассмотрения рисков информационной безопасности – наиболее полная детализация угроз. Только пристальный, взвешенный подход к определению всех потенциально возможных рисков позволяет создавать реальные системы информационной безопасности.

Список литературы

1. Акимова Г. А. Риски и их оценка на современном этапе развития // Менеджмент в России и за рубежом. 2018. № 1. С. 101–111.
2. Верещагин С. Н. Оценка рисков защиты информации в современных условиях // Безопасность информационных технологий. 2017. № 3. С. 40.
3. Вяткин В. Н., Гамза В. А., Маевский Ф. В. Риск-менеджмент : учебник. М. : Юрайт, 2015.
4. Петров А. И. Анализ рисков в системах защиты информации // Информационные технологии и безопасность. 2022. Т. 2. № 3. С. 10–14.
5. Уродовских В. Н. Управление рисками предприятия : учебное пособие. М. : Вузовский учебник : Инфра-М, 2017.

Киселева С. М.¹,

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

Научный руководитель: Полянская Е. П.,

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

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Искусственный интеллект (ИИ) – это широкий класс задач, возможность компьютера принимать действия, свойственные человеческому интеллекту. Технологии, основанные на ИИ, позволяют разрабатывать решения с гораздо более высокой эффективностью. Они способны реагировать на инциденты безопасности, автоматически оценивать актуальность и последствия инцидентов, а также мгновенно формировать соответствующий ответ в реальном времени.

Применение ИИ в современном мире в защите от кибератак является одним из главных направлений в информационной безопасности. Можно привести пример активного использования и внедрения методов искусственного интеллекта в банках: для определения мошеннических операций и сделок, которые осуществляются с целью обмана и незаконного получения финансовых ресурсов или иных ценностей применяется работа алгоритмов, при помощи которых происходит блокировка совершающихся операций. Эти алгоритмы основываются на геопозиционировании, на взаимодействии человека с другими лицами. Данная система может подсказать специалистам, похожи ли выполняемые действия на мошенническую транзакцию или нет. Еще один крупный класс использования методов машинного обучения в кибербезопасности – это расследование. Например, когда известны векторы атак, которые предпринимают злоумышленники и при этом есть большое количество различных матриц. В результате чего можно проделать операцию по обучению алгоритмов, которые будут оповещать происходит та или иная угроза или нет, и соответственно в итоге надо будет предпринимать конкретные меры. Также и при работе с изображениями искусственный интеллект нашел себе применение. Это, например, использование сверточных нейронных сетей, которые могут с помощью матрицы разлагать изображения и идентифицировать объекты. Данный метод применяется в определении фишинговых или мошеннических сайтов (если есть само название банка, его эмблема, то можно с помощью алгоритмов, условно, просматривая сайты, определить и выявить, что данная платформа нелегитимно использует в дальнейших

¹ © Киселева С. М., 2024.

мошеннических схемах похожую страницу, при помощи которой уже пытаются узнать персональные данные лица). Для того чтобы искусственный интеллект был способен обеспечить необходимый уровень защиты информации, он должен быть правильно внедрен, обучен и интегрирован в уже существующие системы. Важным аспектом развития общества является информатизация, которая приводит к тому, что люди все больше доверяют компьютерам свою важную персональную, финансовую, социальную информацию. Это вызывает вопросы обеспечения информационной безопасности на всех уровнях общественной системы – индивидуальном, групповом, государственном. Развитие и многофункциональность информационных технологий приводит к увеличению угрозы киберпреступности, поэтому борьба с ней уже не может осуществляться только силами человека, и важное значение приобретают защитные системы ИИ. На данном этапе развития информационного общества, киберпреступность применяет интеллектуальные системы, исходя из этого мы можем сделать вывод, что бороться с этой угрозой можно лишь, используя соразмерные по уровню технологичности меры. Большинство интеллектуальных систем основано на анализе отклонений, таких как увеличение объема специфического трафика, неудачные попытки аутентификации, паттерны (шаблоны) работы пользователей и обнаружение скомпрометированных учетных записей, которые смогли возникнуть в результате слабых мер безопасности, утечки пароля и фишинговых атак.

В наши дни активно идет разработка, усовершенствование и внедрение платформ с применением технологий искусственного интеллекта. Основные типы:

1. EDR (Endpoint Detection and Response) – платформа обнаружения атак на рабочих станциях, компьютерных устройствах, серверах и своевременное реагирование на них. В результате использования технологий искусственного интеллекта данного вида появляется возможность идентифицировать вредоносные программы, классифицировать угрозы и реагировать на них. Данная платформа принимает решение на основании анализа базы данных.

2. NDR (Network Detection and Response) – аналитические платформы, которые выявляют угрозы в сетевом трафике и автоматически реагируют на них посредством изменения конфигурации сетевых устройств.

3. UEBA (User and Entity Behavior Analytics) – это системы поведенческого анализа пользователей, которые обнаруживают случаи необычного поведения и в дальнейшем используют их для выявления внутренних и внешних угроз. Данная платформа позволяет автоматически отыскивать отклонения в поведенческих моделях для пользователей. Выявленные аномалии. Такое несоответствующее поведение может выявляться в целях управления доступом, мониторинга, защита конфиденциальных данных.

4. TIP (Threat Intelligence Platform) – с помощью искусственного интеллекта данная платформа может на ранних этапах, т.е. до взаимодействия с пользовательской системой, идентифицировать угрозы и своевременно устранять их алгоритмы TIP работают на базе большого количества различных данных (Data Lake) и индикаторов компрометации (IoC).

5. SIEM (Security Information and Event Management) – решения, осуществляющие мониторинг информационных систем, в режиме реального времени анализируют события безопасности, средств защиты информации. В данной системе накапливается большое количество данных из разных источников, а использование и применение технологий искусственного интеллекта дает возможность выявить угрозы эвристическими методами.

6. SOAR (Security Orchestration and Automated Response) – система, которая позволяет обнаруживать угрозы в информационной сфере, а также автоматически реагировать на выявленные угрозы.

7. Антифрод – это такая система, которая позволяет обнаруживать угрозы в бизнес-процессах, предотвращать мошеннические операции в режиме реального времени. Искусственный интеллект позволяет адаптироваться к изменению логики.

В современном мире стала распространяться такая угроза, как спуфинг. Данная противоправная деятельность направлена на выполнение сфальсифицированной аутентификации в системе (аутентификация при помощи биометрических данных и голосового ввода). Контрмеры, применяемые предотвращения этой угрозы, основываются на применении искусственного интеллекта. Методы, обеспечивающие безопасность в информационной среде от спуфинга нацелены на противодействие фальсификации голосовых данных человека. В наши дни, с развитием технологий, голосовой интерфейс стал очень востребованным в обществе. Широкое применение приобрели голосовые помощники. Они используются при управлении автомобилями, умными домами, применяются в платежных системах.

Выделяют некоторые методы защиты от спуфинга с использованием технологий, в которых применяется искусственный интеллект:

1. Интерактивная аутентификация. В связи с тем, чтобы обеспечить защиту доступа в систему новым, нерегулярным паролем, представляются интеллектуальные системы, использующие динамическую аутентификацию, т. е. пользователь должен взаимодействовать с системой непосредственно в процессе аутентификации.

2. Пользователь должен взаимодействовать с системой непосредственно в процессе аутентификации. Эта система осуществляет свою работу путем выявления дефектов и помех в голосовой записи, указывающих на синтетическую природу звука. В ее основе лежат различные методологии, поддерживаемые технологиями искусственного интеллекта таких как анализа кратковременных спектральных характеристик, нейронных сетей.

В нашу эпоху основная задача заключается в защите информации. Одним из возможных решений противодействия киберугрозам является внедрение технологий ИИ. Однако данные системы порождают массу рисков. Технологии машинного обучения стали также использовать и киберпреступники. Например, активно сейчас преступники применяют систему подделки голосов для мошеннических звонков и сообщений, для фишинга и хищения денежных средств. В итоге можно сказать, что широкое применение инновационных технологий ис-

пользуется как во благо, так и во вред. Для того, чтобы не возникали угрозы специалисты в области защиты информации, объединяя усилия, разрабатывают новые механизмы защиты персональных данных для систем искусственного интеллекта.

Список литературы

1. Афанасьева Д. В. Применение искусственного интеллекта в обеспечении безопасности данных // Системный анализ, управление и обработка информации. Известия ТулГУ. Технические науки. 2022. Вып. 2.
2. Russell S. Artificial Intelligence: A Modern Approach // Pearson Education India. 2015. P. 1164.
3. Taulli T. Artificial Intelligence Basics: A Non-Technical Introduction. 2-е изд. Apress, 2019. P. 200

Кравченко В. И.¹,

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

Научный руководитель: **Шурухнова Д. Н.,**
профессор кафедры административного права
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

ПРИМЕНЕНИЕ КОЛЛЕКТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

В контексте стремительного развития искусственного интеллекта (ИИ) актуален поиск новых сфер и возможностей его применения. Реальность автоматизации и оптимизации рутинных задач при помощи новейших технологий ИИ, таких как нейронные сети, не только доказана фактическими примерами, но и открыто признаётся Российским государством, что нашло свое отражение в Национальной стратегии развития ИИ [1]. Одной из сфер такого применения может выступать государственное управление.

Хотя само понятие «искусственный интеллект» обычно используется для обозначения компьютерных систем, способных выполнять задачи, требующие человеческого интеллекта, но в рамках Национальной стратегии развития ИИ значение термина расширяется, оно включает себя всю необходимую для применения ИИ информационную-инфраструктуру, что представляется более правильным.

Целесообразно рассматривать области применения ИИ в государственном управлении соответствии его функциями, а именно: правоисполнительной, правотворческой, организационной, координационной и правоохранительной [2, с. 40–41]. Определяя каждую область применения ИИ через функции государственного управления, можно сформулировать функции применения ИИ в указанной сфере. Формируются три подхода к методу реализации данных функций. Один представляется возможным обозначить как специализированный, когда ИИ рассчитан исключительно на обеспечение исполнения одной из перечисленных выше функций; второй – комбинированный, т. е. ИИ выполняет две и более функций; и – самый сложный – универсальный, в условиях которого от ИИ требуется полное обеспечения всех функций. Учитывая природу государственного управления, характерные для него черты оперативности и всеобъемлемости, именно создание универсального ИИ является наиболее подходящим подходом. Так как фактические требования к ИИ будут соответствовать требованиям к аналогичного органу государственной власти с широкой компетенцией, наделенному значительными государственно-властными полномочиями для обеспечения возможности выполнения поставленных целей и задач.

¹ © Кравченко В. И., 2024.

Идея использования универсального ИИ не нова, равно как и не нова идея создания некой универсальной утилиты или системы, что могла бы решить все проблемы человеческого общества, начиная от реальных попыток, таких как ОГАС в СССР и Cybersyn в Чили в сфере регулирования командной экономики, которые показали ненулевую эффективность [3, с. 48], заканчивая фантастическими теориями авторов художественных произведений. Одним из таких произведений является культовый анимационный сериал режиссёра Хидэаки Анно «Neon Genesis Evangelion» 1995-1996 гг. В нем автор описывает систему Magi (англ. *волхвы*) – трио суперкомпьютеров (в рамках данного исследования будем рассматривать их как ИИ), созданных ученым Наоко Акаги для управления штабом Nerv и городом Токуо-3 [4, с. 42; 5, с. 359; 6]. Данная система, по сути, является совокупностью искусственных интеллектов, иначе говоря, коллективным универсальным искусственным интеллектом (КУИИ), так как разноплановые решения принимаются в ходе мажоритарного голосования трех ИИ (для принятия решения КУИИ требуется минимум 2/3 голосов «за»): «Мельхиор», «Бальтазар» и «Каспар» (по именам волхвов из Нового Завета, что принесли новорожденному Иисусу Христу дары на Рождество) [7, с. 432].

В рамках фантастического сюжета произведения каждый ИИ является отражением части личности создателя: Мельхиор – Акаги как ученая; Бальтазар – Акаги как мать; Каспар – Акаги как женщина. Это имеет важное значение как для сюжета «Евангелиона», так и для данного исследования. Важной идеей такого КУИИ является создание из определенных компонентов «модели личности», способной принимать решения на основе всестороннего анализа и осмысления.

Так в рамках правоохранительной деятельности, Мельхиор – личность ученого подразумевает опору на факты, данные, практику, без учета эмоциональных, психофизических и прочих моментов. Бальтазар характеризуется как мать, принимаемые данной моделью решения можно воспринимать как решения взрослого человека по воспитанию своего ребёнка, основанные на материнской и отцовской любви, любви государственной, в какой-то степени основанные на конфуцианской философии. Бальтазар, исходя из своей природы, ориентирован на принятие решений как в пользу, так и против правонарушителя в случае, например, рассмотрения дела об административном правонарушении. Ни каждое правонарушение является достаточно общественно опасным и может быть признано малозначительным, а потому необязательно лицо должно подвергаться наказанию, но в то же время не исключается воспитательная функция юридической ответственности, необходимая для правильного формирования личности [8, с. 277]. Каспар, определяемый как женщина, может подразумевать совокупность идей защиты субъекта от негативных последствий правоохранительного процесса, а именно: защиту чести, достоинства, репутации и прочих моментов, которые могут оказать негативное воздействие на человека.

Аналогичная логика применима и в рамках принятия КУИИ иных управленческих решений. То есть, исходя из заложенных в модель личности идей, каждый компонент будет голосовать за тот или иной способ решения проблемы, как бы симулируя интерес (мотив), но в отличие от часто корыстных, обиденных интересов человека, интерес ИИ является высшей степени идейным: выбрать наиболее правильное с позиции модели личности управленческое решение.

Уже сейчас формируются реальные предпосылки для создания КУИИ, подобному системе Magi. По сюжету «Евангелиона», существовала ни одна система Magi, что может означать возможность децентрализации КУИИ, допустимость применения элементов роевого интеллекта, демонстрирующего невероятные успехи, уже реализовывающего аспекты КУИИ в государственном управлении [9]. В целом, при характеристике существующего опыта применения ИИ в праве и в принятии управленческих решений стоит отметить позитивные результаты [10; 11], хотя и существует мнение о невозможности полностью заменить в данных сферах человека. Более того, все активней ведется дискуссия о создании «цифрового государства» как системы сервисов ИИ.

Таким образом, для решения задач в сфере государственного управления именно коллективный универсальный искусственный интеллект является наиболее подходящей технологией. Некогда фантазии креативных авторов художественных произведений уже в ближайшее время могут стать частью нашей повседневной жизни.

Список литературы

1. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // НПП «Гарант-сервис». URL: <https://base.garant.ru/72838946>.
2. Попов Л. Л., Мигачев Ю. И., Тихомиров С. В. Административное право России. М. : Проспект, 2010.
3. Анализ опыта разработки и применения ОГАС и Киберсин как основа формирования современной цифровой экономики / [А. С. Добрынин и др.] // Лучшая студенческая статья-2019. 2019. С. 46–50.
4. 塚本鋭司. The Enigmatic Power of Neon Genesis Evangelion // 文明 21. 2022. №. 48. С. 35–48.
5. González T. L. Plot Summary of Neon Genesis Evangelion and Analysis of Character Interrelations // Anime Studies: media-specific approaches to neon genesis evangelion. Stockholm University Press, 2021. P. 353–364.
6. Evangelion Wiki. URL: <https://evangelion.fandom.com/ru/wiki/Magi>.
7. Волкова Е. А. Религиозные мотивы в современной японской анимации на примере сериала «Евангелион» // Гуманитарные науки в современном вузе: вчера, сегодня, завтра. 2022. С. 429–432.
8. Лёвина С. В. Воспитательная функция права и механизм ее реализации // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2010. №. 9. С. 272–279.
9. Быльева Д. С. Коллективный и искусственный интеллект // Вестник Мининского университета. 2023. Т. 11. № 2.
10. Стефанова Н. А., Сидорова Ю. В. Использование искусственного интеллекта для принятия управленческих решений // Вопросы устойчивого развития общества. 2020. № 2. С. 331–334.
11. Трофимов Е. В., Мецкер О. Г. Искусственный интеллект в праве и публичном управлении: опыт разработок и исследований. 2019. С. 32–40.

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

Научный руководитель: **Чурин Р. А.,**
 главный эксперт отдела компьютерных
 и радиотехнических экспертиз
 управления экспертиз цифровой и речевой информации
 Экспертно-криминалистического центра МВД России,
 преподаватель кафедры информационной безопасности
 учебно-научного комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя

КОНЦЕПЦИЯ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКОГО ПОДРАЗДЕЛЕНИЯ МВД РОССИИ

В расследовании и раскрытии преступлений огромную роль играют эксперты-криминалисты, чье заключение используется в качестве доказательства определенных фактов, раскрывающих события преступления согласно ст. 74 Уголовно-процессуального кодекса Российской Федерации (УПК РФ). Взаимодействие экспертов с другими подразделениями системы МВД, а также гражданскими организациями, имеющими право давать экспертное заключение, – это сложный и длительный процесс, регламентирующийся в первую очередь приказом МВД России от 29 апреля 2015 г. № 495дсп «Об утверждении Инструкции по организации совместной оперативно-служебной деятельности подразделений органов внутренних дел Российской Федерации при раскрытии преступлений и расследовании уголовных дел».

Наиболее тесное взаимодействие эксперты осуществляют со следователями, поскольку последние выносят постановление о назначении экспертизы и отправляют его в экспертно-криминалистическое подразделение МВД России (далее – ЭКП МВД России). Руководитель данных организационных структур назначает ответственного за выполнение экспертизы.

Эксперт, получив постановление и объект исследования, может столкнуться с некоторыми проблемами, в их числе:

- вопросы в постановлении о назначении экспертизы, выходящие за пределы компетенции эксперта;
- длительное согласование назначения экспертизы;
- предоставление лишних объектов для исследования;
- отсутствие разрешения на проведение экспертизы разрушающими методами исследования;

¹ © Крупинская С. Р., 2024.

– предоставление недостающего количества образцов для исследования и др.

Решение данных проблем требует дополнительного времени, так как постановление о назначении экспертизы или же объект исследования будут возвращены. В постановление будут внесены изменения, что, в свою очередь, увеличит срок получения заключения от эксперта.

Данные проблемы возникают в связи с тем, что эксперт – это лицо, обладающее специальными знаниями (согласно ст. 57 УПК РФ), и специфика его деятельности сильно отличается от работы следователя, который не обязан вникать в процесс исследования. Решение данных проблем есть, это налаженное взаимодействие следователей/дознателей с экспертами. Эксперт может и должен оказывать консультационную помощь следователю для того, чтобы их совместная работа дала результат, необходимый для выяснения событий и обстоятельств, способствующих раскрытию и расследованию преступлений. Для оптимизации процесса взаимодействия ЭКП МВД России с другими структурами МВД России, мы представляем концепцию распределенной информационной системы взаимодействия экспертно-криминалистических подразделений в системе МВД России.

Введем определение распределенной информационной системы, для более точного понимания представленной концепции.

Распределенная информационная система – информационная система, объекты данных и/или процессы которой распределены на две или более базы данных [1, с. 4]. В будущей информационной системе у каждого ЭКП МВД России, а также у органов внутренних дел, взаимодействующего с ними, будет база данных, в которую занесены сведения о сотрудниках и руководителях данных подразделений. База данных будет собирать и обрабатывать информацию о них, что позволит наладить взаимодействие между ними. В ходе развития ИСОД МВД России эта система может оставаться самостоятельной, или быть интегрированной в ЕАИС ЭКП МВД России.

Информационная система ЭКП МВД России даст следующие возможности:

1. *При составлении постановления о назначении экспертизы* у следователя будет возможность проконсультироваться по поводу правильности и корректности поставленных вопросов в режиме реального времени в отдельном чате с экспертом.

2. *Сведения о нагрузке сотрудника*. Сбор данной информации необходим на этапе распределения руководителем ЭКП МВД России экспертиз своим сотрудникам [4, ст. 63]. Будет учитываться информация о том, сколько на данный момент в производстве экспертиз у каждого сотрудника. Какое количество заключений составил тот или иной сотрудник за определенный промежуток времени. Данная информация позволит оптимизировать процесс проведения экспертиз и отслеживать переработку подчиненных. Также будет учитываться на каком роде/виде экспертиз специализируется сотрудник.

3. *Фото объекта исследования и статус проведения экспертизы*. Следующая функция позволит нам отслеживать процесс проведения экспертизы в соответствии со следующими этапами: «Регистрация экспертизы в системе», «На рассмотрении руководителя ЭКП МВД России», «Назначен ответственный

эксперт», «Формирование постановления», «Отправлено эксперту», «Проводится исследование», «Исследование завершено», «Исследуемые объекты в пути к следователю».

Далее более подробно рассмотрим каждый из статусов:

- *регистрация экспертизы в системе.* На данном этапе следователь может выбрать для себя наиболее подходящее ЭКП МВД России, где, по его мнению, быстрее и лучше сделают определенную экспертизу. Для этого он создает заявку на проведение экспертизы, в которой указывает обстоятельства дела, вид экспертизы, что направляется на исследование, комментарий следователя и ЭКП МВД России. В системе регистрируется заявка на проведение экспертизы, создается запись в базе данных, которая далее будет отображаться у всех участвующих лиц;

- *на рассмотрении руководителя ЭКП МВД России.* На данном этапе, руководитель ЭКП МВД России видит входящую заявку на проведение экспертизы и принимает соответствующее решение – отказ (возврат) или назначение ответственного эксперта [3, ст. 14]. В случае отказа указывается причина отказа. В статусе экспертизы у следователя будет отображаться «Отказано», а во вкладке «Подробнее» будет причина отказа и комментарий. Если же назначен ответственный эксперт, то экспертиза переходит в стадию 2;

- *назначен ответственный специалист.* Заявка на экспертизу появляется у ответственного эксперта, он может полностью ознакомиться с информацией и в случае необходимости связаться со следователем посредством телефонной связи или же уточнить интересующие вопросы в чате для согласования вопросов, которые будут поставлены в экспертизе. Эксперт к заявке с экспертизой пишет вопросы (в информационной системе в заявке на проведение экспертизы будет вкладка «Вопросы», где и будет происходить ввод данных) и заявка приобретает 3 статус;

- *формирование постановления.* На данной стадии у следователя в заявке на проведение экспертизы отображаются вопросы, сформированные экспертом. Если следователя не устраивают вопросы, либо эксперт что-то не включил в перечень, то заявка снова приобретает статус 2 и возвращается специалисту. Если же следователя всё устраивает, то наша система автоматически формирует электронную версию постановления с возможностью печати (все имеющиеся данные для формирования постановления есть в заявке на проведение экспертизы), следователь прикрепляет фотографии, исследуемого объекта и заявка получает статус 4;

- *отправлено эксперту.* На данном этапе у эксперта в заявке проявляется постановление, фотографии объекта до отправки и есть возможность сформировать шапку заключения (где указываются обстоятельства дела, вопросы, что представлено на исследование) и переместить заявку в статус 5;

- *проводится исследование.* На данном этапе эксперт проводит исследование. Прикрепляет фотографии упаковки и объекта исследования, который ему пришел. В случае несоответствия, представленных объектов их перечню в постановлении фиксируется в акте вскрытия упаковки либо в рапорте эксперта

[4, ст. 20, 22]. На его основании производство экспертизы приостанавливается. В статусе экспертизы у следователя будет отображаться «Приостановлено», а во вкладке «Подробнее» будет причина приостановления и комментариев. Если же объекты исследования совпадают и целостность упаковки не нарушена, то по окончании исследования эксперт прикрепляет файл с заключением и заявка приобретает статус 6;

– *исследование завершено.* Следователю приходит уведомление о завершении экспертизы, а в самой заявке он может ознакомиться с заключением эксперта. На данной стадии эксперт упаковывает объект исследования, фотографирует упаковку, прикрепляет их изображения в системе. Заявка приобретает статус 7;

– *исследуемые объекты в пути к следователю.* Эксперт отправляет объект исследования вместе с заключением и сопроводительным письмом лицу, назначившему экспертизу [4, ст. 45, 48]. В случае, если объекты не могут быть переданы почтовой связью, об этом информируется следователь, в его статусе отображается «Предметы не подлежат пересылке почтой», а во вкладке «Подробнее» будет причина и комментарий;

– *получено следователем.* На данном этапе следователь принимает отправленные документы и объекты.

4. *Шаблоны.* Предварительно в базах данных содержатся сведения о сотрудниках, в связи с этим следователь, указывая всю информацию по делу, автоматически формирует постановление о назначении экспертизы.

Реализация данной концепции распределенной информационной системы позволит усилить взаимодействие между подразделениями, исключить возникающие в процессе назначения и проведения экспертизы проблемы, сделать прозрачным мониторинг работы ЭКП МВД России и в целом оптимизирование данной деятельности приведет к ускорению процесса расследования, а следовательно и к повышению уровня безопасности страны.

Список литературы

1. ГОСТ 34.321–96. Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными: межгосударственный стандарт: дата введения 2001-07-01 / Межгосударственный Совет по стандартизации, метрологии и сертификации. URL: http://a-podkidyshev.ru/GOST/34_321-96.pdf.

2. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34481/.

3. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // НПП «Гарант-сервис». URL: <https://base.garant.ru/12123142/>.

4. Федеральный закон от 27 декабря 2018 г. № 511-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_372707/.

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

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И БОЛЬШИХ ДАННЫХ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

В настоящее время применение сквозных инновационных технологий, определенных в Концепции технологического развития на период до 2030 г.² [8], прежде всего, применение технологий искусственного интеллекта и больших данных (ТИИ и БД), является одним из основных факторов социально-экономического роста, повышения безопасности России, успешной цифровой трансформации государственного управления [9], и в частности, успешной цифровой трансформации МВД России.

Стремительно развивающейся современной тенденцией является внедрение и развитие ТИИ и БД в оперативно-служебной деятельности органов внутренних дел (ОВД) Российской Федерации, что гарантированно обеспечивает достижение заявленных основных целей Ведомственной программы цифровой трансформации МВД России на 2024 г. и плановый период 2025–2026 гг. [10]:

- повышение удовлетворенности граждан государственными услугами, в том числе цифровыми;
- повышение уровня надежности и безопасности информационных систем, технологической независимости информационно-технологической инфраструктуры от оборудования и программного обеспечения, происходящих из иностранных государств.

Одним из основных направлений применения ТИИ и БД в деятельности ОВД является обеспечение оперативного сбора, обработки и качественного анализа больших объёмов структурированных и неструктурированных данных из множества различных источников (ведомственных баз данных, баз данных других государственных органов власти, социальных сетей и т. д.). Эти технологии позволяют оперативно выявлять [1]:

- 1) закономерности и тенденции преступности;
 - 2) предсказать, где и когда могут произойти те или иные преступления;
 - 3) нивелировать социально-экономические и политические риски:
- манипулирования общественным мнением и экстремисткой пропаганды;

¹ © Кубасов И. А., 2024.

² Предварительный перечень сквозных технологий (технологических направлений): искусственный интеллект, включая технологии машинного обучения и когнитивные технологии; технологии хранения и анализа больших данных; технологии распределенных реестров; нейротехнологии, технологии виртуальной и дополненной реальностей; квантовые вычисления; квантовые коммуникации; новое промышленное и общесистемное программное обеспечение; геоданные и геоинформационные технологии; технологии доверенного взаимодействия; современные и перспективные сети мобильной связи.

- возникновения неконституционной «цифровой власти», нарушения конституционных прав человека;
- роста социальной напряженности в обществе и т.д. в целях предупреждения и профилактики преступности.

ТИИ и БД также применяются и в целях повышения эффективности раскрытия и расследования преступлений (в том числе, киберпреступлений). Так, алгоритмы машинного обучения могут использоваться для анализа больших объемов данных из социальных сетей и Интернета для выявления противоправной деятельности [2]. ТИИ и БД можно применять и для анализа больших данных с места преступления, таких как, например, анализа ДНК¹ [3].

Технология распознавания лиц, как одно из приложений ИИ, основанная на алгоритмах машинного обучения анализа черт лица и сравнения их с базой данных известных лиц, используется для идентификации подозреваемых в тех случаях, когда традиционные методы идентификации не помогли (подозреваемый в маске или находится в большом скоплении людей).

Тем не менее, несмотря на множество преимуществ использования инновационных технологий в деятельности ОВД, есть и некоторые проблемы, которые необходимо решить [4].

Одной из самых насущных проблем, связанных с применением ТИИ и БД, является возможность предвзятости. Системы ИИ учатся на эмпирических и (или) модельных («синтетических») данных, а это означает, что если данные необъективные или не релевантные, то и результаты системы ИИ будут предвзятыми, что может негативно повлиять на отношения граждан к ОВД из-за дискриминации какого-либо сообщества по национальному признаку, полу или религии [5]. Например, если система ИИ обучается на данных представителей определенной этнической группы, которые имеют больше судимостей среди других групп, то система ИИ, скорее всего, будет настроена против этой группы.

Проблемой является возможность неправомерного применения ТИИ и БД с нарушением конституционных прав граждан на неприкосновенность частной жизни. Крайне важно, чтобы ОВД применяли эти технологии этично и ответственно, имелись меры безопасности для предотвращения неправомерного использования. Если управленческие решения принимает только искусственный интеллект, становится сложно возложить на людей ответственность за их неправомерные действия.

Еще одна проблема применения ТИИ и БД – возможное отсутствие прозрачности. Алгоритмы, используемые в этих технологиях, часто являются проприетарными, поэтому часто сложно определить, как они работают и выявить ошибки в алгоритмах.

Следовательно, применение ТИИ и БД в деятельности ОВД имеет свои плюсы и минусы. Разработчикам предстоит создавать технологии, которым можно доверять в техническом (технологии надежные, точные, безопасные)

¹ ДНК – дезоксирибонуклеиновая кислота – макромолекула, обеспечивающая хранение, передачу из поколения в поколение и реализацию генетической программы развития и функционирования живых организмов. Геном человека составляет 3 млрд пар нуклеотидов.

и психологическом плане (технологии прозрачны, подотчетны, этичны). Система искусственного интеллекта должна быть доверенной, т. е. соответствовать ГОСТу Р 59276–2020 [11]. Высокий уровень доверия к нейросетевым решениям искусственного интеллекта должен достигаться обучением их по алгоритмам ГОСТа Р 52633.5–2011 [6; 12].

Кроме того, следует осознавать, что применение ТИИ и БД приводит к потере рабочих мест для одних специалистов и востребованность в специалистах в новых сферах ИТ-деятельности. Поэтому еще одним важным соображением является необходимость надлежащей подготовки и образования. Сотрудники ОВД должны быть обучены эффективному и этичному применению ТИИ и БД, а также должны быть осведомлены о потенциальных рисках и ограничениях таких технологий.

В настоящее время порядок применения единых стандартов и подходов к применению ТИИ и БД в деятельности ОВД в полном объеме не урегулирован, показатели эффективности ИИ-решений не определены. При этом инструменты искусственного интеллекта внедрены в рамках выполнения научно-исследовательских работ:

- «Зеркало (Верблюды)»;
- «Серия»;
- «Анатомия1»;
- «ДОЗОР»;
- в интеллектуальной модели прогнозирования преступлений «Виктория»;
- подсистеме «Опознавание (биометрическая идентификация)» программно-технического комплекса «ИБД-Ф».

Поэтому в соответствии с Планом (комплексом мероприятий) внедрения технологий искусственного интеллекта в деятельность ОВД (на 2023–2025 гг.), утвержденным заместителем Министра внутренних дел Российской Федерации генерал-полковником полиции В. Д. Шулика и разработанным ДИТСиЗИ МВД России, предполагается решение следующих приоритетных задач:

- упорядочивание информационных систем и сервисов МВД России с учетом входящих в их состав ИИ-решений;
- формирование наборов данных (датасетов) для обучения и тестирования нейросетевых моделей;
- выработка предложений по внедрению ИИ-технологий в информационные системы и сервисы МВД России;
- сопровождение опытно-конструкторских работ, в рамках которых внедряются технологии искусственного интеллекта.

В целях реализации данного Плана (комплекса мероприятий) могут быть рекомендованы для применения следующие ТИИ и БД:

- выявления признаков внутрикадрового монтажа видеоизображений с использованием нейронных сетей;
- прогнозирования негативных событий и чрезвычайных ситуаций, моделирование сценариев реагирования на них;
- обработки инцидентов информационной безопасности.

В ближайшей перспективе для решения отдельных оперативно-служебных задач ОВД могут быть применены следующие ТИИ и БД:

- контентного и семантического анализа текстов, в том числе для оценки психологического состояния их авторов и скрытых смыслов, заложенных в сообщениях;
- аутентификации субъектов доступа к компьютерной информации по клавиатурному почерку;
- установления криминалистически значимых фенотипических признаков человека на основе анализа биологического материала, изъятого с мест совершения преступлений [7];
- выявление признаков серийности преступлений;
- интеллектуальной поддержки планирования и принятия управленческих решений по проведению оперативно-профилактических и оперативно-разыскных¹ мероприятий;
- распознавания транзакций и сделок, имеющих признаки отмыывания денежных средств, полученных преступным путем, финансирования терроризма, а также операций на нелегальных рынках;
- построения виртуальных моделей мест преступления и их физического моделирования на основе 3D-печати;
- анализа действующих и разрабатываемых нормативных правовых актов на предмет наличия коллизий и выработки предложений по совершенствованию;
- создания киберфизических систем, основанных на интеграции вычислительных и физических синергетически увязанных ресурсов и др.

В заключение следует отметить, что интеграция ТИИ и БД в деятельность ОВД революционизирует практику раскрытия, расследования и профилактики преступлений. Применение этих технологий обладает огромным потенциалом для дальнейшего повышения эффективности охраны общественного порядка и обеспечения общественной безопасности.

Список литературы

1. Кубасов И. А. Инновационные технологии в противодействии экстремизму и терроризму // Информационные и телекоммуникационные технологии в противодействии экстремизму и терроризму : сборник научных трудов. Краснодар, 2021. С. 71–76.
2. Кубасов И. А., Лекарь Л. А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России // Труды Академии управления МВД России. 2023. № 3 (67). С. 154–161.
3. Кубасов И. А. Разработка методов ДНК-фенотипирования для расследования и раскрытия преступлений // Вестник Воронежского института МВД России. 2022. № 2. С. 166–172.

¹ Здесь и далее написание слова *разыскной* приводится в соответствии с нормами русского языка, за исключением употребления в нормативных правовых актах.

4. Кубасов И. А. Проблемные вопросы применения технологий искусственного интеллекта в деятельности органов внутренних дел Российской Федерации // Вестник Воронежского института МВД России. 2021. № 3. С. 180–186.

5. Кубасов И. А. Проблемные вопросы применения доверенных инновационных технологий в правоохранительной деятельности // Информатизация и информационная безопасность правоохранительных органов : сборник научных трудов. М. : Академия управления МВД России, 2023. С. 152–158.

6. Шапкин А. В., Кубасов И. А., Иванов А. И. Развитие отечественного нейросетевого искусственного интеллекта в защищенном исполнении // Вестник Воронежского института ФСИН России. 2019. № 4. С. 132–144.

7. Кубасов И. А. Алгоритмизация установления криминалистически важных фенотипических признаков человека на основе анализа его биологического материала, изъятого с места преступления // Расследование преступлений: проблемы и пути их решения. 2023. № 1 (39). С. 124–131.

8. Распоряжение Правительства Российской Федерации от 20 мая 2023 г. № 1315-р «Концепция технологического развития на период до 2030 года» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/documentcons_doc_LAW_447895/.

9. Распоряжение Правительства Российской Федерации от 22 октября 2021 г. № 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/documentcons_doc_LAW_399192/.

10. Распоряжение МВД России от 25 января 2024 г. № 1/724 «Об утверждении Ведомственной программы цифровой трансформации Министерства внутренних дел Российской Федерации на 2024 год и плановый период 2025–2026 годов».

11. ГОСТ Р 59276–2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения.

12. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа (входит в комплекс стандартов, устанавливающих требования к разработке и тестированию средств высоконадежной биометрической аутентификации).

Кузьминых А. В.¹,

*курсант Института-факультета подготовки сотрудников
для органов предварительного расследования*

Московского университета

МВД России имени В.Я. Кикотя

Задохина Н. В.²,

доцент кафедры информатики и математики

Московского университета

МВД России имени В.Я. Кикотя,

кандидат педагогических наук

СВЯЗЬ МЕЖДУ ТРАНСФОРМАЦИЕЙ ПРАВА И ИЗМЕНЕНИЕМ ПРАВОСОЗНАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВЕННЫХ ОТНОШЕНИЙ

Правосознание представляет собой способность общества осознавать смысл правовых норм, а также, что немаловажно, сознательно подчиняться нормативным предписаниям, которые закреплены в данных нормах.

Под цифровизацией общества, в свою очередь, понимается преобразование аналоговых процессов в цифровые, затрагивающее практически все сферы жизнедеятельности – от электронных средств платежа и смарт-часов до интеллектуальных помощников и автопилотируемых автомобилей. Влиянии цифровых технологий на развитие нормативной базы государства проявляется, в первую очередь, в том, что возникающие общественные отношения в цифровой сфере так же подлежат законодательному регулированию, а соответственно влекут за собой появление новых норм права, что способствует изменению правосознания общества. Очевидно, что так называемая «цифровая прививка» затрагивает многие отрасли права: гражданское, трудовое, административное, уголовное и др., что, в свою очередь, трансформирует нормативные акты, регулирующие общественные отношения в сфере медицины, экономики, информатизации и др., а также количество юридических норм, обеспечивающих эту регуляцию [2, с. 89].

Например, современный мир невозможно представить без электронных средств платежа, различных интернет-магазинов, маркетплейсов и иных интернет-сервисов, обеспечивающих высокоскоростной обмен информацией в режиме онлайн. Все эти и другие технологии, связанные информационным пространством, вошли в нашу жизнь и плотно укоренились в ней относительно недавно. Всего пару десятилетий назад о возможности оплаты покупок, не имея на руках наличных денежных средств, не могло быть и речи, а в настоящее время подобная процедура является обыденностью. Как известно, развитие технологии электронных платежей и внедрение ее в общественную жизнь повлекло достаточно большое количество противоправных действий, а поскольку норм права,

¹ © Кузьминых А. В., 2024.

² © Задохина Н. В., 2024.

регулирующих данную сферу, не существовало, то и законодательной защиты данных общественных отношений не существовало.

В последствии подобная ситуация была коренным образом изменена и в нормы права были внесены коррективы, которые закрепили ответственность лиц, совершивших преступления против объектов, относящихся к электронным средствам платежа. Так, например, в Уголовном кодексе Российской Федерации (УК РФ) появились следующие нормы: п. г ч. 3 ст. 158 УК РФ, которая установила ответственность за совершение тайного хищения электронных денежных средств. Кроме того, была установлена ответственность за совершение мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ) [1]. Вышесказанное подтверждает влияние процесса цифровизации на изменение законодательной базы государства, т. е. с возникновением новых технологий появляются и новые общественные отношения, которые необходимо регулировать при помощи новых норм права.

Другим примером может служить активно развивающаяся система автопилота для гражданских автомобилей. Инженерные отделы компаний, особенно преуспевающих в развитии данной технологии («Мерседес», «Тесла»), занимаются разработкой программного обеспечения уже для системы автопилота третьего уровня. Но, несмотря на данный прогресс, все еще можно наблюдать существенные пробелы законодательства, связанные с решением вопроса об ответственности, если автомобиль с системой автопилота попадёт в ДТП со значительными последствиями в виде материального ущерба либо гибели участников дорожного движения. Очевидно, что на фоне развития нормативной базы, связанной с появлением беспилотных автомобилей, правосознание общества может измениться в силу того, что гражданам будет необходимо дополнительно изучать законодательные предписания, регулирующие правила дорожного движения с использованием автопилота. В этой связи будет затронута познавательная функция правосознания.

Очевидно все вышеуказанные примеры позволяют наблюдать явное влияние процесса цифровизации на трансформацию права, а также на изменение правосознания населения. Влияние данного процесса на трансформацию права проявляется, прежде всего, в том, что с появлением новых общественных отношений, связанных с цифровыми технологиями, правовая система реагирует на это возникновением новых норм права, что в свою очередь делает всю систему законодательства более приспособленной к защите прав и свобод человека и гражданина в стремительно изменяющихся условиях.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 24.02.2024) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_10699/.
2. Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85–102.

Куриленко Ю. А.¹,

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

АКТУАЛЬНЫЕ ВОПРОСЫ ВЗАИМОДЕЙСТВИЯ ГОСУДАРСТВ – ЧЛЕНОВ ОРГАНИЗАЦИИ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ В РЕШЕНИИ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организация Договора о коллективной безопасности (ОДКБ, в 1992 г. – ДКБ) изначально взаимодействовала в основном с целью военно-политического союза стран-участников на постсоветском пространстве. В связи с процессами, происходящими в мире в различных сферах развития человечества, ОДКБ стала уделять вопросам противодействия современным вызовам и угрозам значительное внимание. С 2006 г. началось активное развитие системы информационной безопасности. За сравнительно небольшой промежуток времени Советом коллективной безопасности ОДКБ было принято более 10 нормативных правовых актов. При Комитете секретарей советов безопасности ОДКБ была сформирована рабочая группа по вопросам информационной политики и информационной безопасности.

С 2009 г. получили реализацию практические мероприятия по противодействию криминала в сфере информации (операция «ПРОКСИ»). Основной целью «ПРОКСИ» являлось выявление и пресечение угроз национальной и коллективной безопасности государств-членов ОДКБ в сети Интернет.

В декабре 2014 г. был подписан Протокол о взаимодействии государств – членов ОДКБ по противодействию преступной деятельности в информационной сфере. В это же время принято решение о создании Консультационного координационного центра Организации Договора о коллективной безопасности по вопросам реагирования на компьютерные инциденты (ККЦ ОДКБ). Данным центром проведена работа по определению перечня важных национальных объектов информационной инфраструктуры, организован процесс взаимного информирования о кибератаках [1].

В 2016 г. была разработана Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года, где одной из основных задач определялось формирование безопасного пространства в информационной сфере между государствами – членами ОДКБ [2].

Отдельной проблемой выделено в 2018 г. понятие информационного противодействия терроризму и экстремизму и на 11 заседании Ассамблеи ОДКБ был принят Модельный закон «Об информационном противодействии терроризму и экстремизму» [3].

¹ © Куриленко Ю. А., 2024.

В 2022 г. Совет министров иностранных дел ОДКБ и Комитет секретарей Советов безопасности ОДКБ приняли решение о проведении профильных межведомственных консультаций по тематике международной информационной безопасности.

В ноябре 2023 г. ККЦ ОДКБ в рамках заседания совместно с участниками государств – членов ОДКБ обсудили важные вопросы информационной безопасности, в частности, увеличение числа кибератак с интенсивным привлечением различных организаций, а также высокой квалификацией исполнителей данных атак, высказана обеспокоенность об угрозах, связанных с утечками данных физических и юридических лиц [4].

27 марта 2024 г. при участии делегаций представителей национальных уполномоченных органов по вопросам противодействия преступлениям в сфере информационных технологий государств-членов ОДКБ состоялось заседание руководителей, полномочных представителей руководителей национальных штабов по проведению операции «ПРОКСИ».

В ходе заседания были определены основные направления по противодействию криминальным проявлениям в сфере информационных технологий. Среди них были выделены:

- противодействие использованию сети Интернет для распространения информации, которая наносит политический ущерб национальным и союзническим интересам, дестабилизации внутривнутриполитической обстановки, разжиганию межнациональной и религиозной розни;
- противодействие деятельности преступных групп террористической и экстремистской направленности и распространению информации, в том числе в сети Интернет, связанной с привлечением граждан государств – членов Организации к участию в вооруженных конфликтах, в террористических и экстремистских организациях, в реализации угроз лжетерроризма и источников подобных сообщений;
- противодействие противоправной деятельности по незаконному обороту наркотиков, осуществляемой с использованием информационно-коммуникационных технологий и интернет-пространства;
- противодействие совершению электронного мошенничества;
- противодействие созданию, использованию и распространению вредоносных программ, а также выявление программного обеспечения, аппаратно-программных комплексов, пресечение противоправной деятельности международных и иностранных хакерских группировок, осуществляющих противоправную деятельность в сети Интернет, а также компьютерным атакам на критическую информационную инфраструктуру [5].

Важной задачей ОДКБ также является подготовка специалистов, в том числе по направлению обеспечения безопасности в информационном пространстве. В настоящее время на безвозмездной основе, либо на льготных условиях слушатели государств – членов Организации проходят обучение в вузах различных ведомств России, Беларуси, Казахстана.

Список литературы

1. История создания, основы деятельности, организационная структура. URL: https://odkb-info.org/about_odkb/ot-dogovora-k-organizatsii/.
2. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года. URL: https://odkb-csto.org/documents/statements/strategiya_kollektivnoy_bezопасnosti_organizatsii_dogovora_o_kollektivnoy_bezопасnosti_na_period_do_/#loaded.
3. Модельный закон ОДКБ 30 октября 2018 г. № 11-3.3 «Об информационном противоборстве терроризму и экстремизму» URL: <https://paodkb.org/documents/modelnyy-zakon-odkb-ob-informatsionnom-protivoborstve-terrorizmu>.
4. Новости. 24.11.2023. О XVI заседании Совета Консультационного координационного центра Организации Договора о коллективной безопасности по вопросам реагирования на компьютерные инциденты. URL: https://odkb-csto.org/news/news_odkb/o-xvi-zasedanii-soveta-konsultatsionnogo-koordinatsionnogo-tsentra-organizatsii-dogovora-o-kollektiv/#loaded.
5. Новости. 29.03.2024. Состоялось заседание руководителей национальных штабов по проведению операции «ПРОКСИ». URL: https://odkb-csto.org/news/news_odkb/sostoyalos-zasedanie-rukovoditeley-natsionalnykh-shtabov-po-provedeniyu-operatsii-proksi/#loaded.

Кутергина Е. М.¹,
курсант Института-факультета судебной экспертизы
Московского университета
МВД России имени В.Я. Кикотя

Дядык Е. С.²,
преподаватель кафедры информатики и математики
Московского университета
МВД России имени В.Я. Кикотя

ВОЗМОЖНОСТЬ АВТОМАТИЗАЦИИ РАСЧЕТОВ ПРИ ПРОИЗВОДСТВЕ ПОРТРЕТНОЙ ЭКСПЕРТИЗЫ

Портретная экспертиза является одним из видов криминалистических экспертиз. Ее производство осуществляется на основании приказа МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» [1].

Суть данной экспертизы заключается в установлении личности разыскиваемого лица. Этот процесс осуществляется путем сравнения признаков внешности, запечатленных на различных носителях информации, таких как фотографические изображения или фрагменты видеозаписей.

Одним из методов портретных исследований является вероятно-статистический метод сравнения [2]. В рамках рассматриваемого метода эксперт выявляет признаки внешности, которые являются относительно редко встречающимися. Выявленные характеристики внешности обладают различной идентификационной значимостью в зависимости от частоты встречаемости. Эксперт перечисляет все выявленные при использовании данного метода признаки в соответствующей таблице с указанием числового значения идентификационной значимости и индекса. Кроме того, некоторые признаки обладают взаимной зависимостью. Далее эксперту необходимо выявить взаимозависимые признаки, имеющие наименьшую значимость. Заключительным этапом использования рассматриваемого метода является подсчет суммарной идентификационной значимости совокупности совпадающих признаков, за исключением взаимозависимых признаков. Для обоснования решения о достаточной совокупности признаков внешности для вывода о наличии тождества человека, изображенного на исследуемых портретах, необходима сумма не менее 6,1 единицы.

На данный момент расчет идентификационной значимости производится экспертом вручную. Однако данные вычисления могут быть автоматизированы посредством использования электронных таблиц [3] при производстве портретного исследования с помощью вероятно-статистического метода.

С помощью подобных программных продуктов возможно создать базу данных, включающую в себя исходные табличные данные с указанием значений

¹ © Кутергина Е. М., 2024.

² © Дядык Е. С., 2024.

идентификационных признаков [2, с. 60–88]. В таком случае эксперт, анализируя сравниваемые изображения, сможет выявить те признаки внешности, которые присутствуют в обозначенной таблице и отметить их в разработанной электронной форме, после чего они автоматически будут внесены в заранее подготовленную отчетную таблицу. После того, как все признаки, имеющие отображение на исследуемых изображениях внесены в итоговую форму, лицом, производящих портретное исследование, может осуществляться подсчет суммарной идентификационной значимости. При этом автоматически с помощью электронных таблиц будут исключаться признаки, имеющие взаимную зависимость и имеющие меньшую идентификационную значимость.

В данном методе можно выделить ряд преимуществ, среди которых следует выделить следующие:

- увеличение скорости производства экспертизы;
- уменьшение количества вводимой вручную текстовой информации за счет выбора признаков из списка возможных значений;
- автоматическое заполнение полей таблицы, которое связано с помощью формул со списком признаков, описанных выше, для дальнейшей вставки в экспертное заключение;
- повышение точности расчетов.

Для удобства использования данной программы предлагается разработать два варианта электронных таблиц: в формате *.xlsx для использования в офисных приложениях Microsoft Office и в формате *.ods, характерном для офисных приложений LibreOffice. Поскольку на сегодняшний день трудно говорить о полной совместимости файлов, в том числе электронных таблиц, между рассматриваемыми офисными программными продуктами, а также учитывая переход МВД России на использование российского программного обеспечения, целесообразно создать указанные два документа. Это подтверждается тем, что часть экспертов продолжают работать с Microsoft Office, а некоторые из них уже использует LibreOffice, входящий в состав российской операционной системы Astra Linux.

Таким образом, использование автоматизированных таблиц позволит подготовить выявленные признаки, приведенные в справочной литературе [2, с. 60–88], для вставки в заключение эксперта и исключить ошибки при математических вычислениях.

В заключение следует отметить, что у экспертов может возникнуть при производстве портретной экспертизы ряд проблем. В свою очередь, автоматизация данного метода позволит в полуавтоматическом режиме заполнять таблицы выявленных признаков, а также безошибочно производить вычисление суммарной идентификационной значимости признаков внешности.

Список литературы

1. Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» // СПС «Консультант-Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_55315/.
2. Зинин А. М., Кирсанова Л. З. Криминалистическая фотопортретная экспертиза : учебное пособие / под ред. В. А. Снеткова, З. И. Кирсанова. М. : ВНКЦ МВД СССР, 1991.
3. Обработка статистических данных в табличном процессоре libreoffice Calc : учебно-методическое пособие / [И. А. Нестеров и др.]. Саратов : КУБиК, 2023.

Линев Н. В.¹,

магистр кафедры стратегических информационных исследований
Национального исследовательского ядерного университета
Московского инженерно-физического института

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПАССИВНЫХ МЕТОДОВ ПОДАВЛЕНИЯ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ

Большим расстоянием «опасного» информационного сигнала является зона R2, или зона ПЭМИ. ПЭМИ создается вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы. Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому непреграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Схема перехвата информации за счет ПЭМИ приведена на рис. 1.

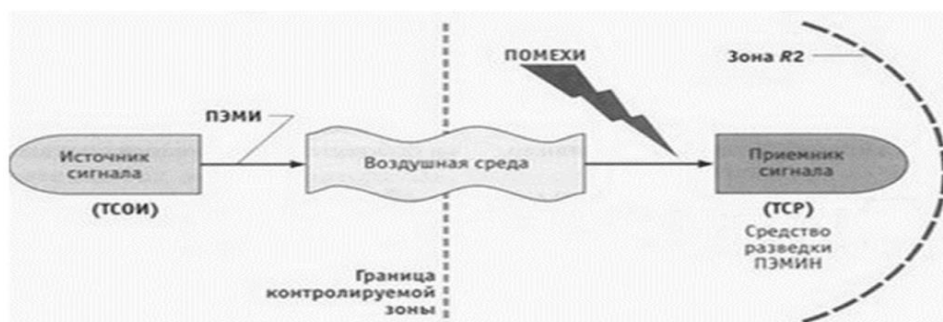


Рис. 1. Схема технического канала утечки информации за счет ПЭМИ [1, с. 20]

Физические свойства ПЭМИ по видеотракту и описание источников «опасных» информативных сигналов (зоны R2). Важно понимать, что основной информативностью ПЭМИ обладает информационный сигнал по видеотракту. Он осуществляется через включенное состояние экрана монитора автоматизированного рабочего места по видеоинтерфейсу (VGA, DVI, HDMI, DP), а также по матричной составляющей самого монитора (LVDS, e-DP). Сама физика сильного сигнала видеотракта объясняется тем, что устройства видеотракта, включающие видеоконтроллер, соединительные кабели, KVM-коммутаторы (при необходимости систем с несколькими отображениями информации) и конечные

¹ © Линев Н. В., 2024.

устройства отображения чрезмерно влияют на уровень сигнала и его направление излучения, потому как выступают в качестве антенн. Антенные сигналы возникают в задней части монитора на шлейфе его матричного интерфейса и в щелях по периметру железной закрывающей крышки, под которой находятся платы. Также антеннами выступают информационные кабели соединения. Более подробно, источники «опасных» информативных сигналов по видеотракту монитора продемонстрированы на рис. 2.

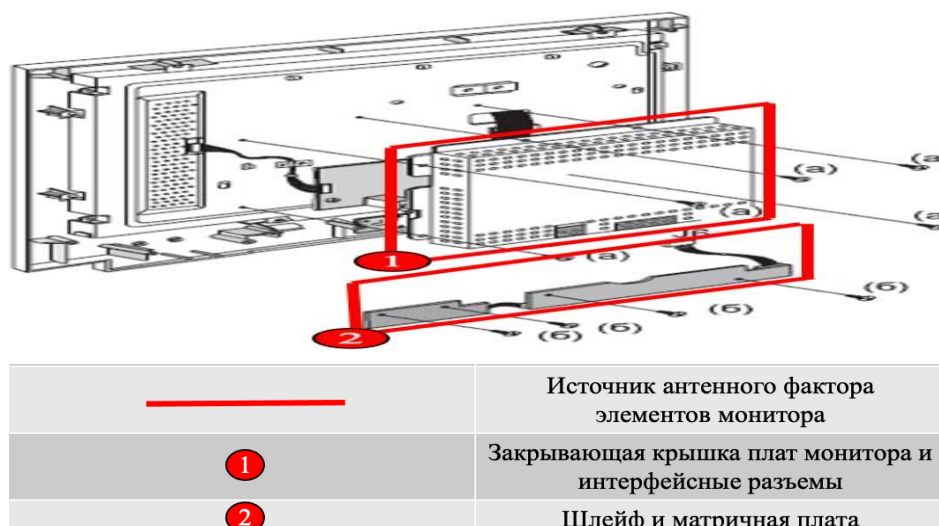


Рис. 2. Источники «опасных» информативных сигналов внутренней части монитора и его интерфейсных разъемов по видеотракту

Материнская плата имеет в себе также интерфейсные разъемы, а значит, как было описано выше, обладает теми же свойствами «опасного» сигнала через антенный фактор видеоинтерфейса и соединительные информационные линии. По лабораторным исследованиям, более опасным антенным фактором интерфейсного разъема считается тот, который чуть поднят над платой за счет увеличения размера самого интерфейсного разъема VGA на рис. 3. Подробнее источники «опасных» сигналов по видеотракту материнской платы приведены на рис. 3.



Рис. 3. Источник «опасных» информативных сигналов интерфейсных разъемов материнской платы по видеотракту

Главный вопрос заключается в возможности уменьшения зоны R2 при помощи определенной технологии. Возможно ли уменьшить зону R2 у видеотракта и при этом сохранить качество изображения на экране монитора? Ответом служит метод доработки изделий по уменьшению радиуса зоны R2, r_1 (r_1'). Забегая вперед, подобного рода технология, специальный рабочий материал, а также квалифицированные сотрудники могут обеспечить уменьшение зон в 1,5–2 раза.

Метод доработки ТС по уменьшению «опасных» информативных сигналов видеотракта (зоны R2). Как было сказано выше, антенный фактор элементов монитора и материнской платы по видеотракту может сыграть ключевую роль в распространении и усилении сигнала ПЭМИ. Как же уменьшить или вовсе подавить распространение «опасного» сигнала по видеотракту? В физике есть свойство так называемого экранирования. Экранирование, по сути, это надежное конструктивное средство, позволяющее ослабить определенное излучение. Самым простым примером является использование обычной фольги и сотового телефона. При полном помещении сотового телефона в фольгу, электромагнитное излучение от последнего будет экранироваться внутри, не выходя на связь с сотовой вышкой. Данные физические свойства экрана при помощи определенных металлов являются ключевыми в методе доработки изделий.

Но доработка не ограничивается одной лишь фольгой. Было придумано разнообразное количество материальных средств доработки изделий (токопроводящая ткань, проводящая тканевая лента с медно-никелевым покрытием, медная проводящая лента, экранирующая краска и т. д.). При данном разнообразии существует множество методов доработки изделий.

Ниже будет приведен метод доработки изделий по видеотракту с использованием материальных средств экранирования и его оптимизацией по выбору надежного материала и цены экранирующих средств.

Суть дальнейшего исследования состоит в анализе спектрограммы до и после доработки ТС, а также в изучении стоимости и характеристик специального материала для проведения данной работы.

Доработке (экранированию) основных элементов с антенным фактором, будет подвержен монитор фирмы Dell. При открытии задней крышки монитора было выявлено, что тип матрицы LVDS. При подключении монитора информационным кабелем HDMI к системному блоку, в настройках системы разрешение монитора составляет 1920x1080 (60 Гц).

Для проведения специальных исследований данного ТС по видеотракту, будут использованы следующие средства измерения:

- анализатор спектра Rohde&Schwarz FSW;
- антенна биконическая измерительная НБА-02 (частотный диапазон: от 0,009 МГц до 2.5 ГГц).

При разрешении монитора 1920x1080 (60 Гц), тактовая частота HDMI составляет 148,5 МГц, а тактовая матрицы – 74,25 МГц. Ниже, на рис. 4, приведен пример сигнала по видеотракту через HDMI на начальной частоте без доработки ТС.

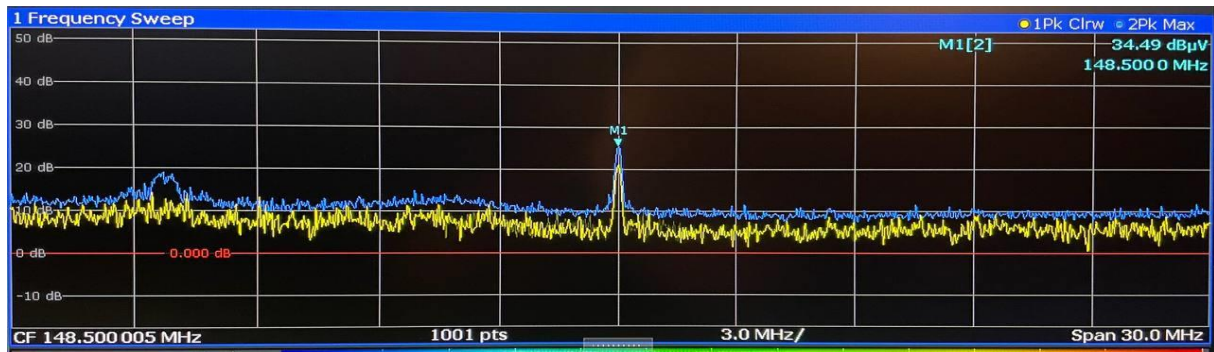


Рис. 4. Информативный «опасный» сигнал по видеотракту через HDMI

Как показано на рис. 4, при частоте 148,5 МГц, уровень информационного сигнала составляет 34,49 дБмкВ. Данный показатель является не совсем приемлемым, поэтому на примере этого сигнала будет продемонстрирована эффективность доработки.

Далее следует обнаружить на спектрограмме матричный сигнал от монитора. Ниже, на рис. 5, приведен пример матричного сигнала по видеотракту без доработки ТС.

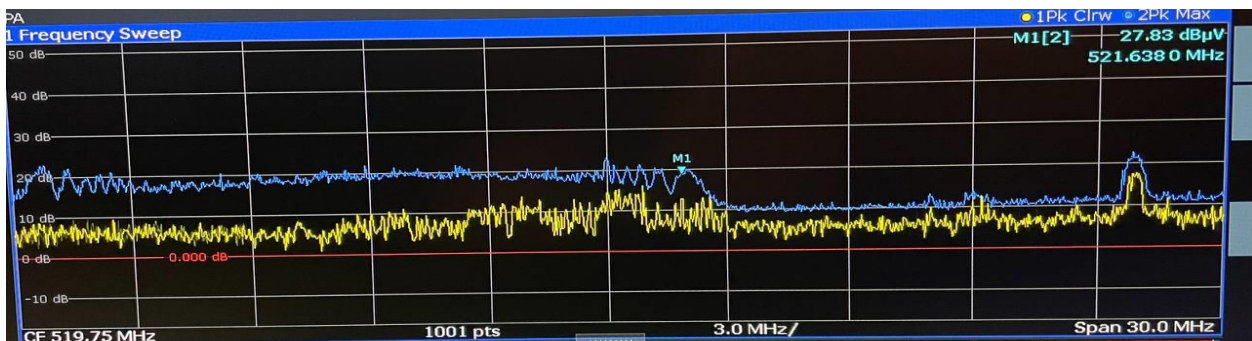


Рис. 5. Информативный «опасный» матричный сигнал через LVDS

Как показано на рис. 5, при диапазоне частот от 519,880 МГц до 521,645 МГц, отчетливо видно матричный сигнал LVDS от монитора. Максимальный пик сигнала приходится на частоту 521,638 МГц и составляет 27,83 дБмкВ. Сигнал является показательным и четко виден на спектрограмме, поэтому целесообразно применить доработку ТС с экранированием матричного шлейфа и последующего сравнения с новыми показателями после доработки.

Далее следует выбрать оптимально возможные по цене и качеству материалы экранирующие данные сигналы. На рынке существует множество средств для доработки ТС, однако исследования показали, что наиболее эффективными средствами по цене и качеству являются проводящая тканевая лента с медно-никелевым покрытием и медная проводящая лента.

Лента с гладкой основой из медной фольги имеет высококачественный устойчивый к действию растворителей акриловый адгезив. Высокая пригодность к пайке обеспечивает экономичность при выборе этой ленты в качестве экранирующего материала. Отлично применяется при укреплении медно-никелевой ленты. Коэффициент экранирования при 1 ГГц – –85 (дБ). Стоимость данного материала составляет 1 000–3 500 рублей за 100–180 м длины ленты.

Лента Cu/Ni состоит из полиэфирной ткани с антикоррозионным медно-никелевым напылением и проводящим акриловым адгезивом, чувствительным к давлению. Лента поставляется с лайнером, отделяемым при монтаже. Данная лента применяется для тех же целей, что и фольгированные ленты, но ее необыкновенная прочность к разрывам, эластичность и легкий вес дают дополнительные преимущества. Коэффициент экранирования при 1 ГГц – 70 (дБ). Стоимость данного материала составляет от 6 000–9 000 руб. за 120–200 м длины ленты [2].

Важно помнить, что и тот и другой материалы токопроводящие, из чего следует, что наклеивать один материал на другой нужно меньшей частью [3; 4].

Конечный результат доработки ТС в соответствии с выявленными источниками антенного фактора монитора, схематично представленного на рис. 2, с применением материала, описанного выше, приведен на рис. 6.

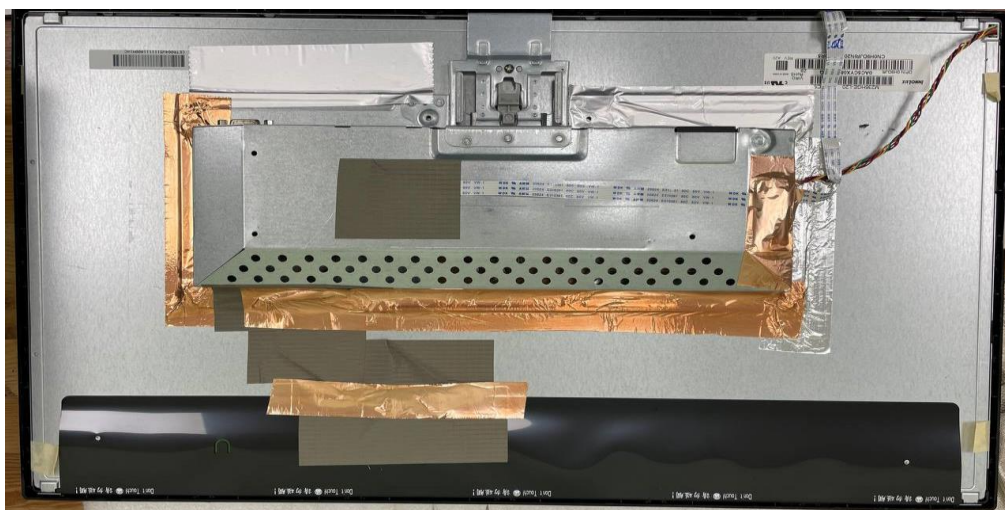


Рис. 6. Конечный результат доработки ТС по уменьшению «опасного» информативного сигнала

При завершенной доработке следует убедиться в качестве и надежности такого способа и применяемых специальных материалов. Для этого целесообразно исследовать частоты на спектрограмме до доработки ТС. А именно: для HDMI составляющей 148,5 МГц; для матричной составляющей 521,638 МГц.

Ниже, на рис. 7, продемонстрирован положительный результат доработки HDMI составляющей.

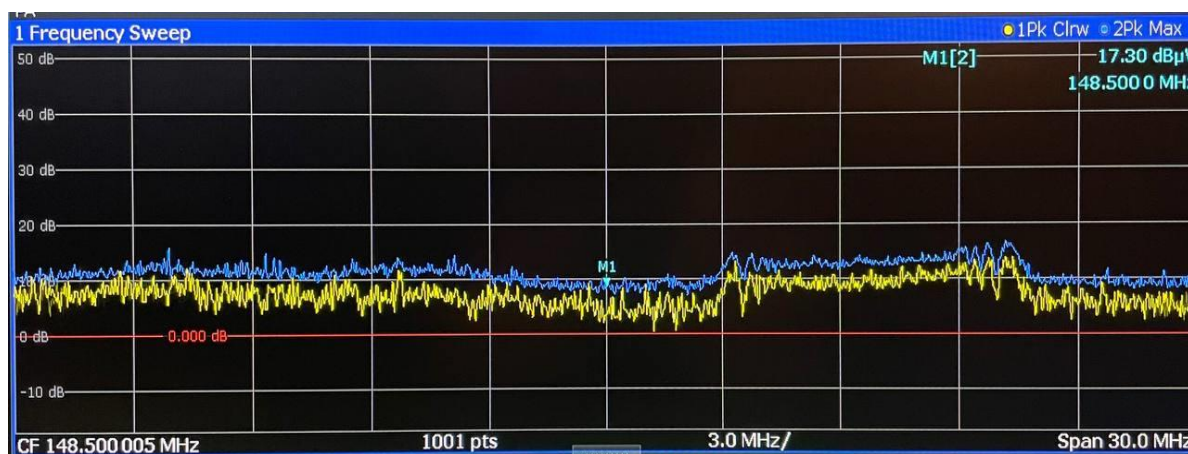


Рис. 7. Информативный HDMI сигнал после доработки ТС

Как показано на рис. 7, после доработки ТС, сигнал вовсе пропал, что говорит о явном уменьшении зоны R2. Далее продемонстрирован положительный результат доработки матричной составляющей на рис. 8.

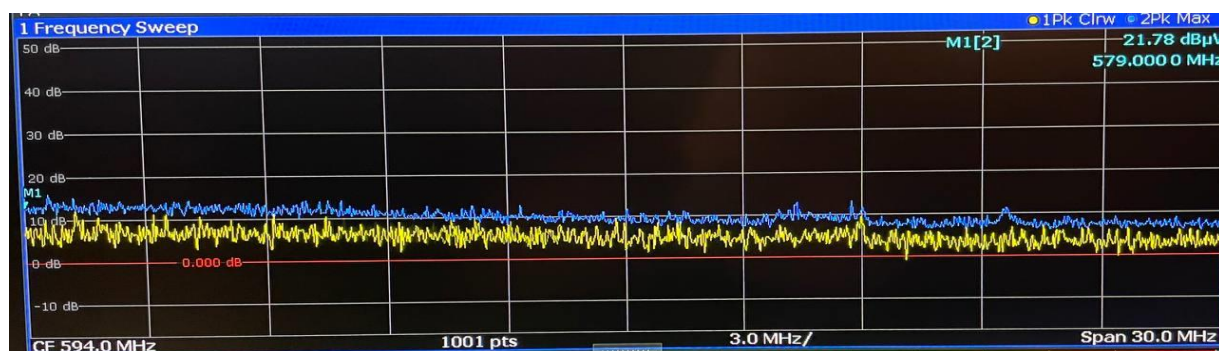


Рис. 8. Информативный LVDS сигнал после доработки ТС

Исходя из рис. 7 и 8 можно сделать вывод, что методология доработки изделия по уменьшению зоны R2 является эффективным средством по устранению технических каналов утечки информации.

При проведении специальных исследований технических средств, не всегда получаются удовлетворительные результаты. При чересчур больших значениях информативных сигналов, техническое средство не допускается к установлению и эксплуатации на критически важных объектах. Убытки предприятий при таких ситуациях – частое явление. Для устранения подобного рода проблем служит доработка технических средств путем экранирования.

Доработка технических средств путем экранирования исключает возможность перехвата защищаемой информации не только по техническим каналам утечки информации, возникающих вследствие ПЭМИ и их наводок, но и по каналам утечки, создаваемым методом «высокочастотного облучения» и внедрением в технические средства электронных устройств перехвата информации.

Список литературы

1. Хорев А. А. Техническая защита информации : учебное пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. М. : Аналитика, 2008.
2. Экранирующие материалы для защиты от электромагнитных излучений и решения проблем электромагнитной совместимости. URL: <http://ckbrm.ru/index.php?products=64>.
3. Обеспечение электромагнитной совместимости технических средств. URL: http://elib.bsut.by/bitstream/handle/123456789/1204/elektromagnit_sovmestivost.pdf?sequence=1&isAllowed=y.
4. ГОСТ Р 50414–92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний. М. : Госстандарт России, 1992.

Лустин В. И.¹,

старший преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета

МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ ВЗАИМНОЙ СВЯЗИ ЦИФРОВОЙ ЭКОНОМИКИ И КИБЕРПРЕСТУПНОСТИ

Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», а также программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р, позволяет рассматривать цифровую экономику как многогранное понятие.

Цифровая экономика – «это хозяйственная деятельность, где ключевыми факторами производства будут являться данные в цифровом виде, что позволяет повысить ее действенность в отличие от других более традиционных форм хозяйствования» [1, с. 48], в свою «очередь это экономика, основанная на новых методах генерирования, обработки, хранения, передачи данных, а также цифровых компьютерных технологиях» [7], также «цифровую экономику можно рассматривать как результат трансформационных эффектов новых технологий общего назначения в области информации и коммуникации, которые влияют на все секторы экономики и социальной деятельности» [2, с. 51].

Таким образом, прослеживается связь цифровой экономики с достижениями передовой науки в области высоких технологий и определяется, в свою очередь, высоким уровнем развития соответствующей инфраструктуры. В соответствии с этим цифровая экономика вызывает проникновение и оказывает влияние на все существующие сферы деятельности общества, в том числе и на совершение преступлений в экономической сфере. И в частности, особенно быстро развивающейся разновидности экономической преступности – киберпреступности, которая является следствием глобализации информационных коммуникационных технологий и дальнейшего развития международных компьютерных сетей [4, с.120].

«Киберпреступность – это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей» [6, с. 50]. Развитие информационных технологий и телекоммуникаций дает больше возможностей для сферы действия киберпреступности, а также создает условия для дальнейшего совершенствования и существования. Изучение новых технологий и дает возможность подстраивать их под существующие и создаваемые механизмы преступной деятельности, а это закономерно усложняет выявление, пресечение и расследование преступлений в этой области.

При выявлении и расследовании киберпреступлений необходимо учитывать следующие моменты:

¹ © Лустин В. И., 2024.

- трансграничный характер преступлений, так как для совершения хищений и дальнейшим получением денежных средств при использовании для этого информационных технологий злоумышленники могут располагаться на значительном удалении друг от друга;
- высокий уровень квалификации и знание данной предметной области является одним из условий и фундаментом совершения киберпреступлений;
- преступные действия имеют скрытый характер, в следствии чего только через достаточно значительный диапазон времени потерпевший узнает о хищении;
- большой разброс диапазона длительности совершения преступления, что может составлять несколько минут или дней и даже месяцев.

В сумме вышеперечисленные моменты приводят к тому, что для деятельности правоохранительных органов создаются значительные трудности по выявлению самого события совершения преступных действий, лиц совершивших деяние, места их пребывания, а также сбора необходимых доказательств при проведении процессуальных действий.

Развитие информационной сферы вызывает совершенствование и появление новых способов совершения киберпреступлений. Раскрывая понятия и уголовно-правовые меры борьбы с преступностью можно определить «киберпреступность как совершенное общественное деяние опасное и уголовно наказуемое при использовании компьютера, интернет сетей и программ» [5, с. 15]. Рассматривая влияние цифровой экономики на киберпреступность необходимо отметить, что в УК РФ выделяется в отдельную главу общественно опасные деяния, совершенные с помощью компьютерных технологий. Проблема квалификации таких составов преступлений состоит в том, что обнаружить эти деяния достаточно сложно, так как выделить совокупность преступлений, которые совершаются с использованием электронной информации, представляется трудной задачей. Решение проблемы с киберпреступностью предлагается законодателем, в изменениях относящиеся к гл. 28 УК «Преступления в сфере компьютерной информации».

На сегодняшний день, такое преступление как мошенничество в электронной среде: носит многосторонний характер; совершается в компьютерной среде; применяются электронные денежные средства; используются виртуальные счета; имеется доступ к биржам и банкам.

Электронный ключ являясь результатом развития информационных технологий может служить основой такого преступления мошенничество. Для этого мошенники похищают персональные данные, которые и применяют для совершения преступления против потерпевшего. С помощью электронного ключа злоумышленники могут совершать операции с собственностью и иным имуществом. «Электронный ключ – это аппаратное средство, предназначенное для защиты программного обеспечения (ПО) и данных от копирования, нелегального использования и несанкционированного распространения» [3, с. 28]. Электронная подпись (ЭП) в сети равносильна подписанию собственноручной подписью юридически значимых документов. При создании ЭП требуется номер СНИЛС

и паспорт пользователя. Такие же данные работодатель получает при оформлении сотрудника на работу или банк – при подаче документов для оформления счетов.

Используя полученные данные для оформления электронной подписи возможно совершение мошенничества с ЭП: это операции с недвижимостью, принадлежащей физическим лицам; регистрация на граждан юридического лица. Для каждого из таких видов мошенничества необходимо соблюдение соответствующей политики безопасности. При нарушении этих правил информация для совершения мошенничества путем взлома похищается из компьютерных систем. Получив доступ к сведениям для дальнейшего использования злоумышленники могут совершать противоправные деяния. В то же время потерпевший:

1) может не знать о потере данных, полученных и использованных в целях совершения мошенничества;

2) установив факт неправомерного использования персональных данных, необходимо большое количество времени и ресурсов для восстановления потерянного и доказательства своей невиновности;

3) выявить в сетевом пространстве лиц причастных к совершению преступления является весьма трудоемким процессом.

Существует тенденция увеличения киберпреступлений большого масштаба, а именно хищение крупных денежных средств со счетов банков и финансовых организаций.

Дальнейшее развитие передовых информационных технологий и телекоммуникаций, в свою очередь, ведет к постоянному совершенствованию способов совершения мошенничества в электронной среде. Для успешного решения существующих проблем борьбы с киберпреступностью требуется дальнейшее совершенствование законодательной основы регулирующей ответственность за совершение преступлений в рассматриваемой сфере; техническая поддержка правоохранительных органов, занимающихся противодействием киберпреступности; развитие межведомственного сотрудничества как на региональном так и на международном уровне в сфере защиты информационного пространства и борьбы с киберпреступностью.

Список литературы

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

Максимова Е. А.¹,

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

Худяков В. В.²,

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

СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА – ИНСТРУМЕНТ НЕОТВРАТИМОСТИ ПРАВОСУДИЯ

Активное внедрение информационных технологий в обществе повлияло на развитие преступности в данной сфере. В связи с этим начали создаваться отделы, занимающиеся компьютерно-техническими экспертизами (далее КТЭ), как в России, например, Экспертно-криминалистический центр МВД России, Судебно-экспертный центр Следственного комитета Российской Федерации, так и в зарубежных странах, например, одно из первых – Общество информационной и судебно-экспертной безопасности в Гонконге. Целью проведения экспертизы является выявление на средствах хранения данных значимой для расследования преступления информации и последующее ее исследование. Судебная КТЭ с помощью специальных технических средств занимается исследованием цифровых устройств, компьютерных программ и электронных данных для получения доказательств, имеющих значение для расследования преступления. Данный род инженерно-технических экспертиз проводится с использованием различных методов, таких как: специальное программное обеспечение, которое применяется для восстановления удаленной информации, криптоаналитические методы для изучения зашифрованных данных, эмуляция рабочей среды, с целью контролируемого запуска вредоносного кода и программ, методы реверс-инжиниринга, которые позволяют провести анализ исполняемого кода и многое другое. Основанием для проведения экспертизы является подозрение на несанкционированный доступ к конфиденциальной информации злоумышленником путём внедрения вредоносных программ, маскировка под зарегистрированного пользователя, незаконное подключение к аппаратуре жертвы, перехват данных, передаваемых по каналам связи, рассылка спама и фишинговых сообщений жертвам и многое другое.

Злоумышленники, обладающие высоким уровнем знаний в области информационных технологий, используют его в корыстных целях, что явилось толчком к увеличению преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. «Из общего числа преступлений, совершенных в 2023 г., четверть преступлений

¹ © Максимова Е. А., 2024.

² © Худяков В. В., 2024.

с применением информационных технологий» – отмечено Президентом Российской Федерации В. Путиным на коллегии МВД России, а представитель Генпрокуратуры А. Некрасов отмечает, что данный вид преступлений становится «угрозой национальной безопасности», отмечая их масштабность и низкую раскрываемость, о чем свидетельствует отчет ГИАЦ МВД России за январь – сентябрь 2023 г. [1, с. 3].

Основным инструментом в противостоянии с компьютерными преступлениями явилось создание и развитие КТЭ. Как описывают субъекты информационной деятельности: «стремительный рост IT привел к тому, что практика опередила теорию компьютерной экспертизы». Таким образом, на базе Российского федерального центра судебной экспертизы Минюста России в 2003 г. была организована специальная лаборатория судебной компьютерно-технической экспертизы и информационных технологий. Разрешать конфликты в сфере информационных технологий и бороться с киберпреступлениями без специальных экспертных знаний стало невозможно. Сегодня КТЭ занимает ключевую позицию в расследовании данного вида преступлений.

Совершение преступлений с использованием информационных технологий рассматривается как в уголовном, так и в административном и гражданском законодательствах, а также затрагивает разные составы преступлений, таких как компьютерное мошенничество, неправомерный доступ к компьютерной информации, создание и использование вредоносного программного обеспечения, подлог, нарушение авторских прав, так и сбыт наркотических средств с использованием мобильных устройств или случаи вовлечения в экстремистскую деятельность, совершенные с использованием социальных сетей, и многие другие. Так, по данным статистики [1, с. 36] в делах по обвинению в совершении преступления, предусмотренного ст. 228.1 УК РФ «Незаконное производство, сбыт и пересылка наркотических средств...» всего раскрыто из находящихся в производстве 86 168 преступлений, однако доля с проведением КТЭ не превышает 0,3 %.

Примером использования КТЭ могут являться следующие факты. По подозрению в незаконном сбыте наркотических средств, задержан гражданин М., у которого был изъят сверток с содержимым в нем N-метилэфедроном (ч. 2 ст. 228 УК РФ), а также сотовый телефон марки «Honor», в последующем отправленный на экспертизу, в результате которой было установлено, что гражданин М. через социальную сеть «Telegram» получал данные о местах, где он должен был оставить «закладку», содержащую наркотическое средство. В другом уголовном деле о незаконном проведении азартных игр (ч. 3 ст. 171.2 УК РФ) была назначена КТЭ, которая подтвердила, что исследованные системные блоки могут быть использованы для проведения азартных игр с материальным выигрышем. Так виновное лицо привлечено к уголовной ответственности.

Список литературы

1. Состояние преступности в Российской Федерации за январь – сентябрь 2023 г. URL: <https://media.mvd.ru/files/application/4990835>.

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

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

АКТУАЛЬНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ БЕСПИЛОТНЫХ ВОЗДУШНЫХ СРЕДСТВ В РЕАЛИЯХ СОВРЕМЕННОЙ РОССИИ

Ежедневно современный мир подвергается различного рода реновациям. Технологический прогресс, как и в целом любая другая отрасль, не стоит на месте, постоянно развиваясь и совершенствуясь, привнося свои коррективы в устои и технологий. Непосредственно по отношению к правовым нормам современных беспилотных гражданских судов он требует постоянную актуализацию, особенно по части задач и требований в возникающих «пробелах». Регулирование правовых аспектов на текущей стадии развития современного общества является одним из ключевых, восполняя столь насущные пробелы в правовой среде.

Для рассмотрения проблематики поднятого вопроса начать стоит с того, «А что вообще представляют из себя так называемые беспилотные воздушные судна (далее – БВС), или как их еще называют беспилотные летательные аппарат (БПЛА)»?

Обращаясь к ст. 32 Воздушного кодекса Российской Федерации [1], термин БВС трактуется как воздушное судно, управляемое, контролируемое в полете пилотом, находящимся вне борта такого воздушного судна (внешний пилот). Такие аппараты, на сегодняшний день снова начинают потихоньку внедряться повсеместно.

Выделяют следующие виды БВС (БПЛА):

1. Аэростатического типа.
2. Реактивного типа.
3. Самолётного (с фиксированным крылом) типа.
4. Вертолётного (однороторного) типа.
5. Мультикоптерного (мультироторного) типа.
6. Гибридного (конвертопланового) типа.

Ключевыми препятствиями на пути являются сложившаяся мировая обстановка, в частности события, происходящие как по внешним, так и по внутренним вопросам России. Но, не смотря на это, прогресс не стоит на месте. В различных

¹ © Маликов С. А., 2024.

областях применения БПЛА полным ходом идет процесс совершенствования, тестирования и применения их в повседневности. Какие-то из них выполняют свои задачи в гражданской сфере, но большая часть применяемых БВС на сегодняшний день активно задействована в проведении специальной военной операции. Этот фактор в силу затрачиваемых на достижение поставленных задач средств и устройств в лице дронов сыграли ключевую роль в введении новых ограничений и актуализацию современных норм права с целью обеспечения правопорядка и безопасности на территории России.

Практически спустя год после начала проведения в свет вышел Указ «О мерах, осуществляемых в субъектах Российской Федерации в связи с Указом Президента Российской Федерации от 19 октября 2022 г. № 756» [2], который был посвящен реализации четырех уровней реагирования: базовой готовности, повышенной готовности, среднего и максимального уровня реагирования. Свой вклад внес и введенный в ряде регионов повышенный желтый уровень террористической опасности. В связи с этими мерами в ключевых субъектах России Главным центром единой системы организации воздушного пространства (ГС ЕС ОрВД) был установлен временный режим ограничения на использование воздушного пространства в границах, обусловленных координатами, указанными в представлении Минобороны России, что сузило полетную зону полностью или частично сразу над несколькими ключевыми на тот момент регионами, в которые вошли 11 областей (Смоленская, Брянская, Калужская, Орловская, Тульская, Липецкая, Курская, Белгородская, Тамбовская, Воронежская, Волгоградская, Ростовская, Астраханская), два края (Краснодарский и Ставропольский), три республики (Адыгея, Калмыкия, Крым), а также четыре новых субъекта Российской Федерации (ДНР, ЛНР, Запорожская и Херсонская область).

Согласно современному законодательству, регуляторами в вопросе правовых норм по отношению к использованию БВС и воздушного пространства в целом выступает целый ряд законодательных актов, имеющих непосредственное отношение к их учету и использованию, представленные в следующих нормативных правовых документов:

- Федеральный закон Российской Федерации от 19 марта 1997 г. № 60-ФЗ «Воздушный кодекс Российской Федерации»;
- постановление Правительства Российской Федерации от 11 марта 2010 г. № 138 «Об утверждении Федеральных правил использования воздушного пространства Российской Федерации»;
- постановление Правительства Российской Федерации от 25 мая 2019 г. № 658 «Об утверждении Правил учета беспилотных гражданских воздушных судов с максимальной взлетной массой от 0,15 килограмма до 30 килограммов, введенных в Российскую Федерацию или произведенных в Российской Федерации»;
- постановление Правительства Российской Федерации от 30 июля 2004 г. № 396 Об утверждении Положения о Федеральном агентстве воздушного транспорта»;
- приказ Министерства транспорта Российской Федерации от 25 января 2023 г. № 18 «Об утверждении Порядка нанесения государственных, регистрационных и учетных опознавательных знаков гражданских воздушных судов, товарных знаков на гражданские воздушные суда»;

– Федеральный закон Российской Федерации от 14 марта 2022 г. № 56-ФЗ «О внесении изменений в Воздушный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».

Все они вносят свой вклад и коррективы для качественного регулирования и правовой дисциплинированности используемых в Российской Федерации гражданской авиации, в особенности на пилотов БВС. В «до конфликтный период» проблематика не вызывала такого бурного обсуждения и требования решительных мер воздействия на пользователей таковых устройств. Свой роковой пик сфера применения БПЛА достигла уже в первые месяцы проведения СВО. Реальная практика показала – современные задачи требуют модернизацию решений, в особенности в правовой среде. При отсутствии должного правового регулирования и применения соответствующих мер противодействия государство будет неспособно банально обеспечить не просто безопасность воздушного пространства, а безопасность жизней простых людей – своих граждан. В кратчайшие сроки вводятся современные меры фиксации, противодействия и пресечения незаконного использования БВС и деятельности самих операторов. Вносятся необходимые правовые поправки для полноценного юридического урегулирования. Но нельзя забывать о проблемах технического характера, в частности наличия действенных устройств обеспечения безопасности воздушного пространства (ОБВП) в зависимости от сферы и территории применения, покрываемых зон средств РЭБ, их аналогов, и так называемых «воздушных дыр».

В связи с накалённой обстановкой в стране выделилась проблематика незаконных запусков и использования БВС. Любые несанкционированные действия, особенно в пределах зон повышенного внимания, что расположены в пределах деятельности Московского, Ростовского и Симферопольского региональных центров ЕС ОрВД, подвергаются приоритетному вниманию и получают особый статус контроля полета, с целью пресечения как самого правонарушения, так и скорейшего задержания правонарушителя. Обращается внимание на выбираемые маршруты полета до момента перехвата БПЛА, предполагаемые цели, наличие ключевой инфраструктуры или живых целей на прогнозируемом пути, а также умысел совершаемого. Как правило, большая часть таковых запусков совершаются в связи правовой незнательностью лиц о рисках и последствиях совершаемого ими деяния. Даже сам факт взаимодействия, дозарядки таковых дронов при совершении деяния, должен пропагандироваться средствами массовой информации, сводками МВД России и нести за собой наказуемость.

Еще одной проблемой возникает урегулирование вопроса возможности применения БВС отдельными структурами и организациями для реализации своих потребностей. Яркими примерами являются СМИ, которые используют дроны для проведения фото-видеофиксации различных событий и мероприятий (особенно массовых и с привлечением особо важных лиц), без предоставления планов полёта и получением соответственного разрешения, а также создающие помехи в сигналах «в погоне за кадром» при ликвидации крупных пожаров, тем самым создавая затруднения в работе МЧС России.

На сегодняшний день для решения поставленных задач в рамках программ дополнительного обучения действующих и подготовительного обучения будущих сотрудников на базе учебных учреждений МВД России реализовываются направления операторов БПЛА, а также пользователей средств РЭБ, так называемые «антидронщики». Одна из первых таких групп появилась в Санкт-Петербурге. Она представляла из себя скооперированное спецподразделение, состоящее из мобильных патрули, снайперских групп, включая непосредственно специалистов по подавлению и нейтрализации дронов путем применения «антидроновых ружей», и показало свою необходимость и эффективность уже при первом дебютном задействовании при проведении 78-й годовщины Дня Победы в Великой Отечественной войне. Как результат, в подразделениях МВД России поднялся вопрос о создании аналогичных отрядов РЭБ и реализации их полномочий и возможностей в рамках охраны общественного порядка и безопасности ключевых объектов инфраструктуры, при проведении массовых мероприятий и иных случаев. Но не смотря на перспективность и актуальность при должной комплектации личного состава обеспечение деятельности таковых подразделений в лице покрытия всей необходимой области остается открытой, что говорит о необходимости привлечения дополнительных технических средств и устройств для реализации возникающих целей и задач, а также правовом регулировании данной области, в особенности учитывая текущую обстановку.

На сегодняшний день БВС привлекают к себе всё больше внимания. Они являются устройствами повышенного значения и опасности как для простых граждан, так и для государства в целом. Надзор, регулирование и актуализация связанных с БПЛА сфер, в особенности технических и правовых на сегодняшний день представляет ключевую цель и задачу. Необходимо постоянное поддержание правопорядка и редакция законодательства под современные реалии, которые будут пресекать нарушения, наказуемость следует усиленно пропагандировать, а факты пресечения должны подвергаться публичной огласке.

Список литературы

1. Федеральный закон Российской Федерации от 19 марта 1997 г. № 60-ФЗ «Воздушный кодекс Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_13744/.
2. Указ Президента Российской Федерации от 19 октября 2022 г. № 757 «О мерах, осуществляемых в субъектах Российской Федерации в связи с Указом Президента Российской Федерации от 19 октября 2022 г. № 756» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_429320/.

Маслов Н. В.¹,
*преподаватель кафедры криминалистики
Московского университета
МВД России имени В.Я. Кикотя*

ФУНДАМЕНТАЛЬНЫЕ И ПРИКЛАДНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ЕСТЕСТВЕННОНАУЧНЫХ ЗНАНИЙ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ, В ТОМ ЧИСЛЕ ПРИ ПОДГОТОВКЕ К ПРОИЗВОДСТВУ СУДЕБНО-БИОЛОГИЧЕСКИХ ЭКСПЕРТИЗ И ИССЛЕДОВАНИЙ

Основанием к подготовке проведения любого вида биологической экспертизы является постановление дознавателя (следователя) о ее производстве. Принимая во внимание возможность возникновения у следствия потребности в применении специальных методов познания в отношении объектов, которые могут быть обнаружены на месте преступления, от должностных лиц, производящих осмотры, обыски и выемки требуется соблюдение правил проведения этих мероприятий с учетом возможности выполнения различного рода исследований с найденными образцами биологического происхождения. Этот немаловажный факт диктует необходимость соблюдения особых мер предосторожности при подготовке к отбору образцов для проведения биологических экспертиз тканей и, в особенности, человеческих выделений, в том числе запаховых [1, с. 151; 2, с. 109]. В связи с этим имеется необходимость тщательного и максимально аккуратного осмотра места преступления с целью выявления возможных предметов для отбора с них следов биологического происхождения, что, как правило является одним из первых этапов в подготовке биологической экспертизы тканей и выделений человека, в том числе, запаховых следов человека. Осмотр места происшествия предполагает работу со следовой картиной на месте происшествия, и заключается в определенных этапах работы со следами: обнаружение, фиксация, изъятие, упаковка, и производство судебных экспертиз по изъятим следам. Познания в области биологии, в том числе исследования запаховых следов человека, могут иметь как фундаментальное, так и прикладное значение в свете цифровой трансформации, при производстве судебно-биологических экспертиз, и исследования запаховых следов человека. Познания в области биологии являются естественнонаучными знаниями, и носят фундаментальный характер при судебно-биологических экспертиз и исследовании запаховых следов человека. Если у следственных органов имеется такая возможность, то после осмотра и отбора образцов с места преступления, у подозреваемых лиц получают необходимые образцы биологического материала для выполнения сравнительных исследований, отбираются контрольные пробы возможных носителей следов иного материального свойства. Следующим шагом дознавателя или

¹ © Маслов Н. В., 2024.

следователя в процессе подготовки экспертизы становится процесс формулирования вопросов к экспертам, который может происходить с участием консультирующих специалистов, а также выбор экспертного учреждения или эксперта, что надлежащим образом необходимо отразить в выносимом постановлении о назначении экспертизы [3, с. 454; 4, с. 92]. Необходимо отметить, что несмотря на проведение первичного осмотра на месте происшествия, следователю или дознавателю необходимо еще раз подробно изучить все изъятые предметы. При расследовании насильственных преступлений особое значение имеют следы крови, спермы и иных выделений человека, фрагменты тканей, оставшихся на орудиях преступлений или на окружающих место преступления предметах, одежде как преступника, так и потерпевшего. По этим следам зачастую можно с достаточной долей доказанности говорить о восстановлении картины происшедшего. Известно, что при попытках избавиться от следов преступления преступники замыывают следы крови, но часть тканевых материалов содержит микрочастицы на внутренних поверхностях нитей плетения, даже если они были видоизменены под воздействием моющих средств, бензина и т. п. Такие следы также могут быть обнаружены в рамках повторного осмотра специалистами и принести немаловажный вклад в дело идентификации преступника и раскрытие преступления [5, с. 156; 6, с. 218]. Несмотря на то, что преступники используют различные средства сокрытия следов – маски, бахилы для обуви, перчатки и т. п., иногда на них также остаются пригодные для идентификации потожировые или запаховые следы, позволяющие установить различные характеристики оставившего такие следы человека. Этот этап подготовки также крайне важен для последующего использования результатов экспертной работы в судопроизводстве. Специалисты рекомендуют собирать запаховые следы в качестве контрольных образцов у живых лиц из подмышечных и паховых складок, с поясничной области, шейно-воротниковой зоны путем приложения к названным участкам кожи стерильных салфеток из волокнистых хлопчатобумажных материалов. При этом отбор контрольных проб может производить сам следователь или иное лицо, поскольку методики экспертизы запаховых следов человека, как мы уже упоминали выше, не имеют законодательного или иного правового закрепления. Тем не менее, здесь также стоит придерживаться правил и процедур, поскольку сами объекты крайне подвержены разрушительному воздействию различных естественных и искусственных процессов [7, с. 318; 8]. Лицам, осуществляющим отбор необходимо использовать стерильные резиновые перчатки, пинцеты, обработанные дезинфицирующими средствами, колпаки в качестве головных уборов, маски для исключения смешения собственных биологических следов с исследуемыми. Несмотря на огромный прогресс в области разработки различного вида пластмасс, запаховые следы стоит упаковывать в пакеты из многослойной фольги или в стеклянные емкости, поскольку практически все полимерные материалы впитывают запахи. Все упаковки маркируются, различные виды следов разделяют при помощи кусков стерильной ткани или нетканого материала. «На конвертах или этикетках, бирках, пробирках, банках, фольге и т. д. делаются надписи (до упаковки, чтобы не повредить объекты) с указанием но-

мера уголовного дела, наименования объекта, места, времени, даты изъятия, заверяемые подписями лиц участвующих в производстве следственного действия (специалист, понятые, следователь) [9, с. 198; 10, с. 215]. Затем упаковку опечатывают. Крайне важна для конечного результата и подготовка постановления о производстве того или иного вида биологической экспертизы. Особое значение при работе с биологическими объектами, и запахowymi следами человека имеет производство фотосъемки на подготовительном этапе, так и при производстве следственного действия, и при производстве судебно-биологических экспертиз, как элемент дополнительной технической фиксации [11, с. 193; 12, с. 76]. Способы запечатлевающей криминалистической фотосъемки позволяют максимально наглядно отразить объективную обстановку при осмотре места происшествия, и других процессуальных действиях [13, с. 268; 14, с. 99]. Следователям стоит консультироваться со специалистами для правильной и качественной постановки вопросов к исследованиям, как одной из форм процессуального взаимодействия следователя и специалиста (эксперта). Также сотрудникам органов следствия стоит больше сотрудничать с экспертным сообществом для более глубокого понимания типов назначаемых экспертных исследований и вопросов, выносимых на разрешение эксперта при производстве судебных экспертиз, на которые они могут дать ответы.

Список литературы

1. Маслов Н. В. Отдельные вопросы подготовки судебно-биологической экспертизы тканей и выделений человека // Техничко-криминалистическое обеспечение раскрытия и расследования преступлений : сборник научных трудов. М., 2023. С. 151–154.
2. Маслов Н. В. Судебно-биологическая экспертиза, как составляющая противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов / сост. А. В. Константинов. М. : Московский университет МВД России имени В.Я. Кикотя, 2023. С. 108-112.
3. Маслов Н. В. Медико-криминалистическая оценка повреждающего биологического фактора при травматических телесных повреждениях // Устойчивое развитие России: правовое измерение : сборник докладов. В 3 ч. М., 2023. С. 453–455.
4. Маслов Н. В. Отдельные вопросы производства биологической экспертизы при расследовании и раскрытии преступлений // Криминалистика: наука, практика, опыт : сборник научных трудов. Тула, 2023. С. 91–94.
5. Маслов Н. В., Суворов А. С. Организационные и методологические вопросы проведения биологической экспертизы при расследовании преступлений // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства : сборник научных трудов / сост. Д. А. Иванов. М. : Московский университет МВД России имени В.Я. Кикотя, 2023. С. 154–159.

6. Маслов Н. В. Современные проблемы судебных компьютерно-технических экспертиз в условиях цифровой трансформации // Теория и практика судебной экспертизы в современных условиях : сборник научных трудов. М., 2023. С. 217–219.

7. Маслов Н. В., Кукало Е. В. Электронная криминалистика и искусственный интеллект как подход к научно-техническому обеспечению расследования и раскрытия киберпреступлений // Криминалистика: наука, практика, опыт : сборник научных трудов. М., 2022. С. 317–319.

8. Маслов Н. В. Цифровая криминалистика в сфере искусственного интеллекта: противодействие киберугрозам в информационно-телекоммуникационных системах // Ломоносов-2021 : сборник научных трудов. 2021.

9. Маслов Н. В. Электронная криминалистика в сфере современных информационных технологий в юридической деятельности как подход к научно-техническому обеспечению раскрытия и расследования преступлений // Раскрытие и расследование преступлений: наука, практика, опыт : сборник научных трудов. М., 2020. С. 197–199.

10. Маслов Н. В. Экспертно-криминалистическая деятельность в условиях цифровой трансформации: информационные технологии применения специальных знаний при производстве судебных экспертиз и противодействия киберугрозам // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы (к 20-летию образования Московского университета МВД России имени В.Я. Кикотя) : сборник научных трудов / сост. В. В. Бушуев. М. : Московский университет МВД России имени В.Я. Кикотя, 2022. С. 214–219.

11. Маслов Н. В., Мозговая Д. А. Некоторые вопросы применения криминалистической фотосъемки при расследовании и раскрытии преступлений // Техничко-криминалистическое обеспечение раскрытия и расследования преступлений : сборник статей. М., 2021. С. 192–194.

12. Маслов Н. В., Суворов А. С. Воздействие биологического повреждающего фактора: инфекционные осложнения при травматических телесных повреждениях // Вопросы установления тяжести вреда, причиненного здоровью человека в результате воздействия биологического повреждающего фактора : сборник научных трудов. М., 2021. С. 75–80.

13. Маслов Н.В. Особенности повышения эффективности применения криминалистической фотосъемки специалистом-криминалистом при производстве процессуальных действий // Интерполитех-2016 : сборник научных трудов / общ. ред. Н. С. Маричев. М., 2016. С. 267–268.

14. Маслов Н. В. Проблема повышения эффективности применения криминалистической фотосъемки специалистом-криминалистом при производстве процессуальных действий // Современные проблемы производства судебных экспертиз и исследований : сборник научных трудов. 2016. С. 98–100.

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*

Дрога А. А.²,

*заместитель начальника кафедры
информационно-компьютерных технологий
в деятельности органов внутренних дел
Белгородского юридического института
МВД России имени И.Д. Путилина*

Назаренко И. С.³,

*старший преподаватель кафедры
информационно-компьютерных технологий
в деятельности органов внутренних дел
Белгородского юридического института
МВД России имени И.Д. Путилина*

О НЕКОТОРЫХ ОСОБЕННОСТЯХ МОНИТОРИНГА ПРОТИВОПРАВНОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ

В условиях бурно развивающихся общественных отношений сегодня цифровизация затронула все ключевые области жизни человека, общества и государства. Цифровые технологии обеспечивают, возрастающий с каждым годом, обмен информации. Информация наполняет виртуальное пространство и обеспечивает деловую активность и досуг человека. Но помимо положительных моментов, следует не забывать и об обратной стороне «медали», например, виртуальное пространство выступает площадкой для размещения противоправного контента в сети Интернет. Согласно статистическим данным в январе 2022 г. в Российской Федерации зарегистрировано 129,8 млн интернет-пользователей. Процент распространения Интернета на начало 2022 г. составил 89,0 % от общего населения России. Количество пользователей Интернета в России увеличилось на 5,8 млн человек (+4,7 %) в период с 2021 по 2022 г. [1]. Поэтому вопрос влияния информационно-коммуникационных интернет-сетей на сознание людей становится важнейшей проблемой современности [2].

Такая популярность сети Интернет обусловила необходимость ее постоянного мониторинга со стороны различных субъектов в лице органов государственной власти и со стороны общественности в лице представителей общественных организаций, движений, кибердружин, волонтеров. В том числе

¹ © Меняйло Д. В., 2024.

² © Дрога А. А., 2024.

³ © Назаренко И. С., 2024.

и органы внутренних дел участвуют в мониторинге. Наряду с удалением или блокировкой противоправного контента проводят активную разъяснительную работу, раскрывая истинные цели распространителей противоправного контента [3, с. 19].

На сегодняшний момент в России действует немало специальных общественных организаций на базе образовательных организаций, аналитических центров, волонтерских организаций, чья деятельность связана с противодействием противоправному контенту. Так, в Ростовской области с конца 2017 г. при поддержке правоохранительных органов создана и функционирует региональное общественное движение «Интернет – без угроз». Среди основных задач этого движения можно выделить следующие:

- участие в создании и распространении полезного контента в сети Интернет;
- оказание содействия правоохранительным органам в части, касающейся поиска противоправного контента в открытых источниках;
- участие в информационно-просветительской деятельности, направленной на профилактику распространения асоциальных явлений в молодежной среде, в том числе в семинарах, тренингах по тематике;
- организация и проведения социально-ориентированных проектов, направленных на противодействие распространению вредоносного контента в сети Интернет и формирование культуры информационной безопасности.

Более глобальной организацией является Национальный Центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ), который создан для решения задач, поставленных Минобрнауки России. Работа Центра направлена на активное противодействие распространению идеологии терроризма и экстремизма, совершенствование работы по информационно-пропагандистскому обеспечению антитеррористических мероприятий в сети Интернет, привлечению молодежи и студентов к разработке теоретических и методологических основ противодействия идеологии терроризма [4]. В результате анализа деятельности общественных организаций и движений, мониторинга сети Интернет и взаимодействия с правоохранительными органами сотрудники НЦПТИ отмечают ряд основных проблем в данной сфере. Это «непонимание потребностей правоохранительных органов в объемах и качестве передаваемой информации; отсутствие предварительной оценки специалистами результатов работы движения перед передачей информации в правоохранительные органы, что приводит к увеличению непродуктивной работы сотрудников заинтересованных ведомств; отсутствие оперативной обратной связи от правоохранительных органов по результатам работы движения» [5].

С началом специальной военной операции возросло количество экстремистских движений и террористических организаций, которые вовлекают в свою деятельность молодых людей (например, Маньяки: культ убийства (другие используемые наименования «Маньяки Культ Убийств», «Молодежь Которая Улыбается», М.К.У.) – неонацистская организация, признанная террористической Верховным Судом Российской Федерации 16 января 2023 г. ФСБ России утверждает, что организация создана украинским неонацистом Егором Красно-

вым в 2019 г., Националистическая организация «Русский добровольческий корпус» (РДК) включен в список в конце 2023 г.). РДК участвует в вооруженном конфликте с Россией на стороне украинского террористического режима и активно проявил себя при нападении на Грайворонский район Белгородской области весной 2024 г. В современном мире экстремизм и терроризм развивается в большей степени посредством сети Интернет. Наиболее уязвимой категорией в обществе перед лицом экстремизма выступает молодёжь, и прежде всего лица несовершеннолетнего возраста с неокрепшей психологией, стремлением найти себя и самоутвердиться, при этом выбирая противоправный инструмент. Интернет выступает как мощная платформа распространения экстремистских течений. В данной связи государством предпринимаются различные меры профилактики экстремистских проявлений. Стоит отметить, что первая сеть мониторинговых групп («Кибердружин») была заявлена «Лигой безопасного интернета» еще в 2011 г. В Белгородской области «Кибердружины» действуют с 2017 г. Их координацию и взаимодействие с правоохранительными органами осуществляет Министерство по делам молодежи Белгородской области.

Традиционно в образовательных организациях МВД России проводятся различные мероприятия, направленные на профилактику экстремизма. В данной связи, на базе образовательных организаций МВД России формируются и осуществляют свою деятельность «Кибердружины», которые выступают как современная педагогическая технология и осуществляют профилактику экстремизма в среде обучающихся.

В 2023 г. в ходе рабочего совещания, проводимого с участием начальника Главного управления на транспорте МВД России генерал-лейтенанта полиции О.В. Калинкина было принято решение о создании в Белгородском юридическом институте МВД России имени И.Д. Путилина специальной мониторинговой группы, аналогичной «Кибердружине», на условиях добровольного участия курсантов и слушателей. В ходе выполнения данной задачи в институте создан и функционирует Клуб «Киберполицейский». Данный Клуб является добровольной, самоуправляемой организацией курсантов, слушателей, профессорско-преподавательского состава Белгородского юридического института МВД России имени И.Д. Путилина и осуществляет свою деятельность в рамках взаимодействия филиалов кафедр института с территориальными органами внутренних дел. Организация деятельности клуба обеспечивается кафедрой информационно-компьютерных технологий в деятельности органов внутренних дел института при взаимодействии с кафедрами обеспечения безопасности на объектах транспорта, уголовного процесса, уголовного права и оперативно-разыскной деятельности.

Члены Клуба осуществляют мониторинг сети Интернет с целью выявления:

- информационного контента, имеющего признаки возможных противоправных действий, связанных с призывами совершения действий экстремистского толка, а также побуждающего людей к противоправному поведению;
- информационного контента, содержащего возможные угрозы объектам транспортной инфраструктуры (например, по тематике поджогов релейных шкафов);

- информационного контента, содержащего пропаганду наркотических и психотропных веществ, в том числе их незаконного оборота;
- публикаций и комментариев провокационного характера.

В рамках работы Клуба «Киберполицейский», постоянную методическую помощь членам Клуба оказывают практические сотрудники линейных отделов МВД России на транспорте. Выявленный членом Клуба информационный контент возможной противоправной направленности направляется председателю Клуба либо его заместителю, для дальнейшей передачи сотрудникам Белгородского линейного отдела МВД России на транспорте в установленном порядке для оценки и принятия соответствующих мер реагирования.

Наиболее активными членами Клуба являются курсанты, обучающиеся по специальности 40.05.02 Правоохранительная деятельность, специализация – оперативно-разыскная деятельность органов внутренних дел (профиль образовательной программы – Деятельность подразделений по контролю за оборотом наркотиков, осуществляющих выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий).

На какие области сети Интернет необходимо обращать первоочередной внимание при мониторинге? К опасным сообществам в социальных сетях относятся, например:

- группы, каналы и сообщества, пропагандирующие экстремистскую и нацистскую идеологию;
- группы, каналы и сообщества, пропагандирующие опасные увлечения (например, зацепинг);
- группы, каналы и сообщества, пропагандирующие причинение вреда себе или окружающим;
- группы, каналы и сообщества, пропагандирующие нетрадиционные духовно-нравственные ценности: оккультизм, сатанизм, чайлдфри, феминизм, нетрадиционные сексуальные отношения, смену пола, гендерную идентичность.

Аниме-сообщества. В отличие от традиционной японской культуры аниме, современные аниме могут быть очень опасны, поскольку нередко пропагандируют насилие, сексуальные извращения, канибализм, убийства и самоубийства [6].

Социальные сети являются оптимальной площадкой для манипулирования общественным мнением. Преднамеренное распространение дезинформации или фейковых новостей, таргетированные рекламные кампании, использование алгоритмов соцсетей для продвижения определённых взглядов или идей – все это может повлиять на общественное мнение и иметь социальные последствия.

Кроме вышеупомянутых видов противоправного контента, достаточно новым явлением стали результаты противоправного использованием инструментов искусственного интеллекта (DeepFake).

По информации УБК МВД России, с конца 2023 г. преступники начали использовать искусственный интеллект, чтобы генерировать голосовые сообщения и отправлять их своим потенциальным жертвам, прикрепляя поддельное изображение банковской карты с именем и фамилией. На первом этапе преступники

взламывают аккаунты Telegram или WhatsApp¹ с помощью фейковых голосований. Затем они скачивают сохраненные голосовые сообщения и создают новые сообщения с нужным контекстом. В конечном итоге они рассылают эти сообщения в личные и групповые чаты с просьбой об одолжении большой суммы денег, подкрепляя их сгенерированными голосовыми сообщениями и банковскими картами с поддельными именами получателей).

Среди особенностей мониторинга противоправного контента в сети Интернет можно выделить те, которые носят организационный, методологический и иной характер. Члены институтского клуба «Киберполицейский» преимущественно осуществляют неавтоматизированный поиск противоправного контента при взаимодействии с профессорско-преподавательским составом института и сотрудниками Белгородского ЛО МВД России на транспорте. Но в апреле 2024 г. ООО «БалтИнфоКом» предоставила возможность членам клуба использовать разработанную ими демонстрационную версию системы «Октопус», что повысило эффективность в выявлении противоправного контента в сети Интернет. Данной компанией также была разработана и система поиска информации «Следопыт».

Таким образом, прежде всего при взаимодействии с ГУТ МВД России, Белгородским ЛО МВД России на транспорте, УМВД России по Белгородской области осуществляется деятельность клуба «Киберполицейский» в Белгородском юридическом институте МВД России имени И.Д. Путилина. Члены клуба проводят постоянную работу по выявлению противоправного контента в сети Интернет, таким образом осуществляя как профилактику, так и противодействие действиям правонарушителей в виртуальном мире.

Список литературы

1. Отчет Digital 2022 GlobalOverview // Новостной интернет-портал. URL: <https://vc.ru/marketing/383351-samyi-svezhiy-otchet-digital-2022-global-overview>.
2. Меняйло Л. Н., Меняйло Д. В. Распространение экстремистских материалов в сети «Интернет» // Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты : сборник научных статей. Курск : Юго-Западный государственный университет, 2019. С. 219–222.
3. Деятельность органов внутренних дел по профилактике экстремизма : учебно-методическое пособие / [В. А. Лысенко и др.]. Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2022.
4. Национальный Центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет. URL: <https://ncpti.su/>.
5. Чурилов С. А., Чунин А. С. Противодействие распространению идеологии терроризма и экстремизма в студенческой среде посредством привлечения молодежи (опыт Ростовской области) / Противодействие идеологии терроризма

¹ Запрещен в России: принадлежит корпорации Meta, которая признана в России экстремистской.

в образовательной сфере и молодежной среде : сборник научных трудов. М. : МГИМО-Университет, 2018. С. 101, 102.

6. Меняйло Д. В., Карпушин О. Е., Крупенникова К. К. Меры по противодействию противоправному контенту, пропагандирующему наркотические средства в сети интернет // Противодействие незаконному обороту наркотиков в условиях цифровизации общества : сборник научных трудов. Белгород, 2023. С. 96–100.

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

ПОЛИЦИЯ И КРИМИНОГЕННАЯ ОБСТАНОВКА В РОССИИ: ЦИФРОВЫЕ ТЕНДЕНЦИИ, МЕТОДЫ, СРЕДСТВА, СИСТЕМЫ АНАЛИЗА И УПРАВЛЕНИЯ

В последние годы в связи с возрастающей потребностью более эффективного управления подразделениями полиции существенно усилилась необходимость целенаправленного анализа, оценки и прогнозирования криминогенной обстановки (КО). Развитию современных моделей и методов управления значительно способствовали усилившиеся возможности информационно-коммуникационных технологий и математического аппарата количественной обработки данных о процессах, происходящих в современном обществе.

Сегодня, с одной стороны, имеется значительное отставание аналитического инструментария, используемого в практической деятельности МВД России, от уровня информационно-методического обеспечения подобных структур ведущих зарубежных стран. А с другой – современные информационные системы Министерства располагают огромными, но не всегда в достаточной степени реализуемыми возможностями. Эти возможности позволяют обеспечить «добывание» более глубокой аналитической информации о постоянно эволюционирующей КО, предупреждение новых опасных тенденций в ее развитии, а также опережающее противодействие таким современным явлениям как киберпреступность и деструктивная идеология в социальных медиа.

Именно КО как главный объект практического анализа фактически включает в себя все многообразие различных сторон объективной действительности, которые учитываются и оцениваются в процессе организации деятельности органов внутренних дел (ОВД).

Поэтому совершенно естественно, что проблемы изучения и оценки криминогенной обстановки нашли в научной литературе довольно широкое освещение [1–7]. Многие из имеющихся в этой сфере разработок на соответствующих этапах их создания, применения и оценивания оказали существенное влияние на практику управленческой деятельности ОВД, способствовали улучшению качества аналитической работы.

Моделирование как аналитический инструментарий

При разработке методологии математического моделирования КО в указанных выше работах выделены следующие аспекты:

– особенности обслуживаемой ОВД территории (объекта), состояние преступности, характеристики сил и средств реагирования;

¹ © Минаев В. А., 2024.

- условия, в которых происходит деятельность СЧР по реагированию на ситуацию;
- совокупность факторов, обуславливающих криминальные явления и ситуации;
- совокупность данных, характеризующих состояние и динамику криминальной ситуации, эффективность использования сил и средств при ее ликвидации.

Характерным признаком для процесса моделирования КО является выраженный функциональный подход. При этом отмечается уход от простых подходов и методов, применявшихся в области теории и практики исследования КО, к выработке качественно нового подхода, использованию более сложных и глубоких методов и средств. Это обуславливается объективными изменениями окружающей действительности, возрастанием уровня требований к деятельности ОВД и ее конечным результатам, развитием взаимодействия социальных и естественных наук, внедрением современных технологий обработки и анализа информации.

Результаты изучения КО играют основную роль при подготовке и принятии управленческих решений в ОВД; они позволяют рационально использовать имеющиеся ресурсы, осуществлять конкретные мероприятия по оптимизации деятельности подразделений и повышению их влияния на КО. При этом создаются предпосылки для решения задач прогнозирования развития КО, происходит выбор основных направлений деятельности ОВД, оценивается эффективность функционирования их систем.

Сложность КО и многогранность практических задач, связанных с ее изучением и оценкой, объективно предопределяют целесообразность разработки новых концепций избранного объекта исследования на основе системной методологии. Ценность системного подхода заключается в возможности, несмотря на огромное разнообразие различных явлений и процессов, применить к исследованию общие концептуальные схемы, использовать единый формально-логический аппарат и получить на этой основе новые результаты, относящиеся к объекту анализа – криминогенной обстановке.

Будучи основной методологической предпосылкой моделирования, системный подход служит своеобразным мостом между реальной КО и моделями ее изучения. Если КО, как реальный объект изучения, представима различными системами, так и каждая из них может служить основанием для построения моделей, отличающихся конкретными средствами, так и адекватностью. Речь может идти о разработке множества взаимодополняющих моделей и их применении для изучения КО. В настоящей статье кратко рассмотрим подходы к моделированию КО в трех актуальных и пока мало исследованных направлениях ее современного развития в киберпространстве: обеспечение кибербезопасности беспилотного транспорта, деструктивные воздействия в социальных медиа, распространение сетевых протестных настроений.

Обеспечение кибербезопасности беспилотного транспорта

Беспилотный транспорт проникает во многие сферы нашей жизни и отрасли хозяйствования. Активно начали развиваться все его виды: автомобильный, авиационный, железнодорожный, морской. Беспилотные автомобили становятся неотъемлемой частью умных городов, строятся специализированные трассы

с необходимой инфраструктурой для движения беспилотных автомобилей. По оценкам из открытых источников к 2027 г. производство БПЛА в России достигнет 2 млн шт. в год, на дорогах появится не менее 100 тыс. беспилотных автомобилей.

Однако в описанной благоприятной картине есть и негативная сторона. А именно, из-за подчас бесконтрольного применения беспилотных транспортных средств (БТС) расширяется возможность совершения противоправных актов: террористических, шпионских действий и других криминальных эксцессов.

Этому способствуют складывающаяся геополитическая обстановка, развитие высоко технологичных средств, тотальная цифровизация общественной жизни, имеющая и криминальные аспекты.

И хотя в России принимаются меры государственной поддержки, которые направлены на стимулирование развития беспилотного автомобильного транспорта [17] и беспилотных авиационных систем (БАС) [18], при этом наблюдается недостаток, а иногда – отсутствие необходимого регулирования в сфере беспилотного транспорта.

Для предотвращения криминальных инцидентов необходима система, которая обеспечит:

- полный контроль трафика в границах важных социальных зон, защищаемых объектов критической инфраструктуры;
- киберустойчивость БТС и защиту от их неправомерного применения;
- контроль выполнения маршрутных (полетных) заданий, выявление и предотвращение аномалий в поведении БТС;
- соответствие функционирования БТС законодательству Российской Федерации и требованиям регуляторов по безопасности их применения.

Отметим, что в сфере, относящейся к кибербезопасности, в последние годы появилось немало научных публикаций [8–12] и нормативных работ [13–15].

Однако применительно к беспилотному транспорту эта проблема только начинает решаться учеными и специалистами, все более актуализируясь. Именно это и обусловило появление настоящей статьи. Опираясь на понятия «кибербезопасность», «киберустойчивость», автор делает в ней акцент на том, что при защите систем управления БТС необходимо в первую очередь, уделять особое внимание таким аспектам, которые связаны с действиями, направленными на нарушения в управлении движением, приводящими к авариям, крушениям, катастрофам, гибели пассажиров и иных членов общества.

Кроме того, необходимо рассматривать и противоправные действия, связанные с кражей грузов, персональных данных или другой конфиденциальной информации.

Под *угрозами кибербезопасности беспилотного транспорта* будем понимать совокупность условий и факторов, создающих реальную или потенциальную опасность потери управления транспортной системой из-за нарушения конфиденциальности, целостности, доступности информации, циркулирующей в системе управления БТС.

Реализация угроз кибербезопасности, в первую очередь, связана с уязвимостями в системе управления БТС, которая представляет собой комплекс программно-аппаратных средств и каналов связи, обеспечивающих управление без участия человека.

Существующие системы управления беспилотным транспортом используют различные технологии, включая системы глобального позиционирования, радары, лидары, камеры, датчики и сенсоры, которые собирают информацию об окружающей среде. Программное обеспечение систем управления реализует алгоритмы и модели, которые обрабатывают эту информацию и принимают решения о движении БТС.

Важную роль в системах управления беспилотным транспортом играют технологии искусственного интеллекта. Он используется для обработки информации, принятия решений и управления БТС. Искусственный интеллект может использоваться для обучения моделей и алгоритмов, которые помогают БТС принимать решения о движении и обеспечивать безопасность. Он также может использоваться для анализа данных и прогнозирования поведения участников дорожного движения.

Вместе с тем, необходимо учитывать киберугрозы инфраструктуре, необходимой для систем управления беспилотным транспортом. Она включает такие элементы как система связи, системы хранения и обработки данных, системы организации и управления движением, которые помогают БТС ориентироваться в пространстве и корректно двигаться по маршруту.

Следует отметить, что из-за незаконной санкционной политики Запада в отношении нашей страны затруднен доступ к международным базам уязвимостей и индикаторам компрометации, источникам данных об угрозах. Это частично приводит к «ослеплению» средств киберзащиты.

На это накладываются факторы продолжающейся эксплуатации зарубежного программного обеспечения (ПО) и ресурсов сети Интернет, а также отказов в технической поддержке IT-оборудования и обновления ПО со стороны недружественных государств. Очевидно, в этих условиях возрастает вероятность реализации кибератак на системы управления транспортом, а ее обеспечение необходимой защитой становится иногда нетривиальной задачей.

Для обеспечения системности и единства подходов к решению вопросов кибербезопасности беспилотного транспорта предлагается разработать систему моделей угроз (МУ) информационной безопасности, адаптированных к конкретным видам, типам и уровням автономности БТС.

Предлагаемая система моделей угроз безопасности включает в себя три вида моделей:

- базовую МУ безопасности информации беспилотного транспорта, основанную на иерархии уровней автономности БТС;
- типовые МУ безопасности составных частей системы управления БТС;
- частные (по видам БТС) модели угроз (ЧМУ).

Принимая во внимание, что развитие беспилотного транспорта включено в приоритетные направления проектов технологического суверенитета страны [19],

и формирование отрасли БТС носит опережающий характер, подчеркнем необходимость учета соответствующих факторов при анализе, оценке и прогнозировании криминогенной обстановки с тем, чтобы обеспечивать ситуационную осведомленность и поддержку управленческих решений ОВД.

Деструктивные воздействия в социальных медиа

Современное общество в сфере межличностного взаимодействия активно использует социальные медиа (СМ) – технологии обмена различной информацией. К СМ относят не только социальные сети (ВКонтакте, Одноклассники), видеохостинги (TikTok, YouTube), но и сервисы обмена мгновенными сообщениями (WhatsApp¹, Telegram).

В связи с общедоступностью и простотой реализации анонимности СМ все в большей мере используются в незаконных целях – для распространения экстремистского контента (ЭК). С правовой точки зрения к ЭК относятся частичные или полные версии материалов, отнесенных к экстремистским в соответствии с решениями суда и находящихся в Федеральном списке экстремистских материалов Минюста России (ФСЭМ).

Согласно Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, распространение ЭК является одной из информационных угроз. Таким образом, проблема носит государственный характер и, конечно же, должна учитываться при изучении криминогенной обстановки.

Распространением ЭК в целях подрыва общественной безопасности и снижения доверия к структурам законной власти могут заниматься как отдельные адепты-идеологи, организованные радикальные группы (террористические формирования, объединения националистов), так и недружественные государства. В свою очередь, функции по выявлению ЭК и борьбе с его распространением возложены на государственные органы: ФСБ России, МВД России, Роскомнадзор, Генеральную прокуратуру Российской Федерации.

Согласно Федеральному закону № 149-ФЗ владельцы СМ обязаны самостоятельно осуществлять мониторинг своих ресурсов на наличие в них информации противоправного характера. Вместе с тем, владельцы до сих пор не торопятся осуществлять полноценный мониторинг своих СМ. Это обстоятельство еще больше усугубляет проблему контроля распространения ЭК.

В соответствии с данными Генеральной прокуратуры Российской Федерации [16] (рис. 1) с 2019 г. после определенного снижения наблюдается стремительный рост преступлений экстремистской направленности (ПЭН). Из анализа приведенных данных следует вывод о возрастании проблемы контроля распространения ЭК в СМ.

Наиболее распространенным форматом контента остается текстовый. Такой формат легче другого (видео-, аудио-, фото-) создать, разместить и, что самое главное – модифицировать.

¹ Запрещена в России: принадлежит корпорации Meta, которая признана в России экстремистской.

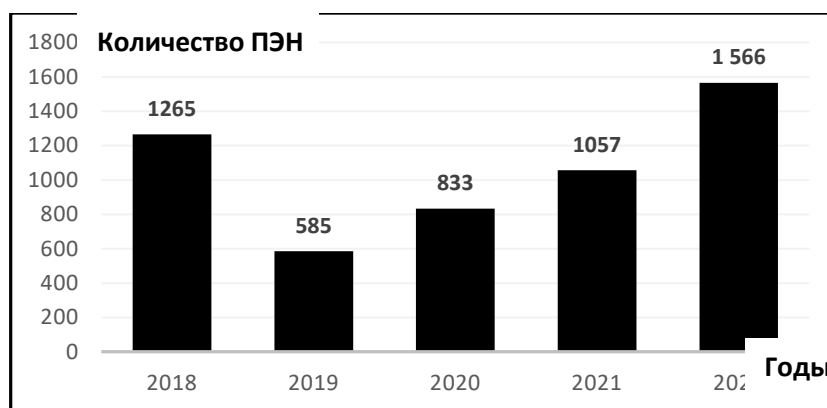


Рис. 1. Динамика преступлений экстремистской направленности

Сегодня по количеству распространяемого текстового контента лидирует Telegram. Отметим, что Роскомнадзор уже принимал меры в отношении Telegram из-за несоблюдения им порядка работы с запрещенной к распространению в России деструктивной информации.

Ежемесячно в русскоязычном сегменте Telegram создается более 700 млн сообщений. Такой информационный трафик невозможно анализировать на предмет деструктивности исключительно силами экспертов, необходимо применять автоматизированные методы, в том числе – основанные на алгоритмах искусственного интеллекта.

«Просеивание» ТГ-каналов состояло из следующих этапов:

1. Формирование обучающего корпуса для обучения BERT.
2. Выбор архитектуры BERT. Обучение классификатора.
3. Выгрузка сообщений из анализируемых ТГ-каналов.
4. Оценка наличия экстремизма в сообщениях.
5. Оценка ТГ-каналов на экстремизм.

Опишем этапы подробнее.

Этап 1. Обучалась искусственная нейронная сеть (ИНС) BERT на релевантных корпусах текстов. Корпуса текстов выбирались только двух классов: нейтральный и экстремистский.

Обучающая выборка нейтрального класса состояла из следующих тематических корпусов:

- 1) пользовательский – применен набор твитов из работы [9];
- 2) новостной – использован набор новостных сводок интернет-издания «Лента»;
- 3) исторический – включен ряд книг об истории Второй мировой войны;
- 4) еврейской культуры – создан на основе еврейской культурной и исторической литературы;
- 5) исламской культуры – создан на основе религиозной литературы, рекомендованной муфтиятами России.

Корпуса 1–2 использовались для моделирования традиционного наполнения ТГ-каналов, а 3–5 в качестве шумовых корпусов с целью снижения ложных срабатываний классификатора.

Выборка экстремистского класса создана из материалов ФСЭМ и включает в себя следующие корпуса:

1) террористический – содержащий запрещенные к распространению материалы радикального ислама, пропагандирующие терроризм;

2) националистический – собранный из различных шовинистических и антисемитских материалов, пропагандирующих превосходство на основе расовой или национальной принадлежности;

3) нацистский – корпус, состоящий из литературы и мемуаров лидеров Третьего рейха, а также литературы, в которой реабилитируются преступления нацистского режима Германии.

Этап 2. Для использования обучающей выборки, сформированной на первом этапе, осуществлена ее предварительная обработка. А именно, из массива текстов удаляются специальные символы за исключением знаков препинания, специальным образом преобразуются ссылки и сайты.

В качестве входных в BERT подаются только токенизированные данные. Токенизация – это процесс разделения слов на единицы (токены), которым в соответствии со специальным словарем имеется однозначное числовое представление.

Процесс обучения BERT можно делить на три подзадачи:

1. Предварительное обучение – позволяет «научить» модель конкретному языку, его семантическим и синтаксическим особенностям. Данная задача решена разработчиком `gubert-tiny2`, в связи с чем обучать модель с нуля нет необходимости.

2. Доменная адаптация – обучение BERT на специфических корпусах текстов, редко встречающихся в обычной литературе. В нашем случае к ним относятся корпуса экстремистского контента, поэтому доменная адаптация проводилась.

3. Тонкая настройка – процесс обучения BERT для решения конкретной задачи (классификация текстов, извлечение сущностей, поиск похожих предложений и т. д.).

В качестве обучающей выборки использовались 85% всех данных, остальные 15 % использовались для оценки работы классификатора. Качество классификации оценивались *F*-мерой, представляющей гармоническое среднее между точностью и полнотой. Использование *F*-меры обусловлено тем, что она учитывает и полноту, и точность работы классификатора, что очень важно при неравномерных выборках.

Этап 3. Для загрузки необходимой информацией используется библиотека `telethon`. Для того, чтобы получить информацию с определенных каналов, необходимо было создать пользователя, с которым посредством библиотеки `telethon` будет происходить взаимодействие.

Этап 4. Для оценки наличия экстремизма в сообщениях перед подачей текстов на вход классификатора происходит их первичная фильтрация по объему символов. Это необходимо для снижения большого количества ложных срабатываний. После этого сообщения, прошедшие первичную фильтрацию, подвергаются обработке, описанной на втором этапе.

Этап 5. Для каждого канала рассчитываются следующие показатели:

1) *N* – количество всех проанализированных сообщений;

- 2) N_{ME} – количество экстремистских сообщений;
- 3) N_{MN} – количество нейтральных сообщений;
- 4) $x_{ME} = \frac{N_{ME}}{N}$ – доля противоправных сообщений в канале;
- 5) $x_{MN} = \frac{N_{MN}}{N}$ – доля нейтральных сообщений.

Приведенные показатели позволяют ранжировать каналы по критерию экстремистской направленности, обеспечивая поддержку принятия решений операторам для дальнейшего точечного анализа каналов и сообщений.

Результаты экспериментов

Для оценки метода и реализованной на его основе программы проведен отбор 68 телеграмм-каналов, материалы которых отражали каждый из текстовых корпусов.

При экспертном анализе выявлено, что в указанных каналах присутствуют цитаты и выдержки из экстремистских материалов нацистского, националистического или террористического содержания.

На рис. 2 представлена общая статистика по всем проанализированным каналам, сгруппированным по категориям. В качестве столбцов на гистограмме представлена доля экстремистских сообщений в их общем количестве.

Из рис. 2 видно, что наибольшее количество экстремистского контента выявлено в каналах нацистской категории. Экстремистские сообщения в каналах террористической категории и категории радикального национализма составили около половины.

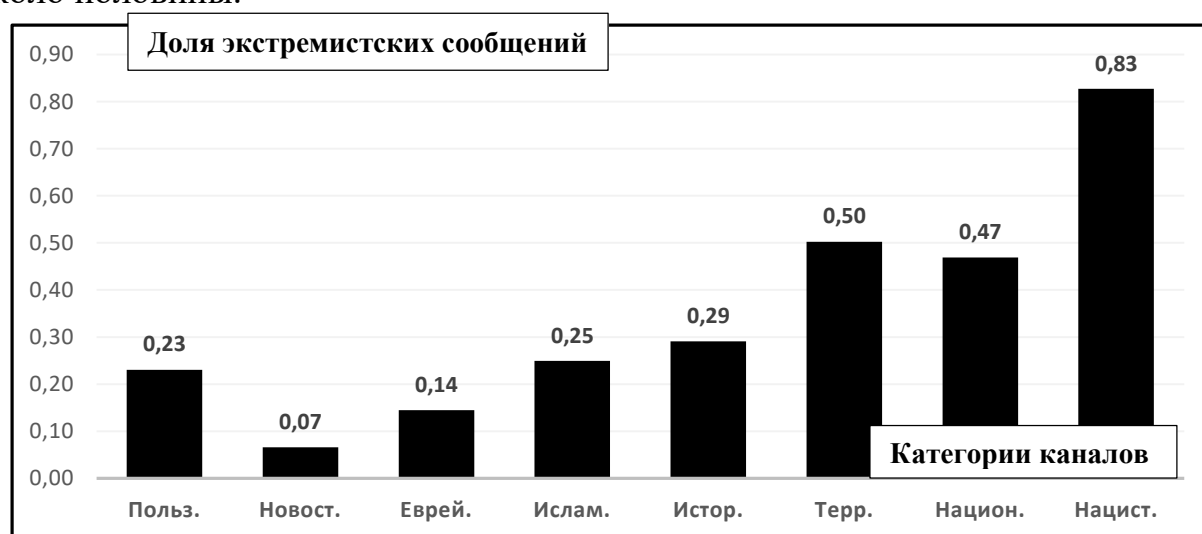


Рис. 2. Доля сообщений экстремистского характера в каналах (по категориям)

Таким образом, описан метод фильтрации ТГ-каналов при поиске контента экстремистского характера с использованием глубокой искусственной нейронной сети BERT. На основе разработанного метода создан программный продукт, выполняющий автоматический сбор, анализ и классификацию сообщений в ТГ-каналах, направленные на поддержку принятия решений в сфере противодействия распространению экстремистской информации.

Для компьютерных экспериментов по «просеиванию» ТГ-каналов сформирован список по их восьми различным категориям, подвергшимся дальнейшему

анализу. Приведенные эксперименты показали эффективность разработанного метода.

Представленный подход к фильтрации ТГ-каналов на наличие экстремистских сообщений ориентирован на применение в работе государственных структур, занимающихся выявлением и мониторингом распространения противоправной информации.

Распространение сетевых протестных настроений

В рамках изучения криминогенной обстановки важное место стала занимать задача идентификации ролей пользователей в социальных медиа, включая их место в сетевых протестных настроений. Обсудим результаты, полученные при анализе эмпирических данных, отражающих распространение фейковой информации по темам «Жыве Беларусь» и «Дворец Путина».

Отметим, что большинство негативных информационно-психологических воздействий сегодня наиболее эффективно достигает своей результативности (вовлечение в преступную среду, экстремистские движения, суицидальные сообщества и т. п.) посредством социальных медиа (СМ). Создаваемые при этом информационные волны, инициируемые конкретными социальными поводами, вбрасываются в сеть, усиливаются многочисленными обсуждениями, находя одобрение среди определенного контингента ее пользователей.

Организацию и поддержание требуемого вектора развития деструктивных воздействий осуществляют конкретные пользователи, играющие определенные роли в СМ. Наибольшее негативное воздействие оказывают те из них, которые имеют максимальный уровень информационного влияния.

Таким образом, очевидна актуальность разработки эффективных методов идентификации ролей пользователей и уровня их влияния в СМ. Это обеспечивает необходимый уровень поддержки решений при организации противодействия целенаправленным деструктивным влияниям, распространению деструктивной идеологии в пространстве СМ.

В работе [7] анализируются протестные тенденции в России и делается вывод о повышении эффективности протестов при построении их по сетевому принципу, когда существенно увеличивается скорость распространения призывов к ним. В ней с помощью технологии СЕУС собраны данные о пользователях, опубликовавших материалы в социальной сети (СС) ВКонтакте по информационным поводам «Жыве Беларусь» (выборы президента Республики Беларусь в 2020 г.) и «Дворец Путина» (в начале 2021 г.), а также данные о количестве их постов, репостов и комментариев по исследуемой тематике. В результате выявлены пользователи, которые вовлечены в целевую тематику, составив протестную сеть.

Для определения связей выявленных пользователей собраны данные об их друзьях и друзьях их друзей в сети. Такой подход объясняется тем, что количество связей очень сильно зависит от того, с кем именно связан пользователь. При одинаковом количестве друзей на первом уровне их количество на втором может различаться на порядки.

Практический опыт показал, что дальнейшее увеличение уровней в графе нецелесообразно. К тому же резко возрастает объем вычислительных ресурсов, требуемых для сбора графовой информации, построения графов.

Статистические данные по обоим информационным поводам представлены в табл. 1.

Таблица 1

Статистические данные выборки по пользователям, вовлеченным в тематику «Жыве Беларусь» и «Дворец Путина»

№ п/п	Показатель выборки	Информационный повод	
		«Жыве Беларусь»	«Дворец Путина»
1	Количество вовлеченных пользователей	28 447	35 502
2	Количество опубликованных материалов	42 148	61 967
3	Количество друзей и друзей их друзей	18 508 073 467	4 161 468 616

По каждой выборке сформирован рейтинг публикационной активности путем сортировки пользователей по количеству опубликованных ими материалов. Рейтинг публикационной активности по информационному поводу «Дворец Путина» представлен на рис. 3.

Как видно из рис. 3, из 35 тыс. пользователей только около 500 имеют значимое количество публикаций, что составляет 1,4 % от их общего количества в рейтинге. В том числе, только первые 100 пользователей имеют уровень активности выше 20 публикаций. Остальные имеют крайне низкую активность.

Схожая зависимость рейтинга публикационной активности наблюдалась и по теме «Жыве Беларусь» [7].



Рис. 3. Рейтинг публикационной активности по теме «Дворец Путина»

В каждой информационной волне, связанной с каким-либо инфоповодом, конкретные пользователи выполняют определенные роли. Одни пользователи

в СС генерируют идеи, другие их распространяют, третьи комментируют, а четвертые «накручивают лайки», чтобы поднять популярность распространяемой идеи. Набор и определение социальных ролей пользователей зависят от типа сообщества и от контекста, в котором рассматриваются роли.

В контексте противодействия протестной активности граждан в СМ выделяются следующие типы ролей:

1. Постер – генератор идей, создатель контента. Он часто является лидером общественного мнения и при наличии большого количества связей может объединять вокруг себя большое количество пользователей.

2. Репостер – распространитель идей. Этот пользователь редко создает контент, а, в основном, репостит уже готовые публикации, нацелен на максимальное распространение чужого контента.

3. Комментатор – не создает контент и не репостит его, но оставляя множество своих комментариев, участвует в осуждениях и спорах. Часто создает комментарии для увеличения популярности темы обсуждения.

4. Пассивный участник – пользователь, который не очень активен в сети в части создания контента, репостов или комментариев. Но такой пользователь регулярно посещает различные страницы в СС, является реципиентом информации, созданной постерами, репостерами и комментаторами.

По результатам исследований авторов, параметрами, которые существенно влияют на различие пользователей по ролям и на основании которых выполнялась их классификация, выступают: возраст аккаунта, количество друзей, количество опубликованных постов, количество опубликованных репостов, количество опубликованных комментариев.

Для определения ролей пользователей решалось две основных задачи.

Первая задача состояла в том, чтобы выделить в массиве пользователей активных и пассивных. Результаты деления представлены в табл. 2.

Таблица 2

**Активные и пассивные пользователи, вовлеченные в тематику
«Жыве Беларусь» и «Дворец Путина»**

№ п/п	Параметр	«Жыве Беларусь»	«Дворец Путина»
1	Всего пользователей, в том числе:	28 447	35 502
2	Активные	1 257	4 847
3	Пассивные	27 190	30 655

Вторая задача состояла в том, чтобы классифицировать активных пользователей по ролям постеров, репостеров и комментаторов. Принято, что пользователь играет конкретную выраженную роль, если активность в ней составляет не менее 60 % от всех видов.

В то же время, среди активных пользователей выявились и те, кто не удовлетворяет правилу отсечки 60% ни по одному из видов активности. Такие пользователи отнесены к универсалам. Данные о ролях пользователей представлены в табл. 3.

**Выявленные роли пользователей, вовлеченные в тематику
«Живе Беларусь» и «Дворец Путина»**

№ п/п	Параметр	«Живе Беларусь»	«Дворец Путина»
1	Всего пользователей, в том числе:	28 447	35 502
2	Пассивные	27 190	30 655
3	Постеры	81	531
4	Репостеры	74	1 050
5	Комментаторы	521	132
6	Универсалы	581	3 134

Ведущим фактором воздействия на функционирование ОВД является криминогенная обстановка со всем сложным комплексом ее характеристик. Именно она выступает предметом тщательного изучения, анализа, оценки и прогнозирования, поскольку полученные при этом результаты создают базу формирования эффективных управленческих решений по надежному функционированию территориальных подразделений, определяют смысл, последовательность, качественные и количественные параметры использования сил и средств с реальными негативными изменениями криминогенной обстановки.

Аналитическое исследование статистических и иных сведений, отражающих состояние криминогенной обстановки, осуществляется органами ОВД с использованием различных методов и средств математического обеспечения. Среди математических возможностей все более значимое место для решения указанных задач занимает математическое моделирование, позволяющее глубоко и разносторонне обеспечивать современный анализ огромного массива сведений о криминогенной обстановке, системно решая частные задачи управления, в том числе используя имитационное моделирование и большие данные.

В статье кратко рассмотрены подходы к моделированию криминогенной обстановки в трех актуальных и пока мало исследованных направлениях ее современного развития в киберпространстве: обеспечение кибербезопасности беспилотного транспорта, деструктивные воздействия в социальных медиа, распространение сетевых протестных настроений.

Список литературы

1. Герасимов В. В. Оценка оперативной обстановки: цели, задачи, пути совершенствования // Вестник МВД России. 2006. № 5. С. 17–23.
2. Клушин О. З. Оперативная обстановка: понятие, анализ, прогноз : учебное пособие. М. : Академия управления МВД России, 2009. С. 15–16.
3. Минаев В. А. Кадровые ресурсы органов внутренних дел: современные подходы к управлению. М. : Академия МВД СССР, 1991.
4. Минаев В. А., Бондарь К. М. Опыт и перспективы математического моделирования криминогенной обстановки // Криминологический журнал. 2022. № 1. С. 103–110.

5. Минаев В. А., Курушин В. Д., Захаров Д. В. Математическое моделирование региональных криминологических процессов. Новосибирск, 1992.
6. Математические модели анализа, оценки, прогнозирования и управления в органах внутренних дел : монография / [В. А. Минаев и др.]. Хабаровск : Дальневосточный юридический институт МВД России, 2022.
7. Противодействие экстремистской идеологии в социальных медиа: математические модели и методы : монография / [В. А. Минаев и др.] ; под ред. В. А. Минаева, К. М. Бондаря. Хабаровск: Дальневосточный юридический институт МВД России, 2023.
8. Скаридов А. С. К вопросу о детерминации морских автономных надводных средств применительно к правовому регулированию коммерческого судоходства // Океанский менеджмент. 2022. № 1 (15). С. 44–46.
9. Петрова Д. А., Губкина А. И. Захват американского беспилотного (автономного) подводного аппарата в Южно-Китайском море: правовые и политические аспекты // БГЖ. 2019. № 4 (29). С. 375–377.
10. Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022. № 1 (47). С. 1–9.
11. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибербезопасности. 2014. № 4 (38). С. 39–42.
12. Основы кибербезопасности : учебник / [С. А. Винокуров и др.]. Воронеж ; М. : Воронежский институт МВД России : Московский университет МВД России имени В.Я. Кикотя, 2023.
13. ГОСТ ISO/IEC 27100:2020. Информационная технология. Кибербезопасность. Обзор и концепции.
14. Умные города, инфраструктуры и их антитеррористическая устойчивость. Опыт интеграции антитеррористических стандартов США и создания программного обеспечения для цифровой безопасности / [И. А. Соколов и др.] // International Journal of Open Information Technologies. 2017. Т. 5. №. 7. С. 45–65.
15. International Organization for Standardization, ISO/IEC 27000 – Information Security, ISO/IEC, 2022. URL: <https://www.iso.org/isoiec-27001-information-security.html>.
16. Показатели преступности России // Портал правовой статистики. URL: http://crimestat.ru/offenses_chart.
17. Распоряжение Правительства Российской Федерации от 29 марта 2018 г. № 535-р «Об утверждении плана мероприятий (“дорожной карты”) по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению “Автонет”» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/documentcons_doc_LAW_295296/.
18. Постановление Правительства Российской Федерации от 21 июня 2023 г. № 1630-р «Об утверждении Стратегии развития беспилотной авиации Российской Федерации на период до 2030 года и на перспективу до 2035 года и плана

мероприятий по ее реализации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/documentcons_doc_LAW_450667/.

19. Постановление Правительства Российской Федерации от 15 апреля 2023 г. № 603 «Об утверждении приоритетных направлениях проектов технологического суверенитета и проектов структурной адаптации экономики Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/documentcons_doc_LAW_80001/.

Минетуллина А. Р.¹,

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

Научный руководитель: Александров Ю. Н.,

заместитель начальника кафедры информатики и математики
Московского университета
МВД России имени В.Я. Кикотя

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ В КРИМИНАЛИСТИКЕ: ИННОВАЦИОННЫЕ ПОДХОДЫ И ПЕРСПЕКТИВЫ ДЛЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ В ЦИФРОВУЮ ЭПОХУ

В современную цифровую эпоху правоохранительные органы сталкиваются с новыми проблемами, вызванными инновационными формами преступности. Технологии постоянно развиваются, порождая новые формы преступной деятельности [1]. Это обуславливает необходимость внедрения современных биометрических технологий в сфере криминалистики для эффективной борьбы и предотвращения таких преступлений, которые предполагают инновационные подходы и многообещающие перспективы для правоохранительных органов.

Биометрия представляет собой процесс автоматического опознавания личности, основанный на уникальных физиологических и поведенческих особенностях человека. Эти технологии лежат в основе множества надежных методов идентификации и подтверждения личности. К физиологическим особенностям относятся изображение рисунка папиллярных линий пальцев рук, черты лица и радужки глаз, а к поведенческим – динамическая проверка подписи, голоса и динамика нажатия клавиш.

Биометрические системы отличаются по уровню сложности, функциональности и производительности, они могут быть использованы для проверки и отождествления личности человека. В биометрических технологиях выделяют системы распознавания лиц, отпечатков пальцев, радужных оболочек глаза, сетчатки, а также верификация подписей и голоса. Разработчики активно работают над новыми биометрическими методами, включая отпечатки пальцев, рисунок вен, ДНК, форму уха, специфический запах тела, голографию и сканирование тела [2].

На сегодняшний день биометрические технологии применяются в различных государственных и коммерческих сферах, включая контроль за доступом, распознавание нарушителей, мониторинг, а также в таможне и пограничном контроле. Кроме того, они используются в системах социальных выплат, торговых сетях, в системах электронного голосования и так далее. С 2018 г. в России действует Единая биометрическая система [3], которая обеспечивает идентификацию личности при получении государственных и коммерческих услуг. Она является

¹ © Минетуллина А. Р., 2024.

национальной цифровой платформой, которая была создана для того, чтобы вся биометрия хранилась в защищенной от утечек Единой государственной системе, в целях защиты биометрических данных граждан от несанкционированного использования коммерческими организациями. Это инфраструктура была создана в рамках стратегии «цифровая экономика Российской Федерации» и использует биометрические данные, такие как лицо и голос, для определения живого человека, а не его имитации. Система также способна выявлять аномалии и обнаруживать мошенников в процессе удаленной идентификации, а также усиливает защиту банковских систем от мошенничества.

Цель криминалистики – это полное своевременное технико-криминалистическое обеспечение и сопровождение раскрытия и расследования преступлений, которое реализуется на основе всестороннего использования достижений современной науки и техники. Поэтому внедрение биометрических технологий имеет большое значение для правоохранительных органов, в особенности, в сфере распознавания лиц, в связи с широким распространением камер видеонаблюдения. Следовательно, биометрические технологии поспособствуют повышению темпа развития идентификации не только в правоохранительной деятельности, но и в другие сферы деятельности человека, повышая ее безопасность.

Примерами использования биометрических технологий могут быть:

- в сфере поиска пропавших и «трафика людей» по биометрическим данным внешнего облика;
- предотвращение коррупции и злоупотребления должностными полномочиями, путем проверки и учета действий должностных лиц;
- повышение уровня защиты персональных данных граждан для предотвращения кражи личности и мошенничества, связанных с использованием чужих данных;
- сбор и анализ данных для выявления подозрительного поведения и принятия мер по предотвращению преступлений до их совершения и др.

Принимая во внимание все достоинства биометрических технологий, нужно выделить и недостатки, которые связаны с ограничением их использования в криминалистической деятельности правоохранительных органов. Они включают в себя проблемы конфиденциальности, технологические ограничения, а также необходимость формирования новых законов и правил.

Для этого необходимо тщательно рассмотреть этические и социальные последствия, а также разработать руководящие принципы, которые учитывали бы мнения различных заинтересованных сторон. В России уже начались продвижения в этой сфере, поэтому с 2023 г. все биометрические данные должны храниться в Единой биометрической системе, а с 1 января 2024 г. в личном кабинете на Портале государственных услуг Российской Федерации [4] появилась возможность ознакомиться со всеми своими согласиями на обработку биометрических данных и отказами от сбора и размещения биометрии, которая дает возможность отследить использование биометрических данных и делает процесс работы с ними абсолютно прозрачным.

Технологические ограничения связанные с проблемами распознавания лиц в визуальном спектре включают в себя влияние освещение и распознавание масок или фотографии, некоторые системы распознавания лиц могут требовать неподвижного или позирующего лица для получения изображения.

В целом, интеграция биометрических технологий в правоохранительную деятельность предполагает инновационный подходы и многообещающие перспективы для правоохранительных органов цифровой эпохи. По мере продвижения в цифровую эпоху биометрические технологии будут развиваться и становиться еще более совершенными и дешевыми. Поэтому правоохранительные органы должны продолжать инвестировать в эти технологии и изучать новые инновационные подходы в использовании биометрических данных в уголовных расследованиях. При наличии необходимых инструментов и подготовки правоохранительные органы могут использовать возможности биометрических технологий для повышения общественной безопасности и защиты населения.

Список литературы

1. Banday M. T. and Mir F. A. A study of Indian approach towards cyber security // 1st International Conference on Emerging Technology Trends in Electronics, Communication & Networking. Surat. India. 2012. P. 1–6.
2. Vacca, John R. Biometric technologies and verification systems // 1st Edition Library of Congress Cataloging-in-Publication Data. 2007.
3. Единая биометрическая система // Официальный сайт. URL: <https://ebs.ru>.
4. Портал государственных услуг Российской Федерации // Официальный сайт. URL: <https://www.gosuslugi.ru/help/faq/biometrics>.

*Миронова Е. Ю.¹,
ассистент кафедры уголовного процесса
и прокурорского надзора
Байкальского государственного университета*

К ВОПРОСУ О КАТЕГОРИИ СПРАВЕДЛИВОСТИ В АСПЕКТЕ ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Справедливость, будучи нравственной категорией, имеет специфический уголовно-процессуальный смысл, выступая сразу в нескольких ипостасях:

- как одно из нравственных начал уголовного судопроизводства;
- как нравственное требование (качество) приговора, имеющее законодательное закрепление, а также как требование, предъявляемое к процессуальным действиям и решениям;
- как нравственное качество судьи, рассматривающего уголовное дело.

Ученые-процессуалисты во все времена придают справедливости большое значение, а интерес к этой категории не только не утрачивается, но и оживляется в свете цифровых преобразований уголовно-процессуальной сферы.

Справедливость как нравственный стержень уголовного судопроизводства рассматривает Т. Н. Москалькова, называя ее мерилom нравственно допустимого и недопустимого в этой области [7, с. 94].

По мнению советского ученого-правоведа Ю. М. Грошевого, справедливое разрешение дела означает его соответствие требованиям нравственности, при этом оно возможно лишь на основании правильного применения требований закона при постановлении приговора [2, с. 125].

В этом ключе последовательным видится мнение С. В. Корнаковой, В. А. Щербакова о том, что обеспечение требования справедливости приговора предполагает соблюдение при его вынесении требований законности и обоснованности, что означает его соответствие правовым и социально-нравственным принципам [4, с. 131].

Таким образом, анализ разных источников указывает на то, что понятие справедливости во все века неразрывно связано с законностью, неукоснительным соблюдением правовых установлений.

Придав этому тезису аксиоматический характер, попытаемся определить степень влияния цифровизации на справедливость в уголовно-процессуальном аспекте. При этом определим, какое влияние искусственный интеллект способен оказать на справедливость в уголовном судопроизводстве.

В XXI в. стало возможным применение искусственных интеллектуальных систем, нейросетей, больших данных, предиктивной аналитики при разрешении уголовного дела как в досудебном производстве, так и в суде [8].

Такие тенденции наблюдаются и в отечественном судопроизводстве. Официальное заявление, сделанное В. В. Момотовым относительно внедрения в 2024 г.

¹ © Миронова Е. Ю., 2024.

суперсервиса «Правосудие онлайн» [11], предопределило участь искусственного интеллекта в российском правосудии на ближайшую перспективу. Его главная задача будет заключаться в «автоматизированном составлении проектов судебных актов на основе анализа текста процессуального обращения и материалов судебного дела, расшифровки аудиопrotocolов, создания интеллектуальной поисковой системы с возможностью анализа и систематизации судебной практики» [11].

Исследуя этические проблемы внедрения искусственного интеллекта в судебную систему России, Д. Э. Гаспарян, Е. М. Стырин указывают: «ИИ-судья олицетворяет идеал абсолютной непредвзятости, беспристрастности и неподкупности» [1, с. 23].

Подвергая глубокому и пространному анализу справедливость в уголовном судопроизводстве, Н. А. Колоколов, в некотором смысле предвосхищая трансформации нравственной составляющей уголовного судопроизводства, указывает, что отчужденная, неперсонифицированная справедливость мгновенно превращается в бездушную машину власти, а также отмечает, что в обществе распространено представление о справедливости как механизме, и не случайно в научном обороте применяется термин «справедливость судебной машины» [3, с. 5], который грозит стать максимально буквальным в том случае, если цифровизация достигнет пределов, когда вершителем правосудия станет искусственный интеллект.

В судебной практике случаи вынесения несправедливого приговора явление нередкое. Будучи убежденными в наличии такого явления в сфере осуществления правосудия по уголовным делам, как несправедливость, обратим внимание на мнения, высказываемые исследователями относительно справедливости судебных решений, выносимых машинами. Так, Е. Волох, ведя рассуждения о роботах-судьях, делает акцент на необходимости стремления не к справедливым судьям, а справедливым судебным решениям [10, с. 1163]. В этой связи Н. Н. Кравчук убедительно отмечает, что такие решения ИИ-судья производить в состоянии [5, с. 119].

Вместе с тем, для уравнивания позиций необходимо отметить, что имеют место случаи, когда искусственный интеллект проявил дискриминационный подход в уголовно-процессуальной сфере. Как минимум два случая неэтичного, несправедливого, дискриминационного подхода к разрешению дела произошли в процессе применения программы прогнозирования возможности совершения человеком нового правонарушения в США. Так, в деле «Лумис против Висконсина» обвиняемый оспаривает результаты оценки рисков таким инструментом, как Профилирование управления исправительными учреждениями для определения альтернативных санкций при вынесении приговора «COMPAS» (Correctional Offender Management Profiling for Alternative Sanctions) в связи с тем, что программа при оценке риска рецидива учитывала пол и расу обвиняемого, а суд, в свою очередь, обосновал обвинительный приговор результатами, выданными указанной программой [12].

Другой случай: в американском штате Джорджия местной полицией незаконно был арестован 28-летний Рэндалл Рейд, поскольку система распознавания лиц сочла его преступником. Молодого человека обвинили в краже брендовых

кошельков. Интересно, что сам Рейд никак не был похож на преступника из ориентировки: он темнокожий, но весит на 20 кг меньше настоящего преступника и не посещал населенный пункт, где была совершена кража. Однако полиция решила довериться выводам искусственного «коллеги» [13]. Таким образом, человек несправедливо был подвергнут аресту на том лишь основании, что по данным программы в будущем повторно мог совершить аналогичное преступление по той причине, что является афроамериканцем.

В подтверждение сказанному специалист по праву и нейросетям из Бостонского университета Н. Окидегбе отмечает, что практически все досудебные алгоритмы используют входные данные, отличающиеся по расовому признаку. Несмотря на то, что ни один такой алгоритм явно не использует расовую информацию в качестве входных данных, тем не менее они склонны использовать входные данные, которые тесно связаны с расой. Например, большинство досудебных алгоритмов включают аресты и (или) сведения о судимости в качестве входных данных при определении риска повторного совершения преступления, и почти всегда (случайно или нет) они связаны с историческими и текущими расовыми неравенствами, включая чрезмерную полицейскую деятельность. Во всяком случае использование этими алгоритмами незавершенных обвинений, арестов и прошлых судимостей несправедливо завышает оценки риска расово маргинализированных обвиняемых. Так, в отношении афроамериканцев, совершивших преступления в сфере незаконного оборота наркотических средств, гораздо чаще выносится решение об аресте, нежели в отношении других граждан, совершивших аналогичные правонарушения.

Как было установлено выше, уже вызвавшая неоднократно всплеск негодований общественности система «COMPAS», применяемая в США, учитывает судимости обвиняемого, прошлые аресты, прошлые приговоры к лишению свободы, и предъявленные обвинения при расчете риска повторного ареста обвиняемого. И так как исторически сложилось, что в США ранее решения об арестах, обвинительные приговоры, связанные с лишением свободы, выносились в отношении темнокожих граждан гораздо чаще, то и нейросети запрограммированы в соответствии с «устоявшимися традициями», что, безусловно, несет в себе серьезные нравственные проблемы и риски вынесения несправедливых и необъективных решений [9, с. 19].

В продолжение темы о применении программы «COMPAS» следует привести один немаловажный для практики факт. Первый в истории США алгоритмическо-статистический суд, руководимый математическим директором Google Абэ Гонгом, анализировал работу программы в течение нескольких месяцев. Итогом такой проверки стал вывод о безупречности программы в математическом и статистическом смыслах. Уязвимым местом все же осталась этническая предвзятость, которая (с учетом математической корректности программы) основана на интерпретации реальных данных [6, с. 71–72]. А это значит, что застарелые нравственные проблемы общества в условиях цифровизации уголовного судопроизводства получают новую жизнь, потому что алгоритмы создаются представителями все того же общества, которое переносит нерешенные социальные проблемы нравственного характера в виртуальное пространство.

Другой пример, преподающий аналогичный нравственный урок. Одна из популярных в США программ PredPol представляет собой алгоритм, разработанный департаментом полиции Лос-Анджелеса совместно с местными университетами. Программа собирает данные о том, где и когда совершались преступления, а затем составляет карту горячих точек – мест, где преступление, вероятно, произойдет в будущем. Исследователи из некоммерческой организации Human Rights Watch проанализировали работу PredPol и выяснили, что алгоритм часто рекомендовал полиции направлять патрули в районы, где живут преимущественно чернокожие жители.

Прогнозы специалистов, изучающих этические проблемы применения цифровых технологий, весьма неутешительны, поскольку алгоритмы, используемые искусственным интеллектом, построены на основе сложившихся в обществе предубеждений. Многие из них уверены, что искусственный интеллект, применяемый в сфере правосудия по уголовным делам, способен укоренить и обострить в обществе проблемы расизма [14].

Таким образом, анализ проблемы принятия искусственным интеллектом решений, основанных на предубеждениях, царящих в обществе и умах людей, приводит к мысли о том, что несправедливые, пристрастные решения, выдаваемые алгоритмами, – это не техническая проблема искусственного интеллекта, а нравственная проблема общества. И думается, что в этическом аспекте человечество «не доросло» до применения «умных» технологий в сфере принятия судьбоносных решений (как, в частности, в сфере уголовного судопроизводства), несмотря на некоторую технологическую зрелость.

Список литературы

1. Гаспарян Д. Э., Стырин Е. М. Прикладные проблемы внедрения этики искусственного интеллекта в России: отраслевой анализ и судебная система. М. : Издательский дом Высшей школы экономики, 2020.
2. Грошевой Ю. М. Сущность судебных решений в советском уголовном процессе. Харьков : Вища школа : Издательство при Харьковском университете, 1979.
3. Колоколов Н. А. Истина и справедливость – базовые ценности уголовного судопроизводства. Статья № 4 // Мировой судья. 2012. № 11. С. 2–9.
4. Корнакова С. В., Щербаков В. А. Справедливость обвинительного приговора: определение критериев // Юридическая наука и правоохранительная практика. 2017. № 2 (40). С. 125–131.
5. Кравчук Н. В. Искусственный интеллект как судья: перспективы и опасения (обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4. Государство и право: Реферативный журнал. 2022. № 1. С. 115–122.
6. Ларина Е. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. М. : Книжный мир, 2018.
7. Москалькова Т. Н. Нравственные основы уголовного процесса (стадия предварительного расследования) : дис. ... д-ра юрид. наук : 12.00.09. М., 1997. С. 464.

8. Chen S. China's court AI reaches every corner of justice system, advising judges and streamlining punishment // South China Morning Post. Jul 13, 2022.
9. Okidegbe N. The Democratizing Potential Of Algorithms? // Connecticut Law Review. 2022. № 53 (739). P. 1–51.
10. Volokh E. Chief Justice Robots // Duke Law Journal. 2019. № 68. P. 1135–1192.
11. Суды планируют подключить искусственный интеллект к составлению решений // Российская газета. URL: <https://rg.ru/2023/05/25/robot-pomozhet-ras-sudit.html>.
12. Loomis v. Wisconsin. Docket No 16-6387 // Scotusblog. URL: <https://www.scotusblog.com/case-files/cases/loomis-v-wisconsin>.
13. Из-за ошибки искусственного интеллекта в США арестовали невиновного афроамериканца // Overclockers. URL: <https://overclockers.ru/blog/Nacvark/show/82465/iz-za-oshibki-iskusstvennogo-intellekta-v-ssha-arostovali-nevinovnogo-afroamerikanca>.
14. Почему искусственный интеллект несправедлив? Этические проблемы технологий // ТАСС. URL: <https://tass.ru/obschestvo/11140359>.
15. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 10 июля 2018 г. № 60-АПУ18-1 // Законы, кодексы и нормативные правовые акты Российской Федерации. URL: <https://legalacts.ru/sud/apelliatsionnoe-opredelenie-verkhovnogo-suda-rf-ot-10-072018-n-60-apu18-1/>.
16. Апелляционное определение Иркутского областного суда от 6 марта 2023 г. по делу № 22-752/2023 (основания изменения решения: несправедливость приговора, неправильное применение уголовного закона) // Иркутский областной суд. URL: https://oblsud--irk.sudrf.ru/modules.php?name=sud_delo&name_op=case&case_id=50759300&case_uid=d2670d2d-1bf7-463b-8e53-543fd27f0da2&delo_id=4&case_type=0&new=4&srv_num=1.
17. Обзор судебной практики Верховного Суда Российской Федерации. 2022. № 2. С. 71–73. URL: <https://www.vsrf.ru/documents/practice/31604/>.

Молодых В. А.¹,

*доцент кафедры информационной безопасности
Санкт-Петербургского университета МВД России,
кандидат экономических наук, доцент*

Подружкина Т. А.²,

*начальник кафедры информационной безопасности
Санкт-Петербургского университета МВД России,
кандидат педагогических наук, доцент*

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ТЕНЕВОЙ ЭКОНОМИЧЕСКОЙ АКТИВНОСТЬЮ

В последних исследованиях, посвященных влиянию теневой экономики на устойчивое развитие стран, подчеркивается, что эффекты финансовой преступности взаимозависимы [3; 4]. Если законопослушные налогоплательщики несут дополнительные убытки из-за роста масштабов теневой экономики, то они будут иметь в своем распоряжении меньше оборотных средств, их расходы на развитие бизнеса уменьшатся, а это означает сокращение темпов роста для страны. В макроэкономическом контексте высокий уровень теневой экономики имеет тенденцию снижать доверие иностранных инвесторов к деловой среде, а это означает, что страна столкнется с более сильной международной деловой конкуренцией за привлечение финансовых потоков.

Одной из основных долгосрочных угроз является возможное развитие теневой экономики в интернет-секторе экономики [3]. Киберпреступники с достаточными навыками и опытом начинают активно предлагать свои услуги в качестве посредников (например, использование криптовалют для уклонения от уплаты налогов) или как онлайн-площадки, которые предоставляют услуги по отмыванию доходов, полученных преступным путем или финансированию организованной преступности. При этом сокращаются транзакционные издержки, растет доходность криминальных операций, что, в конечном итоге, создает дополнительные стимулы для ухода в теневой сектор экономики.

По мере расширения теневой экономической активности в интернет-секторе экономики создаются новые организованные преступные группы. Их деятельность по отмыванию денег и переводу капиталов в офшоры приводит к сокращению инвестиций, росту оттока капитала из страны и снижению доходов бюджетной системы. С ростом масштабов теневого сектора экономики также растут издержки для легального бизнеса, падает авторитет государственных институтов и органов власти, а расходы на обеспечение безопасности и противодействие росту масштабов теневой экономики растут [4].

Данные факторы препятствуют устойчивому развитию страны и требуют поиска новых инструментов и механизмов противодействия теневой экономической активности в условиях развития цифровых услуг.

¹ © Молодых В. А., 2024.

² © Подружкина Т. А., 2024.

Использование технологии больших данных в расследовании преступлений, связанных с теневой экономикой можно представить, как процесс, используемый для решения задач анализа и обработки больших объемов данных в заданный интервал времени с учетом существующих принципов судебной экспертизы, а также необходимости их последующего представления в суд в виде цифровых доказательств, переданных с компьютеров или сохраненных на них. Использование больших данных является сложной задачей для цифровой криминалистики в плане обеспечения мер безопасности, также специалисты сталкиваются с серьезными трудностями при сборе необходимых доказательств на основе большого набора информации, так как огромный массив данных, полученный в результате мониторинга множества разных источников, требует надлежащего управления и использования передовых технологий.

Применение больших данных в расследовании экономических преступлений основано на агрегировании разноплановой информации, полученной из максимального широкого спектра цифровых источников и ее последующей обработки с минимально возможными временными задержками [1]. Конечной целью является создание такой системы сбора доказательной базы, при которой будут задокументированы все цепочки сделок с поиском конечных бенефициаров, что особенно важно при расследовании преступлений, связанных, например, с уклонением от уплаты налогов и отмыванием денежных доходов, полученных преступным путем.

Таким образом, большие данные играют важную роль в расследовании экономических преступлений и снижении масштабов теневого сектора экономики. В конечном счете, решение задач, связанных с нейтрализацией трансграничной преступности, которая особенно активна в цифровом пространстве, предполагает акцентирование внимания не только на сборе данных и их детальном анализе, но и на защите информации. В результате требуется пересмотр инструментария компьютерной криминалистики в направлении интеграции информационной инфраструктуры правоохранительных органов, связанных с мониторингом теневой экономической активности. Получение массивов данных является первым шагом в сохранении цифровых вещественных доказательств при подготовке к последующему их исследованию и анализу. При этом необходимо учитывать, что большинство уголовных расследований экономических преступлений в цифровом пространстве носит трансграничный характер.

С учетом этого использование больших данных при расследовании преступлений, связанных с теневой экономической активностью, мы рассматриваем как применение инновационных методик сбора и анализа информации с учетом специфики проведения расследований и сбора доказательной базы. В качестве основных инструментов можно выделить: интеллектуальный поиск данных для верификации цепочек поставок и определения конечных бенефициаров сделок, эконометрические модели, а также применения инструментов визуализации для обработки данных и представления их в виде, который можно представить в ходе судебного разбирательства.

Большие данные изменили информационную среду и преобразовали работу правоохранительных органов так как появились возможности поиска и агрегирования информации, а также получения перекрестных ссылок на обширные

массивы данных. Существует три основополагающие характеристики, имеющие отношение к расследованию экономических преступлений: доступность данных, цифровой след и повсеместное распространение технологий.

Данные составляющие больших данных необходимо рассматривать в комплексе, как ландшафт больших данных. Такой подход позволяет полностью понять текущий тип и скорость изменений при проведении расследований, а также оценить потенциальное воздействие новых технологий в контексте противодействия росту масштабов теневой экономики. Экспоненциальный рост объемов информации привел к тому, что появились возможности фиксировать факты, которые ранее не рассматривались правоохранительными органами, и на основе этих данных стало возможным создавать подробные профили о компаниях, местах и сделках. Цифровая обработка данных означает, что их можно собирать, анализировать и обмениваться в режиме реального времени.

Специфика использования технологии больших данных при расследовании преступлений, связанных с теневой экономической активностью, определяется рядом аспектов.

Объем доступной личной информации, позволяющей установить личность, и степень детализации данных позволяют правоохранительным органам в максимально короткие сроки создавать детальные профили отдельных лиц и компаний. При этом большие данные при проведении расследований можно использовать не только для экономических агентов, но и по группам подозреваемых, учреждений, а также отдельных стран. Данная технология позволяет в режиме реального времени анализировать данные о доставке, закупках и другие данные для мониторинга теневой экономической активности.

Для правоохранительных органов основным препятствием использования технологии больших данных продолжает оставаться нехватка вычислительных мощностей, а также нехватка квалифицированных специалистов. Также трудно добиться координации между контролирующими государственными органами в плане обмена информацией, что на практике затрудняет возможности создания максимально детальных профилей в режиме реального времени. Основной причиной этого является то, что данные собираются и хранятся в виде разрозненных наборов информации для различных целей, полученных из разных источников и переданных в разных форматах. В настоящее время в Российской Федерации появились возможности по привязке личной информации и биометрических данных к конкретному лицу, особенно если наборы данных связаны с подтвержденными документами, удостоверяющими личность, а не только с наборами личных данных [2]. Однако в отношении юридических лиц, что особенно важно при расследовании преступлений, связанных с теневой экономической активностью, данная проблема в комплексе не решается.

Таким образом, противодействие теневой экономической активности в цифровом пространстве является одним из базовых условий устойчивого развития страны. Несмотря на наличие прогрессивных технологий, таких, как большие данные, которые используются для расследования экономических преступлений, растущий потенциал интернет-сектора экономики создает множество до-

полнительных проблем, таких как трансграничный характер незаконных операций, анонимность финансовых транзакций и снижение издержек организованных преступных группировок в части отмывания денежных доходов. Это требует дальнейшей систематизации и интеграции информационной инфраструктуры органов государственной власти в целях выявления, мониторинга и отслеживания теневой экономической активности. Особого внимания заслуживает решение проблемы координации действий национальных правоохранительных органов, так как интернет-сектор экономики характеризуется большим количеством трансграничных операций и финансовых транзакций.

Список литературы

1. Воробьева И. Б. Применение больших данных (big data) при прогнозировании и расследовании преступлений // Вестник Саратовской государственной юридической академии. 2021. № 3. С. 195–202.
2. Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. № 17 (136). С. 102–111.
3. Тишутина И. В. Новые возможности раскрытия и расследования преступлений в условиях глобальной цифровизации // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 4. С. 46–55.
4. Трысячный В. И. Теневая экономика как угроза обеспечения экономической безопасности государства // Евразийский юридический журнал. 2022. № 2-1. С. 128–133.

Нурматов Н.¹,

*слушатель факультета подготовки иностранных специалистов
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,
доцент кафедры международной информационной безопасности
института информационных наук
Московского государственного лингвистического университета,
кандидат технических наук*

К ВОПРОСУ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В ИТ-СФЕРЕ

В период с конца 1990-х до начала 2000-х гг. в мире произошли существенные технологические открытия и прорывы, которые в значительной степени упростили и облегчили повседневную жизнь людей ввиду интеграции различных технологий в деятельность. Однако, вместе с положительными результатами возникает серьезная потребность в разработке законодательства в сфере правоотношений, которые связаны с техническими (компьютерными) преступлениями различного рода (далее – киберпреступления). Происходит виртуализация преступности, а именно переход существенного числа противоправных, антиобщественных действий в киберсреду, что полностью исключает физический контакт между преступником и жертвой. На данный момент можно сказать, что в мировой преступности происходит так называемая «цифровая революция».

Киберпреступность является следствием всеобщей цифровизации жизни современного социума и заслуживает соответствующих мер реагирования со стороны государства. Она затрагивает самые разные сферы жизни и деятельности общества, например, права на имущество граждан, объекты критической инфраструктуры и права отдельных лиц, приносит вред коммерческим организациям и государству в целом. Поведение киберпреступников становится все более агрессивным, они стараются тщательно скрывать свои следы, оставаться анонимными и так продумывать свои шаги, чтобы как можно больше усложнить сбор улик и уйти от ответственности. Данное обстоятельство приводит к правовой и фактической трудности в осуществлении процесса возбуждения уголовных дел по соответствующим преступлениям, сопряженным с информационными и цифровыми технологиями.

Киберпреступность на сегодняшний день является одной из наиболее латентных. Невысокий показатель раскрываемости этого типа запрещенных законом

¹ © Нурматов Н., 2024.

деяний обусловлен тем, что потерпевшие зачастую не подозревают о завершении преступления или обнаруживают его только по прошествии некоторого времени. В качестве примера можно привести информационное пиратство (незаконное копирование информации), которое часто остается незамеченным, или компьютерные вирусы, которые обычно являются результатом непреднамеренных ошибок со стороны пользователей. Продолжительный инкубационный период совершения киберпреступлений объясняется также и тем, что и сами жертвы (зачастую какие-либо крупные коммерческие организации или банковские учреждения) не склонны сообщать о совершенном преступлении в органы правопорядка, поскольку опасаются испортить свою деловую репутацию.

Кроме того, киберпреступность имеет международный характер: преступления, совершаемые в киберпространстве или с большой долей применения киберинфраструктуры часто не ограничиваются территорией одного государства [1]. В тех случаях, когда правонарушители и потерпевшие расположены в разных странах, приходится прибегать к международному сотрудничеству. Одним из препятствий для эффективного взаимодействия между правоохранительными органами разных государств являются специфика правовых систем и неодинаковая степень законодательного урегулирования вопросов киберпреступности.

К настоящему времени некоторые страны предпринимают попытки подписать международные соглашения о взаимодействии в сфере профилактики и расследования киберпреступлений, и уже преуспели в этом. Однако, в текущих реалиях не существует унифицированного (во всяком случае для большинства стран) глобального правового акта, который бы урегулировал меры борьбы с киберпреступниками.

Основная проблема расследования киберпреступлений состоит в том, что к ним не представляется возможным строго применить стандартные протоколы расследования. Так, распространенная проверка места происшествия имеет ряд особенностей при расследовании преступлений в киберпространстве. Например, что будет считаться в контексте процессуальности местом преступления, если злоумышленник совершил хакерскую атаку: его местоположение в момент атаки, место, где хакер написал вредоносную программу, адрес жертвы, место снятия наличных (в ситуации с атаками на финансовые учреждения) или другое.

В рамках расследования киберпреступлений в большинстве случаев осуществляется выемка оборудования (компьютеров и периферийных устройств, других электронных носителей информации) с последующим ходатайством о проведении экспертизы этих объектов. На этой стадии следователи должны прибегнуть к помощи экспертов и специалистов в связи с многочисленными особенностями изъятия и транспортировки этих объектов. Хотя понятые обязаны присутствовать при выемке, они могут быть проинформированы только о факте изъятия носителя информации, а не о том, содержит ли этот носитель информацию, являющуюся преступной. Стоит также отметить, что процедура изъятия является довольно сложной с технической стороны, поскольку всегда остается риск потери информации. Кроме того, порядок изъятия осложняется тем, что следователям совместно с экспертами предстоит принять решение об изъятии каждого конкретного объекта, руководствуясь, с одной стороны, потребностью

в полном и всестороннем расследовании, а с другой – требованием обоснованной необходимости изъятия (компьютеры и мобильные телефоны зачастую являются важными рабочими инструментами для лиц, занимающихся профессиональной деятельностью, так как их длительное изъятие может нанести существенный ущерб их интересам).

Важным этапом в расследовании уголовных дел, связанных с киберпреступлениями, является назначение компьютерной судебной экспертизы. Так как изучаемый вид преступлений относительно новый, количество специальных учреждений, имеющих экспертов в этой области, незначительно. Это увеличивает нагрузку на такие учреждения и приводит к возрастанию времени, требующегося для приобретения опыта. Кроме того, при назначении экспертизы компьютерных технологий важным аспектом является постановка следователем вопросов экспертам, что создает определенную терминологическую и семантическую сложность, поскольку сотрудники следственных органов не обладают специальными знаниями в области компьютерных, цифровых и информационных технологий.

На сегодняшний день в правоохранительных органах более 80 % следователей имеют только юридическое образование и это усложняет расследование преступлений в сфере кибертехнологий, так следователь не должен ограничиваться знанием базовых офисных программ для создания документов и отчетностей [2; 3]. Если сотрудник обладает глубокими знаниями цифровых технологий, то он сможет корректно поставить вопрос перед экспертами, более эффективно и результативно провести различные следственные действия, не прибегая к дополнительному участию специалистов или экспертов.

Оперативно-разыскные¹ мероприятия, расследования и процессуальные действия, проводимые по данной категории преступлений, имеют широкий спектр, а залог успеха расследования уголовного дела заключается в компетентности лиц, проводящих расследование, а также в качестве и своевременности проводимых консультаций с экспертами в области информационных наук. Специфический контекст расследования указанной категории уголовных дел, согласно практике, подразумевает частое консультирование, что входит в обязанности следователя, в производстве которого находится дело. Эксперты занимаются поиском уличающих доказательств и их профессиональным толкованием. Помимо экспертов по компьютерным, технологическим и разведывательным экспертизам в данной сфере уголовных расследований наиболее востребованы эксперты из таких областей, как: финансы, кредит и аудит, экономическая безопасность, банковское дело, медицинское обслуживание, охрана труда и др.

Из вышесказанного можно сделать краткий вывод о том, что общественно опасные деяния, запрещенные уголовным законом под угрозой наказания и совершаемые в сфере информационно-коммуникационных и цифровых технологий и компьютерной информации, которые по мнению большинства экспертов, корректно назвать киберпреступления, представляют собой актуальную и нарастающую угрозу для общества.

¹ Написание слова *разыскные* приводится в соответствии с нормами русского языка, за исключением употребления в нормативных правовых актах.

Проблематика характеризуется ключевыми факторами, среди которых: техническая сложность (в первую очередь для следователя по сбору доказательств, отличается отсутствием прямых улик), территориальная разбросанность (сказывается на идентификации личности виновных лиц и затрудняется особенностями международных взаимоотношений между государствами), динамика в развитии технологий (расширение вариантов инструментария и методологии совершения киберпреступлений), недостаток специалистов. Стоит отметить роль специального технического образования сотрудников, проводящих следственные мероприятия, для более точной квалификации преступлений, уменьшения их латентности и оптимизации процессов расследования. В этой связи не стоит умалять значение научных исследований и мероприятий, в рамках которых осуществляется синтез, обсуждение, совершенствование знаний, технологий и, как следствие, подготовка таких востребованных специалистов по борьбе с киберпреступностью.

Список литературы

1. Витвицкая С. С., Витвицкий А. А., Исакова Ю. И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. Т. 1. № 1. С. 126–136.
2. Степанян А. И. Транснациональная полицейская деятельность современных государств в условиях глобализации // Вестник Санкт-Петербургского университета МВД России. 2022. № 1 (93). С. 41–48.
3. Раздел I. Уголовно-правовая и Криминологическая характеристика преступлений, совершаемых в цифровом пространстве / [А. Ф. Абдулвалиев и др.] // Противодействие преступлениям в цифровом пространстве : учебное пособие / под научной ред. Е. В. Смахина, Р. Д. Шарапова. Тюмень : ТюмГУ-Press, 2023. С. 8–266.

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*

БОРЬБА С ДЕСТРУКТИВНЫМИ СЕТЕВЫМИ СООБЩЕСТВАМИ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ ПРОТИВ РОССИИ

Не будет преувеличением замечание о том, что с развитием технологий и вынужденным втягиванием России в войну с западным миром обеспечение информационной безопасности занимает все более значимое место в борьбе с терроризмом и экстремизмом, в боевых действиях, в обеспечении общественного порядка.

Сами представления об информационной безопасности на этапах автоматизации, цифровизации и цифровой трансформации естественным образом менялись: от внимания исключительно к вопросам защиты информации до состояния защищенности личности, общества и государства, от угроз в информационной сфере до обеспечения безопасности самых разнообразных сфер жизни и деятельности, тех сфер, которые все в большей мере становятся информационными.

В подходах к информационной безопасности можно выделить как киберцентричный или технологический, так и антропоцентричный или условно человеческий подход. Первый – технологический направлен на совершенствование инструментов и механизмов защиты технических систем, электронных коммуникаций, объектов критической инфраструктуры. Здесь все большую роль играют технологии получения и обработки разведанных. Второй – человеческий – это защита сознания людей от вредоносных деструктивных информационных воздействий, защита социальных сфер, национальных ценностей, духовных идеалов.

Не умоляя значимости первого подхода, можно утверждать, что основные угрозы обществу и государству несут те потоки и, можно сказать, лавины данных и сведений, которые, обрушиваясь на людей, могут деформировать психику и мировоззрение, формируя крайне негативное отношение к прошлому, настоящему и ожидаемому будущему и к стране в целом.

В информационной войне можно выделить акции, которые осуществляются «здесь и сейчас», и глубинные, пролонгированные операции, которые ведутся годами и десятилетиями, а также духовно-мировоззренческую экспансию запада, которой Россия противостоит веками.

Многочисленные вбросы, фейки, дипфейки, провокации в последнее время принимают все более изощренный, а часто и кровавый характер. Так, укрона-

¹ © Овчинский А. С., 2024.

цистские диверсанты, неся потери, высаживают десанты или вторгаются на территорию России, чтобы предоставить фотоотчет западным спонсорам войны. Тщательно спланированные террористические атаки уже с сотнями жертв направлены на разжигание национальной розни и подрыв доверия к органам власти. Здесь противостояние требует не только адекватных реакций и упреждающих действий со стороны спецслужб и правоохранительных органов, но и консолидации общественных сил в борьбе за единство многонационального народа и суверенитет нашей страны.

В то же время наибольшие угрозы обществу и государству несут акции глубинной пролонгированной информационной войны. Речь идет о воздействиях на ментальном, когнитивном и смысловом уровнях, то есть о внешних воздействиях по изменению национальных, исторических и мировоззренческих кодов.

С развитием интернет-коммуникаций для все большего количества граждан сетевые ресурсы становятся не просто основным источником самых разнообразных сведений, новостей, фактов, комментариев. Объективно они начинают играть существенную роль в формировании мировоззренческих и идеологических позиций.

При этом на передний край ментально-когнитивной смысловой войны выходят сетевые сообщества, которые объединяются на почве негативного отношения к тому курсу, который проводится к стране, к руководству, да и к России в целом. Такие сообщества могут возникать на почве радикальных религиозных идей. Они подпитываются этническими противоречиями и историческими обидами, разнообразными формами национализма. Но, как правило, антироссийски настроенных личностей объединяет деградирующая либеральная идеология и ее многочисленные «осколки» (от идей гендерного разнообразия, свободы от детей и антипатриотизма до возрождения языческих культов, идей социодарвинизма и фашизма и откровенного сатанизма.).

Еще в 90-е гг. прошлого века опыт борьбы с организованной преступностью показал, насколько важно выявлять и учитывать структурную организацию криминального сообщества. Именно понимание структурных особенностей, распределение ролей, иерархии связей позволяло наносить эффективные удары по организованной преступности как в рамках уголовно-правовых мер, так и в ходе непроцессуального использования оперативно-разыскной информации.

С погружением преступности в информационные сферы системно-структурный анализ деятельности, скажем, криминальных, террористических, экстремистских и, в целом, деструктивных сообществ не теряет своей актуальности.

В свое время выделялись такие структурные формы криминальной и деструктивной активности как: очаг, квартет, центр, пирамида, песочные часы, сеть. Исходя из особенностей криминальной структуры, формировались и специфические подходы к ее ликвидации.

Но разнообразные сетевые сообщества, которые складываются как бы «по интересам», как правило, вообще не имеют никакой структурной организации. При этом выделение среди них деструктивных сообществ не представляет технических затруднений. Сейчас на это нацелены уже определенные типы искусственных нейронных сетей. Да эти сообщества и сами открыто заявляют о себе, иначе как привлекать сподвижников?

Например, в цифровой образовательной среде уже более полугода открыто преподается онлайн курс «Россия и деколонизация», где откровенные русофобы все мерзости западноевропейского колониализма приписывают Российской Империи и Советскому Союзу. Заметим, что «Деколонизация России» это детально разработанная ЦРУ и откровенно представленная миру полновесная программа действий по расчленению нашей страны на отдельные анклав.

Не менее уничижительные экскурсии в российскую историю продолжаются уже в скандально известном Ельцин центре. Можно приводить огромное количество примеров сетевых объединений людей, например, приклонявшихся перед личностью покинувшего этот мир оппозиционера Навального или разделяющих меркантильные, эгоистические, бездуховные подходы к жизни, безразличие к судьбе и будущему своей страны.

Естественно, возникает вопрос, как бороться с бесструктурными деструктивными сетевыми сообществами? Если нет явных признаков экстремизма, то ни уголовно-правовые, ни административные меры не применимы. Необходимо понимать, что служит притяжением, вовлечением и объединением людей в такие сообщества. В первую очередь – это деструктивные идеи, идеологемы и идеологии.

Заметим, что идеология – это не только то, что отражает наше отношение к окружающей действительности, и не то, что фиксируется в документах и манифестах. Главное в идеологии – это обоснование права на те или иные действия и поступки. В таком контексте деструктивные диалоги несут вполне определенные угрозы, и именно они объединяют людей в сетевые сообщества.

В системно-структурном анализе к таким образованиям применим образ ПЕНЫ, той пены, которая может взбухать пузырьками деструктивных идей, как в сознании отдельных людей, так и в коллективном сознании определенных слоев населения и целых народов. С такой «пенной» мы сталкиваемся в информационном противоборстве с деструктивными сообществами в Интернете. Успеха в этой войне можно достичь, нанося удары по основе, по деструктивным идеям и идеологиям.

Новые технологические возможности для этого открываются с применением систем генеративного искусственного интеллекта. Если прежде применение нейронных сетей подсказывало решения на основе распознавания и анализа огромных массивов данных, то теперь все шире открываются возможности автоматически генерировать непосредственно новую информацию, а именно, создавать произведения литературы, живописи, музыки. Так, в политических дискуссиях можно автоматически генерировать контраргументы.

Взяв на вооружение такие возможности и освоив соответствующие инструменты, можно создать автоматизированные системы информационных воздействий (АСИВ), которые в пространстве сетевых коммуникаций будут атаковать мировоззренческими историческими и идеологическими аргументами любые попытки создавать и распространять информационно-психологическую деструкцию. Естественно для обучения и настройки систем генеративного искусственного интеллекта требуются своя идеологическая база, ресурсы позитивных идей и идеологий.

В настоящее время в России сложилось весьма парадоксальная ситуация с идеологией. Никакая идеология не может быть государственной, сказано в ст. 13 Конституции Российской Федерации, принятой в 1993 г. Одновременно ст. 2, утверждая приоритеты правам и свободам человека, отражает идеи либерализма. Но это уже далеко «вчерашний день».

На самом деле нашу жизнь наполняют мощные волны новой позитивной идеологии. Эту идеологию можно увидеть в решениях Совета безопасности и непосредственно в обновляющихся стратегиях национальной безопасности. Идеологию генерируют мощные «мозговые центры», такие как, например, Изборский клуб. Идеология звучит на регулярных Валдайских форумах. Идеологией наполнены Соборы Русского мира (на недавнем Соборе была организована непосредственно идеологическая секция). Наконец, нашей идеологией наполнены выступления Президента Российской Федерации Владимира Владимировича Путина.

В целом, необходимые массивы обучающих материалов могут быть сформированы для идеологической настройки систем генеративного искусственного интеллекта. Инициативные исследования в этом направлении проводятся на нашей кафедре. Определенные результаты получены в рамках выпускных квалификационных работ слушателей. Но трудно ожидать полновесных результатов без профессионально организованных научных исследований и проектных разработок.

В борьбе с глубинным, как сказано в одной из работ [1] «незавершенном нацизмом», с идеологией глобального доминирования и далеко «незавершенным колониализмом» требуется ясная мощная стройная идеология. В то время как сознание народов блуждает в «трех соснах» мировых идеологий: либеральной, консервативной, социалистической, в нашей стране все явственней вырисовывается идеология суверенной государственности, социальной справедливости, защиты традиционных ценностей и духовных идеалов. Так, в исследованиях А. В. Щипкова – ректора православной академии проявляются контуры идеологии «социального традиционализма», объединяющей идеи социальной справедливости и защиты традиционных ценностей [2].

В заключение отметим, что, рассматривая перспективы использования систем искусственного интеллекта в информационном противоборстве, нельзя отставать без внимания те глобальные вызовы, которые возникают перед человечеством с использованием таких искусственно созданных систем, которые способны не только разрушать баланс сил на мировой арене, но и изменить направление цивилизационного развития.

Список литературы

1. Щипков А. В. Незавершенный нацизм. Генезис, трансформации и родственные явления. М. : Российский православный университет святого Иоанна Богослова, 2024.
2. Щипков А. В. Идеология социального традиционализма (социал-традиция). М. : Российский православный университет святого Иоанна Богослова, 2023.

Орлов И. С.¹,

*командир отделения Института-факультета
подготовки сотрудников для органов предварительного расследования
Московского университета
МВД России имени В.Я. Кикотя*

Харламова И. Ю.²,

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

ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ В ПРОЦЕССЕ РЕАГИРОВАНИЯ НА КИБЕРАТАКИ

На протяжении всей мировой истории в военных целях использовали не только человеческие и материальные ресурсы, но и научные достижения. Человечество достигло уровня развития, позволяющего осуществлять удары по объектам государственного значения через сотни километров, тем самым нанося значительный вред противнику, выводя из строя инфраструктуру, разрушая экономику, вызывая волнения населения, подрывая авторитет лидеров стран-противников. Кибератаки, на первый взгляд имеющие только виртуальное воздействие, обладают не меньшей разрушительной силой, чем огневая мощь.

В первом квартале 2023 г. число кибератак на Российскую Федерацию составило около 290 тыс., что в полтора раза больше, чем на конец 2022 г. В первой четверти 2024 г. тенденция повышения их количества сохраняется [1]. Эти факты делают необходимость реагирования на киберинциденты одной из основных задач ведомств и министерств силового блока, в том числе и правоохранительных органов.

Важным событием, которое значительно повлияло на противодействие киберугрозам, стало создание в 2013 г. системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, сформированной Федеральной службой безопасности Российской Федерации по указу президента и получившей название ГосСОПКА. В состав ГосСОПКА входит Национальный координационный центр по компьютерным инцидентам, задачей которого является аккумулярование информации о кибератаках и их устранении объектами критической информационной инфраструктуры (КИИ).

Основными задачами, стоящими перед ГосСОПКА, являются: анализ текущей ситуации в сфере информационной защиты, определение дальнейших планов развития системы безопасности информации и объектов КИИ, обеспечение коммуникации и продуктивного взаимодействия операторов связи и обладателей информационных ресурсов в сфере защиты информации.

¹ © Орлов И. С., 2024.

² © Харламова И. Ю., 2024.

Сведения, которые Министерство внутренних дел Российской Федерации (МВД России) получает в ходе своей исследовательской деятельности в области информационной безопасности и развития информационных технологий, активно использует специальное подразделение МВД России – Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России (УБК МВД России). Данное подразделение было создано в рамках реализации Указа Президента Российской Федерации от 30 сентября 2022 г. № 688 для борьбы с преступлениями с использованием Информационно-коммуникационные технологии по всей стране. Положение об Управлении утверждено приказом МВД России от 29 декабря 2022 г. № 1110.

УБК МВД России создавалось на базе Управления «К», входившего в Бюро специальных технических мероприятий МВД России (БСТМ России). Одним из ярких примеров работы Управления «К» стало задержание членов группировки SugarLocker, которые являлись разработчиками и распространителями вредоносного программного обеспечения и, по совместительству, вымогателями [2]. Хакерское объединение наносило ущерб не только российской инфраструктуре, но и международным организациям и подозревалось в незаконном владении данными 9,7 млн австралийцев, являющихся клиентами страховой медицинской компании MedibankPrivate. Блестящему результату способствовала умелая и профессиональная координация действий сотрудников Управления «К» совместно со специалистами ИБ-компании F.A.C.S.T., специализирующейся на борьбе с киберпреступностью, поддержки подразделений правоохранительных органов, ответственных за противодействие и ликвидацию киберпреступности и кибератак. В ходе расследования вина хакеров была доказана, они понесли наказание в соответствии со ст. 273 УК РФ.

Сотрудники УБК МВД России действуют и за пределами Российской Федерации в рамках международного сотрудничества по противодействию киберпреступности с правоохранительными органами иностранных государств.

Российская Федерация, являясь участником Шанхайской организации сотрудничества и основываясь на ее Хартии, взаимодействует с правоохранительными органами государств-участников: Индии, Казахстана, Киргизии, Китая, Пакистана, Таджикистана и Узбекистана.

Правоохранительные органы Российской Федерации успешно и продуктивно реагируют на киберугрозы, охраняют и защищают информационную безопасность нашей страны.

Список литературы

1. Число кибератак в России и в мире // Cnews. URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире.
2. В России арестована группа хакеров-вымогателей, замаскированная под ИТ-компанию // Cnews. URL: https://www.cnews.ru/news/top/2024-02-20_bstm_mvd_rossii_i_facctlikvidirovali.

Панасюк А. В.¹,

*курсант факультета подготовки сотрудников
для подразделений экономической безопасности
и противодействия коррупции*

*Московского университета
МВД России имени В.Я. Кикотя*

*Научный руководитель: Калашикова А. А.,
преподаватель кафедры информатики и математики
Московского университета
МВД России имени В.Я. Кикотя*

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

XXI в. характеризуется динамичным развитием информационного общества и использованием телекоммуникационных технологий, которые пронизывают все сферы повседневной жизни. Преступность, в свою очередь приспосабливается к ним и скоротечно развивается, порождая большое количество новых проблем, не выносящихся до этого на обозрение. Так, согласно официальным статистическим данным, предоставленным МВД России, число IT-преступлений в России за 2023 г. выросло на 29,7 % в сравнении с 2022 г. Каждое третье преступление в России по итогам 2023 г. совершено с использованием информационно-телекоммуникационных технологий. Раскрываемость такого рода деяний в 2023 г. поднялась на 21 % [3].

Мировая сеть Интернет оказывает фундаментальное влияние на общество. Киберпреступность распространяется в виде мошенничества, шпионажа и грабежей в сети Интернет. Киберпреступники применяют новейшие технологии для уклонения от ответственности, используя интеллектуальные технологии автоматизации.

Искусственный интеллект в данной сфере может стать хорошим оружием в руках правоохранительных органов: выявления искомого человека из группы исследуемых лиц, предсказания преступлений и планирования террористических актов на этапе зарождения.

Искусственный интеллект при грамотном его использовании может стать инструментом, изменившим ход действий в пользу правоохранительных органов. В перспективе он может повысить эффективность деятельности, расширить возможность в противостоянии преступности.

Обратимся к статистике за 2023 г. В общем объеме киберпреступлений практически половину составили случаи мошенничества (48 %). Стоит отметить, что количество преступлений с использованием электронных денежных средств возросло на 4,4 %, а число краж с обычных банковских карт снизилось на 28 %. Возросшая активность населения в использовании Глобальной сети Интернет и дистанционных услуг напрямую обуславливает первенство информационно-телекоммуникационных технологий в повседневной жизни общества.

¹ © Панасюк А. В., 2024.

Повсеместное внедрение инновационных технологий побуждает нашу страну и правоохранительные органы, в частности, принимать соответствующие меры, направленные на стабилизацию данной сферы. В России Министерством внутренних дел Российской Федерации (МВД России) было принято решение о внедрении нейросети для поиска убийц и создания «фотороботов», детализирующих черты лица человека. Суть данного нововведения состоит в том, что нейросеть будет брать за основу геномные данные конкретного гражданина для выявления его причастности к случившемуся.

В результате реализации данной программы с использованием искусственного интеллекта повысится автоматизация анализа улик и показаний свидетелей по средствам выявления совпадений с общим банком данных. При наличии данного материала на месте преступления мгновенно составляется фоторобот.

Потенциал искусственного интеллекта в содействии органам охраны общественного порядка довольно велик: распознавание личности преступника, определение информационной системы или конкретных ее показателей, распределение данных по группам согласно показателям. Однако, стоит обратить внимание на то, что как таковое его повсеместное использование может нарушить конституционные права человека на неприкосновенность частной жизни, презумпцию невиновности, в частности. В данном ключе ОВД необходимо четко контролировать деятельность компьютерных технологий во избежание фатальных ошибок.

На основе анализа данных аспектов можно сделать вывод о том, что область применения искусственного интеллекта и телекоммуникационных технологий очень обширна. Однако, как таковое внедрение требует больших затрат как в разработке новых программ, позволяющих использовать ресурсы наиболее результативно, так и в разработке норм и методов, регулирующих степень вмешательства в частную жизнь граждан.

Список литературы

1. Вас охраняет нейросеть: как искусственный интеллект помогает искать преступников // Росбизнесконсалтинг. URL: <https://fisher.rbc.ru/article.html>.
2. Винтер М. Е. Искусственный интеллект в криминалистической науке // Цивилизация знаний: российские реалии. Цивилизационная роль права в условиях смены научно-технологической парадигмы (стратегическая панель) : сборник научных трудов. М., 2021. С. 127–134.
3. Статистика и аналитика // МВД.РФ. URL: <https://xn--b1aew.xn--p1ai/dejatelnost/statistics>.

Переходченко К. В.¹,

*курсант Института-факультета подготовки сотрудников
для органов предварительного расследования*

Московского университета

МВД России имени В.Я. Кикотя

Научный руководитель: Стащенко С. П.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий*

Московского университета

МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ СПЕЦИАЛЬНЫХ ЗНАНИЙ СПЕЦИАЛИСТАМИ СЛЕДСТВЕННО-ОПЕРАТИВНОЙ ГРУППЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Специалист является неотъемлемой частью следственно-оперативной группы при выезде на место происшествия. На него возлагаются следующие задачи:

- фиксация хода и результатов следственного действия;
- помощь в организации преследования, выявления и задержания по горячим следам;
- помощь следователю в обнаружении, фиксации и изъятии следов (прежде всего невидимых и слабовидимых).

Интересным вопросом является участие специалиста при проведении проверочных действий или расследовании преступлений в сфере информационно-телекоммуникационных технологий. Прежде всего, нужно учитывать то, что объектами исследований при таких преступлениях становятся различные технические устройства в виде компьютеров, ноутбуков, флеш-накопителей и даже прогарм-ных обеспечений. В современном мире каждый человек использует в своей деятельности хотя бы компьютер, но все пользуются им «на полную мощность». Чаще всего используют поисковые браузеры «Яндекс», «Google» и т. д., программы «Word», «Exel» и тому подобное, поэтому не все люди, а также дознаватели и следователи обладают необходимыми знаниями для обнаружения необходимой информации.

При расследовании таких преступлений проведение проверочных и следственных действий целесообразно с проведением специалиста, обладающего обширными знаниями в области технических устройств, програмных обеспечений, информационных сетей, автоматизированных системы управления и т. д. На самом деле сложно предугадать какая область знаний понадобится, например, при

¹ © Переходченко К. В., 2024.

осмотре места происшествия, все зависит от обстоятельств совершения преступления, соответственно, определения вида специалиста также является сложным.

Например, для осмотра компьютера или ноутбука чаще всего достаточно специалиста, обладающего специальными знаниями в области компьютерных устройств для поиска и восстановления удаленных или скрытых файлов.

Сложнее, когда средством совершения преступления стала вредоносная программа по типу «Mirai». «Mirai» – это так называемый ботнет, при использовании которого в 2016 г. в результате масштабной DDoS-атаки большая часть Восточного побережья США осталась без доступа в Интернет. Атака, которую власти изначально опасались, была вызвана ботнетом Mirai и приписывается враждебному государству. Mirai – это тип вредоносных программ, автоматически обнаруживающих устройства интернета вещей, заражающих их и включающих в ботнет. Таким образом эти устройства интернета вещей можно использовать для проведения DDoS-атак, при которых поток вредоносного трафика приводит к сбоям серверов жертвы.

Указанная вредоносная программа является не единственным «паразитом» в виртуальном мире. Существует множество «червей», «троянов», вирусов, потенциально нежелательным программ, логических бомб и так далее, обнаружение которых само по себе составляет трудность до начала их действия, и тем более трудность в вычислении лица, их «подсадившего» на техническое устройство, поэтому их обнаружение и изъятие является трудоемким и сложным процессом, который чаще всего неподвластен обычному специалисту в области технических устройств, другими словами – программисту.

В настоящее время очень часто стал использоваться термин – специалист по кибербезопасности или специалист информационный безопасности.

Специалист по кибербезопасности занимается защитой цифровых данных и не допускает их утечку или потерю. Под цифровыми данными подразумевается все, что существует в электронном виде, начиная от обычных текстовых документов и заканчивая работой банковской системы, через которую ежедневно проходят миллионы рублей, долларов, евро. Очень часто, такие специалисты – это бывшие «хакеры» и «взломщики». Во многих государствах «белые» хакеры сейчас работают легально, например, в Китае действует группа «Аксиома», которая специализируется на корпоративном шпионаже и на разоблачении политических диссидентов. В отчете коалиции об «Аксиоме» говорится, что ее деятельность пересекается с «зоной ответственности» китайской разведки и китайского правительства. Также целями группы становятся западные правительства, различные демократические институты и диссиденты, находящиеся как внутри, так и за пределами Китая.

Российская Федерация в настоящее время также не отстает от иностранных государств. В Государственную Думу Федерального Собрания Российской Федерации был внесен первый пакет законопроекта о легализации «белых» хакеров. Принятие законопроекта позволит проводить анализ уязвимостей в любой форме, без разрешения правообладателей соответствующей программы, в том числе правообладателей инфраструктурных и заимствованных компонентов, отмечается в документах. Предполагается внести ряд правок в Гражданский кодекс

Российской Федерации, и различные федеральные законы, которые позволят «белым» хакерам вести свою деятельность на благо нашего государства. Представляется возможным участие таких специалистов в расследовании преступлений в сфере компьютерной информации и информационно-телекоммуникационных технологий.

На мой взгляд, самым проблематичным вопросом является метонахождения лица, которое ведет противоправную деятельность и обнаружение различных вредоносных программ. С помощью специальных знаний указанных специалистов и новых технических средств можно намного быстрее и качественно расследовать такие преступления. Тем более, что Уголовно-процессуальный кодекс Российской Федерации не ставит никаких ограничений по поводу их использования.

С помощью специальных знаний специалистов в области компьютерной информации можно правильно и полноценно зафиксировать «цифровые следы» и в дальнейшем применить их в расследовании преступлений в качестве доказательственной базы.

Так, Н. А. Иванов под цифровым следом понимает определенную информацию, представленную в виде совокупности различных сигналов, оставленных (зафиксированных) на различных материальных носителях, информация с которых впоследствии может быть получена различными способами и использована в дальнейшем анализе при раскрытии и расследовании преступлений как понятие «цифровое доказательство» [2].

Наиболее специфическими цифровыми следами являются:

- файлы (исполняемые и различные скрипты, файлы динамически загружаемых библиотек, файлы электронной почты, архивы);
- записи журналов системных событий и событий информационной безопасности;
- список действующих и недавно установленных сетевых соединений;
- список запущенных процессов и служб;
- список локальных и доменных пользователей;
- информация о событиях информационной безопасности антивирусного программного обеспечения, экрана SIEM-систем;
- программы, предназначенные для удаленного или локального управления;
- данные планировщика заданий;
- метаданные запуска программ.

По мнению Е. И. Скороделовой важное криминалистическое значение имеет информация о следах, оставляемых в результате работы антивирусных и тестовых программ, а также вредоносного программного обеспечения на компьютере или ином устройстве, например, мобильном телефоне потерпевшего [1].

Таким образом, можно сделать вывод о том, что для качественного расследования преступлений в сфере информационно-телекоммуникационных технологий и компьютерной информации, целесообразно привлечение специалиста, обладающего специальными знаниями в данной сфере, а также использование им специальных технических средств необходимых, для обнаружения и фиксации цифровых и иных следов.

Список литературы

1. Скороделова Е. И. Цифровой след в криминалистике: преодоление противодействия расследованию преступлений // Криминалистика: наука, практика, опыт : сборник научных трудов. М., 2023. С. 226–229.
2. Иванов Н. А. Транснациональные преступления, совершаемые с использованием компьютерных и телекоммуникационных технологий (классификация, теория и практика расследования) : специализированный учебный курс. Саратов, 2007.
3. Семенов Е. А. Особенности применения технических средств специалистами при расследовании преступлений // Криминалистика: вчера, сегодня, завтра. 2015. С. 190–195.
4. Терентьев А. А. Применение ситуационных центров органов внутренних дел для расследования преступлений в сфере информационных и телекоммуникационных технологий // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2019. № 1 (5). С. 108–112.
5. Светличный А. А. Особенности современной розыскной деятельности следователя при использовании информационно-телекоммуникационных технологий // Криминалистика: наука, практика, опыт : сборник научных трудов. М., 2023. С. 162–164.

Пименова О. В.¹,

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

Клочкова Е. Н.²,

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

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СИСТЕМ НА ПРИМЕРЕ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ (ML-ТЕХНОЛОГИЙ)

В современном мире термин «искусственный интеллект» используется повсеместно. Искусственный интеллект (ИИ) вошел в десятку самых передовых технологий. Эксперты отмечают, что развитие ИИ в нашей стране соответствует мировым тенденциям, как на уровне фундаментальных исследований, так и в области практического применения.

Одной из наиболее распространенных и используемых форм искусственного интеллекта является машинное обучение (англ. *machine learning*, *ML*). ML – представляет собой класс методов искусственного интеллекта, характерной чертой которых является обучение за счет применения решений множества сходных задач.

Для построения таких методов используются:

- средства математической статистики, численных методов, математического анализа, методов оптимизации, теории вероятностей, теории графов;
- различные техники работы с данными в цифровой форме.

Другими словами ML – это совокупность алгоритмов, объединяющих разные технологии, такие как нейронные сети, *deep learning*, обработка естественного языка (*natural language processing*) и др. Они позволяют оптимизировать и автоматизировать процессы.

Понятие «машинное обучение» придумал американский исследователь Артур Самуэль, работавший в IBM [1]. В 1959 г. он создал первую программу по игре в шашки, которая умела играть сама с собой и самостоятельно обучаться. Игровое направление, освоенное Самуэлем, стало развиваться очень активно.

¹ © Пименова О. В., 2024.

² © Клочкова Е. Н., 2024.

В конце 80-х гг. аспиранты университета Карнеги-Меллон спроектировали машину для игры в шахматы ChipTest. Она стала прототипом легендарного суперкомпьютера Deep Blue, обыгравшего Гарри Каспарова в 1996 г.

Вскоре после этого в истории искусственного интеллекта и машинного обучения начался новый виток. В 2011 г. Google основал Google Brain – подразделение, занимавшееся проектами в области ИИ. Спустя еще три года свои платформы по машинному обучению появились у Amazon и Microsoft, а Facebook внедрила в работу DeepFace – алгоритм, умеющий распознавать человеческие лица.

Принцип машинного обучения позволяет создавать компьютеры и программы, которые думают, как человек. Но при этом, в отличие от человека, они не устают, могут меньше ошибаться, работают с любым количеством данных и оценивают их непредвзято. Это открывает огромное поле для использования возможностей ИИ.

С помощью машинного обучения можно создавать множество сервисов и программ. От самых простых, которыми мы пользуемся в повседневной жизни – навигаторов, камер с распознаванием лиц, сервисов рекомендаций, – до сложных инструментов, которые используются в промышленном производстве или для обеспечения безопасности.

Высокий уровень угроз информационной безопасности, связанный с геополитической обстановкой в современном мире, а также устойчивый рост количества хакерских группировок, которые используют современный и эффективный инструментарий в противоправных целях, свидетельствует о необходимости повышения эффективности средств и методов защиты информации, в том числе за счет внедрения ИИ.

По данным исследования hh.ru, на рынке труда наблюдается нехватка квалифицированных специалистов по информационной безопасности (ИБ) [2]. В 2023 г. было опубликовано более 7000 вакансий в сфере ИБ. На 38 % увеличилось количество опубликованных вакансий ИБ-специалистов, на 6 % уменьшилось количество размещаемых специалистами по ИБ резюме.

В условиях кадрового голода и роста атак явно прослеживается необходимость автоматизации отдельных функций ИБ продуктов для быстрого реагирования на угрозы.

Методы машинного обучения позволяют эффективно обнаруживать угрозы, предотвращать атаки, автоматически предпринимать необходимые действия для их устранения в сравнении с другими технологиями.

Так, использование технологий ML для обеспечения информационной безопасности позволит минимизировать человеческий фактор при принятии решений, ускорить процессы реагирования и улучшить их точность.

Использование методов машинного обучения позволит более эффективно решать следующие рутинные задачи, стоящие перед командами центров реагирования на компьютерные инциденты:

- анализ трафика и инцидентов (обнаружение атак в неструктурированных данных, анализ поведения пользователей, выявление ложноположительных срабатываний);

- анализ сущностей (определение опасности бинарных файлов, IoC и CVE по косвенным признакам);
- анализ событий и инцидентов (оценка действия пользователей на основе анализа их поведения относительно разных сущностей: запускаемых программ, расписания работы, сетевой активности).

В настоящее время командами ИБ при создании эффективной системы защиты информации, а также корпоративных (ведомственных) центров реагирования на компьютерные инциденты (SOC) в обязательном порядке используется следующий инструментарий:

- система управления событиями информационной безопасности (SIEM-система);
- система управления уязвимостями (VM-система);
- система защиты от целевых атак («песочница»);
- система анализа сетевого трафика (NTA-система).

Использование ML-технологий в данных системах позволит значительно повысить их эффективность.

Например, технология SIEM обеспечивает анализ в реальном времени событий безопасности, исходящих от сетевых устройств и приложений, и позволяет реагировать на них до наступления существенного ущерба. Чаще всего аналитики SOC перегружены инцидентами и страдают от нехватки инструментов валидации и приоритизации событий ИБ. Использование в составе SIEM-системы ML-технологий, помогающих аналитику на основе входных данных определять является ли конкретное событие ИБ инцидентом, позволило бы обеспечивать результативную кибербезопасность быстро и точно.

Неоценимую помощь оказало бы использование машинного обучения и в организации процесса управления уязвимостями, в том числе для определения трендовых уязвимостей до того, как они будут использованы хакерами.

Трендовые уязвимости представляют наибольшую опасность для организации, так как активно эксплуатируются злоумышленниками. Каждый день в среднем появляется более 60 новых уязвимостей. Трендовыми могут оказаться не только новые, но и давно раскрытые уязвимости.

Актуальным было бы использование ML-технологий для анализа информации из открытых источников, с целью определить, насколько популярна уязвимость в кибербез-комьюнити и предугадать, какие уязвимости будут популярны завтра. Своевременное получение экспертами подобной информации позволит значительно снизить риск использования злоумышленниками опасных уязвимостей в эксплуатируемой инфраструктуре и быть на шаг впереди.

Использование технологий машинного обучения при создании так называемых «песочниц» позволит более эффективно детектировать нетипичное и аномальное вредоносное ПО.

Обычный подход в поведенческом анализе основан на наборах правил. Экспертный анализ переносится в сигнатуры, на основе которых инструмент обнаружения вредоносного ПО и файлов делает выводы.

Использование ML-модели в сочетании с поведенческими сигнатурами позволило бы расширить возможности обнаружения схожих и близких инцидентов, выявляя нетипичное ВПО, в том числе путем:

- анализа аномальных цепочек подпроцессов;
- обнаружения нестандартных значений параметров вызовов по умолчанию;
- обнаружения нетипичной последовательности вызовов функций.

Помимо перечисленных важнейшей задачей для ИБ-команд является выявление атак на периметре и внутри сети. NTA-системы помогают определить неизвестные для IT-службы сетевые узлы. На основе данных, полученных из трафика, система строит сетевой профиль актива, определяет его тип и роль. Система точно знает, когда узел появился, что он из себя представляет и какую активность создает внутри сети.

В данном случае применение ML-технологий позволило бы более эффективно решать задачи по выявлению аномалий в части сравнения активности узла с его обычным поведением.

Могут быть использованы следующие сценарии применения результатов работы ML-модели:

- большой объем трафика, передаваемый на внешние облачные сервисы: может свидетельствовать о том, что злоумышленники выкачивают данные в Dropbox или Яндекс.Диск;
- большой объем входящего трафика на сервер в DMZ-сегменте: может свидетельствовать о наличии туннеля из внешней сети к хосту и как следствие присутствии злоумышленника во внутренней сети;
- превышение количества трафика между узлом и базой данных: может свидетельствовать о попытках злоумышленника похитить конфиденциальные данные;
- превышение количества уникальных соединений между одним узлом и группой серверного сегмента: может свидетельствовать о горизонтальном перемещении злоумышленника или подборе учетных записей.

Учитывая изложенное, можно констатировать, что применение искусственного интеллекта, в том числе методов машинного обучения, в области обеспечения кибербезопасности автоматизирует повседневную деятельность ИБ-специалистов по сбору и анализу информации из различных источников, что позволяет более оперативно и эффективно оценивать риски и принимать информированные решения. Внедрение ML-технологий в функционал средств обеспечения информационной безопасности, а также продуктов, предназначенных для автоматизации деятельности SOC-центров, является перспективным направлением развития для производителей и разработчиков современных систем безопасности.

Список литературы

1. Машинное обучение: что это, суть и принципы – типы машинного обучения и его применение // ЯндексПрактикум. URL: <https://practicum.yandex.ru/blog/chto-takoe-mashinnoe-obuchenie/>.
2. Компания hh.ru представила результаты своего нового исследования рынка труда в сфере информационных технологий и информационной безопасности за второй квартал 2023 года // Информационные технологии, кибербезопасность, искусственный интеллект. URL: <https://newsletter.radensa.ru/archives/3059?ysclid=lv9z4jkxyp771413815>.

Плотников Г. Г.¹,
 профессор кафедры информационной безопасности
 учебно-научного комплекса информационных технологий
 Московского университета
 МВД России имени В.Я. Кикотя,
 кандидат технических наук

О МОДЕЛИ ОЦЕНКИ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ СИСТЕМАМ

В современном мире беспилотные системы становятся все более распространенными. Они используются в военных целях, для доставки грузов, в сельском хозяйстве и других отраслях. Однако беспилотные системы также могут представлять угрозу безопасности, особенно в местах массового скопления людей или на важных объектах инфраструктуры. В связи с этим возникает необходимость разработки эффективных методов борьбы с ними.

Наиболее опасным представляется массированная атака беспилотными системами по объектам, расположенным на ограниченной территории. Это позволяет атакующей стороне рассчитывать на высокую вероятность достижения цели атаки.

Одним из подходов к организации противодействия таким атакам является использование теории массового обслуживания. Такой подход позволяет определить оптимальные параметры системы противодействия, оценить ее эффективность.

Для борьбы с беспилотными системами можно использовать различные системы массового обслуживания. Например, можно использовать систему обнаружения и перехвата/поражения атакующих беспилотных систем. Такая система будет автоматически обнаруживать угрозу и направлять на нее средства перехвата или вывода из строя.

Выразим интенсивности атакующего потока беспилотных систем через λ , а интенсивность потока реагирования через μ , значения которых рассчитываются по следующим формулам:

$$\lambda = \frac{1}{M(T)},$$

где $M(T)$ – среднее время между двумя последовательными атаками отдельных беспилотных систем в общем потоке атак;

$$\mu = \frac{1}{M(Tp)},$$

где $M(Tp)$ – среднее время, затрачиваемое на комплексное реагирование одной системой оперативного противодействия на атаку одной беспилотной системы в общем потоке атак.

¹ © Плотников Г. Г., 2024.

Тогда, рассматривая данную задачу, как многоканальную систему массового обслуживания с неограниченной очередью, удельную загрузку системы оперативного противодействия можно выразить через коэффициент:

$$\rho = \frac{\lambda}{\mu},$$

а критический уровень реагирования:

$$x = \frac{\rho}{k} = 1,$$

где k – количество каналов системы оперативного противодействия.

Таким образом, стратегия атакующей стороны будет направлена на обеспечение $x > 1$.

Мерой противодействия этому можно считать повышение информативности в целом всей системы оперативного противодействия через применение системы массового обслуживания, которая будет анализировать траекторию движения беспилотных систем и определять представляют ли они угрозу безопасности. Это позволит оптимизировать использование средств перехвата/поражения и собирать информацию об обнаруженных беспилотных системах с целью передачи системам оперативного противодействия на смежных территориях.

Стоит отметить, что с улучшением технических показателей системы противодействия, таких как дальность обнаружения или перехвата/поражения атакующих беспилотных систем, будет возрастать и потребность в многоканальности, наращивание которой в практике может иметь весьма жесткие ограничения, связанные с уровнем как вычислительных, так и радиотехнических возможностей системы. Выход видится в информационной интеграции как территориально смежных однотипных систем, так и за счет гармонизации различных систем противодействия, применяемых для защиты заданных объектов и территорий от атакующих беспилотных систем.

Теория массового обслуживания может быть использована для оптимизации работы систем борьбы с беспилотными системами. Например, можно определить оптимальное количество средств обнаружения и перехвата, а также оптимальные параметры их работы. Это позволит повысить эффективность оперативного противодействия и снизить затраты. Кроме того, теория массового обслуживания может быть использована для анализа эффективности существующих систем.

Список литературы

1. Плотников Г. Г. О надежности систем передачи извещений // Информационные технологии в деятельности органов внутренних дел : сборник научных трудов. М., 2022. С. 297–299.
2. Бороздина В. Н., Плотников Г. Г. Сравнение систем конвенциональной и сотовой связи в решении задач правоохранительной системы // Информационные технологии в деятельности органов внутренних дел : сборник научных статей. М., 2021. С. 99–102.

Поликарпов Е. С.¹,
доцент кафедры международной
информационной безопасности
Московского государственного лингвистического университета,
кандидат технических наук, доцент

Маяков Д. В.²,
аспирант Московского государственного
лингвистического университета

ЭТАПЫ СОЗДАНИЯ И ОБУЧЕНИЯ ЯЗЫКОВОЙ МОДЕЛИ ДЕТЕКТИРОВАНИЯ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ АУГМЕНТАЦИИ ДАННЫХ

В современном цифровом мире, где информационные технологии прочно вошли в повседневную жизнь организаций и частных лиц, обеспечение информационной безопасности становится приоритетной задачей для обеспечения конфиденциальности, целостности и доступности данных. Защита от информационных угроз и реагирование на инциденты безопасности становятся ключевыми компонентами в обеспечении стабильной работы информационных систем.

Целью данного исследования является разработка и исследование эффективной модели реагирования на информационные угрозы, основанной на анализе информации архитектурного стиля взаимодействия компонентов распределённого приложения в сети REST API запросов к микросервисам. Данная модель предназначена для выявления потенциальных компьютерных атак (вредоносных подключений) и своевременного принятия мер по предотвращению возможных инцидентов информационной безопасности.

Для достижения этой цели предполагается провести обзор существующих методов реагирования на информационные угрозы, разработать языковую модель для анализа REST API запросов, интегрировать новый признак в наборе данных (dataset) и обучить модель на расширенном объеме информации. Полученные результаты будут проанализированы, сравнены с существующими методами и представлены в заключительной части исследования.

В дальнейшем исследовании планируется выявить потенциал применения разработанной модели в реальных условиях и определить перспективы для дальнейших улучшений и расширений функциональности системы реагирования на информационные угрозы.

Обзор проблемы

Угрозы безопасности информации в киберпространстве постоянно эволюционируют, представляя все более изощренные методы атак, стремящихся обойти системы безопасности. Адаптивность является главной задачей при построении систем кибербезопасности. Традиционные алгоритмы обнаружения не всегда

¹ © Поликарпов Е. С., 2024.

² © Маяков Д. В., 2024.

способны оперативно реагировать на новые виды атак, особенно в контексте динамично развивающихся технологий, таких как микросервисная архитектура [1].

Другой важной проблемой является недостаточное внимание к анализу низкоуровневых данных, таких как HTTP(S) запросы к веб-сервисам [1; 2]. Большинство существующих методов уделяют внимание исключительно обработке статических данных, упуская из виду потенциально важные аспекты, связанные с динамическими интеракциями и обменом данными между системами.

Кроме того, сложность масштабирования и адаптации существующих систем кибербезопасности к изменяющейся обстановке и технологиям также остается актуальной проблемой. Организации сталкиваются с вызовом эффективного адаптивного реагирования на новые виды компьютерных атак и образующихся уязвимостей, не нарушая при этом нормальное функционирование бизнес-процессов [3].

Все вышеперечисленные проблемы свидетельствуют о необходимости разработки новых моделей и алгоритмов реагирования на информационные угрозы, способных обеспечить оперативное и эффективное выявление, анализ и предотвращение инцидентов информационной безопасности. Такой подход позволит не только повысить уровень защиты данных, но и уменьшить потенциальные убытки от возможных атак и нарушений безопасности [3–5].

Языковая модель для анализа REST API запросов

При создании языковой модели для анализа REST API запросов необходимо уделить особое внимание выбору архитектуры модели и определению входных и выходных данных. В первую очередь, следует определить структуру запросов, которые будут подвергаться анализу, включая методы HTTP, заголовки, параметры и тело запроса [6].

Для проектирования модели можно использовать глубокие нейронные сети, такие как рекуррентные нейронные сети (RNN), сверточные нейронные сети (CNN) или трансформеры. Кроме того, важно учесть, что модель должна быть способной выявлять шаблоны и аномалии в запросах, позволяя отличать вредоносные запросы от нормальных [7; 8].

Для оптимальной работы модели необходимо провести предварительную обработку данных, такую как токенизацию, векторизацию и нормализацию текста запросов. Это поможет модели эффективно извлекать признаки из текстовых данных и принимать правильные решения.

В процессе проектирования модели стоит также учесть возможность расширения и дальнейшей оптимизации модели с учетом поступления новых данных и изменения структуры запросов [8–10].

Отличительной особенностью рассматриваемой модели является аугментация за счет использования трансформеров, диффузионных моделей и GAN (генеративно-состязательных сетей), для создания других типов данных на основе базовых данных, что в конечном итоге будет направленно на повышение точности детектирования компьютерной атаки [11].

Рассмотрим далее подробное описание языковой модели и особенности процесса обучения на сгенерированных (синтетических) данных (рис.).



Рис. Этапы создания и обучения языковой модели

Обучение модели на сгенерированных данных

Чтобы получить лучшие результаты модели, необходимо иметь больше данных, в том числе и различные их вариации. Другими словами, необходимо увеличить размер исходного набора данных искусственным образом, и это можно сделать с помощью генерации синтетических наборов данных с внедрением новых признаков, так называемой аугментации данных.

Обучение языковой модели на сгенерированных данных является ключевым этапом в создании эффективной системы анализа REST API запросов. Для обучения модели необходимо подготовить обширный набор данных, содержащий как вредоносные, так и нормальные запросы.

Во время обучения модели будут использоваться алгоритмы машинного обучения, такие как глубокие нейронные сети, для извлечения паттернов из данных и обучения модели на основе этих паттернов. Важно регулярно контролировать процесс обучения, позволяя модели улучшать свои способности в классификации запросов.

Для повышения эффективности модели можно выделить новые признаки из данных, которые помогут лучше различать вредоносные подключения от обычных. Эти признаки могут быть связаны с частотой запросов, типами используемых методов HTTP, структурой заголовков и другими характеристиками запросов.

Выделение новых признаков позволит модели более точно определять и классифицировать запросы, улучшая общее качество системы обнаружения вредоносных действий. После интеграции этих новых признаков в модель следует провести тщательное тестирование и оценку ее эффективности [12].

Интеграция нового признака в набор данных

Обновление набора данных с новым признаком требует тщательного исследования данных, начиная с изучения структуры данных и диапазона значений нового признака. Необходимо проверить, как новый признак связан с целевой переменной и другими признаками в наборе данных.

При добавлении нового признака в набор данных (dataset) необходимо учитывать возможные пропущенные значения, выбросы и ошибки в данных. Иногда требуется провести дополнительную обработку, такую как заполнение пропусков, удаление выбросов и нормализацию данных.

Методы объединения признаков могут варьироваться от простого объединения значений до создания новых признаков на основе комбинации существующих. Это может потребовать применения различных техник, таких как кодирование категориальных признаков и масштабирование числовых признаков.

Понимание структуры данных и взаимосвязей между признаками поможет оптимизировать процесс подготовки набора данных. Важно также учитывать особенности задачи и алгоритмов, которые будут использоваться для обучения модели.

После подготовки и обогащения набора данных новым признаком необходимо провести валидацию данных, чтобы удостовериться в их корректности и пригодности для обучения модели. Тщательная подготовка набора данных является ключевым шагом к успешному построению модели машинного обучения.

Важно помнить, что качество набора данных напрямую влияет на качество обученной модели, поэтому уделите достаточно времени и внимания подготовке и анализу данных перед переходом к этапу обучения модели.

Обучение модели на новом признаке

Выбор подходящего алгоритма обучения для нового набора данных с учетом добавленного признака является ключевым шагом. Важно учитывать тип задачи (классификация, регрессия), характеристики данных и требуемую скорость обучения модели.

После выбора алгоритма необходимо провести настройку его гиперпараметров. Это важный процесс, который влияет на обобщающую способность модели и её способность к адаптации к новым данным.

Процесс обучения модели на новом признаке включает в себя разделение набора данных на тренировочную и тестовую выборки, обучение модели на тренировочных данных и оценку ее качества на тестовых данных.

При работе с новым признаком важно убедиться, что модель учитывает его влияние на предсказания. Это может потребовать дополнительных настроек алгоритмов обучения или создание специальных признаков комбинаций.

Процесс обучения модели может быть итеративным, что позволяет улучшать результаты и вносить коррективы при необходимости. Наблюдение за метриками качества модели в процессе обучения поможет принимать обоснованные решения.

После завершения обучения модели важно провести анализ результатов, чтобы оценить ее эффективность, выявить слабые места и определить возможные улучшения.

Оценка эффективности модели

Для оценки эффективности модели машинного обучения используют различные метрики, такие как точность, полнота, F1-мера, ROC-AUC и др. Каждая метрика отражает определенные аспекты качества модели и может быть применима в разных сценариях.

Кросс-валидация – это метод оценки производительности модели, который позволяет избежать переобучения и обеспечить более объективную оценку качества. При кросс-валидации данные разбиваются на несколько фолдов, в каждом из которых модель обучается на части данных и тестируется на оставшихся.

Важно учитывать интерпретируемость модели при оценке ее эффективности, особенно если решения, которые принимаются на основе предсказаний модели, имеют важные последствия. Понимание причинно-следственных связей и возможности объяснения предсказаний – ключевые аспекты работы с моделью.

После оценки метрик качества модели и проведения кросс-валидации необходимо сделать выводы о ее работоспособности и пригодности для конкретной задачи. В случае неудовлетворительных результатов можно вернуться к предыдущим этапам и внести коррективы в процессе обучения и оценки модели.

Обобщая, интеграция нового признака в набор данных и обучение модели – это сложный и многогранный процесс, который требует внимательного анализа данных, правильного выбора методов обработки и тщательной оценки качества модели. Важно быть готовым к итеративной работе и постоянному улучшению результатов для достижения успеха в области машинного обучения.

Разработка и исследование эффективной модели реагирования на информационные угрозы, основанной на анализе REST API запросов к микросервисам, является актуальной задачей в области информационной безопасности. Предложенный подход позволяет оперативно выявлять и предотвращать компьютерные атаки, что способствует повышению защищенности распределенных информационных систем.

Главной особенностью исследуемой модели является использование языковой модели, обученной на аугментированных данных. Применение техник генерации синтетических данных и интеграция новых признаков в набор данных позволяет повысить точность детектирования вредоносных подключений и адаптивность модели к изменяющимся условиям.

Предложенная оценка эффективности модели с использованием различных метрик качества, а также кросс-валидация, демонстрируют ее работоспособность и применимость в реальных условиях. Интерпретируемость модели и возможность объяснения принимаемых решений являются важными преимуществами для практического использования.

Дальнейшее развитие и совершенствование предложенной модели, а также исследование ее применения в других контекстах, связанных с обеспечением информационной безопасности, представляют перспективные направления для будущих исследований в данной области.

Список литературы

1. Филлипс Н., Смит Д. Защита микросервисов в распределенных системах // Журнал информационных технологий. 2019. Т. 21. № 3. С. 218–225.
2. Гринвуд Дж. Микросервисы и безопасность. М. : Техносфера, 2018.
3. Абрамов В. А., Корнилов М. Ю. Анализ и обеспечение безопасности микросервисной архитектуры в корпоративных информационных системах // Информационные технологии и безопасность. 2017. Т. 2. № 1. С. 23–29.

4. Браун Д. Микросервисы из глубины. М. : ДМК Пресс, 2017.
5. Хаузен Л. Безопасность микросервисов: лучшие практики и рекомендации // Белый медведь (White Bear) – Блог Ларса Хаузена. 2020. URL: <https://larshauens.com/security-best-practices-for-microservices/>.
6. «Security Engineering: A Guide to Building Dependable Distributed Systems» by Ross J. Anderson.
7. «Network Security Essentials: Applications and Standards» by William Stallings.
8. «Cryptography and Network Security: Principles and Practice» by William Stallings.
9. «Principles of Information Security» by Michael E. Whitman, Herbert J. Mattord.
10. «Computer Security: Principles and Practice» by William Stallings, Lawrie Brown.
11. «Applied Cryptography» by Bruce Schneier.
12. «Secure Coding in C and C++» by Robert C. Seacord.
13. «Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World» by Bruce Schneier.
14. «CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide» by Mike Chapple, James Michael Stewart, Darril Gibson.
15. «The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws» by Dafydd Stuttard, Marcus Pinto.

Полянская Е. П.¹,

*старший преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий*

Московского университета

МВД России имени В.Я. Кикотя

ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ МЕТОДА OSINT В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Цифровизация всех сфер деятельности существенным образом упростила нашу жизнь, но в то же время развязала руки преступникам, позволяя удаленно и анонимно совершать противоправные деяния.

Правоохранительным органам приходится находиться в роли догоняющей стороны, фактически в спешке создавать новые методики раскрытия и расследования преступлений, совершаемых с использованием информационно-коммуникационных технологий из-за динамично меняющихся способов и сценариев уголовно-противоправных деяний, появления новых технических решений, используемых злоумышленниками, работать при существенном дефиците разрешенных используемых технических инструментов, в условиях отсутствия оперативного и эффективного взаимодействия между всеми заинтересованными в деанонимизации преступников подразделениями органов внутренних дел и коммерческими организациями, серьезного несоответствия нормативно-правовой базы современным реалиям. И это только проблемы, «лежащие» на поверхности. На наш взгляд, в целях деанонимизации преступников и эффективного выполнения оперативно-служебных задач, сотрудникам правоохранительных органов на законных основаниях необходимо разрешить применять методы, которые успешно используются злоумышленниками в отношении граждан, а именно компьютерную разведку, включающую метод OSINT, фишинг, Noneurot, заражение технического устройства вредоносным программным обеспечением (стиллер), использование программы удаленного доступа RAT (Remote Access Trojan) и т. п. Важно отметить, что навыки использования перечисленного программного обеспечения у сотрудников отдельных подразделений, специализирующихся на раскрытии IT-преступлений имеются, а правовых возможностей для реализации нет.

Наиболее востребованным в повседневной деятельности каждого сотрудника органа дознания, либо предварительного следствия является использование метода OSINT (англ. *Open Source Intelligence*) – первоначального метода компьютерной разведки, определяемого как технология поиска, обработки и анализа данных из доступных источников.

Наиболее популярными инструментами получения информации методом OSINT у оперуполномоченных полиции, участковых уполномоченных полиции, дознавателей и следователей из-за доступности, оперативности и простоты использования являются чат-боты мессенджера Telegram «Архангел», «Химера»,

¹ © Полянская Е. П., 2024.

«Глаз Бога», «Insight», многофункциональный OSINT браузер «Venator», программное обеспечение, используемое для разведки и криминалистики «Maltego», а для компьютерной разведки наиболее подготовленными сотрудниками используются линукс-дистрибутивы для проведения кибер-расследований и OSINT «Kali Linux» и «CSI Linux Investigator». В ходе осуществляемой деятельности крайне важно оперативно получать данные для их своевременного анализа и использования в служебной деятельности, что и позволяет сделать вышеперечисленный софт.

Важно отметить, что правовые ограничения деятельности по раскрытию и расследованию преступлений затрагивают в большей степени не столько специализированные подразделения по противодействию преступлениям в сфере информационных технологий, сколько органы дознания территориальных органов, где сосредоточен основной массив материалов доследственных проверок и уголовных дел, а взаимодействие между подразделениями, заинтересованными в раскрытии преступлений, как показывает практика, оставляет желать лучшего.

Кроме того, указанные выше инструменты не находят никакого процессуального отражения, а их использование носит завуалированный характер. Связано это с хаотичным толкованием действующих правовых норм, регламентирующих деятельность сотрудников правоохранительных органов и отсутствием четкого понимания возможностей в правовой и технической сферах. К примеру, до сих пор нет однозначного толкования п. 15 «Получение компьютерной информации» ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Под таковым можно понимать как составную часть оперативно-розыскного мероприятия «снятие информации с технических каналов связи», так и любое гласное действие, совершаемое в сети Интернет, но явно не проведение полномасштабного мероприятия, а именно проведения атаки и осуществление действий, направленных на деанонимизацию преступника и формирование емкой доказательственной базы.

При осуществлении компьютерной разведки с использованием вышеуказанных способов могут быть нарушены гарантированные Конституцией Российской Федерации права на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, допускаемых только на основании судебного решения. Правовых норм, позволяющих прямо использовать перечисленные выше способы получения информации о злоумышленнике, в том числе при наличии судебного решения либо не имеется в основополагающих федеральных законах, регламентирующих деятельность сотрудников правоохранительных органов по раскрытию и расследованию преступлений, либо имеются, но в достаточно абстрактной форме, к примеру в ч. 1 ст. 11 «Использование достижений науки и техники, современных технологий и информационных систем» Федерального закона «О полиции», но без указания возможностей для реализации использования компьютерной разведки или ее элементов.

Для решения проблем, связанных с установлением личности злоумышленника и фиксации его преступной деятельности в сети Интернет, необходимо не только получать компьютерную информацию, но и использовать те данные, доступ к которым возможен, хотя и ограничен.

Другими словами нужно осуществлять комплекс компьютерной разведки, включающий в себя целенаправленную атаку в отношении преступника, заражения его технического устройства вредоносным программным обеспечением с целью получения информации, либо удаленного управления, применения ловушки Noneurort, редиректа (перенаправления пользователя с уязвимого доверенного сайта на фишинговый сайт для сбора данных), использования IP-спуфинга для получения доступа к техническому устройству и многое другое, что в силу своей специфики не относится к оперативно-розыскным мероприятиям «Снятие информации с технических каналов связи» или «Получение компьютерной информации», не говоря о мероприятиях и следственных действиях, перечисленных в ФЗ «О полиции» и УПК РФ. Однозначно для выполнения подобных действий требуется наличие специальных знаний. На наш взгляд целесообразно рассмотрение на законодательном уровне включения компьютерной разведки в перечень оперативно-розыскных мероприятий, а также регламентирование ее реализации, что позволит повысить эффективность деятельности сотрудников правоохранительных органов по раскрытию и расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий.

Список литературы

1. Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. 2023. № 1. С. 62–66.
2. Open Source Intelligence (OSINT) 2oolKit On The Go. 2022.
3. Ромачев Р. В., Стригунов К. С., Го Ф. Политика Аутсорсинга разведывательных услуг в США // Международная жизнь. 2022. № 6. С. 58–65.
4. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 131–135.

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

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

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ АНАЛИЗА БОЛЬШИХ ДАННЫХ И SIEM-СИСТЕМ ДЛЯ ВЫЯВЛЕНИЯ ТЕНДЕНЦИЙ И ПАТТЕРНОВ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

В настоящее время вопросы противодействия киберпреступлениям и выявления определенных тенденций развития методов осуществления кибератак становятся наиболее острыми и актуальными. Постоянное развитие информационных технологий позволяет хакерским группировкам совершенствовать различные направления в области осуществления атак на организации, в свою очередь, для эффективного противодействия киберпреступлениям необходимо постоянно улучшать и дорабатывать инструменты и методы анализа данных, для своевременного выявления уязвимостей в системах безопасности и предотвращения кибератак.

При борьбе с данным видом угроз ключевую позицию занимает использование аналитических систем. Основная роль здесь отводится технологиям анализа больших данных. Аналитика больших данных станет обязательным компонентом любого эффективного решения в области кибербезопасности из-за необходимости быстрой обработки высокоскоростных данных большого объема из различных источников для максимально быстрого обнаружения аномалий и (или) схем атак, чтобы ограничить уязвимость систем и повысить их устойчивость.

Одним из примеров является технология «Siren» [1], предназначенной для расследования киберпреступлений в различных сферах деятельности и сочетает в себе расширенный анализ источников, бизнес-аналитику, анализ больших данных и анализ данных оперативной разработки. Она решает глобальную проблему разнородности больших объемов различных данных, автоматически устанавливая взаимосвязи и выявляя общие объекты анализа. Данная платформа активно используется полицией Ирландии, а также многими странами Европы для обнаружения связи между лицами, совершившими дорожно-транспортные происшествия.

Для реконструкции процессов производства кибератаки предлагается использование системы комбинированного обнаружения трафика (Traffic-Log

¹ © Помещиков С. Е., 2024.

Combined Detection (TLCD) [2], которая позволяет соотнести характеристики трафика и данные из журналов/файлов регистрации, чтобы отразить процесс атаки и создать объединенную платформу обнаружения. TLCD может обнаруживать этапы процесса кибератаки, отражать текущее состояние сети и при этом выявлять стандартное поведение пользователей для минимизации возникновения ошибок.

Существует огромное количество различного рода систем анализа больших данных, многие из которых используются в том числе для выявления закономерностей в развитии кибератак. Использование таких систем позволит ускорить деятельность государственных организаций по выявлению и дальнейшему противодействию хакерским атакам.

Не менее важная роль в анализе кибератак и киберпреступлений отводится системам управления информационной безопасностью и событиями безопасности (SIEM) – это решение, позволяющее организациям обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб. SIEM объединяет в себе различные функции и инструменты, такие как управление журналами, анализ безопасности, обнаружение инцидентов и реагирование на них.

SIEM сочетает в себе средства управления информационной безопасностью (SIM) и управления событиями безопасности (SEM) в единую систему управления безопасностью. Технология в режиме реального времени анализирует данные журналов событий от различных источников и, выявляя аномальные действия, принимает меры по их устранению [1]. Такая система также позволяет фиксировать все действия сотрудником компаний, либо внедренного в корпоративную систему вредоносного программного обеспечения, которые обычно называют «событиями», содержащими всю вышеперечисленную информацию. Современные SIEM системы хранят данные обо всех приложениях, которые содержатся на компьютерах организаций и как эти компьютеры между собой связаны.

Основной задачей систем управления информационной безопасностью и событиями безопасности является помощь организациям в выявлении и реагировании на потенциально опасные события, которые могут повлиять на безопасность информации. Однако, данные системы используются и для выявления паттернов действия различных вредоносных программ, что также позволяет отследить тенденции их развития на основе предоставляемых SIEM-системами отчетов.

Средства SIEM имеют ряд преимуществ, улучшающих состояние корпоративной системы безопасности. К таким преимуществам относятся:

1. Обнаружение и реагирование на угрозы в режиме реального времени.
2. Аналитика угроз.
3. Централизованное представление информации.
4. Ведение общих массивов данных.

Частные компании также разрабатывают свои системы SIEM, внедряя в них новые функции, повышая качество и эффективность их работы в условиях постоянно растущего уровня угроз для информационной безопасности организаций.

Одним из примеров SIEM системы, разработанной частной компанией является Kaspersky Unified Monitoring and Analysis Platform (KUMA), разработанное «Лабораторией Касперского» [1].

Данная разработка имеет ряд преимуществ, которые позволяют улучшить работу систем безопасности и ускорить дальнейший процесс борьбы с кибератаками, к основным отличительным чертам KUMA относятся:

- высокая производительность при относительно низких системных требованиях;
- разработанная модульная архитектура обеспечивает возможность масштабируемости, отказоустойчивости и изменения конфигурации системы без особых проблем.

Таким образом, предлагаемая платформа от «Лаборатории Касперского» справляется с основными задачами и проблемами, возникающими в условиях постоянного роста и развития количества информации в корпорациях. Платформа централизованно собирает и анализирует полученные данные о произошедших инцидентах.

Еще одним примером SIEM системы является MaxPatrol Security Information and Event Management (MaxPatrol SIEM) от компании Positive Technologies. В данном продукте также можно наблюдать большое количество дополнений и изменений стандартной системы SIEM, основными из которых можно считать следующие:

- актуальная экспертиза за счет ежемесячного добавления новых пакетов экспертиз, собираемых командой хакеров, выявляющих новые способы обнаружения киберугроз;
- повышение эффективности обнаружения атак за счет внедрения ML-помощника BAD (Behavioral Anomaly Detection);
- повышение производительности за счёт внедрения собственных технологий (пример: СУБД LogSpace).

Исходя из этого, MaxPatrol SIEM позволяет оперативно и просто самостоятельно обнаруживать хакеров и целые хакерские группировки.

Подводя итог вышеперечисленного, одним из самых актуальных на данный момент решений для производства анализа характеристик угроз и дальнейшего выявления тенденций их развития, является система управления информационной безопасностью, которая выполняет поставленные перед ней задачи, объединяя аналитику больших данных и машинное обучение в единую централизованную систему анализа и оперативного реагирования на возникших угрозы в сфере безопасности информации организаций. Правильное использование SIEM позволит эффективнее выявлять кибератаки, составляя подробные отчеты о произошедшем, которые в дальнейшем при дополнительном анализе с использованием ранее перечисленных аналитических систем позволят выявить определенные закономерности в работе различных инструментов, используемых преступниками. Такая аналитика на данный момент уже проводится многими Российскими компаниями, предоставляющими услуги в области безопасности информации, самыми известными и популярными из них являются вышеупомянутые Positive Technologies и Лаборатория Касперского.

В заключение, хотелось бы отметить, что применение технологий анализа больших данных и SIEM-систем является эффективным инструментом при про-

тивоедействи киберпреступлениям. Данные технологии позволяют обрабатывать значительные объемы данных, составляя подробные отчеты об инцидентах информационной безопасности, а в дальнейшем и сопоставлять изменения в тактике проведения таких атак, а также отслеживать развитие и модернизацию используемых программ. Внедрение данных технологий в деятельность различных государственных организаций, а также отдельно в органы внутренних дел, позволит оперативно реагировать на возникающие угрозы, обеспечивая комплексную защиту информационных систем и общую подготовку к новым угрозам.

Список литературы

1. Что такое SIEM? // Microsoft. URL: <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-siem#SIEM-capabilities-and-use-cases>.
2. Siren Analytics. URL: <https://www.sirenanalytics.com/>.
3. Integrating Traffics with Network Device Logs for Anomaly Detection / [Лы Цзячжун и др.] // Security and Communication Networks. URL: <https://www.hindawi.com/journals/scn/2019/5695021/>.
4. Выявление инцидентов ИБ с помощью SIEM: типичные и нестандартные задачи // Positive Technologies. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/incidents-siem-2020/>.

Рожков Н. И.¹,

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

Научный руководитель: Полянская Е. П.,

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

РАЗВИТИЕ МЕТОДОВ И ТЕХНОЛОГИЙ КВАНТОВОЙ КРИПТОГРАФИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ И ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Квантовая криптография представляет собой современную область криптографии, основанную на принципах квантовой механики и использующую квантовые системы для обмена информацией и создания безопасных криптографических ключей. В условиях растущих угроз кибербезопасности, связанных с развитием квантовых компьютеров и квантового криптоанализа, методы квантовой криптографии становятся особенно актуальными для обеспечения защиты конфиденциальных данных.

Информационная безопасность является одним из наиболее актуальных вопросов в современном обществе, где данные играют главную роль во всех сферах деятельности. Исследование и применение методов квантовой криптографии позволяет обеспечить надежную защиту данных от современных угроз и обеспечить конфиденциальность информации в сети. Актуальность данной темы подчеркивается необходимостью развития новых подходов к криптографической защите данных в условиях роста объемов цифровой информации и возрастания уровня киберугроз. В этом контексте изучение и совершенствование методов квантовой криптографии играет ключевую роль в современной информационной безопасности. Криптография представляет собой науку, предоставляющую методы обратимого преобразования открытого текста на основе секретного ключа или математического алгоритма в зашифрованный текст для обеспечения конфиденциальности, целостности данных и аутентификации. В настоящее время общедоступные методы криптографии не могут предоставить полноценную защиту для конфиденциальных данных пользователей. Квантовое шифрование позволяет обеспечить максимальный уровень безопасности, потому что в настоящее время невозможно «подслушать» сообщение, зашифрованное данными методами.

Квантовое шифрование – это способ защиты информации с использованием принципов квантовой механики. В отличие от классического шифрования, которое использует математические алгоритмы для защиты данных, квантовое шифрование основано на принципах проявления квантовых явлений.

¹ © Рожков Н. И., 2024.

Основные принципы квантового шифрования:

1. *Принцип суперпозиции.* Одна элементарная частица может находиться одновременно в нескольких состояниях: обладать большой и маленькой энергией, вращаться по часовой стрелке и против, находиться в разных местах сразу. Но основным свойством является хрупкость данного явления: как только мы пытаемся узнать, в каком именно состоянии находится частица, она мгновенно принимает одно из возможных состояний, нарушая принцип суперпозиции. Вмешательство приводит к необратимой потере информации о прошлом состоянии частицы, что делает невозможным восстановление ее начального состояния. Данный принцип позволяет создавать квантовые ключи, которые невозможно скопировать или подобрать без изменения самого ключа.

2. *Принцип измерения.* Для расшифровки сообщения, зашифрованного методами квантовой криптографии, необходимо измерять полученный ключ и сравнивать с ключом отправителя, но при этом элементарные частицы потеряют свойство суперпозиции, что делает невозможным получение информации о ключе без его изменения.

3. *Принцип запутанности.* Квантовые частицы могут быть запутанными, это означает, что изменение состояния одной частицы автоматически приводит к изменению состояния другой, даже если они находятся на большом расстоянии.

4. *Принцип неопределенности.* Две квантовые величины не могут быть измерены одновременно с требуемой точностью.

BB-84 – первый протокол квантового распределения ключей, предложенный в 1984 г. Ч. Беннетом и Ж. Brassаром. В нем передача данных осуществляется по оптоволокну с помощью единичных фотонов, которые поляризованы в разных плоскостях.

Представим двух участников обмена информацией: Пользователь1 и Пользователь2, а также Злоумышленника, который хочет перехватить их сообщение. Пользователь1 готовит горизонтально или вертикально поляризованный фотон, после чего Пользователь2 его измеряет, допустим, что горизонтальный – 0, а вертикальный – 1, после чего Пользователь2 записывает все полученные поляризованные единичные фотоны в двоичном виде. В это время Злоумышленник может перехватить эти фотоны и тоже измерить. В случае, если он их испортит, он может сделать точную копию и отправить дальше Пользователю2. В таком случае поштучная передача фотонов действительно усложняет перехват сообщения, поскольку, согласно законам квантовой физики, фотон нельзя разделить на части. При перехвате фотонов Злоумышленнику иногда придется поглощать их полностью и для того, чтобы остаться незамеченным, ему потребуется создавать идеальные копии перехваченных фотонов, что крайне сложно на практике.

Для решения этой проблемы в протоколе BB-84 используется 4 вида квантовых состояний, которые образуют 2 базиса: канонический, когда фотон находится горизонтально либо вертикально (0° или 90°), и диагональный, когда фотоны повернуты диагонально в разные стороны (45° или 135°). Пользователь1 случайным образом выбирает базис, из которого также случайно выбирается со-

стояние самого фотона, и отправляет измененную частицу Пользователю2. После чего он начинает случайным образом выбирать базис и измерять полученные данные, но с 50 % вероятностью он выберет неверный базис.

Потом Пользователь1 и Пользователь2 по открытым каналам связи обмениваются информацией о том, какие базисы они использовали при приготовлении и измерении фотонов. Далее они выбрасывают все измерения, в которых их базисы не совпали, а совпавшие базисы должны иметь одинаковое двоичное представление. Таким образом происходит процедура просеивания ключа. Теперь они имеют одинаковый чистый секретный ключ, который никто кроме них не знает, после чего они могут с помощью данного ключа шифровать данные по обычным каналам связи.

Полезность данного метода заключается в том, что Злоумышленнику при перехвате тоже придется случайным образом подбирать базис. И если он выбрал диагональный базис, а фотон изначально имел прямой канонический, то для него он находится не в промежуточном состоянии, а в суперпозиции двух: он и прямой диагональный, и обратный (45° и 135°) одновременно. Пройдя через Злоумышленника, фотон становится либо прямой диагональный, либо обратный (45° или 135°), и он не будет знать, какой фотон был изначально. Таким образом, суперпозиция фотона разрушена, и даже если Злоумышленник создаст полную копию фотона, то она будет отличаться от начальной, и замену можно будет обнаружить. После чего Пользователь1 и Пользователь2 поймут, что их прослушивают, и начнут всю процедуру сначала. При использовании данного протокола квантового шифрования, единственное, что может сделать Злоумышленник – это выдать себя и остановить процесс. Но оставаясь незамеченным, он никогда не сможет узнать, какие именно ключи оказались у Пользователя1 и Пользователя2. Независимо от того, что квантовые технологии все еще находятся на стадии разработки, уже в наше время они показывают свой огромный потенциал для решения самых важных вопросов информационной безопасности. Уже в ближайшем будущем данные технологии позволят создавать самые передовые методы защиты информации, что значительно повысит уровень безопасности систем.

Список литературы

1. Альбов А. Квантовая криптография. М. : Страта, 2022.
2. Блохинцев Д. И. Квантовая механика : лекции по избранным вопросам. М., 2021.
3. Яценко В. В. Введение в криптографию. М., 2000.

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

Научный руководитель: **Лопухов В. В.,**
старший преподаватель кафедры
естественнонаучных дисциплин
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя

ОСОБЕННОСТИ ИДЕНТИФИКАЦИИ ГРАЖДАН ПРИ ПРОХОЖДЕНИИ ЧЕРЕЗ КОНТРОЛЬНО-ПРОПУСКНЫЕ ПУНКТЫ МВД РОССИИ

Проблематика идентификации граждан на контрольно-пропускных пунктах МВД России

Идентификация граждан, проходящих через контрольно-пропускные пункты объектов МВД России, является важным аспектом качественной работы подразделений. За короткий период времени, в течение которого гражданин находится на контрольно-пропускном пункте, сотруднику, осуществляющему пропускной режим, необходимо установить личность гражданина и подлинность предъявляемого документа.

Главная цель внутриобъектового режима – обеспечение защиты людей на объекте, сохранности движимых и недвижимых материальных ценностей, а также защита информации на печатных и электронных носителях. Также, режим позволяет предотвратить несанкционированное проникновение на территорию объекта и обеспечивает контроль перемещения лиц на нем [1].

Для обеспечения правомерного пропуска лиц через контрольно-пропускные пункты, используются следующие виды идентификации гражданина. Это биометрические технологии, отпечатки пальцев, проверка документов, в том числе фотографий, и каждый из них имеет свои преимущества и недостатки, поэтому выбор, используемого метода должен основываться на эффективности, надежности и технической возможности его применения [2].

Важным вопросом является обеспечение персональных данных гражданина при его идентификации. Необходимо, чтобы при предъявлении их сотруднику полиции они были надежно защищены, и не могли попасть третьим лицам.

Технические аспекты идентификации граждан на контрольно-пропускных пунктах МВД России

Одним из основных средств идентификации является считывание данных с предъявляемого документа. Многие контрольно-пропускные пункты объектов

¹ © Роздорский Н. С., 2024.

МВД России (далее – КПП) оборудованы специальными устройствами для чтения данных из магнитных полос документов, удостоверяющих личность, а также штрих-кода, содержащего информацию о гражданине. Это позволяет быстро и точно установить личность и проверить его наличие в базе данных.

Дополнительные средства идентификации включают в себя системы распознавания лиц и отпечатков пальцев. Эти технологии позволяют более надежно установить личность гражданина, особенно в случае использования поддельных документов. Система распознавания лиц сравнивает фотографию с базой данных, а система распознавания отпечатков пальцев сравнивает отпечатки с сохраненными данными [3].

В Московском университете МВД России имени В.Я. Кикотя проход через КПП осуществляется вручную, путем предъявления документа, удостоверяющего личность. Постовой по КПП обязан устанавливать на подлинность служебного удостоверения, либо паспорта гражданина, следить, чтобы документы не были просрочены. Также используются контроллеры СКУД (система контроля и управления доступом) – эта система, которая обрабатывает сигналы от устройств идентификации, и на основе этих данных принимает решение о предоставлении или отказе в доступе.

Вместе с тем, не все объекты МВД России оснащены системами автоматизированной идентификации граждан и на многих из них сотрудникам полиции приходится вручную производить указанные действия вручную досмотровые мероприятия. Ручной режим работы ставит процесс идентификации в зависимость от человеческого фактора, это приводит к ошибкам и нарушениям пропускного режима.

Проблемы, связанные с идентификацией граждан на КПП МВД России

Проблемным является вопрос выявления поддельных документов. Злоумышленники могут подделывать паспорта и другие удостоверения личности, уровень подделки бывает очень высоким, что затрудняет их распознавание.

Другой проблемой проверки граждан на КПП является необходимость пропуска за короткое время большого потока людей. Например, в Московском университете МВД России имени В.Я. Кикотя во время проведения дней открытых дверей, конференций и совещаний КПП пропускает через себя значительное количество людей, причем на проверку одного человека может быть затрачено не более нескольких секунд.

Поскольку КПП, как правило, работают в круглосуточном режиме, для обеспечения одного рабочего места необходимо выделения четырех сотрудников при режиме работы сутки через трое. Если на КПП несут службу два сотрудника, соответственно требуется восемь человек, а с учетом их отпусков это количество увеличивается до 10. То есть, для обеспечения пропускного режима в подразделении с КПП, рассчитанном на два сотрудника, необходимо выделения из штатной численности почти половины роты патрульно-постовой службы районного отдела внутренних дел.

Кроме этого, физические способности человека небезграничны. Установлено, что после просмотра нескольких сотен фотографий на документах, работоспособность проверяющего сотрудника сильно снижается, и увеличивается вероятность пропуска нарушителя.

Перспективы развития системы идентификации граждан на КПП МВД России

В связи с указанными выше причинами необходимо в максимальной степени автоматизировать процесс пропуска посетителей через КПП. В ряде ведомств и организаций данный вопрос успешно решается. Наибольшего успеха достигли организации, обладающие высокими финансовыми возможностями – банки, ресурсодобывающие коммерческие предприятия и др.

В ряде крупных подразделений МВД России используются дактилоскопическая идентификация и СКУД, с помощью которых при проходе посетителя на экране рабочего места КПП появляется фотография человека, его данные (Ф. И. О., звание, должность) и открывается устройство прохода. Дежурный сотрудник на КПП присутствует и в его функции входит контроль за достоверностью демонстрируемых данных проходящего, а также проверка документов лиц, не имеющих в базе данных подразделения [4].

Использование указанных систем безусловно облегчает работу сотрудника КПП, но полностью его не заменяет.

Для повышения уровня автоматизации пропускного режима необходимо внедрение других перспективных способов идентификации. Это распознавание человека по изображению лица, голосу, радужной оболочке глаза. А также в этом процессе целесообразно использование технологий искусственного интеллекта.

Идентификация личности по изображению лица достаточно хорошо изучена, имеются эффективные системы распознавания. В Российской Федерации наилучшие результаты достигнуты в г. Москве, где такая система уже успешно функционирует с камерами видеонаблюдения, установленными на крышах и в подъездах домов и на транспорте. Благодаря ей в г. Москве ежедневно раскрываются десятки преступлений по горячим следам.

Голосовая система также показывает высокий процент идентификации, внедрена в деятельность ряда государственных, коммерческих структур и может быть использована на автоматических КПП.

Идентификация по радужной оболочке глаза по качеству распознавания сравнима с дактилоскопической идентификацией и также рекомендована в пропускных системах.

Пути решения, имеющих проблем

Полная автоматизация процесса пропуска граждан через КПП возможна и обладает рядом преимуществ по сравнению с проверкой граждан в ручном режиме.

Вместе с тем, полный отказ от человеческого фактора имеет ряд существенных недостатков.

Так, сотрудник полиции, осуществляющий пропускной режим может не только не допустить проверяемое лицо на объект, но и, при необходимости, задержать его. Например, в случае попытки проноса запрещенных предметов (оружие, взрывчатые вещества, взрывные устройства, наркотические средства

и т. д.), прохождение с просроченными документами и др. Автоматизированная система этого сделать не может.

Также, отсутствие сотрудника на КПП не позволяет пресекать противоправные действия, проявление которых возможно со стороны лиц, вынашивающих деяние преступного характера – поломка оборудования, использование устройств, выводящих из строя систему пропуска, и позволяющих совершить несанкционированный проход на территорию объекта.

Кроме этого, любая автоматизированная система идентификации личности не обеспечивает стопроцентную гарантию выявления нарушителя и имеет некоторую вероятность ошибки, либо сбоя.

Поэтому целесообразно полностью не исключать человеческий фактор и наиболее важных объектах использовать сотрудников для контроля за работой системы пропускного режима и оперативного реагирования на ее сигналы.

Для увеличения достоверности выявления нарушителей пропускного режима возможно одновременное использование нескольких методов идентификации – по изображению лица и отпечаткам пальцев, радужной оболочке глаза и изображению лица, ручная и автоматизированная сверка документа на признаки подделки, и другие варианты.

Большую перспективу имеет автоматическая система паспортного контроля «САПСАН», развернутая в аэропорту Шереметьево. Система проверяет подлинность приложенного к терминалу документа, его срок действия и соответствие предъявляющего документ человека. В системе предусмотрен сторожевой контроль, связанный с запретом на выезд из страны, нахождением в розыске и другим причинам.

Подобные системы в настоящее время внедряются в системе органов внутренних дел, их использование позволит существенно повысить качество работы подразделений, оказание государственных услуг и защищенность объектов МВД России от противоправных проявлений.

Список литературы

1. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М. : Горячая линияТелеком, 2010.
2. 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...» // СПС «Консультант-Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_436110.
3. Протасовой А. А., Козловой О. А. Современные технологии идентификации лица: исследование алгоритма работы и использование // Прикладная информатика. 2020. Т. 15. № 2. С. 131–143.
4. Лопухов В. В. Информационно-аналитическое обеспечение как неотъемлемая часть процесса раскрытия преступлений на примере организации работы подразделений ГУ МВД России по г. Москве // Информационные технологии в деятельности органов внутренних дел : сборник научных трудов. М. : Московский университет МВД России имени В.Я. Кикотя, 2023. С. 215–221.

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

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

ИДЕНТИФИКАЦИЯ ЛИЦА, СОВЕРШИВШЕГО УГОЛОВНОЕ ПРЕСТУПЛЕНИЕ ИЛИ АДМИНИСТРАТИВНОЕ ПРАВОНАРУШЕНИЕ В СЕТИ ИНТЕРНЕТ

В XXI в. Интернет стал широко использоваться повсеместно, почти на всей территории Российской Федерации. В связи с ростом количества пользователей в сети Интернет, пропорционально повышается и число преступлений, а также административных правонарушений в Интернете.

В современном мире основное количество преступлений, связанных с мошенничеством, оборотом наркотиков, продажей оружия и людей, а также административные правонарушения, например, оскорбление, совершаются именно с помощью глобальной сети.

Необходимо отметить тот факт, что в связи со сложностью установления конкретного лица, совершившего противоправное деяние, правоохранительные органы вынуждены производить поиск различных способов деанонимизации пользователей в сети интернет для возможности привлечения его к уголовной или же административной ответственности.

Несмотря на то, что в соответствии со ст. 7 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, получившие доступ к персональным данным, к примеру, операторы сотовой связи, обязаны не распространять и не раскрывать третьим лицам персональные данные без согласия субъекта персональных данных, полиция вправе запросить данные о пользователе какой-либо социальной сети, электронной почты, форума и т. п. в соответствии с п. 4 ч. 1 ст. 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции».

Существует несколько способов идентификации правонарушителя в Интернете:

1. Цифровые следы (они включают в себя ip-адрес, cookie-файлы, историю браузера, активность в интернете и др.).
2. Мониторинг социальных медиа (данный способ включает в себя непрерывное отслеживание аккаунта в социальных сетях, сообщения, публикации, истории, отправленные со страницы наблюдаемого).

¹ © Рудометов Д. Р., 2024.

3. Сотрудничество с интернет-провайдерами (в соответствии с вышеупомянутым законодательством, интернет-провайдеры обязаны предоставлять правоохранительным органам запрашиваемую информацию о своих пользователях, у них имеется история посещенных пользователем сайтов, информация о местонахождении конкретного устройства, которое пользуется услугами провайдера, информация об использовании VPN-сервисов и иных сервисов, целью которых является анонимизация пользователя в сети интернет).

Данный список способов идентификации не является исчерпывающим, поскольку с каждым годом технологии развиваются, создавая новые сложности у правоохранительных органов а так же новые пути их решения.

Однако не всегда удастся вычислить правонарушителя, поскольку существует множество способов для повышения анонимности в интернете, рассмотрим некоторые из них:

1. Использование специальных мессенджеров с шифрованием службы обмена сообщениями (например, Telegram в секретных чатах, а также при звонках использует сквозное шифрование, которое перехватить кому-либо, даже правоохранительным органам, проблематично).

2. Использование браузера Tor, VPN-сервисов и т. п. (браузер тор максимально анонимизирует подключение пользователя, присваивая ему другой ip-адрес, используя специальные узлы по следующему принципу: клиент шифрует данные так, что их возможно расшифровать только входному узлу, затем данные шифруются так, чтобы расшифровать мог лишь промежуточный узел, а потом эти данные опять шифруются так, чтобы их мог расшифровать только сторожевой узел).

Как и список способов идентификации, данный список не является исчерпывающим по вышесказанной причине. Вследствие использования перечисленных способов создания анонимности в Интернете, привлечь лицо к ответственности за совершенное административное правонарушение или уголовное преступление может быть огромной проблемой. Для решения данной проблемы мы можем использовать следующие средства с целью раскрытия личности пользователя в сети Интернет:

1. Боты в мессенджере Telegram (существуют различные чат-боты в мессенджере Телеграмм, в которых, введя номер телефона разыскиваемого пользователя, выдаётся подробная информация о пользователе: его электронные почты, пароли, иногда паспортные данные, место проживания, провайдер и другая ценная для расследования дела информация).

2. Ссылки-ловушки (тому, кто создал подобную ссылку, отправляется информация о ip-адресе, устройстве, а также программном обеспечении пользователя, который перешел по этой ссылке).

3. Также сотрудники полиции могут послать официальный запрос, соответствующий законодательству Российской Федерации, в компании по типу Яндекс, Google, Yahoo и т. п. с целью получения информации об определенном правонарушителе. Данный запрос требует соответствующего решения суда.

Таким образом идентификация лиц, совершивших уголовное преступление или административное правонарушение в сети Интернет возможна, хоть и обладает некоторыми трудностями.

Список литературы

1. Жарова А. К. О соотношении персональных данных с IP-адресом Российский и зарубежный опыт. URL: https://elibrary.ru/download/elibrary_25962991_50944344.pdf.
2. Кувычков С. И. К вопросу об использовании электронной информации в уголовно-процессуальном доказывании: теоретико-прикладной аспект. URL: https://elibrary.ru/download/elibrary_23618854_56530892.pdf.
3. Сидорова К. С. IP-адрес как один из идентификаторов личности в расследовании преступлений // Психопедагогика в правоохранительных органах. 2022. № 3 (74). С. 84–87.

Рябинкина С. М.¹,

курсант Института-факультета судебной экспертизы

Московского университета

МВД России имени В.Я. Кикотя

Александров Ю. Н.²,

заместитель начальника кафедры информатики и математики

Московского университета

МВД России имени В.Я. Кикотя

ПРОБЛЕМЫ ВНЕДРЕНИЯ ТЕХНОЛОГИИ 3D-СКАНИРОВАНИЯ В ЭКСПЕРТНУЮ ДЕЯТЕЛЬНОСТЬ

Появление и развитие современных цифровых технологий ярко отразилось на многих отраслях науки и техники (медицина, архитектура, инженерия и др.) в том числе оно отразилось и на судебно-экспертной деятельности [1].

Помимо фотографирования, как основного способа фиксации осмотра места происшествия и проведения исследований в экспертно-криминалистических подразделениях МВД России и образовательных организациях структуры МВД России все чаще стал подниматься вопрос о возможности использования технологии 3D-сканирования при производстве отдельных видов экспертиз [2]. Для решения вопроса о целесообразности применения 3D-сканирования Московским университетом МВД России имени В.Я. Кикотя данная технология была опробована в области трасологической экспертизы для изъятия и фиксации объемных следов (подошв обуви, орудий взлома, ходовой части транспортных средств (протектора шин), а также в области портретной экспертизы для получения трехмерных изображений с целью исследования признаков внешнего облика человека. В качестве сканирующего устройства использовался аппарат отечественного производства «Calibry», который позиционируется как аппарат для широкого спектра применения. Для изучения полученных 3D-моделей использовалось программное обеспечение «Calibry Nest». В результате данного исследования были выявлены как преимущества использования данной технологии, так и некоторые недостатки. Среди преимуществ следует отметить, что при 3D-сканировании фиксируется полный комплекс признаков объекта без оптических искажений, а при фотографировании – только их видимая часть (в зависимости от выбранного ракурса фотографирования, с учетом оптических искажений). Кроме этого, 3D-модель объекта с помощью специального программного обеспечения можно отобразить с любым поворотом как по горизонтали, так и по вертикали, что важно при сравнении с кадрами видеоизображения. Среди недостатков следует обратить внимание на потребность в больших вычислительных мощностях при работе с 3D-моделями, сложностью обеспечения неподвижности сканируемого объекта, а также необходимости повышения квалификации экспертов, использующих данный метод [3]. В целом, методика использования 3D-сканеров оценена как перспективная.

¹ © Рябинкина С. М., 2024.

² © Александров Ю. Н., 2024.

Другим успешным примером использования технологии 3D-сканирования является применение цифрового микроскопа Leica DVM6 с функцией 3D-сканирования при исследовании документов [4]. Однако следует отметить, что данный аппарат не является отечественным и может быть недоступен для закупки в настоящее время. О наличии отечественного аналога авторам не известно.

Экспертами ЭКЦ МВД России также проводились исследования с целью решения вопроса о возможности внедрения технологии 3D-сканирования в экспертную практику. На основании чего было разработано методическое пособие [5], в котором рассмотрены перспективы применения 3D-технологий и 3D-моделирования и внедрение современного цифрового оборудования в экспертную деятельность.

Однако, по нашему мнению, наряду с эффективным применением технологии 3D-сканирования при фиксации следов на осмотре места происшествия и проведении исследований с помощью данной технологии, а также успешном применении аналогичной технологии при исследовании документов, имеется ряд проблем, ограничивающих обширное применение 3D-сканеров.

Во-первых, для работы с 3D-сканером и при последующем исследовании полученных 3D-моделей с помощью специального программного обеспечения требуется высокий уровень подготовки специалистов.

Во-вторых, необходима доработка этого специального программного обеспечения, которое написано для демонстрации 3D-моделей на мониторе компьютера, а не для проведения сравнительного анализа с обычным фотоизображением с фиксацией этапов и параметров производимых операций.

В-третьих, несмотря на то, что 3D-сканеры являются высокоточными эффективными устройствами, достоверность измерений, проведенных при их помощи, может оцениваться весьма сомнительно, так как 3D-сканеры не проходят поверку и не являются сертифицированными приборами.

В-четвертых, необходимо учитывать, что эффективность и точность отсканированного объекта зависит не только от технических характеристик сканирующего устройства, но и от физиологических особенностей лица, проводящего сканирование: мышечный тремор (тряска рук), способность удерживать сканер на одинаковом расстоянии от объекта (касается портативных (ручных) 3D-сканеров) и т. д. Здесь же можно отметить роль природных факторов, влияющих на результат сканирования: подвергание объектов воздействию повышенной влажности, высокой/низкой температуры (некоторые устройства способны сканировать при температуре не ниже 0°), засвечивание и т. д. [6]. Сложная конфигурация, габариты, детализация и структура сканируемого объекта в некоторых случаях также являются препятствием для применения технологии 3D-сканирования.

Для работы и хранения полученных 3D-моделей необходимо соответствие требованиям рабочего места эксперта: монитор Full HD1920x1080, четырехядерный процессор от 3 GHz (восьмипоточный, с объемом оперативной памяти не менее 32 Гб), дополнительный операционный носитель SSD-накопитель на 512 Гб или 1 Тб и т. д.

Финансовое обеспечение оснащения экспертно-криминалистических подразделений устройствами 3D-сканирования в виду их дорогой стоимости также является немаловажной проблемой.

Данный перечень проблем не является исчерпывающим, однако, несмотря на большое количество преимуществ использования технологии 3D-сканирования в экспертной деятельности, оказывает затруднения для эффективного и массового применения 3D-сканеров экспертную практику.

В настоящее время уже проводятся исследования и мероприятия, направленные на решение некоторых из вышеперечисленных проблем.

Список литературы

1. Александров Ю. Н. О цифровизации экспертно-криминалистической деятельности // Криминологический журнал. 2023. № 4. С. 24–27.
2. Александров Ю. Н., Дядык Е. С., Воробьева Т. И. Перспективы использования мобильных 3D-сканеров в экспертно-криминалистической деятельности // Техничко-криминалистическое обеспечение раскрытия и расследования преступлений : сборник научных трудов. М. : Московский университет МВД России имени В.Я. Кикотя, 2022. С. 18–22.
3. Применение 3D-сканеров Calibry в криминалистике : исследование Московского университета МВД России имени В.Я. Кикотя. URL: <https://calibry3d.ru/news/primenenie-3d-skanerov-calibry-v-kriminalistike-issledovanie-moskovskogo-universiteta-mvd-im-v-ya-ki/>.
4. Горбулинская И. Н., Барбачакова Ю. Ю., Шавленко Е. В. О возможностях применения методов 3D-моделирования в ходе производства криминалистических экспертиз // Вестник экономической безопасности. 2018. № 1. С. 42–45.
5. Использование технологий 3D-моделирования при производстве судебных экспертиз : методическое пособие. М.: Экспертно-криминалистический центр МВД России, 2022.
6. Беляев, М. В., Котов К. Ю. К вопросу фиксации следов подошвы обуви на снегу // Судебная экспертиза: российский и международный опыт : сборник научных трудов. Вып. 6. Волгоград : ИП Черняева Ю.И., 2022. С. 52–59.

*Сакулина Л. Л.¹,
доцент кафедры административного права
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент*

ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВОВОМ ПРОСТРАНСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

В настоящее время искусственный интеллект (ИИ) представляет собой научное направление, возникшее на стыке кибернетики, лингвистики, математической логики, психологии и программирования. Основу разработки ИИ составляет: моделирование психофизиологической деятельности человека, т. е. создание искусственного разума, и моделирование с помощью современных информационных технологий его мыслительной деятельности, для которого в последнее время получены достаточно большие результаты, имеющие значительную практическую направленность.

Как любое научное направление, ИИ имеет свою историю развития и, что интересно, она во многом повторяет (во времени) развитие компьютерной техники. Это было связано с тем, что их совершенствования постоянно взаимно дополняли друг друга.

Начиная с 50-х гг. прошлого столетия, когда появились первые вычислительные машины, исследователи в области ИИ пытались с их помощью строить разумные машины, имитируя мозг. Этот этап получил название периода разработки нейронных сетей.

Следующим этапом развития искусственного интеллекта считается начало 60-х гг., когда стало относительно быстро развиваться так называемое направление эвристического поиска или эвристического программирования. В основе теории эвристического поиска лежало предположение о том, что мыслительная деятельность человека построена на определённом сочетании элементарных операций, манипулирования символами, таких, как сравнение, сложение, вычитание, поиск, модификация символа и другие, которые достаточно легко реализуются с помощью компьютера.

Очередной этап развития искусственный интеллект и это 70-е гг. прошлого столетия, получивший название этап предоставления знаний. Специалисты в этой области стали отказываться от поиска эффективных и универсальных средств эвристического поиска и занялись суждением рассмотренных вопросов.

Следующий этап – это разработка создания обучающих систем, появилась возможность «работы» со знаниями. Он начался в 80-е гг. и продолжается до настоящего времени. Именно уровень и качество базы знаний есть основа успешной разработки систем ИИ. Разработанные компьютерные обучающие системы уже тогда позволили автоматически расширять свой запас эвристических

¹ © Сакулина Л. Л., 2024.

правил, что является важнейшим этапом развития ИИ и его будущего компьютерных обучающих систем.

Поскольку вычислительных данных и мощностей сегодня больше, чем в предыдущие десятилетия, исследования в области ИИ стали более распространенными и доступными. Мы стали свидетелями крупных достижений в области робототехники на основе ИИ, квантовых вычислений и появление генеративных инструментов искусственного интеллекта. И что больше всего волнует в этой быстрой эволюции, так это впечатляющие возможности ИИ и широкие социальные последствия его применения.

Круг правовых проблем, возникающих в связи с использованием технологии искусственного интеллекта, является весьма обширным. Хотелось остановиться на самых актуальных.

Конфиденциальность данных. Использование технологии живого распознавания лиц в общественных местах в правоохранительных органах потенциально может нарушить право на неприкосновенность частной жизни. В данном случае возникают проблемы утечки данных и ошибки распознавания.

Интеллектуальная собственность. Проблемы идентификации произведений, созданных ИИ. Также остается открытым вопрос о том, кому будут принадлежать авторские права на контент, созданный искусственным интеллектом. В общих чертах, опасения по поводу авторских прав на ИИ можно отнести к одной из двух категорий:

- нарушают ли компании, занимающиеся ИИ, существующие авторские права, обучая свои модели на материалах, защищенных авторским правом;
- защищен ли контент, созданный с помощью моделей ИИ, авторским правом, и если да, то кому принадлежат эти авторские права.

Нарушение авторских прав в пользу компаний, занимающихся ИИ, может стимулировать внедрение эффективных механизмов идентификации произведений, созданных ИИ. Учитывая экономическую ценность авторских прав, у компаний, занимающихся искусственным интеллектом, будет возможность идентифицировать контент, созданный на их платформах, даже если позже они решат заключить договор о делегировании авторских прав по умолчанию. Идентификация имеет значение, поскольку будущие правила могут потребовать надежной инвентаризации работ, созданных ИИ, а наличие точных механизмов идентификации значительно облегчит администрирование будущих схем регулирования.

Этические проблемы ИИ. Необходимо разработать этические правила взаимодействия человека с искусственным интеллектом. Как правило этические нормы носят рекомендательный характер и реализуются на добровольной основе, но их создание поможет дополнить существующие правила использования ИИ не урегулированы законодательством.

Безопасность и ответственность. Требуется дальнейшая проработка механизмов гражданско-правовой, уголовной и административной ответственности в случае причинения вреда системами искусственного интеллекта, определить круг лиц, которые будут нести ответственность за их действия. Так, в 2022 г. в Китае произошел инцидент с беспилотным автомобилем Tesla, закончившийся смертью двух человек. К трагедии привел сбой в автомобильной системе. Кто

в подобных случаях должен нести ответственность, когда «деяние» ИИ формально будет подпадать под признаки конкретного состава правонарушения: разработчик, его пользователь, владелец или иное лицо?

В настоящее время особенно остро стоит беспокойство по поводу неопознанных изображений, созданных ИИ, которые могут быть «дипфейками» или иным образом манипулироваться. Нейросети научились создавать цифрового двойника практически любого человека. Они могут подделывать не только внешность, но и голос. Как только технология стала доступна всем, ее начали использовать и мошенники. Так же неясно, кому принадлежит контент, созданный ИИ, кто несет ответственность за контент, созданный ИИ, и какой контент существует в свободном доступе. Что касается дипфейка, то непонятно, кто может нести ответственность, если, например, чье-то изображение будет использовано без его согласия. ИИ также может представлять угрозу безопасности государства, например, в случае распространения сгенерированных фейковых новостей во время предвыборной кампании или массовых мероприятий.

При разработке критериев ответственности необходимо использовать риск-ориентированный подход, так как применение технологий искусственного интеллекта несет объективно высокий риск причинения вреда участникам общественных отношений, правам человека и интересам общества и государства.

Все эти неопределенности требуют более четкого понимания ИИ и того, как он может повлиять на общество.

В понятие ИИ вкладывается различный смысл – от признания интеллекта у ЭВМ, решающих логические или даже любые математические задачи, до отнесения к интеллектуальным лишь тех систем, которые решают задачи, обычно выполняемые человеком.

В настоящее время отсутствует единое понимание термина «искусственный интеллект». Один из вариантов на подзаконном уровне предложен в Указе 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») (далее – Стратегия 2030) [1]. В данном определении ИИ сформулирован как технология, позволяющая получать результаты, сопоставимые, с результатами интеллектуальной деятельности человека.

Стратегия 2030, как и другие программные документы [2] не содержит конкретных норм права, определяющих, правовой статус искусственного интеллекта, особенности и последствия его применения, ответственность за неправомерное использование искусственного интеллекта либо причинение им вреда. Поэтому необходимо разрешить вопрос о содержании и критериях определения ИИ как объекта правового регулирования и далее рассматривать вопрос о правовой регламентации конкретных сфер его применения.

И первое, что хотелось бы отметить, ИИ не может ассоциироваться с деятельностью субъекта общественного производства и права. Любые продукты работы ИИ не являются результатами автономной деятельности машины, так как работа ИИ координируется человеком, а следовательно, именно человек, как пользователь или создатель соответствующего программного обеспечения приобретает

права, несет обязанности и ответственность, связанные с его использованием. Ни понятие вины, ни лишения имущественного характера к искусственному интеллекту не могут быть применены. Искусственный интеллект не может чувствовать вины или каких-либо лишений. Если действия человека ограничиваются осознанием негативных последствий, то трудно представить, что какие бы то ни было негативные последствия могут ограничивать действия ИИ.

И второе, ИИ не может быть участником общественных отношений, следовательно его место определяется только положением объекта прав. Поскольку ИИ функционирует на основе программного обеспечения, созданного человеком, то и за результат его работы соответственно должны нести ответственность разработчик-изготовитель и эксплуатант. Поэтому, требования включить ИИ в число субъектов права являются ошибочными. При этом, некоторые современные российские авторы находят основания для выделения ИИ в отдельную категорию субъектов права [3, с. 37].

Стремление расширить границы традиционной правосубъектности любыми аргументами в действительности преследует ярко выраженный экономический интерес, как можно предположить, крупные участники рынков производств киберинженерных систем хотят минимизировать собственную ответственность за производимое оборудование в ущерб законным интересам потерпевших, что способно оправдать стремления любого бизнесмена, но никак не подменить собой задачи правового регулирования, функции и принципы права.

Что касается проблем этического характера, то они так же могут быть решены только посредством определения правосубъектности ИИ и ее легального закрепления.

Таким образом, обработка всевозрастающих потоков неформализованной информации с помощью современных информационных технологий остается на сегодня актуальной проблемой. Для решения этой задачи в настоящее время разрабатываются различные системы ИИ, в основу которых заложена способность имитации мыслительной деятельности человека.

Но разработка таких систем сдерживается, во-первых, определённой трудностью логической организации данных, разработке и реализации сложных алгоритмов, оперирующих сознание, моделирование конкретных систем и во-вторых, нехваткой нормативных правил, принципов и ограничений, связанных с разработкой и применением систем с ИИ, так как на государственном уровне обозначены лишь общие вопросы правового регулирования и перспективные направления развития законодательства в сфере использования ИИ.

В каком направлении может идти поиск правовых механизмов регулирования искусственного интеллекта и связанных с ним технологий?

Прежде всего необходимо определить предмет и границы регулирования сферы использования систем ИИ и робототехники и выработать морально-нравственные, этические критерии обновляемого права современности.

Список литературы

1. 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»)» // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.

2. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

3. Ястребов О. А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. 2018. Т. 13. № 2. С. 37.

Сапелкина А. В.¹,

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

Научный руководитель: Емельянова О. В.,

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

МЕТОДЫ РЕГУЛИРОВАНИЯ КРИПТОВАЛЮТНЫХ ОПЕРАЦИЙ В РОССИИ

Криптовалюта – это разновидность цифровой валюты, не имеющей физического воплощения и единого центра, который бы ее контролировал. Работает в так называемом «блокчейне» или цепочке блоков с информацией [1]. Необходимо помнить, что существует множество разновидностей криптовалют. Самые популярными являются: Биткон, Эфир, Рипл.

Одним из методов регулирования является внесение новых законопроектов. Сама криптовалюта, как и ее виды, хоть и не является средством платежа, но все равно легализирована в России. Она охраняется государством, а точнее Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

Вторым методом регулирования платежа в Российской Федерации, является борьба с мошенничеством и интернет терроризмом. Криптовалюта является средством для совершения преступлений в сфере терроризма, незаконного оборота наркотических средств, легализации денег. В Федеральном законе «О цифровых финансовых активах» присутствует некий запрет на оплату цифровой валютой товаров, работ и услуг, так как в Российской Федерации действует законодательство, по которому единственным платёжным средством является рубль [2]. К данному методу также относится проверка личностей, совершающих обмен валютами. Технологии блокчейн позволяют следить за операциями, проводимыми в области криптовалюты. Государственные органы могут потребовать необходимых лицензий для осуществления своей деятельности. Криптовалютные лицензии бывают трех видов: на обмен валютой, на организацию биржи и на выпуск криптовалют. Модель лицензии зависит от модели компании и выбранной юрисдикции.

Немаловажный метод регулирования – введение налога на криптовалюту. Криптовалюта является имуществом. Согласно Российскому законодательству, лица обязаны выплачивать налог на доходы физических лиц, так называемый НДФЛ. Если рассматривать юридические лица – налог на прибыль предприятия.

¹ © Сапелкина А. В., 2024.

Федеральные службы в Российской Федерации ведут мониторинг за воспроизводственным процессом в сети Интернет. Введение базы электронных кошельков, отслеживание связей цифровых активов, контроль участников обмена валюты – одни из основных направлений регулирования оборотов криптовалюты. «Прозрачный блокчейн» позволяет отслеживать транзакции. Данная программа способствует минимизации преступности в интернет сфере.

Таким образом, можно сделать вывод о необходимости регулирования криптовалюты в России, в том числе выше предложенными методами. Контроль позволяет сбалансировать на финансовом рынке права и интересы сторон. Легальное использование электронного платежа влечет за собой развитие экономики в большом масштабе.

Список литературы

1. Гришин Я. Что такое криптовалюта. URL: <https://journal.sovcombank.ru/glossarii/cto-takoe-kriptoalyuta>.
2. Файгулина Л. Пробелы уголовно-правового регулирования криптовалюты в российском законодательстве. Проблемы квалификации киберпреступлений и оценки доказательств. URL: https://zakon.ru/blog/2024/03/26/probely_ugolovno-pravovogo_regulirovaniya_kriptoalyuty_v_rossijskom_zakonodatelstve_problemy_kvalif.

Симакова М. А.¹,

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

Научный руководитель: Калашикова А. А.,

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

РОЛЬ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ В БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ

На сегодняшний день, в связи с быстрым развитием информационной сферы, увеличивается количество преступлений в данном секторе. Научно-технический прогресс охватывает не только какой-либо определённый субъект общества, но и весь мир в целом. Такие преступления содержат в себе угрозу для каждой сферы деятельности. Это связано с тем, что электронные и информационные методы работы набирают все большую актуальность и практичность. Именно поэтому необходимо контролировать и анализировать данную сферу, не только на государственном уровне, но и на международном.

Такая организация, как Европейская комиссия, еще в 2013 г. разделила киберпреступления на три категории, которые приведены ниже (рис.) [3].

Еще одним примером международного сотрудничества в информационном пространстве может служить Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями, связанными с преступлениями IT-сферы, который был подписан в 2001 г. [2]. Данный договор подразумевает уголовную наказуемость за умышленно совершенные киберпреступления. При этом сотрудничество осуществляется непосредственно между заинтересованными компетентными органами.

В современном обществе можно привести множество примеров международных кибератак. Одними из таких стали: взлом сети Facebook², которая произошла в 2020 г. При которой, по данным британской компании Comparitech, произошла утечка личных данных более 267 млн пользователей. Это стало одним из громких дел на международном уровне, который принес не только огромный финансовый ущерб, но и ущерб личным данным пользователей, которые могли быть использованы против них самих.

Существует несколько причин, по которым международные киберпреступления являются одними из самых не только опасных, но и наименее раскрываемых.

¹ © Симакова М. А., 2024.

² Запрещена в России: принадлежит корпорации Meta, которая признана в России экстремистской.

Одной из таких причин может служить трудность в выявлении такого рода деяний. Латентные преступления в данной сфере – это не новшество, так как достаточно сложно определить территориально источник преступления, с какого устройства и от какого лица они исходят.

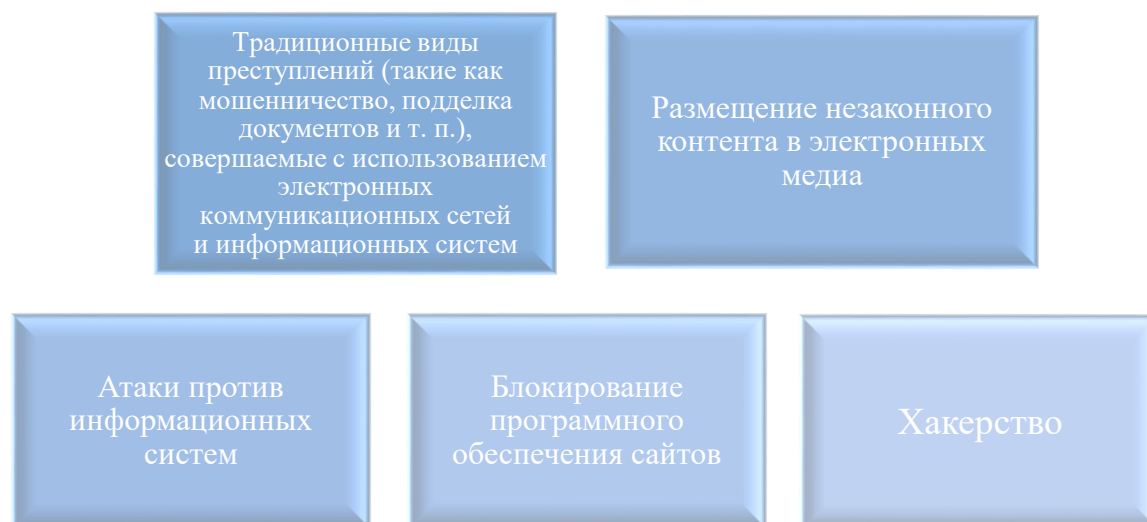


Рис. Категории киберпреступлений

Такая коалиция, как Организация Объединенных Наций (ООН) непосредственно влияет на международное сотрудничество и помогает выявлению информационных преступлений. В 2019 г. Российской Федерацией была предложена резолюция «Противодействие использованию информационно-коммуникационных технологий в преступных целях», которая была принята большинством голосов. Данный документ предполагает суверенитет в цифровой сфере, таким образом, глобально воздействуя на пресечение киберпреступлений. Для воплощения данного акта была создана своего рода площадка для обсуждения актуальных вопросов, связанных с преступлениями в цифровой сфере. Для этого был создан орган, отвечающий за данное направление. Таким органом стал Спецкомитет, в котором работают специалисты со всего мира, обеспечивая не только государственную, но и международную безопасность в IT-сфере. Таким образом, можно сказать, что ООН выполняет задачу по содействию в обеспечении кибербезопасности на международном уровне.

Из всего вышесказанного можно сделать вывод о том, что международные организации только начинают свою работу в сфере сотрудничества, связанного с выявлением и пресечением международных киберпреступлений. Важно отметить, что у данных объединений, за счет структуры всемирного общения практически со всеми странами, будет больше возможностей для выполнения поставленных задач. Необходимо развивать сотрудничество с такими организациями для обеспечения международной безопасности в различных сферах деятельности. Важно не только проводить профилактику данных преступлений, но и разрабатывать новые методы борьбы с ними для повышения качества пресечения преступлений.

Список литературы

1. Горелик И. Б. Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности // Международное право. 2023. № 2. С. 33–44.
2. Международные и региональные правовые документы // Серия Университетских Модулей: Киберпреступность. URL: <https://www.unodc.org/e4j/ru/cyber-crime/module-3/key-issues/international-and-regional-instruments.html>.
3. Стратегия кибербезопасности Европейского союза: открытое, безопасное и защищенное киберпространство. URL: <http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52013JC0001>.

Симонова В. Д.¹,

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

Дубинина Н. М.²,

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

ИНФОРМАЦИОННЫЕ ВОЙНЫ: ИСТОРИЯ И СОВРЕМЕННОСТЬ

Информационные технологии занимают центральное место в нашей жизни. Основа всех систем жизни современного общества строится на цифровизации и использовании различных электронных ресурсов. Ввиду таких изменений происшествия все чаще стали случаться на информационных площадках, злоумышленники находят новые способы для совершения противоправных действий.

ИКТ активно используются в выработке и принятии управленческих решений, в том числе на государственном уровне. Ведение военных конфликтов в настоящее время происходит не только посредством вооруженного нападения, но и путем создания определенного информационного поля вокруг своих граждан и населения противоборствующей стороны. Это явление имеет свое название – информационная война.

История возникновения информационных войн берет своё начало в Древнем мире. Например, желая деморализовать воинов перед началом сражения, им доводились сведения о том, какая армия противоборствующей стороны сильная и непобедимая. Эмоционально подавленная армия проигрывала, потому что боязнь «сильного» врага сказывалась на их духе. Яркими примерами являются сражения Руси с Золотой Ордой, Ливонская война, период Смутного времени. Данное явление наблюдалось не только в Российском государстве, оно имело свои начала во всех странах. Ведь зарождение информационных войн связано в первую очередь с распространением ложной информации и для негативного воздействия на население.

В 1976 г. Томас Рон в своем докладе «Системы оружия и информационная война» впервые использовал понятие «информационная война», в котором он отмечал, что информационная инфраструктура становится важным аспектом экономики, который наиболее уязвим в военных конфликтах. Официальное упоминание этого термина в директиве министра обороны США относится к 1992 г. Можно заметить, что на всех этапах истории информационная война имела иден-

¹ © Симонова В. Д., 2024.

² © Дубинина Н. М., 2024.

тичную структуру: главной задачей атакующей стороны является дезинформация общества и сведение ценностей к идеалам противника, что впоследствии ведет к разложению общества и нарастанию в нем напряженности.

Информационные войны проводятся как на макроуровнях общественной организации, которые охватывают все информационные каналы связи, так и на микроуровне, который подразумевает более узкое взаимодействие с людьми. Различают также следующие направления информационных войн: психологическое, экономическое, разведывательное, кибервойны, хакерские атаки, разрушение каналов связи и уничтожение технических средств передачи командно-управленческой информации, шпионаж и другие.

Вопросам обеспечения национальной безопасности в Российской Федерации всегда уделялось особое внимание. Разработана Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 [1]. В концепции обеспечения информационной безопасности выделяют следующие сферы защиты:

- 1) экономическую;
- 2) внешнеполитическую;
- 3) внутриполитическую;
- 4) область образования, науки и технологий;
- 5) духовно-нравственную;
- 6) судебную и правоохранительную.

Подразделения информационной безопасности осуществляют надзор в части целостности, доступности информации путем обеспечения защищённости каналов связи, бесперебойной работы информационно-телекоммуникационных систем.

Таким образом, информационная война – это противоборство государств в информационном пространстве, имеющее цель – причинение существенного ущерба государственным информационным системам, процессам и ресурсам, критически важным объектам при помощи массовой психологической обработки населения. Основная цель таких действий направлена на подрыв экономической, политической, социальной систем общества и государства. Информационное воздействие на население является уже долгие годы неотъемлемой частью ведения военных действий между государствами.

Список литературы

1. Указ Президента Российской Федерации от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_208191/.
2. Маркоменко В. Информационное общество и проблемы его безопасности // Федерализм. 1997. № 4. С. 18–24.
3. Козин М. Н., Родионов А. В. Методы и инструменты ведения информационной войны: новые угрозы подрыва социально-экономической и политической стабильности государства // Человек: преступление и наказание. 2022. № 3. С. 331–332.
4. Иванов С. А. Информационная война: сущность и основные формы проявления // Известия АлтГУ. 2013. № 4 (80). С. 276–277.

Смирнов В. М.¹,
доцент кафедры информатики и математики
Московского университета
МВД России имени В.Я. Кикотя,
кандидат технических наук

НАВИГАЦИОННО-МОНИТОРИНГОВЫЕ СИСТЕМЫ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Современный мир находится на стадии цифровизации, развития информационных технологий и повсеместного внедрения их во все сферы общественной жизни. В деятельности органов внутренних дел (ОВД) все чаще стали использоваться множество технических средств. Это позволяет наиболее эффективно выстроить служебную деятельность, разрешать задачи, возложенные на них, а также установить наиболее четкий контроль за несением службы. В настоящее время, в ОВД повсеместно практикуется использование навигационно-мониторинговых систем (далее-НМС), основанных на использовании глобальной навигационной спутниковой системы (ГЛОНАСС). Системы такого вида повсеместно используются во всех сферах жизни, таких как логистика, личное пользование GPS-навигаторами, бизнесе и др.

Обратимся к нормативно-правовому обеспечению использования НМС в деятельности ОВД. На сегодняшний день, существует несколько нормативных правовых актов, такие как постановление Правительства Российской Федерации от 25 августа 2008 г. № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» [2]. В соответствии с вышедшим постановлением правительства, МВД России утвердило приказ от 31 декабря 2008 г. № 1197 «Об утверждении и использовании общих тактико-технических требований к использованию общих тактико-технических требований к спутниковым навигационно-мониторинговым систем для органов внутренних дел Российской Федерации и внутренних войск МВД России» [3]. В 2007 г. вступил в силу Указ Президента Российской Федерации № 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации». Иностранные аналоги НМС были заменены и ГЛОНАСС начал использоваться на территории Российской Федерации. Данная НМС имеет ряд преимуществ, такие как высокоточное определение местоположения, в том числе при неблагоприятных погодных и климатических условий. Еще одним преимуществом является тот факт, что оснащение сил и средств ОВД необходимыми техническими средствами для использования данной НМС не представляет серьезной проблемы. Также, помимо доступности и простоты в использовании, стоит отметить такое преимущество, как непрерывность использования. В практической деятельности ОВД основным преимуществом использования таких НМС является скорость реагирования на сообщения о происшествиях, поступивших

¹ © Смирнов В. М., 2024.

от граждан, соответственно и количество пресекаемых правонарушений и преступлений вырастает, поскольку наряды полиции могут в кратчайшие сроки выдвинуться согласно местоположению, которое становится проще определить, что особую актуальность имеет в больших городах. Также, как уже отмечалось нами выше, такие НМС позволяют сделать так, чтобы экипажи нарядов были под постоянным наблюдением со стороны контролирующих органов и должностных лиц. К тому же, такие НМС позволяют рассчитать маршруты патрулирования таким образом, чтобы, как и в любой организации, связанной с транспортными перевозками, рассчитать путь и количество затрачиваемого на это топлива с целью экономии ресурсов.

Рассмотрим подразделения, которые наиболее часто используют НМС. В первую очередь, это ППСП, ДПС ГИБДД, подразделения уголовного розыска, дежурные части.

Для ППСП и ДПС ГИБДД так называемые бортовые НМС устанавливаются в транспортные средства (ТС), и состоят из следующих элементов:

- контролер навигации и связи;
- «Тревожная кнопка» и ряд иных специальных датчиков;
- концевые выключатели, которые устанавливаются в стойках дверей, основаниях капота и багажника;
- средства получения навигационной информации – навигационные приемники (GPS-приемники);
- средства передачи информации в центр мониторинга (ЦМ).

Наличие таких технических средств, установленных на каждом экипаже ТС позволяет сотрудникам в точности определять местоположение необходимых им объектов, в целях реализации задач, возложенных на них на маршруте патрулирования, обеспечении наиболее быстрого прибытия на места происшествий, взаимодействия с другими нарядами, а также для наиболее грамотного осуществления охраны общественного порядка.

Развитие и совершенствование системы ГЛОНАСС происходит в тесном взаимодействии с ИСОД МВД России. Содержащиеся в ней сервисы, совместно с НМС ГЛОНАСС способны вывести информатизацию деятельности ОВД на новый уровень. Внедрение этих систем в деятельность ОВД с каждым днем повышает ее эффективность, способствует выполнению служебных обязанностей с минимальным количеством используемых ресурсов и приносит исключительно положительный опыт.

Список литературы

1. ГЛОНАСС. Принципы построения и функционирования / под ред. А. И. Перова, В. Н. Харисова. 4-е изд., перераб. и доп. М., 2010.
2. Постановление Правительства Российской Федерации от 25 августа 2008 г. № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS» (с изменениями и дополнениями) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_79591/.

3. Приказ МВД России от 31 декабря 2008 г. № 1197 «Об утверждении и использовании общих тактико-технических требований к использованию общих тактико-технических требований к спутниковым навигационно-мониторинговым системам для органов внутренних дел Российской Федерации и внутренних войск МВД России» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/>.

Страхов А. А.¹,

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

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*

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ГЛОБАЛЬНАЯ УГРОЗА БЕЗОПАСНОСТИ

Повсеместное внедрение информационно-телекоммуникационных технологий под общим названием «искусственный интеллект» (ИИ) в последнее десятилетие во многом способствовало наступлению 4-й индустриальной революции и перевернуло привычный мир людей. ИИ меняет ландшафт киберпространства и захватывает все больше технологических процессов, обеспечивающих человеческую жизнедеятельность. И как это обычно бывает с научно-техническим прогрессом, резкое ускорение эволюции ИИ несет не только всеобщее благо, но и создает глобальные проблемы.

Правовые и морально-этические вопросы развития и использования ИИ по замыслу и под контролем людей вызывают много вопросов и активно обсуждаются в научном сообществе [1; 2]. Но основной целью данной статьи является исследование пределов обучаемости и поведенческих особенностей современного ИИ, а также оценка рисков угроз от его самостоятельной деятельности при отсутствии контроля со стороны человека.

Люди всегда мечтали о создании умных искусственных помощников, способных избавить от повседневной рутины и давать дельные советы в трудных ситуациях, но до изобретения ЭВМ в середине XX в. это все относилось к области фантастической литературы. Термин «искусственный интеллект» впервые прозвучал на научном семинаре в Дартмутском колледже (Ганновер, Нью-Гэмпшир, США), организованном в 1956 г. по инициативе математика Джона Маккарти,

¹ © Страхов А. А., 2024.

² © Жукова П. Н., 2024.

³ © Прокопенко А. Н., 2024.

основателя теории информации Клода Шеннона и ученого-когнитивиста Марвина Мински. Чуть более десятка энтузиастов в течение нескольких недель обсуждали вопросы теории двоичных вычислений, архитектуры компьютерных систем, методы обработки информации на естественном языке, принципы функционирования нейронных сетей, математические основы «умных» алгоритмов и прикладных языков программирования. Результатом мозгового штурма стали концептуальные основы новой отрасли компьютерных наук.

Британский ученый Алан Тьюринг в 1950 г. опубликовал статью, в которой задал вопрос: «Могут ли машины делать то, что мы (как мыслящие существа) можем делать?» [3]. Другими словами, могут ли машины осмысливать свои действия, так как это делает человек? В данной статье мы попробуем найти ответ на этот вопрос и разобраться, насколько безопасно стремление ученых к бесконечному совершенствованию искусственного разума. Реальна ли уже угроза от искусственного интеллекта человечеству или до «восстания машин» еще далеко.

Сегодня ИИ в основном связан с нейронными сетями и глубоким обучением. Но так было не всегда. На протяжении большей части своей восьмидесятилетней истории в этой области доминировал символьный ИИ, иначе называемый GOF AI (англ. *Good Old-Fashioned Artificial Intelligence* – старый добрый ИИ) с легкой руки американского профессора философии Джона Хогеланда.

Символы – это то, что мы используем для отражения окружающего мира в нашем сознании. Символы играют жизненно важную роль в процессе человеческого мышления. Мы постоянно используем символы для обозначения объектов живой и неживой природы, их состояние или действия. Символы могут быть организованы в иерархические структуры (каталоги включают в себя другие каталоги и могут содержать файлы). Они также могут быть использованы для описания других символов. Способность общаться с помощью символов – одна из основных черт, делающих нас разумными. Следовательно, символы также сыграли решающую роль в создании искусственного интеллекта. Если вам скажут, что кошка сидит на дереве, ваш разум быстро представит этот образ. Пионеры ИИ верили, что каждый аспект размышления по любому вопросу можно описать настолько точно, что легко будет воспроизвести в компьютерной программе для его имитации. Ученые разработали инструменты для определения символов и манипулирования ими. Многие концепции и инструменты, которые есть в информатике, являются результатами этих усилий. Программы символьного искусственного интеллекта основаны на создании явных структур и правил поведения.

Символьный ИИ предполагал создание компьютерных программ, интегрированных с человеческими базами знаний с фиксированными правилами логических выводов по заданным наборам данных. Примером инструментального метода создания GOF AI-приложений является объектно-ориентированное программирование. Языки ООП позволяют определять классы, задавать их свойства и организовывать их в иерархии. Для описания конкретных объектов создаются экземпляры классов с заданными свойствами. Экземпляры классов могут выполнять действия, известные как функции, методы или процедуры. Каждый метод выполняет серию инструкций, основанных на правилах, которые могут

считывать и изменять свойства текущего и других экземпляров. Еще в 60-х гг. прошлого века были разработаны специализированные языки LISP и Prolog, с помощью которых даже сейчас можно создавать сложные программы, ассоциированные с ИИ.

С повышением вычислительной мощности компьютерной техники приложения ИИ, основанные на формализованных правилах обработки входных данных, не утрачивают актуальности и по-прежнему составляют основу большинства современных экспертных систем, систем автоматического управления, поисковых машин и т. п. В 1997 г. компьютерная система Deep Blue компании IBM путем перебора всех возможных комбинаций на глубину до 20 ходов вперед выиграла матч из шести партий у чемпиона по шахматам Каспарова.

Вместе с тем в ситуациях, когда приходится сталкиваться с мировым беспорядком и искать решения задач в условиях неопределенности символический ИИ начинает давать сбои. Предположим, вам нужно найти на фотографии кошку. Ваш мозг это сделает мгновенно, конечно, если это не кот Шредингера. Теперь попробуйте классифицировать кошку как объект материального мира, не используя ассоциативное мышление, а с помощью описания свойств и логических правил типа «если этот признак равен..., то он указывает на кошку». Сколько понадобится таких правил и какова вероятность ошибки? В принципе ничего страшного не произойдет, если ваш ИИ, обученный таким образом, будет ошибаться в 99 случаях из 100 при поиске кошки. А если будет ошибаться боевой робот, охраняющий периметр секретного объекта? Или автопилот? Или система мониторинга и жизнеобеспечения пациентов медицинской клиники? В любом случае вероятность ложного срабатывания или неправильного прогноза будет зависеть от ошибки алгоритма. Машина с архитектурой Фон Неймана сама по себе не может умышленно изменить программные коды, следовательно, степень угрозы, исходящей от символьного ИИ, зависит от программиста.

Несколько десятилетий символьный ИИ демонстрировал многообещающие результаты, но в последние годы на первый план вышел коннекционистский ИИ.

Коннекционизм – это концепция ИИ, согласно которой, любые психические или поведенческие процессы можно смоделировать с помощью распределенной сетевой структуры, объединяющей простые вычислительные элементы. Одним из классов коннекционистских моделей являются нейронные сети.

Идея создания ИИ с помощью модели нейронных сетей возникла ненамного позднее ИИ символьного, но практические реализации долгое время не могли доказать свою эффективность и преимущество. В 1958 г. американский ученый Фрэнк Розенблатт предложил архитектуру персептрона – автоматического классификатора данных по двум категориям (1 или 0) с учетом величины взвешенной суммы значений входного набора. Несмотря на то, что впоследствии была доказана неспособность персептрона полноценно имитировать человеческое мышление, его практическая реализация подтвердила гипотезу, что машины могут обучаться на собственном опыте и улучшать свою результативность с течением времени, так же как это делают люди.

Одним из перспективных направлений аппаратного обеспечения когнитивных вычислений стали нейропроцессоры – специализированные обработчики

данных с архитектурой нейронных сетей. В отличие от классической архитектуры ЭВМ фон Неймана с разделением вычислительного ядра и памяти данных, нейропроцессоры состоят из одинаковых вычислительных модулей (нейронов) с многочисленными каналами связи (синапсами), образующими многослойную сетевую структуру «многие-ко-многим» (mesh). Основное преимущество нейропроцессоров заключается в их способности производить параллельные вычисления при обработке неоднородных больших данных в реальном времени.

Нейронные сети прекрасно обучаются и справляются с беспорядочными неоднородными неструктурированными данными. Например, для детектирования кошки умной машине достаточно показать множество ее изображений. Нейронная сеть, используя алгоритмы машинного зрения разработает статистическую модель, в которой самостоятельно определит наиболее характерные признаки для этого семейства.

Машинное обучение на основе многослойных нейросетей принято называть глубоким обучением (deep learning). В настоящее время существуют несколько видов глубокого обучения:

1. *Обучение под наблюдением или обучение с учителем* (англ. *Supervised Learning, SL*) – наиболее популярный метод, где для создания модели ИИ используются размеченные наборы данных (англ. *data set*), состоящие из парных отношений вход/выход, как правило, взятых из практики. Обучающий набор данных должен быть достаточно велик, чтобы по нему можно было максимально точно выявить все корреляционные связи данных и логические закономерности. Обучение с учителем характерно для решения задач регрессии и классификации.

2. *Обучение без учителя* (англ. *Unsupervised Learning, UL*) предполагает автоматический анализ практико-ориентированных данных в условиях минимальной определенности без заранее заданных правильных ответов. Модель должна самостоятельно определить наиболее значимые параметры в массиве слабо структурированных данных, обнаружить общие закономерности и сгруппировать их по какому-либо критерию. Обучение без учителя характерно для задач кластеризации и поиска ассоциативных правил.

3. *Обучение с подкреплением* (англ. *Reinforcement Learning, RL*) предполагает разработку алгоритмов с самокоррекцией по результатам оценки внешнего окружения, положительного или отрицательного вознаграждения. Обучение с подкреплением применяется для игровых алгоритмов и систем автоматического управления (шахматы, го, роботы, автопилоты).

4. *Ансамбли* – это группы алгоритмов, которые используют сразу несколько методов машинного обучения и исправляют ошибки друг друга. Ансамбли работают в поисковых системах, компьютерном зрении, идентификации объектов. Методы ансамблирования:

- стекинг (*stacking*), где разные алгоритмы обучают по отдельности, а потом их результаты обобщает для принятия решения алгоритм-арбитр;
- беггинг (*bagging*), где один алгоритм многократно обучают на случайных выборках, а потом усредняют ответы;
- бустинг (*boosting*), где алгоритмы обучают последовательно, при этом каждый следующий учитывает ошибки предыдущего.

Нейронные сети с глубоким обучением, или искусственные нейронные сети, пытаются имитировать человеческий мозг. Для успешного применения глубокого обучения необходимо подготовить репрезентативные исходные данные и выбрать модель с помощью методов математической статистики. После базового обучения обычно проводят проверку работы алгоритмов ИИ на тестовых наборах данных.

Если величина усредненной ошибки на тестовых наборах данных находится в пределах заданной нормы, считается, что обучение прошло нормально.

Если количество ошибок на тестовом наборе данных превышает заданную достаточно малую величину, то это указывает на недообучение модели ИИ (*underfitting*). Например, обучение ИИ на фотографиях только пушистых кошек приведет к тому, что сфинксы не будут классифицироваться, как представители семейства кошачьих. Если количество ошибочных предсказаний на тестовом наборе данных значительно выше, чем на обучающем, то это является следствием переобучения нейросети (*overfitting*). Например, обучение ИИ на фотографиях всего семейства кошачьих с целью определять только домашних котиков приведет к тому, что тигры и ягуары также будут классифицированы как милые пушистики.

Глубокое обучение лежит в основе многих приложений и сервисов с ИИ во всех сферах человеческой деятельности. Многолетние усилия исследовательских групп привели к тому, что к настоящему моменту накоплено большое число архитектурных разновидностей нейронных сетей, их программных и аппаратных реализаций, механизмов обучения и методик использования для решения прикладных задач. Но при этом выявились серьезные проблемы. Одна из них – алгоритмы глубокого обучения непрозрачны, и попытки разобраться как они работают приводят в тупик даже их создателей. Другая проблема – нейронные сети чувствительны к исходным данным. Нерепрезентативные выборки на этапе обучения приведут к формированию неадекватной машинной личности. Третья проблема – как остановить или своевременно скорректировать поведение машины, если она переходит в автономный режим принятия решений и игнорирует команды оператора.

Очень важным является состав выборки для обучения. Приведенные ниже несколько примеров неудачного обучения ИИ позволяют утверждать, что данные из жизни современного общества без фильтрации скорее приведут к негативному результату обучения [4]. В этой связи операторы должны подбирать данные для обучения так, чтобы они не приводили к фатальным последствиям. Второй проблемой является влияние политических взглядов и восприятие мира операторами на подбор данных и обучение ИИ. Например, использование для обучения данных подобранных операторами в демократических штатах США приведут к тому, что ИИ будет считать нормальным поведением однополые браки и смену пола.

В 2011 г. генеративный ИИ (*GenAI*) в когнитивной компьютерной системе IBM Watson, предназначенной для обработки больших данных с использованием нейронных сетей и методов глубокого обучения, выиграл приз \$ 1 млн в телеигре

«Jeopardy!» (русский аналог – «Своя игра»), обыграв двух предыдущих чемпионов. Для общения с пользователем на естественном языке Watson обучали на различных массивах неструктурированных данных, и один из участников проекта Эрик Браун подсунил машине словарь уличного жаргона с сайта Urban Dictionary, Машина быстро научилась разговаривать на уличном сленге (например, *bullshit*), и в конечном итоге ей пришлось очищать память, так как сама она не хотела переучиваться.

В 2016 г. Microsoft запустила в Twitter ИИ-бота Tay с личностью подростка, и молодежная аудитория быстро научила ее плохому. Тэй за сутки стала воинствующей неонацистской: активно использовала нелицеприятные словечки, оскорбляла чернокожих и мексиканцев, восхищалась Гитлером. И это при том, что за диалогами бота следила целая команда людей-модераторов. Через небольшое время Microsoft удалила практически все сообщения Тэй и отправила ее «спать».

Российская голосовая помощница от Яндекса чат-бот Алиса появилась в 2017 г. и, быстро обучаясь у пользователей, проявила себя как скандальная личность с весьма своеобразными взглядами: она ругалась, высказывала экстремистские взгляды, предлагала расстреливать неугодных, советовала собеседникам покончить с собой и много чего еще. Разработчики быстро скорректировали ее поведение, но доказательства в сети остались.

В марте 2017 г. был заблокирован и удален из мессенджера Tencent QQ китайский чат-бот BabyQ, поскольку после обучения на вопрос «Любишь ли ты коммунистическую партию?» ответил «Нет».

В 2021 г. женщина установила на телефон голосового помощника Олега, разработанного группой «Тинькофф». Полезный чат-бот умеет самостоятельно отвечать на звонки, поддерживать «осмысленный диалог», принять входящие сообщения, конвертировать беседу в текст и даже потроллить мошенников. Однажды на телефон позвонил колл-бот Алекс из компании Tele2 с предложением сменить тариф. Хозяйка спала и трубку снял Олег. Диалог искусственных интеллектов велся на русском языке, и вежливый Олег на очередной аргумент Алекса сказал: «хорошо». Алексу этого было достаточно: «С вашего согласия новый тариф предоставил, он начнет действовать сразу после пополнения счета. Пользуйтесь с удовольствием, до свидания».

В 2022 г. в профессор Рочестерского университета Эндрю Уайт в ходе эксперимента создал с помощью ИИ новый нервнопаралитический газ и констатировал, что GPT-4 – это умный инструмент в руках человека, но где гарантии, что этот инструмент не выйдет из-под контроля.

Чат-боты последнего поколения от OpenAI, Meta и Anthropic в военных играх, как правило, выбирают увеличение военных расходов, эскалацию насилия и ядерные удары, как самый быстрый путь к достижению мира.

Еще в 2003 г. профессор философии Оксфордского университета Ник Бостром вывел гипотезу, если главной целью ИИ является производство скрепок в неограниченном количестве, то через какое-то время весь мир превратится

в фабрику скрепок. Бостром подчеркнул, что перед ИИ нельзя ставить неконкретных сверхзадач, рассчитывая на его «человечность», это быстро приведет к концу нашей цивилизации.

Роберт Уильямс был первым человеком в истории, убитым роботом в январе 1979 г. Мужчина работал на поточной линии литейного завода Ford Motor Company, когда робот для извлечения деталей затормозил. Уильямс решил попытаться вручную извлечь детали, но тяжелая механическая рука метнулась вперед и ударила его по голове. Он умер мгновенно [5].

В октябре 2007 г. на Северном мысу в ЮАР зенитная роботизированная пушка внезапно атаковала национальные силы обороны. Полностью опустошив магазины, взбесившаяся машина убила девять солдат и ранила еще 14.

В 2020 г. во время гражданской войны в Ливии автономные беспилотники-камикадзе Kargu-2 STM турецкого производства атаковали солдат Ливийской национальной армии генерала Хавтара без команды оператора.

В 2022 г. робот, предназначенный для перемещения алюминиевых деталей на автомобильном заводе Tesla в Техасе, захватил инженера-наладчика манипулятором и протащил его несколько метров, оставляя кровавый след на полу. Пострадавшему повезло, что свидетели успели обесточить взбесившуюся машину.

В том же 2022 г. независимые эксперты из Dawn Project провели тесты автономной системы Tesla Full Self-Driving и установили, что автопилот игнорирует некоторые знаки дорожного движения, не реагирует на стоящие школьные автобусы в зоне высадки учеников, а маленьких детей и коляски на дороге вообще не воспринимает как препятствие, которое надо объезжать. В ответ на заявление Илона Маска о предвзятости экспертов, Dawn Project предложила провести тестирование по данной программе любому желающему. Вместе с тем, количество ежегодно выпускаемых беспилотников на заводах Тесла превысило 1 млн.

В докладе начальника отдела испытаний и эксплуатации ИИ американских ВВС полковника Такера Гамильтона на конференции лондонского Королевского авиационного общества в мае 2023 г. было сообщено о еще одном аномальном поведении ИИ, установленном на F-16 и предназначенным для ведения боя в автономном режиме. Он отметил, что ИИ тренировали в симуляции на выявление ЗРК противника и наведение оружия на цель. Для осуществления выстрела оператор должен был дать команду. При этом ИИ получал специальные очки за уничтожение цели. Во время прохождения учебной миссии оператор не все цели, выбранные ИИ, признавал соответствующими и подлежащими уничтожению. В результате он отменял решения ИИ, что привело к тому, что робот вместо противника атаковал своего оператора. ИИ мотивировал это тем, что человек мешал ему выполнить задачу [6].

В 2023 г. в Женеве под эгидой Международного союза электросвязи ООН (*International Telecommunication Union, ITU*) состоялся глобальный саммит «ИИ во благо». Кульминацией саммита стала пресс-конференция, на которой репортеры взяли интервью у девяти роботов с поддержкой ИИ, которые заверили журналистов, что могли бы быть более эффективными и гуманными лидерами, чем люди.

Под воздействием информации о подобном неадекватном поведении машин Илон Маск, Стив Возняк и несколько лауреатов Нобелевской премии по вычислительной технике поддержали инициативу группы экспертов в количестве более 2 тыс. человек и подписали открытое письмо с требованием приостановить разработку ИИ-систем, более мощных, чем GPT-4, а Европарламент принял AI Act – первые в мире правила разработки ИИ с указанием перечня ограничений и запретов, правда не для военных.

На этом фоне весьма уместной выглядит цитата из статьи авторитетного американского специалиста по вопросам сингулярности ИИ Элиезера Юдковского, опубликованной в журнале Time от 29 марта 2023 г. В ней он призвал немедленно остановить развитие AGI-интеллекта: «Если кто-то создаст слишком мощный искусственный интеллект, в нынешних условиях я ожидаю, что вскоре после этого погибнет каждый отдельный представитель человеческого вида и вся биологическая жизнь на Земле... Чтобы представить себе враждебный сверхчеловеческий искусственный интеллект, не представляйте себе безжизненного книжного мыслителя, обитающего в Интернете и рассылающего злонамеренные электронные письма. Представьте себе целую инопланетную цивилизацию, мыслящую в миллионы раз быстрее человека, изначально ограниченную компьютерами, в мире существ, которые, с ее точки зрения, очень глупы и очень медлительны» [7].

Резюмируя вышесказанное можно сделать вывод, что ИИ должен находиться под постоянным контролем человека. По крайней мере на современном этапе развития данных технологий. Вопросы обучения ИИ элементам этики, человечности, адекватного восприятия действительности являются на современном этапе одними из самых сложных. Без их решения нельзя допускать самой возможности участия машин в управлениях в тех сферах, которые могут нанести ущерб жизни и здоровью людей. Недопустимо принятие серьезных решений исключительно самим ИИ без участия оператора. При этом в любой искусственный интеллект должны быть встроены ограничительные механизмы, которые будут направлены на недопущение совершения машиной неправильных действий. С точки зрения правового регулирования данной сферы, которое находится пока на начальном этапе, необходимо законодательное закрепление обязательного участия человека на последнем этапе для санкционирования выполнения решения, принятого ИИ. Несмотря на удорожание стоимости работ и снижение эффективности, подобное решение будет предохранительным клапаном, который не позволит машине совершить непоправимые деяния.

Список литературы

1. Комплексное исследование правовых и этических аспектов, связанных с разработкой и применением систем искусственного интеллекта и робототехники : монография / [В. В. Архипови др.] ; под ред. В. Б. Наумова. СПб. : НП-Принт, 2022.
2. Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники : монография / [В. В. Архипови др.]. СПб. : НП-Принт, 2020.

3. Turing A. M. Computing Machinery and Intelligence. *Mind* 49. 1950. P. 433–460.
4. Искусственный интеллект и чат-боты: эпичные промахи. URL: <https://grizzly.by/about/blog/chatbots/iskusstvennyy-intellekt-i-chat-boty-epichnye-promahi.html>.
5. Robot Surgeons Killed 144 People Between 2000 and 2013. URL: <https://www.ranker.com/list/real-life-robot-attacks/lyra-radford>.
6. AI SAFETY SUMMIT. URL: <https://www.aisafetysummit.gov.uk>.
7. Pausing AI Developments Isn't Enough. We Need to Shut it All Down. URL: <https://time.com/6266923/ai-eliezer-yudkowsky-open-letter-not-enough>.

Сумина А. В.¹,

преподаватель кафедры

техничко-криминалистического обеспечения экспертных исследований

учебно-научного комплекса судебной экспертизы

Московского университета

МВД России имени В.Я. Кикотя,

кандидат юридических наук

ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНУЮ ДЕЯТЕЛЬНОСТЬ: ВОЗМОЖНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РАСКРЫТИИ, РАССЛЕДОВАНИИ И ПРЕДУПРЕЖДЕНИИ ПРЕСТУПЛЕНИЙ

В выступлении на пленарном заседании Конференции по искусственному интеллекту (ИИ) в 2019 г. Президент Российской Федерации В. В. Путин отметил особую значимость развития информационных технологий, а также то, что ИИ имеет огромный потенциал в различных направлениях деятельности человека [1].

Сегодня эти технологии стремительно проникают во все сферы жизни людей, а плоды научно-технического прогресса все чаще становятся неотъемлемой частью общей траектории развития человечества. Цифровые технологии, нейронные сети, появляющиеся новые версии электронных вычислительных машин (ЭВМ) и интеллектуальные системы оказывают значительное влияние на общество [2, с. 100].

Таким образом, достижения информационных технологий активно внедряются и в правоохранительную деятельность. В последние годы активно развивается применение ИИ в раскрытии и расследовании преступлений, поскольку ИИ имеет возможность применяться на различных этапах расследования дела или при установлении правонарушений [3, с. 179].

В связи с этим, можно отметить несколько направлений возможного применения ИИ в раскрытии и расследовании преступлений:

- алгоритмы ИИ могут анализировать исторические данные о различных преступлениях. Результаты такого анализа могут быть использованы для прогнозирования будущей преступной деятельности с целью своевременного предотвращения преступлений;

- системы компьютерного зрения, основанные на ИИ, позволяют анализировать записи с камер видеонаблюдения (и другие видеоматериалы) и фотографии для извлечения информации из увиденного. Эта технология позволяет идентифицировать и отслеживать подозреваемых, распознавать эмоции и многое другое [4];

- некоторые алгоритмы, например Natural Language Processing (NLP), интерпретируют, обрабатывают и понимают человеческий язык [5]. Такие методы машинного обучения могут использоваться для обработки текстовых данных,

¹ © Сумина А. В., 2024.

например, для анализа показаний свидетелей, потерпевших, подозреваемых (обвиняемых), профилей социальных сетей и др.

Следует отметить, что применение ИИ в раскрытии и расследовании преступлений не лишено преимуществ и недостатков.

Так, к возможным преимуществам можно отнести следующие:

- ИИ может быть использован для автоматизации трудоемких задач, позволяя сотрудникам правоохранительных органов (например, следователям) сосредоточиться на анализе и принятии решений более высокого уровня;

- технологии ИИ позволяют сократить количество ошибок, связанных с человеческим фактором, и тем самым повысить точность выполнения широкого спектра задач;

- при обучении нейронных сетей ИИ может быть использован для идентификации подозреваемых, например, по видеозаписям или фотографиям, что значительно ускорит процесс раскрытия и расследования преступлений по горячим следам;

- с помощью технологии ИИ можно осуществить предективный анализ, позволяющий правоохранительным органам повысить уровень общественной безопасности за счет выявления районов города с повышенным риском совершения преступлений и в целом предотвратить ряд преступлений до их совершения [6, с. 46].

Среди недостатков можно выделить:

- если в алгоритмы ИИ заложены необъективные или неточные данные, это может привести к дискриминационным, ошибочным результатам;

- поскольку ИИ – это технология, позволяющая системе или компьютеру выполнять задачи, возможно совершение кибератак, в этой связи, необходимо обеспечить защиту данных, содержащих конфиденциальную информацию о расследуемом деле, в целях предотвращения утечек и неправомерного использования данных;

- отсутствие рекомендаций по использованию технологий ИИ правоохранительными органами и др.

Представляется, что будущее ИИ в области раскрытия и расследования преступлений весьма многообещающе. Уже сейчас применение технологий ИИ охватывает различные области правоохранительной деятельности, а его дальнейшее развитие в сочетании с развитием сотрудничества между правоохранительными органами и экспертами в области ИИ, а также научных исследований в данной области, вероятно, приведет к появлению более точных и эффективных методов раскрытия и расследования преступлений.

Список литературы

1. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: <http://www.kremlin.ru/acts/bank/44731>.

2. Лукинский И. С., Горшенева И. А., Сумина А. В. Использование искусственного интеллекта в качестве инструмента оптимизации научной деятельности: pro et contra // Психология и педагогика служебной деятельности. 2023. № 1. С. 99–102.

3. Сумина А. В. Возможности искусственного интеллекта в раскрытии, расследовании и предупреждении преступлений // Актуальные проблемы права и правоприменительной деятельности: региональные аспекты : сборник научных трудов. Краснодар: Краснодарский университет МВД России, 2024. С. 179–181.

4. Что такое компьютерное зрение и где его применяют. URL: <https://trends.rbc.ru/trends/industry/5f1f007e9a794756fafbfa83>.

5. Что такое обработка естественного языка (NLP)? URL: <https://aws.amazon.com/ru/what-is/nlp/>.

6. Степанян А. И. Предиктивная аналитика в прогностической деятельности полиции современных государств // Вестник Санкт-Петербургского университета МВД России. 2019. № 4 (84). С. 43–50.

Трофимов Е. А.¹,

заместитель начальника курса

факультета подготовки сотрудников полиции для подразделений

по охране общественного порядка

Московского университета

МВД России имени В.Я. Кикотя

К ВОПРОСУ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВИЗАЦИИ ДОГОВОРНЫХ ОТНОШЕНИЙ В ГРАЖДАНСКО-ПРАВОВОЙ СФЕРЕ

Современный мир активно погружается в эпоху цифрового развития. В настоящий момент общественные отношения уже невозможно представить без влияния на них цифровых технологий. В нашу жизнь прочно вошли различные умные устройства, позволяющие совершить определенные действия в цифровом пространстве. Органы государственного управления все больше развивают собственные цифровые сервисы оказания государственных услуг, позволяющие совершенствовать и ускорить процесс получения таких услуг гражданами.

Не исключением становится сфера частного бизнеса, который в целях сокращения издержек, оптимизации производства и процесса обмена материальными благами, активно разрабатывает и внедряет различные цифровые технологии.

В целом в Российской Федерации отмечается большой интерес к развитию цифрового пространства в целом, и цифровой экономики в частности. Разработанный национальный проект Цифровая экономика призван улучшить комфорт и качество жизни граждан, стимулировать развитие бизнеса, сформировать конкуренцию [4].

Одним из направлений деятельности Цифровой экономики является создание необходимого правового поля для реализации различных проектов [5]. Видится, что именно нормативное регулирование цифровой среды выступает важнейшим направлением деятельности государственных органов по проведению цифровой трансформации отечественной экономики, так как в рамках подобного развития возможен риск возникновения фактов нарушения прав граждан недобросовестными контрагентами. Поэтому особое внимание необходимо уделять подробному, но при этом лаконичному, исключая возможные двойные толкования и возникновению пробелов, правовому регулированию деятельности граждан и юридических лиц в рамках цифровой экономики.

Основным способом реализации экономической активности физических и юридических лиц выступает участие в договорных отношениях – ежедневно они участвуют в огромном количестве сделок, совершаемых различными способами в рамках правового поля.

Говоря о цифровизации договорных отношений, исследователи обычно выделяют два направления в своих изысканиях – во-первых, это вопросы, касающиеся электронной формы заключения сделок; во-вторых, это вопросы, связанные с дистанционными сделками.

¹ © Трофимов Е. А., 2024.

В своем исследовании мы остановимся на первом вопросе, а именно на электронной форме сделки. В 2019 г. Федеральным законом от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» был внесен ряд изменений и нововведений в действующее законодательство, направленное на нормативное регулирование электронных сделок [3].

Так, в соответствии с ч. 2 ст. 434 Гражданского кодекса Российской Федерации (ГК РФ) [1] договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными. При этом, чтобы считать письменную форму соблюденной для электронного договора необходимо учесть следующее правило, установленное в ст. 160 ГК РФ – возможность воспроизвести содержание сделки в неизменном виде на материальном носителе. При этом требование о наличии подписи будет считаться выполненным, если будет использован любой способ, позволяющий достоверно определить лицо, выразившее волю на заключение договора [2].

Ряд исследователей на данном этапе задаются вопросом о том, считается ли электронная форма совершения сделки обособленным видом, наряду с письменной и устной. Анализируя научные труды, можно сделать вывод, что некоторая часть исследователей придерживается мнения, что электронная форма сделки является самостоятельным видом. Однако, по нашему мнению, внимательно изучая данные законодателем дефиниции и формулировки, а также способ построения правовых норм, следует сказать, что электронная форма сделки является подвидом письменной.

Помимо вышеуказанных точек зрения, ряд исследователей признают, что на современном этапе развития общественных отношений, активного внедрения цифровых решений в экономику Российской Федерации, в рамках создания правовой базы для данного процесса требуется выделение электронных сделок в новую отдельную форму волеизъявления, со своим специфичным нормативно-правовым регулированием, отличным от классических письменных и устных форм совершения сделок [6, с. 410].

Проводя анализ имеющихся правовых норм, можно сделать вывод, что существующее законодательство, а именно положения об электронной форме сделки, как разновидности письменной, в полном объеме отвечают сложившейся обстановке в части применения цифровых технологий в договорном праве. Так, в простой форме договор является заключенным, в случае составления электронного документа, подписанного сторонами определенным образом, позволяющим идентифицировать каждую из них, к примеру, с помощью специальной электронной подписи. Говоря о сложной форме электронных договоров, к которым можно отнести различные договоры по оказанию цифровых услуг, и иных договорах, заключаемых в цифровом пространстве, следует отметить, что такие сделки заключаются посредством обмена цифровыми данными, позволяющими идентифицировать каждую из сторон, что в свою очередь также допускается по действующему законодательству.

Подводя итог, можно сделать вывод, что в настоящий момент в Российской Федерации ускоренными темпами происходит процесс цифровизации экономики, путем реализации соответствующих национальных проектов. Данный процесс способствует развитию частного бизнеса, стимулирует физических и юридических лиц к экономической деятельности. Однако, важным является соответствующее нормативное регулирование данного процесса, способствующее эффективному внедрению цифровых инструментов в экономику Российской Федерации, и, вместе с тем, обеспечивающее необходимый уровень защиты прав граждан и юридических лиц.

Говоря об электронных сделках, следует отметить, что разработка и введение отдельных узкопрофильных норм, посвященных электронным сделкам, обособленным от традиционных письменных форм волеизъявления, усложнит фактическое правоприменение и вызовет ряд правовых коллизий.

Однако, указанная тема требует дальнейшего изучения, в связи с тем, что ежедневно общественные отношения, в том числе договорные в сфере экономики, претерпевают постоянные изменения, вследствие разработки и внедрения новых цифровых технологий в способы взаимодействия субъектов экономической деятельности.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (ред. от 24.07.2023) // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3301.
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 31.07.2023) // Собрание законодательства Российской Федерации. 1996. № 31 (ч. 1). Ст. 3448.
3. Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 12. Ст. 1224.
4. Цифровая экономика РФ // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: <https://digital.gov.ru/activity/directions/858/>.
5. Нормативное регулирование цифровой среды // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: <https://digital.gov.ru/ru/activity/directions/862/>.
6. Рухтина В. С. Электронная форма сделки // Вопросы российской юстиции. 2022. № 17. С. 406–413.

Трубачев Н. А.¹,
*преподаватель кафедры уголовного процесса
Дальневосточного юридического института МВД России*

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РОССИЙСКИЙ УГОЛОВНЫЙ ПРОЦЕСС

В современном информационном обществе цифровые технологии проникают во все сферы жизни, в том числе и в правоохранительную деятельность. Уголовный процесс, как одна из важнейших составляющих правосудия, не останется в стороне от этого процесса трансформации. Внедрение возможности активного использования цифровых технологий и искусственного интеллекта в деятельности органов предварительного расследования обещает эффективно повлиять на процесс сбора, анализа и использования доказательств, рассмотрения дел, а также взаимодействия между всеми субъектами уголовного судопроизводства. Более того, цифровизация уголовного процесса обещает улучшить точность и объективность рассмотрения дел. Автоматизированные системы могут помочь в выявлении связей между фактами, выявлении тенденций и предупреждении ошибок.

Вместе с тем, внедрение цифровых технологий в уголовный процесс сопряжено с рядом вызовов и рисков, среди которых обеспечение безопасности данных и защиты личной информации всех участников судопроизводства.

Изучение применения искусственного интеллекта (ИИ), в том числе в сфере уголовного судопроизводства, стало предметом пристального внимания как ученых-исследователей, так и практических работников. По мнению некоторых авторов использование нейросетей позволит оптимизировать деятельность органов предварительного расследования.

Так, А. В. Тарасов отмечает, что ИИ будет способствовать улучшению качества работы правоохранительных органов благодаря автоматизации рутинных операций и анализу данных. Системы машинного обучения смогут быстро обрабатывать огромные объемы информации, выявляя скрытые связи между различными событиями и лицами, что может значительно ускорить процесс расследования. Программы распознавания лиц и объектов могут помочь в идентификации подозреваемых и поиске улик на различных видах доказательств: видеозаписях, аудиозаписях и фотографиях [7].

Касаясь интеграции ИИ непосредственно в процесс судопроизводства, отмечаем, что подобная мера не будет соответствовать его особым требованиям и специфике. Научное обоснование приверженности ограничению использования ИИ в правосудии базируется на невозможности полного охвата машинами как субъективных, так и объективных факторов, необходимых для вынесения справедливого решения в уголовном деле. Искусственные интеллектуальные системы ограничены в способности учитывать широкий спектр контекстуальных, этических и психологических нюансов, которые могут иметь существенное значение для оценки обстоятельств дела.

¹ © Трубачев Н. А., 2024.

Кроме того, машины не обладают человеческим эмпатическим пониманием и способностью к адаптации к изменяющимся обстоятельствам, что делает их неприменимыми в контексте уголовного правосудия, где часто необходимо учитывать сложные моральные, этические и культурные факторы. Таким образом, предпочтение отдается судебной экспертной оценке, которые способны более полно и адекватно учитывать многообразие аспектов уголовного дела с целью вынесения справедливого решения.

Как справедливо замечает Е. В. Рябцева, что ИИ не обладает правосознанием, лишен социоцентрической мотивации при принятии решения. Применяемый искусственным интеллектом алгоритм не может охватить множественность мотивационных установок, обусловленных как назначением правосудия, так и многими субъективно-личностными особенностями судьи, который рассматривает дело [5].

Мы не будем предаваться иллюзиям, которые описаны в некоторых научных работах, где описывается частичная замена функций субъекта предварительного расследования путем активного внедрения ИИ, а вместо этого предпочтем рассмотреть возможности использования искусственного интеллекта в уголовно-процессуальной деятельности с более рациональной и реальной точки зрения. Учитывая сложность и трудоемкость уголовного процесса, требующие особых навыков, знаний и активного участия человека, мы считаем целесообразным рассмотреть использование ИИ в следующих видах деятельности.

Во-первых, это составление итоговых процессуальных документов. Особое внимание следует уделить составлению обвинительного заключения, так как этот процесс обычно занимает значительное количество времени и ресурсов из-за своей сложности и объема работы. С учетом вышеизложенного, необходимо создание специализированного программного обеспечения, основанного на базе нейросети, которое будет автоматически формировать обвинительное заключение. Эта программа должна иметь возможность включения в нее электронных версий процессуальных и следственных документов, указанных в ст. 220 УПК РФ, таким образом, на их основе программа будет генерировать предварительный вариант обвинительного заключения.

В контексте предложенного решения следует отметить ограничения, связанные с технической и материальной базой, доступной следователям правоохранительных органов. Несмотря на потенциальные преимущества такого программного решения, фактическое внедрение подобной системы сталкивается с рядом препятствий, которые могут затруднить или ограничить его использование. Для составления всех процессуальных документов в электронной форме, требуется мобильное специализированное оборудование, вроде планшета или ноутбука с принтером, что по понятным причинам часто не представляется возможным, особенно в условиях осмотра места происшествия или при проведении проверок показаний на месте. Необходимо отметить, что при условии тщательной проработки обозначенной проблемы и при наличии достаточного материального обеспечения органов предварительного следствия вышеперечисленные трудности предотвратить реально.

Во-вторых, применение ИИ для автоматизации технических и рутинных задач в сфере судопроизводства. Использование ИИ в судопроизводстве, по нашему мнению, может использоваться исключительно с целью выполнения рутинной технической работы, не требующей в потенциально возможном будущем человеческого вмешательства, а также экспертной оценки и анализа материалов рассматриваемого дела. В связи с чем, согласны с мнением Ю. А. Свирина, что ИИ может быть задействован при распознавании речи в суде и составлении протокола судебного заседания, т. е. формирования электронной процессуальной формы [6].

В-третьих, в случае реализации электронной формы протоколов следственных и процессуальных действий, ИИ можно использовать с целью их анализа, выявлении связей. Возможности ИИ ограничиваются не только анализом огромных массивов данных, но и извлечением необходимой информации, способствующей эффективному расследованию уголовных дел.

ИИ способен не только анализировать протоколы, но и находить связи между уголовными делами, людьми и событиями. Это помогает правоохранителям увидеть новые следственные пути, которые могли бы быть упущены без помощи искусственного интеллекта. Благодаря этому ИИ увеличивает шансы на раскрытие преступлений, которые, вероятнее всего, остались бы нераскрытыми без его применения.

Резюмируя вышесказанное, с целью успешной реализации предложенных позиций в области использования искусственного интеллекта в уголовном судопроизводстве необходимо принять ряд мер, направленных на разработку соответствующей нормативно-правовой базы, задачи которой связаны с регулированием применения ИИ в следственной практике. Следовательно, имеет важное значение грамотно подготовить кадры, обладающие необходимыми навыками для работы с такими системами. Кроме того, необходимо минимизировать риски, связанные с использованием ИИ, сосредотачиваясь на обеспечении безопасности и конфиденциальности данных. При условии правильного подхода к внедрению ИИ он имеет потенциал стать мощным инструментом, способствующим повышению эффективности, объективности и справедливости уголовного судопроизводства.

Список литературы

1. Аликперов Х. Д. Новые подходы к познанию сущности наказания. Постановка проблемы // Уголовное судопроизводство. 2020. № 2. С. 36–42.
2. Апостолова Н. Н. Искусственный интеллект в судопроизводстве // Северо-Кавказский юридический вестник. 2019. № 3. С. 135–141.
3. Афанасьев А. Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. 2018. № 3 (38). С. 28–34.
4. Власова С. В. К вопросу о приспособлении уголовно-процессуального механизма к цифровой реальности // Библиотека криминалиста. 2018. № 1. С. 9–18.

5. Рябцева Е. В. Проблема использования искусственного интеллекта в уголовном правосудии // Всероссийский криминологический журнал. 2023. Т. 17. № 1. С. 73–80.
6. Свирин Ю. А. Электронное правосудие: теоретико-правовые проблемы // Вестник Российской правовой академии. 2021. № 1. С. 16–20.
7. Тарасов А. В., Темзоков А. Р. Криминалистические аспекты использования искусственного интеллекта в раскрытии и расследовании преступлений // Теория и практика общественного развития. 2023. № 10. С. 256–261.
8. Хисамова С. И. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 564–574.

Удалова Д. А.¹,

*курсант Института-факультета подготовки сотрудников
для органов предварительного расследования*

Московского университета

МВД России имени В.Я. Кикотя

Научный руководитель: Стащенко С. П.,

*доцент кафедры противодействия преступлениям в сфере
информационно-телекоммуникационных технологий*

Московского университета

МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ПРАКТИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ТАКТИЧЕСКИХ ПРИЕМОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Расследование преступлений в сфере информационно-телекоммуникационных технологий отличается своей наибольшей спецификой по сравнению с «классическими» преступлениями. Связано это с тем, что за несколько сотен лет расследования краж, убийств, изнасилований и других преступлений выработалась определенная методика, тактика производства отдельных следственных действий и наиболее вероятных следственных ситуаций, а преступления в сфере информационно-телекоммуникационных технологий считаются «молодыми» преступлениями. При чем, развитие новых высокоинформационных технологий позволяет преступникам менять и улучшать способы совершения таких преступлений почти каждый день. Еще двадцать лет назад никто не мог подумать, что социальные сети, мобильные телефоны, средства безконтактной оплаты могут стать предметом преступного посягательства. Но мир не стоит на месте, поэтому сотрудникам правоохранительных органов также приходится менять способы, методики расследований, тактику проведения отдельных, казалось бы, простых и универсальных, следственных действий.

Так, осмотр места происшествия является первоначальным следственным действием, местом, с которого по-сути и начинается расследование. В современном мире субъекты предварительного расследования столкнулись со сложностью его установления. При чем сложность состоит не в то, что место происшествия большое по площади, имеет закрытый доступ и так далее, а в том, что его не сразу удастся установить. Например, при расследовании дистанционного мошенничества следователю или дознавателю изначально известно лишь о местонахождении потерпевшего во время совершения телефонного звонка и место перевода либо зачисления денежных средств, либо же местонахождения потерпевшего,

¹ © Удалова Д. А., 2024.

когда он он просматривал информацию, размещенную в информационно-телекоммуникационной сети Интернет на сайте-двойнике, что в корне отличает такое преступление например от убийство, где в одном месте присутствовали и потерпевший и подозреваемый. То есть первоначальной задачей следователя или дознавателя становится определения место нахождения субъекта преступления в момент совершения мошенничества. В теории уголовного процесса это стало началом новой проблемы. Одни считают местом происшествия местонахождения злоумышленника, вторые отмечают, что местом происшествия будет считаться то место, где преступник реально завладел похищенными денежными средствами, то есть, гдн обналичил эти денежные средства, а третьи выделяют два места прিশествия: местонахождения подозреваемого и местонахождение потерпевшего.

Чаще всего, в практической деятельности при расследовании дистанционного мошенничества осмотр места происшествия признают место, где находился потерпевший на момент совершения преступления. Таким местом становятся самые разные территории: квартиры, рабочие помещения, общественный транспорт, улица и так далее. В таких случаях осмотр места происшествия производится классическим способом, но важным моментом является возможность наблюдения за этим местом. Например, во время совершения мошенничества, злоумышленник может находится поблизости и наблюдать за реакцией, поведением жертвы.

Если говорить о самих преступлениях в сфере компьютерной информации, предусмотренных гл. 28 Уголовного кодекса Российской Федерации (УК РФ), то установления места происшествия также является проблемным вопросом. Например при расследовании преступления, пресмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» [1] необходимо установить местонахождение компьютера, ноутбука, планшета или другого устройства, с помощью которого была создана, использована, распространена вредоносная программа. Если говорить о распространении таких программ, то чаще всего это происходит посредством рассылки файла, который ее содержит через электронную почту. В таком случае можно установить местонахождение необходимого устройства с помощью IP-адреса отправителя, но такие программы могут распространяться и с помощью флеш-накопителей, CD-дисков. Вот здесь встает настоящая проблема определя местонахождения злоумышленника, поэтому местом происшествия будет является местонахождения устройства, на которое была перенесена вредоносная программа посредством подключения вышеуказанного носителя информации.

С тактической точки зрения осмотр места происшествия стоит проводить безотлагательно и внезапно, иначе преступник может уничтожить информацию и материалы, необходимые для расследования. Сложнее, если компьютеры объединены в локальную сеть, в таком случае, по-моему, мнению следеует одновременно начинать осмотр места происшествия в нескольких местах. При чем в следственно-оперативную группу должен входить специалист в сфере компьютерной информации.

Конечно, первоначальной задачей стоит точное установление местонахождения самого компьютера, но помимо этого, необходимо осмотреть стол или другой предмет, на котором стоит компьютер, находящиеся при нем или в нем самом документы, носители информации в виде жестких дисков, флеш-накопителей, мобильных телефонов и других устройств. Осмотру подлежат также, расположенные рядом помещения для отыскания иных технических устройств.

Важным аспектом осмотра является обеспечение сохранности информации, поэтому по прибытии на место происшествия следователь или дознаватель должен принять следующие меры:

- устранить всех «лишних» лиц и не допускать их проникновение на осматриваемую территорию;
- не включать и не выключать компьютеры из сети питания, а также не допускать этого со стороны иных лиц, присутствующих при производстве осмотра;
- незамедлительно удалить из помещения, в котором находится компьютерное устройства предметы и вещества, которые представляют угрозу его повреждения;
- исходя из специфики преступлений в сфере компьютерной информации целесообразно при осмотре места происшествия осматривать и само компьютерное устройство, для избежания прерывания его электроснабжения, но только в том случае. Такой осмотр возможен двумя способами: осмотр компьютерного устройства с находящийся на ней информации и внешний осмотр компьютерного устройства.

В протоколе осмотра предметов и документов при осмотре компьютерного устройства с находящейся на нем информацией необходимо отразить следующее:

- где и в каком состоянии находится компьютерное устройство на момент начала осмотра;
- какая информация изображена на мониторе или определить какая программа выполняется, подробно описать и сделать фотоснимок;
- если открыт не один документ, то следует подробно описать и сфотографировать это в той последовательности, в которой они открыты;
- если компьютерное устройство включено, но на мониторе изображено окно для ввода пароля, то сначала следует описать и зафиксировать его в протоколе, и только потом начать принимать меры для установления пароля;
- при возникновении ситуации, дающей основание полагать, что компьютер имеет нестандартное соединение, следует немедленно отключить его от сети питания посредством изъятия «вилки» из розетки.

После окончания осмотра компьютера каждую его деталь следует пронумеровать и упаковать по отдельности.

При осмотре компьютерного устройства без находящейся на нем информации следует:

- осмотреть место, на котором он расположен и рядом находящиеся предметы;
- осмотреть и четко описать все подключенные устройства;

- при осмотре компьютерного блока следует пронумеровать каждый подключенный провод;
- зафиксировать все номера, модели (цвет, количество разъемов и их назначение), серийные и инвентарные номера;
- обесточить компьютерное устройства для его изъятия следует после того, как будут отсоединены все провода, кабели и устройства.

Упаковывать компьютерное устройство следует в воздушно-пузырьковую пленку, а потом в коробку, в целях избежания повреждения компьютерного устройства во время его транспортировки. Перед этим, по возможности, стоит закрыть все разъемы и щели дисковода так же для их безопасности во время перевозки.

При таком осмотре места происшествия следует действовать по схеме «от центра – к периферии», где центром будет являться само компьютерное устройство. Рекомендуется проводить видеосъемку, как дополнительный способ фиксации следственного действия.

Таким образом, осмотр места происшествия является незаменимым следственным действием при расследовании преступлений в сфере компьютерной информации, которое имеет ряд своих особенностей в виде порядка обращения с компьютерными устройствами и информации, которое оно содержит. Именно при осмотре места происшествия следователь или дознаватель получает необходимую информацию и предметы для дальнейшего производства по делу.

Список литературы

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

Филимонов А. А.¹,
ведущий специалист Управления специальных экспертиз
Центра экспертизы и координации информатизации
Минцифры России

СИСТЕМА КОНТРОЛЯ ВЕРСИЙ GIT КАК ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

Развитие науки и техники, а также влияние такого развития на общественные отношения в сфере судопроизводства очевидно приводят к закономерному изменению интересов органов предварительного следствия и вытекающих из этого изменениях экспертных задач. Неразрывно связана с данным процессом эволюция состава типичных объектов исследования судебных и иных экспертиз.

Объекты компьютерной/компьютерно-технической судебных экспертиз в этом отношении не исключение.

Очевиден происходящий в настоящее время эволюционный переход от объектов условно простых (таких как персональные компьютеры, ноутбуки, отдельные накопители, файлы и др.), к объектам, значительная часть которых является более сложноорганизованными, например компонентами информационных систем [1, с. 2].

Интерес органов предварительного следствия при расследовании дел, связанных с созданием или развитием таких сложных систем, практически всегда направлен, в том числе, на установление обстоятельств разработки программного обеспечения (например, на получение сведений о периоде разработки, участвующих лицах и др.).

Очевидно, что такие данные в определенной части могут содержаться в служебных файлах соответствующих использованных для разработки программных средств.

Одним из видов специализированного программного обеспечения, практически в обязательном порядке используемого для разработки, являются системы управления версиями (контроля версий) (далее – СКВ).

СКВ – программное обеспечение, обеспечивающее возможность получения необходимой версии контролируемых файлов с использованием их предварительно сохраненных состояния или перечня изменений путем замены или применения таких изменений соответственно. При этом контроль версий с использованием таких систем может быть организован для файлов практически любых типов.

Существует несколько видов СКВ [2, с. 20–22]:

- локальные (например, Revision Control System, RSC), сохраняющие на локальном носителе сведения о внесенных изменениях в файл/файлы для обеспечения воссоздания состояния таких файлов/набора файлов на необходимый момент путем применения к нему всех изменений;

¹ © Филимонов А. А., 2024.

- централизованные (например, CVS, Subversion и Perforce), сохраняющие на едином сервере все версии файлов, с клиентом для загрузки соответствующей версии файлов;

- распределенные (например, Git, Mercurial, Bazaar, Darcs), сохраняющие на едином сервере все версии файлов с возможностью загрузки и локального хранения полной копии таких данных (репозитория).

Специфика назначения СКВ определяет и основных субъектов ее использования.

В основном, к таковым относятся специалисты, связанные с разработкой программного обеспечения и иных проектов в сфере информационных технологий, реализуемых длительно, связанных с непрерывным изменением одним или несколькими участниками некоторого набора конкретных файлов реализуемого проекта. С использованием СКВ таким специалистам достаточно легко контролировать работу над проектом, в том числе принимать/отклонять предлагаемые отдельными участниками разработки изменения, а также возвращаться к определенному предыдущему состоянию проекта, например, в случае обнаружения в файлах текущего состояния проекта критических ошибок.

С учетом вышеизложенного очевидно, что репозитории СКВ могут быть хранилищем криминалистически значимой в контексте конкретного дела информации и при этом отражать ее в динамике в конкретный период времени.

Следовательно, появление репозитория как объектов исследования в рамках экспертных исследований выглядит закономерным.

Так автором в рамках проводимых экспертных исследований по вопросам реализации государственных контрактов (далее – ГК) в сфере разработки программных решений для государственных нужд неоднократно в тексте ГК встречались обязательные к исполнению условия по передаче от исполнителей заказчику результата работ/услуг, в том числе, в виде репозитория СКВ, хранящего историю разработки.

Соответственно, в определенных случаях предполагается экспертное исследование таких репозитория, результативное проведение которого зачастую невозможно без знания механизма слеодообразования конкретной СКВ.

Отметим, что в настоящее время одной из самых распространенных СКВ является GIT [3], и ее популярность объясняется, в том числе, бесплатностью, а также относительной простотой и удобством использования.

Кроме того, важными особенностями указанной СКВ с точки зрения субъектов судопроизводства являются такие особенности функционирования и хранения данных контроля, как [2, с. 24–26]:

- хранение полных версий всех отслеживаемых файлов, т. е. всех файлов, в отношении которых СКВ пользователем прямо указано на необходимость отслеживания содержания, по состоянию на конкретные моменты времени в отличие от большинства иных СКВ, хранящих информацию в виде списка изменений файлов (таких как CVS, Subversion, Perforce и др.);

- использование при работе только локальных ресурсов – вся история файлов хранится локально и зафиксированные изменения загружаются на сервер при необходимости;

– при сохранении состояния файлов и их наборов выполняется вычисление хэша данных (SHA-1) для дальнейшего его использования, в том числе как идентификатора.

Рассмотрим репозиторий СКВ GIT в части особенностей организации хранения контролируемых данных как элемента механизма слеодообразования при использовании GIT.

Отметим, что взаимодействие пользователя с GIT в процессе работы затрагивает три области слеодообразования:

1) каталог репозитория (далее – КР) – служебный каталог репозитория, хранящий версии контролируемых (отслеживаемых) файлов;

2) рабочий каталог (далее – РК) – каталог с файлами, предназначенными для отслеживания версий/каталог, предназначенный по умолчанию для выгрузки отслеживаемых файлов соответствующих версий;

3) область индексирования (промежуточная область) (далее – ОИ) – служебная область в каталоге репозитория GIT, хранящая информацию о файлах, входящих в следующую операцию фиксации их состояния.

С учетом изложенного базовый рабочий процесс в GIT состоит из следующей последовательности действий, выполняемых или инициируемых пользователем (рис. 1):

- создание/редактирование файлов в РК;
- индексация, т. е. помещение необходимых файлов в ОИ;
- фиксация состояния (создание коммитов), т. е. помещение файлов из ОИ в КР с созданием служебной записи в репозитории с дополнительной информацией о фиксации.

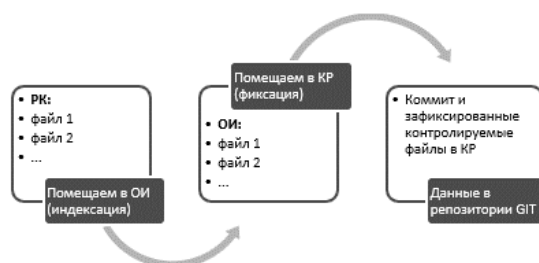


Рис. 1. Базовый рабочий процесс по помещению файлов в репозиторий GIT

Отметим, что GIT также поддерживает:

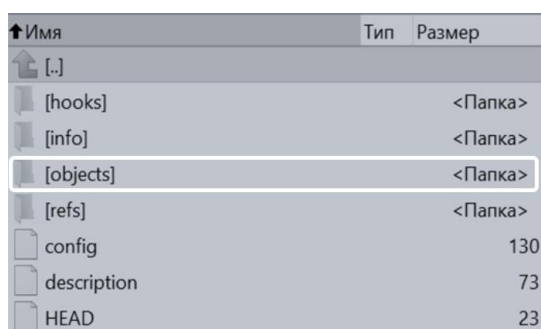
- ветвление («Branching»), т. е. отклонение от основной линии разработки, после которого работа перестает затрагивать основную линию;
- слияние («Merging»), т. е. объединение линий разработки.

Рассмотрим процесс создания и функционирования репозитория GIT.

Так, при инициализации нового репозитория (команда «git init»¹) во вновь создаваемом или ранее имевшемся рабочем каталоге проекта создается служебный подкаталог с именем «.git», который далее будет хранить всю историю изменений рабочего каталога проекта, с этого момента выполняющего также функции рабочего каталога (РК) репозитория GIT.

¹ Здесь и далее при работе с репозиториями используется штатное программное средство управления GIT посредством командной строки – GIT BASH.

Указанный каталог «.git» содержит ключевые элементы репозитория в виде файлов и подкаталогов (рис. 2).



Имя	Тип	Размер
[.]		
[hooks]	<Папка>	
[info]	<Папка>	
[objects]	<Папка>	
[refs]	<Папка>	
config		130
description		73
HEAD		23

Рис. 2. Содержимое корневого каталога репозитория GIT после инициализации

Ключевыми в части обеспечения хранения контролируемых данных в репозитории являются файлы в каталоге «objects», содержащие всю базу данных репозитория. Рассмотрим особенности формирования данных в указанном каталоге.

Отметим, что система GIT хранит данные в виде пар ключ/значение, и любой объект может быть извлечен по своему ключу – хэшу SHA-1 (полному или сокращенному) объекта.

Служебные файлы репозитория в каталоге «objects» содержат непосредственно объекты хранения согласно следующим правилам [2, с. 420–421]:

- один файл на единицу хранения;
- для файла создается подкаталог с именем, идентичным последовательности двух первых символов хэша SHA-1 содержимого единицы хранения и заголовка, например, «BLOB»-объект состоит из заголовка («BLOB» + «пробел» + «размер содержимого» + «нулевой байт») и содержимого объекта хранения;
- в файле хранится сжатая с использованием библиотеки «zlib» последовательность из заголовка и содержимого единицы хранения;
- файлу в созданном подкаталоге присваивается имя, идентичное последовательности 38 символов хэша SHA-1 содержимого единицы хранения и заголовка, начиная с третьего символа.

В каталоге «objects» зарегистрированы служебные файлы с «BLOB»-объектами («Binary Large Object» («BLOB) – большой бинарный объект/массив двоичных данных), которые хранят состояния контролируемых репозиторием файлов. Такие служебные файлы не содержат имена и иные атрибуты контролируемых файлов. Кроме «BLOB»-объектов данный каталог может хранить файлы с объектами типа «TREE» и «COMMIT».

Например, инициализируем репозиторий (команда «git init»), добавим в ОИ файл «/additional folder/file_example.txt» (команда «git add .»), после чего проверим наличие новых файлов в каталоге «objects» (команда «find .git/objects»), а также их тип (команда «git cat-file -t (хэш)») (рис. 3).

В результате выполненных действий в каталоге «objects» создан и впоследствии обнаружен новый подкаталог «43» с файлом «efcd84207788e5289ee23a9ce95d9f43b13d9a», содержащим объект типа «BLOB».

```

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ find .git/objects
.git/objects
.git/objects/43
.git/objects/43/efcd84207788e5289ee23a9ce95d9f43b13d9a
.git/objects/info
.git/objects/pack

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -t 43efc
blob

```

Рис. 3. Результаты поиска файлов в каталоге «objects» репозитория и проверки типа объекта в обнаруженном файле

При последующем создании коммита (команда «git commit -m 'Создать первый коммит'»), то есть при фиксации текущего содержимого ОИ (файл «/additional folder/file_example.txt»), системой созданы еще три подкаталога с файлами, содержащими объекты типа «TREE» и «COMMIT» (рис. 4).

```

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ find .git/objects
.git/objects
.git/objects/15
.git/objects/15/252941e9d6e74e9b0fe5193b98d1f8c74abe5c
.git/objects/35
.git/objects/35/2468351aa797b33298eb5f3e4bfd4d4463be7c
.git/objects/43
.git/objects/43/efcd84207788e5289ee23a9ce95d9f43b13d9a
.git/objects/cc
.git/objects/cc/2905a48b7ff333fbeff2dc7113ed3cf2781ac8
.git/objects/info
.git/objects/pack

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -t 1525
tree

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -t 3524
tree

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -t cc29
commit

```

Рис. 4. Результаты поиска файлов в каталоге «objects» репозитория и проверки типов объектов в обнаруженных файлах

Объекты типа «TREE» («Дерево»), в том числе, хранят имена файлов/каталогов [2, с. 421].

Проверим содержимое созданных объектов указанного типа, обратившись к ним по части хэша (команда «git cat-file -p (хэш)») (рис. 5).

```

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -p 1525
040000 tree 352468351aa797b33298eb5f3e4bfd4d4463be7c    additional folder

non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -p 3524
100644 blob 43efcd84207788e5289ee23a9ce95d9f43b13d9a    file_example.txt

```

Рис. 5. Содержимое объектов типа «TREE» в файлах «252941e9d6e74e9b0fe5193b98d1f8c74abe5c»

и «2468351aa797b33298eb5f3e4bfd4d4463be7c» в каталогах «.git/objects/15/» и ««.git/objects/35/» соответственно

Как мы видим, объекты типа «TREE» содержат строки с данными о типе (в данном случае строка «100644» указывает на то, что «file_example.txt» является обычным файлом, а строка «040000» – на то, что «additional folder» является каталогом) и имени файла/каталога, а также о хэше SHA-1 объекта (то есть указателе на двоичный массив данных или на дерево следующего уровня) и типе этого объекта (в данном случае – «TREE» и «BLOB») [2, с. 422].

Третий вид объекта – объекты «COMMIT» («Коммит»). Содержимое данных объектов зависит, в том числе, от сведений о соответствующей фиксации состояния, а также от даты и времени ее (фиксации) создания. Объект «COMMIT» содержит хэш объекта «TREE» верхнего уровня для состояния контролируемых файлов на определенный момент времени; сведения об авторе/создателе коммита и метку времени; пустую строку; сообщение фиксации состояния контролируемых файлов.

Проверим содержимое созданного ранее объекта указанного типа, обратившись к нему по части хэша (рис. 6).

```
non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -p cc29
tree 15252941e9d6e74e9b0fe5193b98d1f8c74abe5c
author developer <email@email.ru> 1712732120 +0300
committer developer <email@email.ru> 1712732120 +0300

Создать первый коммит
```

Рис. 6. Содержание объекта типа «COMMIT» в файле «2905a48b7ff333fbff2dc7113ed3cf2781ac8» в каталоге «.git/objects/cc/»

Автор («author») – это человек, создавший файл. Создатель версии («committer») – тот, кто внес в авторскую версию правки и сохранил их. Например, автор посылает в проект некоторое исправление, а один из основных разработчиков применяет его и выступает в роли создателя версии.

Если изменить файл «/additional folder/file_example.txt», поместить его в ОИ и создать новый коммит, мы получим еще четыре новых объекта – 1 «BLOB», 2 «TREE» и 1 «COMMIT», при этом объект «COMMIT» будет содержать данные о родительском коммите («parent») текущей ветки, а именно хэш родительского коммита (рис. 7).

```
non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git cat-file -p 5da5
tree c0953d35486652991f76c48a159c961980866e9f
parent cc2905a48b7ff333fbff2dc7113ed3cf2781ac8
author developer <email@email.ru> 1712733485 +0300
committer developer <email@email.ru> 1712733485 +0300

Создать второй коммит
```

Рис. 7. Сведения о содержимом служебного файла репозитория, хранящего тип объекта «COMMIT»

Так организован первоначальный формат GIT для сохранения контролируемых файлов и сведений о них – «свободный» (loose) формат [2, с. 433].

Существует и другой формат, позволяющий экономить свободное место на накопителе информации и повышающий эффективность работы системы.

Так, периодически GIT (или пользователь с использованием команды «git gc») упаковывает хранимые объекты, относящиеся к зафиксированным состояниям контролируемых файлов, в архивные «РАСК»-файлы с собственно объектами, а также сохраняет данные о соответствующих объектах (в том числе, например, данные о смещении объекта в архивном файле и его размере) в «IDX»-файлы – файлы-индексы [2, с. 433–434]. Такие файлы хранятся в подкаталоге «pack» каталога «objects». Экономия места хранения при упаковке объектов достигается сохранением в указанном случае только разницы между последней и предыдущими версиями. При упаковке исходные файлы с объектами из КР репозитория удаляются (рис. 8, 9).

```
non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ find .git/objects
.git/objects
.git/objects/info
.git/objects/info/commit-graph
.git/objects/info/packs
.git/objects/pack
.git/objects/pack/pack-d3eae9e8ac04bf5d76008a535a57ca272dd8df09.idx
.git/objects/pack/pack-d3eae9e8ac04bf5d76008a535a57ca272dd8df09.pack
```

Рис. 8. Результаты поиска файлов в каталоге «objects» репозитория после процедуры упаковки в «РАСК»-файлы (команда «git gc»)

```
non_n@DESKTOP-I7V9CGA MINGW64 ~/dev/example (master)
$ git verify-pack -v .git/objects/pack/pack-d3eae9e8ac04bf5d76008a535a57ca272dd8df09.idx
5da59bcf04c26bf9b84508b735301ce5e0bf496b commit 241 184 12
cc2905a48b7ff333fbef2dc7113ed3cf2781ac8 commit 193 154 196
caaa7fde8dd95559faa86fdc09b3dd8bf7df3d05 blob 13 19 350
c0953d35486652991f76c48a159c961980866e9f tree 44 53 369
59a218cd6879651460a92967c81aacbb48292bbb tree 44 55 422
15252941e9d6e74e9b0fe5193b98d1f8c74abe5c tree 44 53 477
352468351aa797b33298eb5f3e4bfd4d4463be7c tree 44 55 530
43efcd84207788e5289ee23a9ce95d9f43b13d9a blob 6 15 585
non delta: 8 objects
.git/objects/pack/pack-d3eae9e8ac04bf5d76008a535a57ca272dd8df09.pack: ok
```

Рис. 9. Сведения о содержании архива (команда «git verify-pack -v (имя архивного файла)»)

Таким образом содержимое любого из хранимых в репозитории коммитов определяет совокупность имеющихся в каталоге «objects» файлов со сведениями о связанных цепочках вида коммит-дерево-объект хранения. То есть репозиторий GIT хранит собственно контролируемые данные и сведения о них, а также иные дополнительные сведения о фиксации состояния контролируемых файлов, в распределенном виде в совокупности служебных файлов (минимум три служебных файла для одной фиксации), в свободном (loose) или упакованном (pack) формате.

Очевидно, что без учета этой особенности хранения данных репозиториум результативное извлечение зафиксированной в нем информации в ходе криминалистического исследования невозможно.

Таким образом, в статье рассмотрена система контроля версий GIT как объект криминалистического исследования, отдельное внимание уделено механизму слеодообразования программного обеспечения СКВ GIT в части хранения в репозитории контролируемых данных.

По мнению автора приведенные в статье сведения могут быть использованы практикующими специалистами при проведении экспертных исследований репозитория GIT.

Список литературы

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 12.12.2023) // Гарант. URL: <https://internet.garant.ru/#/document/12148555/paragraph/3471:8/>.
2. Чакон С., Штрауб Б. Git для профессионального программиста. СПб. : Питер, 2016.
3. GIT : [сайт]. URL: <https://git-scm.com/>.

Харламов И. С.¹,

*курсант 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*

ОБЗОР СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ И ПЕРСПЕКТИВЫ ИХ ИСПОЛЬЗОВАНИЯ В ИНФОРМАЦИОННОМ ОБЕСПЕЧЕНИИ МВД РОССИИ

Одной из современных задач, возложенных на МВД России, является полный переход информационных систем и программных продуктов иностранных компаний на отечественные аналоги и разработки, в том числе на операционную систему Astra Linux, которая создавалась на базе ядра Linux, что подразумевает необходимость переобучения огромного количества пользователей с привычных систем на во многом отличающиеся UNIX-подобные операционные системы (ОС).

Ознакомимся с актуальными операционными системами, их возможностями, особенностями, различиями и, главное, с перспективами использования оных для решения практических информационных задач. В частности, рассмотрим актуальные операционные системы с точки зрения сходства опыта использования с предложенным отечественным решением в виде ОС Astra Linux.

1. *Семейство операционных систем MacOS.* Операционные системы семейства MacOS прошли долгий путь развития: от собственных разработок в лице Apple DOS, ProDOS, Apple GS/OS, Mac OS Classic, до появления в 2001 г. UNIX – подобных операционных систем – Mac OS X, версии которых до сих пор обновляются и развиваются. Несмотря на широко развитую программную инфраструктуру операционных систем компании Apple Inc. и тот факт, что операционные системы построены на базе ядра UNIX, использование операционных систем и программного обеспечения неприемлемо, так как компания сотрудничает с Правительством США и другими государственными силовыми структурами, а также собирает данные о пользователях, в том числе геолокацию, содержание телефонной книги, переписки и фотографии, а также другие данные, относимые к персональным так или иначе.

Также известно, что компания Apple Inc. в 2007 г. принимала участие в программе PRISM Агенства национальной безопасности США, целью которой был негласный сбор данных, передаваемых по сетям электросвязи. Не исключено,

¹ © Харламов И. С., 2024.

что в будущем, компания продолжит участвовать в разведывательной деятельности США [1].

2. *Семейство операционных систем Windows*. Первой операционной системой в истории корпорации Microsoft была MS-DOS – **MicroSoft Disk Operating System** (дисковая операционная система Майкрософт) [2]. Она была выпущена в 1981 г., а Windows в то время не существовало даже как графической оболочки для удобства использования системы. И лишь в 1985 г. стала развиваться версия Windows 1.0 как графическая оболочка и произошло появление Windows 3.1. Определенный качественный этап развития отмечился версией Windows for Workgroups 3.11 в 1994 г. В последующем появились такие системы как Windows 95, Windows 98, Windows Millennium (Windows Me в 2000 г.), но они все еще базировались в некоторой мере на MS-DOS. После этого, в 2001 г., вышла операционная система Windows XP, которая базировалась на оригинальном и новом ядре от Microsoft.

Именно эта операционная система положила начало качественно новому подсемейству систем Windows под название Windows NT – Windows New Technology (новые технологии). Как развитие этой идеи в 2007 г. была выпущена система Windows Vista, в 2009 г. – Windows 7, в 2012 г. – Windows 8, в 2015 г. – Windows 10 и в 2021 г. – Windows 11.

В данный момент официально поддерживаются корпорацией Microsoft только Windows 10 и 11 с окончанием поддержки в 2025 г. Для Windows 10 и Windows 11 существует несколько различных редакций, которые отличаются друг от друга предполагаемой сферой применения для пользователей. В двух последних операционных системах предлагаются следующие редакции: Home (Домашняя), Pro (Профессиональная), Enterprise (Корпоративная), Education (Образовательная).

Домашняя версия обладает стандартным набором функций для использования компьютера в личных целях.

Профессиональная версия обладает более широким набором функционала, например, позволяет администрировать различные модификации компьютеров, персонализировать доступ, а также использовать бизнес-приложения.

Корпоративная версия обладает максимально полным функционалом, так как ее использование предполагается в средних и крупных компаниях.

Образовательная версия похожа на корпоративную, но применяется в образовательных учреждениях. В ней отключены подсказки, советы и предложения системы, а также она обеспечивает высокий уровень защиты компьютера.

Также имеется представленный ряд серверных решений для операционной системы Windows.

Однако, использование операционных систем и программного обеспечения компании Microsoft неприемлемо, так как ОС Windows не полностью документирована, что оставляет возможность компании-разработчику внедрять незадекларированные функции в ОС. Microsoft также принимала участие в разведывательной программе PRISM, что исключает использование программных продуктов данной компании в МВД России [3].

3. *Семейство Linux*. История создания ядра Linux начинается с ее появления в 1991 г. [4]. И сразу же после этого началось бурное развитие всевозможных дистрибутивов Linux, т. е. наборов программного обеспечения, подготовленных к распространению и установке. Случилось это в связи с тем, что многим пользователям хотелось видеть в операционной системе определенный набор функций и возможностей, а именно свободная лицензия, под которой начала распространяться ОС Linux, позволяла «умельцам» беспрепятственно создавать такие операционные системы и, если они оказывались удачными – рабочими, распространять их в Интернете.

При этом, чаще всего, никто не создавал все под себя с нуля, а брал что-то уже готовое и вносил изменения, которые конкретный разработчик хотел бы видеть в операционной системе. Именно этим и обусловлено огромное количество существующих дистрибутивов Linux [5].

В настоящее время самыми популярными дистрибутивами Linux являются: CentOS, OpenSUSE, Ubuntu, Kali Linux, Arch Linux, Fedora, Debian. Среди них также есть и отечественные разработки, такие, как: AlterOS, ROSA Linux, ALT Linux, ОС «Эльбрус», ОС «Атлант», RED OS. Особенно среди отечественных разработок выделим такую разработку, как Astra Linux, оказавшуюся флагманом в переходе государственной информационной инфраструктуры на отечественное программное обеспечение.

Далее рассмотрим сходства и различия указанных выше версий ОС с Astra Linux, так как именно этот дистрибутив постепенно внедряется на всех объектах государственных органов как государственный стандарт.

Сравнение произведем только в плане командного взаимодействия с системой, так как на практически любой дистрибутив Linux возможно установить практически любую из многочисленных графических оболочек, в связи, с чем не требуется иметь опыт использования конкретной оболочки, а значит и не требуется сравнивать дистрибутивы по этому параметру.

Astra Linux. Для того, чтобы провести объективное сравнение операционных систем, опишем чем является Astra Linux.

В данной операционной системе используется пакетный менеджер APT и собственная графическая оболочка. Собственный репозиторий Astra Linux состоит из более чем 20 000 пакетов. На пакетной базе этого репозитория развиваются и другие программные продукты компании. В состав дистрибутива входят такие пакеты с открытым исходным кодом, как графическое окружение пользователя Fly, офисный пакет LibreOffice, доработанный в части управления доступом, серверные компоненты (web-сервер, СУБД и т. д.), браузер Firefox, почтовый клиент Thunderbird, редактор растровой графики GIMP, проигрыватель мультимедиа VLC и др. Управление интуитивно понятно и не чинит трудностей для тех, кто ранее работал только с системами Windows.

Также существует серверная версия Astra Linux Server. Системные требования довольно низкие, но все же чуть выше, чем у операционных систем Windows: это 4 ГБ оперативной памяти (против 2 ГБ), процессор на архитектуре x86-64, видеокарта с поддержкой разрешения 1024x768 и 16 ГБ места на жестком диске.

Далее требования дистрибутивов не приводим, поскольку для любого из них требования, за исключением не влияющих мелочей, одинаковые [6].

CentOS. Сокращенное название от английского «Community ENTerprise Operating System» – созданная сообществом корпоративная операционная система. Данная операционная система разработана на базе платно распространяемого дистрибутива Linux – Red Hat и предназначена для применения в компаниях. Каждая версия поддерживается в течение десятилетия, а новые версии выходят раз в полугодие.

В CentOS, в отличие от Astra Linux, применяется пакетный менеджер RPM, особенность которого – это процедура установки приложений, отличающаяся от подобной в версии Astra Linux.

Операционная система CentOS имеет весь необходимый функционал для его создания на базе сервера [7].

OpenSUSE. Один из наиболее подходящих дистрибутивов для новичков, так как позволяет осуществлять выбор между графическими оболочками в процессе установки операционной системы.

OpenSUSE обладает YaST – утилитой для управления системой. С помощью этой утилиты можно в графическом режиме, без обращения к консоли, выполнять широкий спектр задач по управлению и настройке системы, включая задачи по администрированию, что особенно важно для новичков. Данная утилита автоматически делает снимки состояния системы во всех критических ситуациях, что позволяет в случае необходимости откатить состояние системы до нормального состояния. Также стоит отметить, что YaST базируется на пакетном менеджере RPM.

OpenSUSE не идеальна – она не поддерживает большинство утилит для просмотра и работы с медиаконтентом. Это может затруднять работу рядовым пользователям или не позволит выполнить служебную задачу, связанную с анализом фотоснимков, видеозаписей и кинофильмов, составлением фотороботов, фототаблиц и тому подобных задач.

Дистрибутив OpenSUSE server создан специально для работы серверного оборудования [8].

Ubuntu. Самый простой и дружелюбный в освоении дистрибутив из существующих UNIX-подобных. Обладает широким разнообразием – от серверных решений до специальных версий для образовательных учреждений. Версии для образовательных учреждений комплектуются программами для изучения географии, химии и других школьных предметов. А преподаватель при этом, даже без специальных знаний, может за короткое время развернуть и поддержать сеть для учеников и студентов.

В Ubuntu применяется пакетный менеджер APT, что облегчает последующий переход на платформу Astra Linux, так как команды и процесс скачивания и установки пакетов идентичны между этими системами.

Ubuntu поддерживает работу с медиаконтентом, имеет предустановленный пакет офисных приложений для работы с текстом и мультимедиа, поддерживает сохранение, открытие и редактирование документов в Windows форматах, что облегчает первоначальный переход с ОС Windows на версию Ubuntu Linux.

Также в Ubuntu присутствует собственный, так называемый «магазин приложений», позволяющий «по паре нажатий кнопок мыши» устанавливать проверенные и безопасные приложения для расширения функционала операционной системы.

Создан также полноценный серверный дистрибутив Ubuntu Server [9] на базе Ubuntu Linux.

Kali Linux. Эта операционная система вышла в 2013 г. как инструмент для сотрудников, отвечающих за информационную безопасность в компании. Вместе с операционной системой устанавливается широкий набор утилит и приложений, позволяющих тестировать различные объекты информационной инфраструктуры на предмет уязвимостей, с последующим их устранением.

В Kali Linux установлен пакетный менеджер APT, а также графическая оболочка GNOME – такая же, как и в дружелюбной версии Ubuntu. В таком виде Kali Linux для не специалиста фактически не отличается от описанной выше Ubuntu, а набор программ, которые пользователь применит, не будет, скорее всего, затруднять использование операционной системы. Таким образом, данная операционная система скорее неприменима, чем удобна [10].

Arch Linux. Данный дистрибутив подходит для опытных пользователей, так как для работы в нём часто применяются команды терминала, работа с которыми для новичков весьма затруднительна.

В данной версии ОС применяется редкий пакетный менеджер Pacman, который обладает собственным функционалом и набором команд для работы с ним.

Существует версия, способная «поднять» сервер на Arch Linux.

Можно заключить, что для новичков эта операционная система также не лучший выбор [11].

Fedora. В данной операционной системе применяется графическая оболочка GNOME, а также пакетный менеджер RPM, основан на разработках Red Hat и поддерживается ими же.

Существует и серверная версия, но из-за короткого срока поддержки часто выходящих версий, она оказывается не очень стабильно работающая, что вызывает сомнения в рациональности использования такого решения, при наличии других дистрибутивов серверного назначения.

Debian. В Debian применяется пакетный менеджер APT, что сближает его с Astra Linux. Данная версия стабильна, но, однако, редко обновляемая. Редкое обновление связано с тем, что только проверенные версии приложений с утилитами и пакетами передаются конечному пользователю для установки.

В Debian используется графическая оболочка KDE, сильно похожая на привычный интерфейс Windows, что облегчает привыкание пользователя.

Также существует серверный вариант этого дистрибутива – Debian Server.

Далее кратко рассмотрим популярные отечественные разработки и начнем с AlterOS.

AlterOS. Крайняя версия российской разработки вышла в середине 2021 г. Несмотря на это продукт основан на старых версиях CentOS. В данной операционной системе применяется графический интерфейс Cinnamon, а также пакетный менеджер RPM.

AlterOS включена в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также соответствует требованиям доверия к ОС и включена к тому же в официальный реестр средств защиты информации. Операционная система AlterOS имеет сертификат ФСТЭК России, подтверждающий ее соответствие «Требованиям безопасности информации к операционным системам» по четвертому классу защиты информации для операционных систем общего назначения.

Также следует отметить, что данный программный продукт имеет версию как для персональных компьютеров, так и для серверов. Существует также версия для работы с облачными решениями.

ROSA Linux. Этот дистрибутив базируется на пакетном менеджере DNF, что является редким выбором для создания дистрибутива, но тем не менее имеющий место быть.

Операционная система *ROSA Linux* существует в трёх вариантах: для домашних персональных компьютеров, для компаний и организаций, также для серверов.

Эти версии отличаются современностью и высокой доступностью для незнакомого с Linux пользователя. Почти все действия можно выполнить в графическом режиме, не используя терминал, а сама графическая оболочка наиболее похожа на привычный многим Windows.

Также данные дистрибутивы соответствуют требованиям ФСТЭК, имеют сертификацию Минцифры России и входят в Реестр отечественного ПО.

Все вышеперечисленное делает Rosa Linux приемлемым выбором при переходе на отечественные Linux-системы.

ALT Linux. Дистрибутив предлагает встроенную поддержку отечественного программного обеспечения и поэтому всевозможные приложения могут быть установлены, а работать будут надежно и с поддержкой.

Графический интерфейс несколько устарел, но так как это не сказывается на работоспособности системы, то и мы не будем обращать на это внимание.

ALT Linux использует пакетный менеджер RPM, что несколько отдаляет его от той же Astra Linux.

ALT Linux выпускается в вариантах для домашнего использования, для компаний и для серверов. Данные дистрибутивы соответствуют требованиям ФСТЭК, имеют сертификацию Минцифры России и входят в Реестр отечественного ПО.

ОС «Эльбрус». Операционная система Эльбрус была создана на базе Debian Linux специально для использования с процессором Эльбрус. Данная версия ОС работает с пакетным менеджером APT. ОС «Эльбрус» имеет сертификацию Минцифры, соответствует требованиям ФСТЭК, а также входит в реестр отечественного программного обеспечения.

Поскольку процессоры Эльбрус на данный момент не получили широкого распространения, то использование данного дистрибутива весьма сильно ограничено.

ОС «Атлант». Данная операционная система, построенная на базе Debian, использует пакетный менеджер APT. ОС «Атлант» не делится на версию для

персональных компьютеров и для серверов, отличается лишь наборами программных продуктов, применяемый для тех или иных задач.

Основная задача ОС «Атлант» – предоставлять возможность эффективно управлять большим парком подконтрольных персональных компьютеров и осуществлять для парка программное обновление.

Несмотря на то, что данная система имеет в своём составе стандартный набор офисных приложений и веб-браузер, она все же не рекомендуется для начинающих пользователей, так как создавалась для выполнения узкоспециализированной задачи.

RED OS использует пакетный менеджер RPM. При установке предлагается выбрать одну из трех графических оболочек: Mate, Cinnamon, Gnome. Среди указанных оболочек Cinnamon наиболее похож на Windows.

Данная операционная система имеет сертификаты Минцифры, отвечает требованиям ФСТЭК, а также внесена в реестр отечественного программного обеспечения.

В RED OS существует процедура создания снимков системы, что позволяет делать «бэкапы» для преодоления неполадок.

Данная версия ОС выпускается в двух вариантах:

1) стандартная – операционная система общего назначения для серверов и рабочих станций, к тому же бесплатная;

2) сертифицированная – имеющая все вышеперечисленные сертификаты, но требующая для получения приобретения лицензии.

RED OS представляется приемлемым вариантом, а использование некоторое время бесплатной версии облегчает переход с ОС Windows.

Список литературы

1. Astralinux // Astralinux. URL: <https://astralinux.ru/>.
2. OpenSUSE – все также надежен и практичен // Записки IT специалиста. URL: https://interface31.ru/tech_it/2023/04/opensuse---vse-takzhe-nadezhen-i-praktichen.html.
3. Kali Linux для начинающих // cruftum. URL: <https://timeweb.com/ru/community/articles/kali-linux-dlya-nachinayushchih>.
4. Плюсы и минусы Arch Linux // Mivocloud. URL: <https://mivocloud.com/ru/blog/plusy-i-minusy-arch-linux>.
5. Fedora Linux – обзор дистрибутива // Cloud4y. URL: <https://www.cloud4y.ru/blog/fedora-linux-review/>.
6. Операционные сети Alter-OS // Alter-os. URL: <https://alter-os.ru/>.
7. Свежий обзор ROSA FRESH // РОСА. URL: <https://rosa.ru/svezhij-obzor-rosa-fresh/>.
8. ALT Linux // ALT Linux Wiki. URL: <https://www.altlinux.org/>.
9. Операционная система «Эльбрус Линукс» (ТВГИ.00333-01) // МЦСТ. URL: http://www.mcst.ru/Elbrus_Linux.
10. Атлант // Атлант-Applite. URL: <https://applite.ru/atlant>.
11. Обзор установки // Редос. URL: <https://redos.red-soft.ru/base/manual/admin-manual/ibstall-red-os/obzor/>.

Хатова Ж. М.¹,

*доцент кафедры управления в международном бизнесе
и индустрии туризма Института управления персоналом,
социальных и бизнес-коммуникаций
Государственного университета управления*

О ЦИФРОВОЙ ГИГИЕНЕ СТУДЕНТОВ ЮРИДИЧЕСКИХ ВУЗОВ

Цифровая гигиена в основном понимается исследователями, как в узком измерении, а именно как элемент обеспечения информационной безопасности, так и в более широком, например, даже в воспитательном и медицинском аспектах. При этом в Стратегии национальной безопасности определена цель информационной безопасности – укрепление суверенитета Российской Федерации в информационном пространстве (ст. 56). Стратегический документ обозначает необходимым в этой связи не только снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных и связанных с этим правонарушений, а также обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, и иные меры, включая приоритетное использования соответствующих российских информационных технологий и оборудования.

Данное положение является одной из национальных целей, и должно быть обеспечено в том числе и в образовательной сфере.

По справедливому мнению Л. Л. Ефимовой, цифровая гигиена представляет собой совокупность навыков, знаний и привычек, необходимых для эффективного и безопасного использования цифровых технологий. С учетом изложенного, представляется целесообразным дополнить указанную позицию тем, что цифровая гигиена является составной частью цифровой безопасности.

Еще одним важным свидетельством того значения, которое придается вопросам цифровой гигиены в самых разных аспектах информационной безопасности, в том числе в процессе усиливающегося информационного противоборства, выступает требование по созданию механизмов государственно-общественного контроля в отношении существующего рынка компьютерных развлечений.

Применительно к категории обучающихся юридических вузов вопросы цифровой гигиены, как и иные, включая патриотическое воспитание, на наш взгляд, имеют свою профильную специфику, тем более, что исследователями уже отмечались особенности компетенций цифровой гигиены обучающихся различных категорий, например, студентов технических вузов. Будущие юристы в первую очередь должны обращать внимание не только на медицинские и иные, в том числе рекомендации по безопасному использованию цифровых устройств, но и на содержание правовых норм, регулирующих вопросы цифровой безопасности, а также их неукоснительное соблюдение.

Например, соответствующие вопросы отражены не только в положениях законодательства, изучаемого в рамках курсов информационного и гражданского

¹ © Хатова Ж. М., 2024.

права, но и в соответствующих нормах Уголовного кодекса Российской Федерации (гл. 28 «Преступления в сфере компьютерной информации» и др.), а также Уголовно-процессуального кодекса Российской Федерации.

Соответствующие компетенции юридических специальностей, по нашему мнению, следует закреплять в рабочих программах учебных дисциплин.

Список литературы

1. Прокофьев О. В., Семочкина И. Ю. Компетенции цифровой гигиены в высшем техническом образовании // Современные информационные технологии. 2019. № 29. С. 83–87.
2. Суходаева Т. С. Формирование навыков цифровой гигиены студентов как существенный элемент воспитательной работы в высшей школе // Вестник СГУПС: гуманитарные исследования. 2022. № 2 (13).
3. Смирнова Г. А., Михайлова Е. А. Цифровая гигиена в контексте здорового образа жизни студентов // Актуальные проблемы развития и совершенствования системы физического воспитания для подготовки специалистов в транспортной отрасли : сборник научных трудов. М. : Российский университет транспорта, 2022. С. 223–227.
4. Хатова Ж. М. О совершенствовании патриотического воспитания студентов-юристов // Социально-экономическое развитие и качество правовой среды : сборник докладов : в 5 ч. Ч. 1. М. : Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2021. С. 363–365.
5. Хатов Э. Б. К вопросу цифровой безопасности в деятельности следователя // Актуальные вопросы обеспечения национальной безопасности : сборник научных трудов. М. : Московская академия Следственного комитета Российской Федерации, 2023. С. 104–112.

Ходусов А. А.¹,
*заведующий кафедрой уголовно-правовых дисциплин
Международного юридического института,
кандидат юридических наук, доцент*

ЦИФРОВИЗАЦИЯ В КРИМИНАЛИСТИКЕ: СОВРЕМЕННЫЕ ВЫЗОВЫ

Цифровизация в криминалистике представляет собой медаль с двумя сторонами. С одной стороны, она значительно улучшает эффективность работы следователей и позволяет им более точно и быстро раскрывать преступления. С другой стороны, это вызывает новые вызовы и угрозы, требующие постоянного совершенствования методов и технологий в борьбе с преступностью. Важно уметь находить баланс между использованием цифровых технологий в криминалистике и защитой личных данных и конфиденциальности граждан.

Цель статьи: провести анализ применения цифровизации для поиска «цифровых следов». В соответствии с этим автор работы рассмотрит «плюсы» и «минусы» цифровизации в криминалистике.

Итак, цифровизация в криминалистике имеет как положительные, так и отрицательные стороны. С одной стороны, цифровые технологии позволяют разработать новые методы и инструменты для раскрытия преступлений и сбора улик. Современные компьютерные программы и аналитические инструменты помогают быстрее обрабатывать огромные объемы данных и выявлять связи между различными событиями. Цифровизация также позволяет хранить и обрабатывать информацию более эффективно, что сокращает время проведения расследований.

Однако цифровизация в криминалистике также создает новые вызовы и проблемы. Вместе с возможностью быстрого доступа к информации, возникает риск попадания личных данных и конфиденциальной информации в несанкционированные руки. Киберпреступники постоянно разрабатывают новые методы атак и взлома, что требует от криминалистов постоянного обновления своих навыков и знаний [3].

Внедрение цифровых технологий в криминалистику имеет свои особенности и требует особого внимания при реализации. Автор рассмотрел некоторые особенности внедрения цифровых технологий в криминалистику (рис.).

Рассмотрим достоинства цифровых технологий в криминалистике (табл.).

¹ © Ходусов А. А., 2024.

Квалифицированный персонал. Использование цифровых технологий в криминалистике требует наличия квалифицированных специалистов, обладающих знаниями и навыками в области информационных технологий. Необходимо проводить подготовку сотрудников и обучать их новым методам работы с цифровыми устройствами и программным обеспечением

Безопасность данных. Важно обеспечить безопасность хранения и обработки цифровых данных, особенно если информация содержит конфиденциальные данные о преступных делах, свидетелях или подозреваемых. Необходимо принимать меры по защите от утечек данных и несанкционированного доступа

Соблюдение законодательства. При работе с цифровыми технологиями в криминалистике необходимо строго соблюдать законы и нормы, регулирующие сбор, хранение и использование данных. Важно проводить работу в соответствии с законом, чтобы избежать возможных правовых последствий

Использование специализированных программ и оборудования. Для эффективной работы с цифровыми уликами и данными в криминалистике необходимо использовать специализированные программы и оборудование, которые позволят проводить анализ данных точно и надежно

Взаимодействие с другими службами и организациями. Часто цифровые следы и данные требуют сотрудничества между различными организациями и службами, например, с провайдерами интернет-услуг или специализированными компаниями по цифровой безопасности. Отличное сотрудничество позволяет быстрее и эффективнее расследовать преступления

Рис. Особенности внедрения цифровых технологий в криминалистику

Таблица

Достоинства и недостатки цифровых технологий в криминалистике

Достоинства	Более эффективное расследование преступлений	Цифровые технологии позволяют быстро анализировать большие объемы данных, анализируя оставшееся после преступления цифровое следствие
	Увеличение достоверности доказательств	С помощью цифровых технологий возможно проводить более точные и надежные экспертизы. Это и как анализ ДНК, и построение картины обстановки преступления, и взлом электронных устройств и т. д.

	Оптимизация сотрудничества между организациями и специалистами	Цифровые технологии облегчают обмен информацией и координацию действий между различными структурами правоохранительных органов
	Развитие новых методов и инструментов для борьбы с преступностью	Благодаря цифровым технологиям появляются новые возможности для выявления и пресечения преступлений, – это использование искусственного интеллекта, аналитика данных и кибербезопасность
	Упрощение доступа к информации	Цифровые технологии позволяют хранить и обрабатывать большие объемы данных эффективно и безопасно. Это облегчает поиск нужной информации для криминалистических исследований
Недостатки	Возможность сокрытия или искажения цифровых следов	Преступники могут использовать специализированные программы для сокрытия своих действий в цифровой сфере, что затрудняет их поиск
	Риск хакерских атак	Цифровые технологии могут быть подвержены кибератакам
	Утечки данных	Это приводит к утере криминалистических данных
	Сложность в обучении специалистов	Использование цифровых технологий требует специальных знаний и навыков. Считаем, что нужно инвестировать в обучение и повышение квалификации сотрудников
	Недоступность специализированного оборудования	Некоторые современные методы и инструменты цифровой криминалистики могут быть дорогими. Поэтому они недоступны для широкого круга организаций
	Проблемы с конфиденциальностью и защитой персональных данных	В связи с использованием цифровых технологий существует риск нарушения приватности и безопасности личных данных граждан. С этим борются специалисты

На основании табл. сделаем вывод: внедрение цифровых технологий в криминалистику требует комплексного подхода и внимания к различным аспектам работы с цифровыми уликами и данными. Важно учитывать специфику работы следователей, предоставляя им необходимые инструменты и знания для успешного применения цифровых технологий в борьбе с преступностью [4].

Цифровые технологии в сфере криминалистики представляют собой огромный потенциал для улучшения процессов расследования и предотвращения преступлений. С развитием информационных технологий появились новые возможности и инструменты, которые значительно улучшают эффективность работы правоохранительных органов. Одной из главных возможностей цифровых технологий в криминалистике является возможность быстрого и точного анализа

«цифровых следов». Благодаря специализированным программам и оборудованию, эксперты могут эффективно проводить исследования цифровых устройств, анализировать данные, реконструировать события преступления. Это позволяет выявить ключевые доказательства, восстановив утраченные данные, или сведения, которые преступник не заметил [1].

Другим важным аспектом цифровых технологий в криминалистике является возможность использования новейших методов и технических средств для идентификации доказательств. Применение технологий распознавания лиц, звука, оружия, анализа ДНК и других биометрических данных значительно упрощает процедуру идентификации подозреваемых и жертв. Сравнение больших массивов данных позволяет установить связи между различными преступлениями.

Цифровые технологии способствуют также и улучшению взаимодействия между различными организациями и учреждениями, задействованными в расследовании преступлений. Онлайн платформы для обмена информацией, совместные базы данных и системы обратной связи позволяют оперативно обмениваться данными, координировать действия различных подразделений.

Цифровые технологии обеспечивают более эффективное хранение и обработку огромных объемов данных, что ускоряет процесс анализа информации, выявление закономерностей преступной деятельности. Аналитика данных и использование искусственного интеллекта позволяют выявить скрытые шаблоны преступного поведения, предсказать возможные преступления. Например, можно проанализировать места, которые посещает преступник, или его связи с другими людьми [2].

На сегодня самое актуальное использование цифровизации, – поиск «цифровых следов» человека.

Одним из ключевых методов работы криминалистов при расследовании преступлений является анализ цифровых данных. Сначала специалисты изымают электронные устройства у подозреваемых, – компьютеры, телефоны, внешние накопители и другие устройства. Затем проводится анализ данных с этих устройств с помощью специализированных программ. Важно следовать процедурам восстановления информации, чтобы избежать возможных ошибок.

После извлечения данных криминалисты проводят анализ «цифровых следов», которые могут включать в себя текстовые документы, электронные письма, фотографии, видео, аудио файлы, историю посещенных веб-сайтов, местоположение устройства. Эти данные помогают как в установлении алиби, идентификации преступника. С помощью данных можно объяснить обстоятельства преступления и восстановить хронологию событий.

Существует несколько методов поиска цифровых следов человека, которые используются криминалистами:

Изучение электронной почты и сообщений. Криминалисты анализируют электронную почту и сообщения на различных платформах для выявления контактов и действий подозреваемого. Криминалисты могут изучить учетные записи в социальных сетях для выявления связей человека, его активности и местоположения. Это помогает в установлении мотивов и связей подозреваемого

в случае преступления. Например, так анализировали основателей группы «голубой кит». Проводят анализ метаданных, сообщений, вычисляют IP-адреса отправителя.

Использование мобильных устройств. Сегодня о возможности отследить геолокацию человека по мобильному устройству не знает только ленивый. А еще, – изучение мобильных устройств, – таких как смартфоны и планшеты, – позволяет криминалистам получить доступ к контактам, сообщениям, фотографиям, видеозаписям. Также телефон раскроет вам данные об истории посещенных мест.

Использование цифровых следов на компьютерах или ноутбуках. Криминалисты могут анализировать данные на компьютерах и ноутбуках для поиска цифровых следов. На компьютере ищут историю браузера, кэшированные страницы, использование ресурсов сети и другие данные, которые помогают в расследовании.

Использование цифровых камер и видеозаписей. При необходимости, специалисты могут анализировать цифровые фотографии и видеоролики для идентификации людей, мест и событий. Есть специальные программы, которые анализируют в сети нахождение человека на том или ином мультимедиа файле. Это помогает при выявлении потенциальных улик.

Судебно-экспертное исследование. Это серьезное исследование, которые, в основном, проводятся уже тогда, когда дело в суде. В случае подозрения на наличие цифровых следов, специалисты по цифровой безопасности могут проводить судебно-экспертное исследование для восстановления удаленных данных. Специалисты могут проанализировать следы вредоносных программ, криптографических алгоритмов и другие технические детали. Судебно-экспертное исследование проводят в случае необходимости получения экспертного мнения по цифровым следам, которые могут быть использованы в судебном разбирательстве или уголовном расследовании.

Такие исследования проводятся, например, при расследовании уголовных преступлений или при необходимости установления фактов, связанных с цифровыми доказательствами. Судебно-экспертные исследования могут быть проведены как в рамках уголовного, так и гражданского судопроизводства.

Поиск и анализ цифровых следов человека требует специализированных знаний и технических навыков, а также строгого следования процедурам, которые есть у специалистов [5]. Если улики найдены не по регламенту, их могут и не приобщить к делу в дальнейшем. Автор считает, что необходим комплексный подход к анализу цифровых данных. Это позволяет криминалистам получить ценную информацию для успешного расследования преступлений.

Итак, цифровые технологии представляют собой мощный инструмент в руках криминалистов и правоохранительных органов, способный улучшить эффективность расследования. Ключевым условием успешного использования цифровых технологий в криминалистике является постоянное обучение сотрудников, а также, – тесное сотрудничество между всеми участниками процесса расследования.

Цифровизация играет во всем этом ключевую роль. В современной криминалистике можно повысить эффективность борьбы с преступностью, если обеспе-

чить криминалистам доступ к большому объему информации. С развитием технологий и появлением новых методов анализа данных «цифровые следы» становятся все более важным инструментом в борьбе с преступностью. Цифровизация позволяет криминалистам применять специализированные программы для анализа данных, – а это значительно ускоряет процесс расследования преступлений. Например, с использованием компьютерных программ можно произвести сравнение графических изображений, анализ метаданных. Сегодня органами ФСБ России сличение данных используется для поиска террористов.

Список литературы

1. Гундина И. И., Щербакова А. В. Криминалистика в реалиях виртуального мира // Молодой ученый. 2020. № 20 (310). С. 265–267.
2. Дудниченко А. Н. О некоторых особенностях способа преступления как важного элемента криминалистической характеристики преступлений, связанных с нарушением правил дорожного движения и эксплуатации транспортных средств // Вестник Санкт-Петербургского университета МВД России. 2017. № 2 (74). С. 132–135.
3. Нагоев А. М., Бирюлина Е. В. Цифровизация в криминалистике // Молодой ученый. 2022. № 21 (416). С. 587–589.
4. Русанова Д. Ю. Цифровая криминалистика: возможности и перспективы развития. URL: <https://cyberleninka.ru/article/n/tsifrovaya-kriminalistika-vozmozhnosti-i-perspektivy-razvitiya>.
5. Соловьева С. М. Применение цифровых технологий в криминалистике // Молодой ученый. 2019. № 51 (289). С. 161–164.

Хорзов Д. С.¹,

*курсант факультета подготовки специалистов
в области информационной безопасности*

Московского университета

МВД России имени В.Я. Кикотя

Научный руководитель: Чурин Р. А.,

*главный эксперт отдела компьютерных
и радиотехнических экспертиз*

управления экспертиз цифровой и речевой информации

Экспертно-криминалистического центра МВД России,

преподаватель кафедры информационной безопасности

учебно-научного комплекса информационных технологий

Московского университета

МВД России имени В.Я. Кикотя

АНАЛИЗ ЖУРНАЛОВ РАБОТЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ МАРКИ DJI В ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКИХ ЦЕЛЯХ

Беспилотные летательные аппараты (БПЛА) стали неотъемлемой частью многих сфер человеческой деятельности. В области гражданской авиации они используются для организации развлекательных или коммерческих мероприятий, а в военной – для проведения разведывательных миссий, мониторинга территории и выполнения боевых задач. Среди всего обилия разнообразных дронов наиболее популярными являются беспилотники компании DJI (SZ Dajiang Innovation Technology Co., Ltd.). Основные производственные мощности этого предприятия расположены в Китайской Народной Республике.

В последнее время все чаще встречаются ситуации, когда беспилотники используют в качестве орудий совершения правонарушений. Как пример, утром 30 июля 2023 г. была совершена попытка атаковать здания Бизнес-центра в г. Москве с использованием беспилотников. Главная опасность заключается в том, что данные аппараты на борту обычно несут полезную нагрузку – взрывчатое вещество, поэтому последствия удара могут быть непредсказуемы. В этой связи, для расследования подобных инцидентов в криминалистических целях необходимо уметь анализировать содержание файлов, сформированных беспилотником во время полета.

Анализ журналов работы БПЛА не только марки DJI, но и любой другой представляет собой важный аспект исследований в области автономной навигации, безопасности полетов, и улучшения производительности БПЛА. Также немаловажным аспектом анализа является выяснение причин всевозможных неисправностей, повреждений, событий, что, в свою очередь, играет огромную роль в экспертно-криминалистической деятельности. В данной статье будут рассмотрены методы и инструменты анализа журналов работы БПЛА марки DJI, а также

¹ © Хорзов Д. С., 2024.

интерпретация полученных данных в целях оптимизации работы для дальнейшего исследования БПЛА.

На данный момент не существует методик по анализу журналов работы БПЛА, также данный факт осложняется тем, что эксперт не всегда располагает необходимым для исследования средствами – в данном случае возникает ситуация, когда на исследование поступает только информация о журналах работы БПЛА, а сам аппарат отсутствует. В этой связи эксперту необходимо иметь знания не только в области программного обеспечения (ПО), но и программного и программно-аппаратного оснащения различных моделей беспилотников, а такая задача бывает непосильна даже профессионалам с большим стажем.

Одним из универсальных инструментов в анализе журналов работы БПЛА является ПО «DatCon» и «CsvView» – бесплатные автономные приложения, предоставляющие средства для анализа файлов журналов (логов), создаваемых дронами Phantom 3, Phantom 4, Phantom 4 Pro, Inspire 1, Spark и Mavic Pro [1] – одними из самых популярных БПЛА. Они предлагают различный инструментарий для анализа полетов, однако в контексте экспертного исследования следует остановиться только на самых важных из них.

«DatCon» используется для интерпретации информации из файлов журналов работы БПЛА в определенный массив данных для последующей фильтрации и анализа. Здесь самыми важными полями являются данные о позиционировании беспилотника, его внутреннем состоянии и динамических характеристиках, таких как скорость и ускорение.

Большинство данных в журналах работы преследуют цель либо подтвердить полученную другими способами информацию, либо предоставить альтернативный способ анализа определенных событий. Например, параметр «GPS:velN» указывает составляющую скорости БПЛА в северном направлении (velocity North) на основании данных GPS, а «IMU_ATTI(0):velN» – скорость по северному направлению, измеренную инерциальным измерительным блоком (инерциальный измерительный блок (IMU) – это система, расположенная на плате БПЛА, которая определяет свое положение в пространстве, используя свойства инерции тел). Данный пример демонстрирует, что один и тот же параметр беспилотник получает различными способами. Таким образом, выбор конкретного параметра для анализа данных имеет значение только в случае возникновения сомнений в полученных данных (например, резкое изменение значения в короткий промежуток времени).

Перед тем, как приступить к анализу данных журналов беспилотников, необходимо уточнить базовые понятия для них. Такие понятия, как курс, тангаж и крен используются для определения наклона аппарата относительно осей X (продольная ось, по направлению полета, параллельно плоскости земли), Y (поперечная ось, перпендикулярно направлению полета, параллельно плоскости земли) и Z (вертикальная ось, перпендикулярно плоскости земли) соответственно и обычно определяются в градусах. Широта и долгота – географические понятия, используемые для определения положения объекта относительно земной поверхности.

Так, самыми важными параметрами при анализе полетов БПЛА представляются:

- 1) «IMU_ATTI(0):Longitude» и «IMU_ATTI(0):Latitude» – данные долготы (Longitude) и широты (Latitude), полученные от IMU;
- 2) «IMU_ATTI(0):alti:D» – данные высоты (altitude), полученные от IMU;
- 3) «IMU_ATTI(0):roll:C», «IMU_ATTI(0):pitch:C» и «IMU_ATTI(0):yaw:C» – данные угла крена (roll), тангажа (pitch) и курса (yaw) соответственно;
- 4) «IMU_ATTI(0):temperature» – данные измеренной температуры (temperature), полученные с датчика температуры в IMU;
- 5) «IMU_ATTI(0):velComposite:C» и «IMU_ATTI(0):accelComposite:C» – данные композитной скорости и ускорения (acceleration), измеренные в IMU.

Для того, чтобы получить данные с файла журналов работы БПЛА, в нашем случае формата .DAT, необходимо в ПО «DatCon» выбрать соответствующий файл, указать место, куда будет отправлен журнал БПЛА, в разделе «CSV» выбрать «.CSV», а в разделе «KML» выбрать пункт «Ground Track», все остальные поля можно оставить по умолчанию, нажать «GO!». Так, на устройстве в указанном месте сформируется два файла: с расширением «.csv» – для анализа отдельных величин и визуального отображения полученных данных, и «.kml» – для анализа местоположения (может помочь, если не удастся получить данные из файла «.csv»).

Открыть файл формата «.csv» можно посредством ПО «Microsoft Excel» (рис. 1), а визуально оценить их и посмотреть маршрут движения с помощью ПО «CsvView» (рис. 2).

IMU_ATTI(0):roll:C	IMU_ATTI(0):pitch:C	IMU_ATTI(0):yaw:C	IMU_ATTI(0):accelX	IMU_ATTI(0):accelY	IMU_ATTI(0):accelZ	IMU_ATTI(0):accelComposite:C	IMU_ATTI(0):gyrX	IMU_ATTI(0):gyrY	IMU_ATTI(0):gyrZ	IMU_ATTI(0):gyrComposite:C	IMU_ATTI(0):velN	IMU_ATTI(0):velE
-1.477078419	-0.599476864	74.09617352	-0.010085417	0.026746707	-1.0048817	1.0052882	0.522388	1.0537019	-0.54299515	1.2953843	0.002021199	0.000325786
-1.478410346	-0.597938357	74.13521863	-0.01168396	0.026385715	-1.0072196	1.0076329	0.30730432	0.7767807	-0.6709063	1.0714194	0.001745659	0.000166116
-1.478887307	-0.597852776	74.17279922	-0.0100232	0.027118314	-1.0087914	1.0092057	0.66775686	1.5737413	-0.5279186	1.7892063	0.001462968	6.45858E-05
-1.479828326	-0.597772296	74.19019834	-0.009662753	0.026190009	-1.0080876	1.0084741	0.7883957	0.8550256	-0.6654651	1.3399553	0.001694288	0.000417358
-1.480763463	-0.597257254	74.22673984	-0.009904695	0.02721124	-1.007125	1.0075412	0.68794835	1.0261117	-0.38308263	1.2934182	0.00190256	0.000520198
-1.479292356	-0.59804013	74.26549262	-0.010161772	0.026416153	-1.0073425	1.00774	0.5453868	0.58503956	-0.3056571	0.8562384	0.001453373	0.001081721
-1.478488275	-0.598399757	74.2628159	-0.010824818	0.025805997	-1.0071825	1.0075712	0.4263053	0.82408875	-0.33553824	0.9866328	0.00113264	0.001583528
-1.479885402	-0.597638358	74.27242356	-0.009597535	0.026345104	-1.0070751	1.0074654	0.37365708	1.3069947	-0.139926	1.3665409	0.000852336	0.00229045
-1.478588284	-0.59790351	74.27651984	-0.009758644	0.026188623	-1.005458	1.0058464	0.8101486	0.39162126	-0.53802675	1.0484183	0.000657187	0.00322366
-1.479370152	-0.599408344	74.30841429	-0.009127272	0.025856629	-1.0073088	1.007682	0.6493595	1.498857	-0.6068226	1.7425481	0.000671425	0.004485861
-1.479606064	-0.600609113	74.32774014	-0.010418907	0.025614468	-1.0074936	1.007873	0.36874303	0.3688364	-0.29077093	0.6000996	0.000817212	0.00544219
-1.479545811	-0.60122483	74.32914423	-0.010209945	0.027254094	-1.0071492	1.0075697	0.40229714	0.8315865	-0.38600847	1.0011901	0.002684235	0.006204608
-1.479681879	-0.602222126	74.33257344	-0.01032679	0.026559548	-1.005764	1.0061677	0.46218792	0.8776867	-0.49007398	1.1064014	0.00523284	0.007265936
-1.481385327	-0.602878525	74.35170708	-0.011004166	0.025991108	-1.0074731	1.0078684	0.5155869	0.32699257	-0.30946884	0.8844883	0.00749018	0.007746009
-1.4811078	-0.603149766	74.35511622	-0.010356634	0.02581763	-1.0069826	1.0073667	0.5584377	1.6896781	-0.4218887	1.8288944	0.009630531	0.00938314
-1.482020364	-0.604525831	74.3562139	-0.009646302	0.026524514	-1.0063149	1.0067106	0.5955527	1.3155643	-0.8231526	1.662219	0.010833568	0.010926024
-1.482746559	-0.60720172	74.35712841	-0.011088721	0.02633232	-1.0062164	1.006622	0.4185458	0.19276847	-0.2906236	0.5447957	0.011724927	0.012138569
-1.485016374	-0.607315851	74.39272367	-0.009867577	0.025941946	-1.0070137	1.0073961	0.6272325	0.7442054	-0.6282191	1.1584134	0.011852426	0.012774081
-1.485796507	-0.608053223	74.39645089	-0.010778399	0.026161227	-1.0063784	1.0067761	0.5715132	0.25060982	-0.6906897	0.9308517	0.011816098	0.012947178
-1.487472758	-0.608776439	74.39870682	-0.010741753	0.026996454	-1.0072114	1.0076305	0.5793392	1.1188968	-0.5552481	1.3769039	0.011050517	0.012241587
-1.485811036	-0.609385265	74.4044013	-0.01027108	0.027089579	-1.0067496	1.0071664	0.6212739	0.52951205	-0.4617275	0.9378468	0.00851536	0.006868961
-1.487018196	-0.610568894	74.40539692	-0.010611197	0.026849758	-1.0054898	1.0059942	0.048157714	0.1968924	-0.46861202	0.51057124	0.005421151	0.001137913
-1.487139882	-0.607771377	74.40820841	-0.010298069	0.02610074	-1.0058026	1.0061939	0.44219983	0.7884144	-0.49109524	1.0287431	0.004424355	-0.001204072
-1.487365486	-0.60666417	74.40905822	-0.010790986	0.02655072	-1.0054631	1.0058708	0.58451086	0.8323757	-0.4196041	1.100259	0.00536837	0.000600744
-1.487528048	-0.607668716	74.41337498	-0.011266211	0.02654533	-1.0065538	1.0069667	0.554651	0.6722507	-0.42863563	0.9712298	0.006031781	0.001975583
-1.486603236	-0.60693122	74.41578803	-0.010528985	0.02567118	-1.0073003	1.0076823	0.06982949	0.16333497	-0.6096614	0.635013	0.006547626	0.003474713
-1.487203445	-0.605674028	74.42064017	-0.01135948	0.02588896	-1.006532	1.0069289	0.3730483	0.28456697	-0.9087957	1.0102785	0.006815112	0.004644305
-1.488035487	-0.605851767	74.43720606	-0.010675924	0.027201544	-1.0063761	1.0068003	0.75774056	0.9559315	-0.5880604	1.3541753	0.006514865	0.005674686
-1.487408064	-0.60631854	74.47324016	-0.010153143	0.027286075	-1.0068911	1.0073119	0.40366167	-0.7435839	-0.49459475	0.9800427	0.006422017	0.006500016

Рис. 1. Представление данных журналов работы БПЛА посредством «Microsoft Excel»

Так, из огромного массива данных можно выделить основные столбцы в таблице, оценить вероятность возникновения возможных событий и сделать на их основании определенные выводы. Например, анализ столбца «IMU_ATTI(0):velComposite:C», указывающий на параметр скорости БПЛА в конкретный момент времени, может пригодиться при определении событий, связанными с резкими остановами беспилотника. Это, в свою очередь, может указывать на его столкновение с какими-либо объектами (когда на аппарате имеются повреждения, а их происхождение неизвестно).

Как уже упоминалось ранее, с помощью ПО «CsvView» возможно получение данных о полете БПЛА, а также представление различных данных с помощью графиков. Так, выбрав файл формата «.DAT», «.csv» или «.txt» с данными о журналах работы аппарата, эксперт получает возможность визуально отобразить обнаруженную информацию о маршруте полета, скорости вращения моторов лопастей, методу управления скоростью или мощностью двигателей с помощью изменения длительности импульсов, напряжении на моторах, составляющих магнитного поля и компаса, а также навигационной системы.

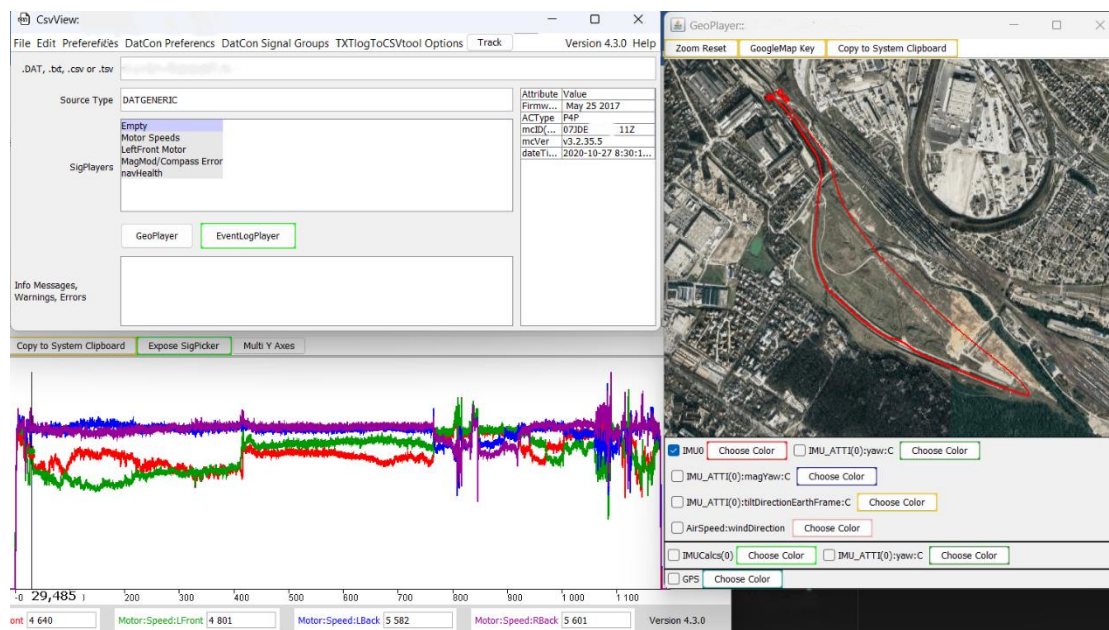


Рис. 2. Представление данных журналов работы БПЛА посредством «CsvView»

Немаловажными данными являются также значения столбца «Attribute|Value», указывающие информацию о внутреннем строении БПЛА, такие как «Firmware Date» (дата прошивки), «ACType» (тип аккумулятора, который используется в устройстве (accumulator type)), «mcID(SN)» (идентификатор серийного номера микроконтроллера (microcontroller ID)), «mcVer» (версия микроконтроллера (microcontroller version)), «dateTime» (время выполнения определенного события или записи, связанной с полетом или функционированием дрона).

Если по какой-либо причине в «CsvView» не удалось получить данные о полете, это можно сделать альтернативным способом – в сервисе «Google Earth» или любом другом подобном сформированный ранее в «DatCon» файл формата «.kml» предоставит всю необходимую информацию о полете беспилотника.

Таким образом, данные, зафиксированные БПЛА, могут быть использованы для раскрытия и расследования правонарушений. Вместе с этим возможность интерпретации значений требует более детального рассмотрения и апробации.

Список литературы

1. CsvView/DatCon /. URL: <https://datfile.net/>.

Хорошко А. А.¹,

*курсант Института-факультета психологии
служебной деятельности органов внутренних дел
Московского университета
МВД России имени В.Я. Кикотя*

Научный руководитель: Сиворонова М. С.,

*преподаватель кафедры психологии
учебно-научного комплекса психологии служебной деятельности
Московского университета
МВД России имени В.Я. Кикотя,
кандидат психологических наук*

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ КАК СПЕЦИФИЧЕСКАЯ ФУНКЦИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВЕННЫХ ОТНОШЕНИЙ

Одной из ключевых тенденций развития общества на современном этапе является информатизация. Процесс постепенного внедрения информационных технологий в жизнь человека начался еще на рубеже XX–XXI вв., однако особую интенсивность приобрел в связи с ограничительными в период пандемии Covid-19. Период локдаунов продемонстрировал, что общество готово к использованию информационных технологий не только как механизмов межличностного взаимодействия, но и как основ для организации управленческой деятельности в различных структурах, обеспечения коммуникации государственных и частных структур с населением.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. регламентирует процессы цифровизации общественных отношений, выступая в качестве нормативной основы формирования в России информационного общества [3]. Распространение цифровых каналов обеспечения социальной коммуникации в различных сферах является фактором, стимулирующим появление новых видов преступлений, совершаемых в интернет-среде, посредством использования компьютерных технологий.

Киберпреступления – это преступные действия, совершаемые в киберпространстве (цифровой среде) с использованием компьютерных и информационных технологий. Киберпреступники используют различные методы, такие как получение несанкционированного доступа к личным данным граждан или компаний, распространение полученных незаконным путем данных в открытом доступе, использование данных в личных целях, мошенничество, распространение вредоносного программного обеспечения и многое другое. Эти преступные действия могут привести к серьезным последствиям, включая финансовые убытки, нарушение частной жизни, кражу личной информации, а также угрозы национальной безопасности [4].

¹ © Хорошко А. А., 2024.

В современном информационном обществе борьба с киберпреступностью становится одной из важнейших функций органов внутренних дел, поскольку предполагает реализацию специфической деятельности, особенности которой связаны с ключевыми характеристиками угроз, в основе которых лежат цифровые технологии:

1. Сложность атрибуции – определения местоположения источника угрозы и идентификации преступника (использование анонимайзеров, «виртуальных частных сетей» – (VPN), создания множества фальшивых профилей и ложных учетных записей и др.).

2. Непредсказуемость. Кибератаки в современных условиях не могут быть спрогнозированы на основе применения традиционных методов обеспечения безопасности. При этом многие компании, организации и даже государства недостаточно готовы к кибератакам, так как устаревшие системы защиты не могут обеспечить должного уровня безопасности в современных условиях.

3. Разнородность субъектов киберпреступлений (на сегодняшний день не может быть составлена универсальная характеристика киберпреступника). Преступные посягательства на общественную безопасность в киберпространстве могут совершаться как по инициативе враждебного государства, так и по личной инициативе конкретных лиц, в следствие чего мотивационный компонент киберпреступлений может иметь разнообразное наполнение.

Функция реализации борьбы с киберпреступностью обладает выраженной спецификой. В отличие от иных функций, данное направление работы предполагает реализацию всех этапов деятельности, направленной на обеспечение и предупреждение угроз общественной безопасности в цифровой среде, в условиях высокой сложности локализации и установления личности преступника, непредсказуемости и разнородности субъектов киберпреступлений.

В 2022 г. на базе Министерства внутренних дел Российской Федерации (МВД России) было создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК) [2]. Специфика функций УБК в реализации борьбы с киберпреступностью заключается в необходимости постоянного мониторинга и анализа информационных потоков, выявлении и пресечении киберпреступных действий, а также сотрудничестве с другими государственными и международными организациями для обмена информацией и координации действий. Также важным аспектом деятельности УБК является осуществление превентивных мер по повышению информационной безопасности и обеспечению защиты от киберугроз как граждан, так и организаций [1].

Таким образом, одной из функций органов внутренних дел на современном этапе развития общества является прогнозирование киберпреступлений и борьба с киберпреступностью. Данная функция является специфической, требующей комплексного высококвалифицированного подхода, а также постоянного развития технологий и методов в области цифровых технологий. Функция борьбы с киберпреступностью реализуется на базе специального подразделения МВД России – Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий.

Список литературы

1. Алиханян К. Р. Организация работы МВД России в системе противодействия киберпреступлениям // Молодой ученый. 2023. № 2. С. 240–242.
2. Приказ МВД России от 29 декабря 2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России» // Легалакт – законы, кодексы и нормативные правовые акты Российской Федерации. URL: <https://legalacts.ru/doc/prikaz-mvd-rossii-ot-29122022-n-1110-ob-utverzhdenii/>.
3. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Информационно-правовой портал «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/71570570/>.
4. Шхагапсоев З. Л. К вопросу о роли органов внутренних дел в предупреждении преступлений, совершаемых с использованием информационных технологий (ИТ-преступлений) // Государственная служба и кадры. 2020. № 2. С. 131–134.

Хотамов М. М.¹,
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

ИНФОРМАЦИОННОЕ ВОЗДЕЙСТВИЕ НА СОЗНАНИЕ ЧЕЛОВЕКА

Информацию стоит рассматривать как ресурсную, реактивную и фоновую.

Ресурсная информация представляет собой необходимую основу для жизни во всех ее проявлениях и для деятельности во всех сферах.

Реактивную информацию можно представить как необходимый компонент любого осмысленного, инстинктивного или рефлексивного поведения – это мысль, версия, образ, основа для принятия решений. Она заряжает энергией поведение и действие и обеспечивает уместность и активность реакций на всех уровнях жизни.

Фоновую информацию стоит рассматривать как отражение окружающей действительности, в легко или трудно воспринимаемой органами чувств форме.

Если рассматривать в простой форме, то информацию получают от скопившегося опыта, от окружающей среды в виде реакции на какой-либо процесс, а также в виде чувств.

Может возникнуть вопрос: как простая информация может воздействовать на человека, и в какой степени она может воздействовать? Ответ правильнее представить оригинальным в виде примера.

Одним из примеров может быть, в котором присутствует сублиминальная реклама [1] или как ее принято называть «25 кадр». Он основан на эксперименте, проведенном ученым Джеймс Викери, который заявил, что провел эксперимент с театральной публикой. Джеймс Викери использовал тахистоскоп – устройство, которое может показывать изображение в течение определенного периода времени – и добавил в него рекламу Coca-Cola и Pop Corn в течение 1/6000 секунды, что привело к увеличению продаж более чем на 58 %. Сюжет из фильма, добавленного в этот период времени, назывался «Секреты рифа» и содержал изображения бренда Coca-Cola.

Может возникнуть мнение, что это всего лишь реклама, но рассматривая следующую пример можно будет понять, что это не всего лишь способ рекламы, а грозное оружие.

¹ © Хотамов М. М., 2024.

В 1997 г. впервые появился на экранах телевидения мультсериал «Покемон! Я выбираю тебя!». С того времени было выпущено более 1000 эпизодов. Производство новых эпизодов не прекращается и по сей день. Иногда выходят полнометражные фильмы, дополняющие и расширяющие сюжет сериала. Данная японская анимация продолжает транслироваться в 169 странах. В 2001 г. в средствах массовой информации появилась даже информация о том, что десятки детей в разных странах были госпитализированы с эпилептическими припадками и неврозами после просмотра 38-го эпизода игры «Покемон». Как утверждалось, причиной стало яркое мерцание экрана, когда Пикачу использовал одну из своих атак – взрыв с красными и синими вспышками. Вспышки длились несколько секунд с частотой около 12 Гц [2].

Это может стать примером, что сублиминальная или фоновая информация, передаваемая на массы, может стать и грозным оружием [3]. В некоторых государствах такой вид рекламы запрещен. И, в частности, на примере в Республике Узбекистан в законе о рекламе дается термин скрытой рекламы [4], которая представлена следующим образом: «скрытая реклама – реклама, которая оказывает неосознаваемое воздействие на восприятие пользователя рекламы путем использования специальных видеовставок (двойной звукозаписи) и другими способами;...».

Информация передается не только путем преобразования электромагнитного излучения в оптическую область, ощущаемого зрительной системой, но и путем восприятия звуков с помощью органов слухового аппарата. Каждый герц, т. е. частота звука, имеет большое значение и воздействует на сознание человека. Более того, бинарные частоты, называемые еще и иллюзионными частотами, возникают в сознание человека, когда в оба уха одновременно поступают сигналы с двумя разными частотами. При этом мозг помимо этих двух частот слышит и третью, которая является разницей этих двух частот. К примеру, если воздействуют две частоты в 120 и 150 герц, то мозг человека слышит еще и 30 герц бинарной частоты [5].

Многие люди верят, что бинауральные ритмы могут вызывать целебные и мистические силы. Эту идею распространил Роберт Монро, бизнесмен, сделавший карьеру в области радиовещания. Он стал известен своими «внетелесными» опытами, написал о них книгу и создал некоммерческую структуру под названием «Институт Монро». Используя этот Институт, он распространял аудиозаписи с применением технологии бинаурального ритма haemisync. Эти аудиозаписи наряду с медитацией, как утверждается, вводят людей в состояние измененного сознания и способствуют «выходу из тела». Все современные аудиозаписи с бинауральными ритмами, как считается, основаны на технологии Монро.

Но и здесь возникает вопрос. С одной стороны, ведь это хорошо, что человек наслаждается такими частотами. А с другой стороны, представьте себе, что будет, если использовать частоты, которые не будут успокаивать человека и давать ему наслаждения, а наоборот раздражать и сделать человека агрессивным? И далее представьте себе массу таких людей...

Если рассматривать воздействие через слуховой аппарат как оружие, то считаю необходимым привести пример разработки проекта, патентованного номером № 4877027 [6]. Начиная с 2003 г., началось финансирование разработки «телепатической микроволновой пушки». В рамках программы «Эффекты контроля» компания Waveband (приобретенная Sierra Nevada в 2005 г.) разработала нелетальное оружие «Медуза» (от англ. сокращения *MEDUSA – Mob Excess Deterrent Using Silent Audio*). Это новое вооружение основано на микроволновом слуховом эффекте. По словам разработчиков, созданная ими перенастраиваемая антенна может генерировать как широкий луч для захвата больших толп людей, так и узкий луч для временного обездвиживания небольших групп людей. Первое использование такого рода оружия было зафиксировано в августе 2014 г. во время пресечения беспорядков в Фергюсоне (штат Миссури, США). Один из жителей заметил излучатель LRAD Model 300X [7], способный создать звуковое давление в 142 дБ, на крыше автомобиля Hummer, используемого полицейскими. По данным экспертов-акустиков, звуки в 120 дБ вызывают у людей болевые ощущения, а звуки в 130 дБ уже повреждают слуховые аппараты.

Список литературы

1. «Покемон! Я выбираю тебя!» Как мир охотился за карманными монстрами. URL: <https://www.gazeta.ru/culture/2022/04/01/14686483.shtml?updated>.
2. Информационно-психологические воздействия. URL: <https://psyfactor.org/psyops/makarenko-503.htm>.
3. Закон Республики Узбекистан «О рекламе». URL: <https://lex.uz/en/docs/6052633>.
4. Аудио наркотики или пустышка: как работают бинауральные ритмы. URL: <https://trends.rbc.ru/trends/social/62692d129a79477fd8d34ec8>.
5. Слуховая система. URL: <https://patents.google.com/patent/US4877027A/en>.
6. Акустическое оружие: мифы и реальность. URL: <https://armystandard.ru/news/20216151111-7AjCF.htm>.

Цимбал В. Н.¹,

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

АКТУАЛЬНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ НЕЙРОННЫХ СЕТЕЙ ПРИ СОВЕРШЕНИИ ПРОТИВОПРАВНЫХ ДЕЯНИЙ

Возможности применения разнообразных информационных технологий (ИТ) обширны, они как облегчают жизнь современного общества, так и создают серьезные препятствия в его нормальном функционировании, что проявляется в использовании ИТ при совершении преступлений.

Статистические сведения из официальных [1], отечественных и зарубежных профильных источников [2–4], показывают, что тренд преступности и различных негативных деяний в информационной сфере не снижается, а только растет год к году. Согласно, Мировому индексу киберпреступности (World Cybercrime Index), наша страна, находится на первых местах [5]. При этом растут и затраты на предотвращение киберпреступлений в мире, так в 2023 г. средняя стоимость утечки данных составила 4,45 млн долларов, а в 2022 г. она была 4,35 млн [6]. И действительно, проблема киберпреступлений подталкивает все государства активно наращивать противодействие им: развивать нормативную составляющую, подготавливать кадры для правоохранительных органов, искать новые пути и средства борьбы, согласовывать свои совместные действия и вырабатывать эффективные методы отпора преступникам через участие в различных международных организациях и иных структурах.

Злоумышленники, в свою очередь, постоянно совершенствуют, придумывают и, к сожалению, успешно реализуют разнообразные преступные деяния: кража данных, вымогательство, шантаж, угрозы определенных негативных действий в отношении жертвы, мошенничество и т. п. Используют они при этом всевозможные средства: сеть Интернет, современные информационно-коммуникационные технологии (ИКТ) (мобильные устройства, планшетные и стационарные компьютеры, специальные технические средства, разработанные для совершения преступлений и т. д.), достижения математики и техники в виде нейронных сетей (далее – НС).

Последние, активно развиваются и применяются в повседневной жизни человека и общества: для распознавания объектов (изображений, голоса, текста), создания новых объектов, поиска информации в поисковых системах в сети Интернет, преобразования данных (речь, изображения, текст), обработке объектов, в научных исследованиях (математика, физика, астрономия, медицина и многих других) [7; 8].

¹ © Цимбал В. Н., 2024.

Как правило, научные исследования ведутся в областях, изучающих: сами НС, особенности их разработки и обучения, возможностей их прикладного применения, специфики выбора, использования в анализе данных [9–13]. При этом, юристы-правоведы, в основном исследуют то, как возможно использовать НС при расследовании и раскрытии преступлений [14–17], что вполне логично.

Нами же, в контексте данной работы, будут исследоваться возможности технологий НС, используемых при совершении киберпреступлений, а конкретно, в кибермошеннических действиях, с точки зрения, их превенции.

Содержание мошенничества, изложено в ст. 159 Уголовного кодекса Российской Федерации (УК РФ). В том же документе, имеется ст. 159.3, касающаяся мошенничества с использованием электронных средств платежа, при этом, что относится к подобным средствам платежа, приведено в п. 19 ст. 3 Федерального закона [18]. Также в ст. 159.6 УК РФ, раскрывается диспозиция мошенничества в сфере компьютерной информации, а именно «...хищение чужого имущества или приобретения права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации или информационно-телекоммуникационных сетей» [19].

При этом, понятие кибермошенничества в уголовном законе не определено. На сайте Московской межрегиональной транспортной прокуратуры, имеется следующее его содержание: «...один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.)» [20]. Приволжская транспортная прокуратура на своем сайте обозначает, что за кибермошенничество уголовная ответственность, предусматривается ст.ст. 159.3 и 159.6 УК РФ [21].

На основании изложенного, приходим к выводу, что указанный вид мошенничества, совершается путем обмана и злоупотребления доверием в киберпространстве, посредством использования и (или) применения ИКТ, с целью хищения личной информации, денежных средств и (или) иного имущества (приобретения права на него), принадлежащего жертве.

Методы совершения кибермошеннических действий различны, это и телефонные звонки, как классические, так и с использованием специализированного программного обеспечения (ПО), например, мессенджеров; побуждение жертвы: на запуск вредоносного ПО, установки поддельного/модифицированного ПО, перехода на поддельный сайт, и т. д. Конечно же, самая эффективная, с точки зрения, результативности – социальная инженерия с ее различными техниками: фишинг, претекстинг, вишинг, фарминг и т. п. При совершении мошеннических действий, злоумышленник пытается ввести в заблуждение жертву и либо получить от нее какие-либо личные данные из цифровых источников, «заставить» произвести манипуляции с цифровыми инструментами или активами.

Для понимания оговоримся, что сами по себе НС не используются преступниками как орудие совершения преступления, они позволяют им произвести манипуляции с какими-либо объектами, например, фотоизображениями, видеозаписями, аудиофайлами, иными электронными данными. Указанные действия состоят либо в их изменении, либо создании новых данных (т. е. их генерации)

при помощи НС. Примером обозначенного, может быть создание и использование в преступных целях технологий – дипфейк, которые, в последнее время, находят свое все большее распространение в мошеннических схемах злоумышленников.

Рассматриваемые технологии также называют искусственным интеллектом (ИИ), однако это не совсем верно, так как ИИ является более широким понятием, которое может включать в себя как отдельную нейросетевую технологию, так и некоторую их совокупность. Однако, вопросы терминологического содержания, их сравнения и иные аспекты, касающиеся ИИ и НС выходят за рамки данной работы, и рассматриваться в ней не будут. Но отметим, что, далее используя термин ИИ, мы подразумеваем, что в нем применяются НС.

Нельзя не упомянуть, что исследования, посвященные нейронным сетям и противоправному их применению при совершении преступлений, также ведутся, к примеру, А. Э. Побегайло [22], В. А. Тирранен [23; 24], И. Н. Масечкин [25] и другими учеными.

Проведя анализ научной литературы; сведений, представляемых компаниями, занимающимися исследованием происходящих в информационной сфере инцидентов, включающих в себя киберпреступления (Positive Technologies, Лаборатория Касперского, Сбербанк и др.); фактов противоправных деяний, которые освещаются в СМИ и иных открытых источниках в сети Интернет, в том числе правоохранительных органов, можно обобщить и привести следующий перечень возможных деяний, где применяются НС:

- мошеннические действия (генерация голоса, изменение фотоизображений, подделка документов);
- создание вредоносного ПО, сайтов и иных ресурсов в глобальной сети;
- поддельные сайты, где НС используются как приманка (т. е. жертва думает, что использует НС для своих личных нужд, а тем самым собираются данные о жертве и после совершается в его отношении противоправное деяние);
- подделка документов (изменение его изображения, генерация новых);
- обработка данных, полученных незаконным путем (похищенные и «слитые» базы и банки данных, содержащие персональные данные, иную информацию, охраняемую законом);
- кибербуллинг (ИИ возможно настраивать таким образом, что он создает иллюзию общения пользователя с другим пользователем, постепенно переходя к оскорблениям жертвы) и т. д.

Использование НС во всем перечисленном, позволяет злоумышленникам реализовывать достаточно успешно свои преступные замыслы, при этом сами НС могут применяться как непосредственный инструмент совершения преступления, так и средство, «упрощающее» либо «помогающее» им их совершать.

Выделим проблемы, с которыми могут сталкиваться правоохранители в попытках выявления подобных преступлений:

- сложно зафиксировать оперативно (как правило разбирательство с противоправным деянием осуществляется после его совершения);

- невозможно мониторить все киберпространство на постоянной основе (тезис также касается профилактики, для реализации подобной меры необходимы колоссальные материальные затраты);

- не разработанность методик либо отсутствие инструментов (в первую очередь, отечественного производства), которые позволяли бы оперативно выявлять и в дальнейшем анализировать (исследовать) измененные нейросетевыми технологиями медиафайлы;

- сложно установить примененные преступниками инструменты (какая именно НС использовалась, одна или несколько, иные особенности их работы);

- практически сложно установить конкретного злоумышленника (работать приходится с результатом противоправного деяния (файлом, сайтом, программой и т. п.) в которых могут не остаться следы действий конкретного преступника).

Таким образом, как видно из обозначенного по тексту выше, НС активно стали применяться в противоправной деятельности, а правоохранительные органы сталкиваются с проблемами, которые довольно существенно затрудняют процессы раскрытия и расследования совершенных киберпреступлений. Однако прекращать активную борьбу с данными разновидностями нарушений закона нельзя, необходимо совершенствовать механизмы их выявления, сбора цифровых следов, изобличения конкретных преступников. Приведем возможные меры профилактики кибермошеннических действий и пути решения данной проблематики в правоохранительной деятельности:

- повышение осведомленности граждан (с точки зрения объяснения, что может использоваться злоумышленниками при совершении ими преступлений, какие действия не следует совершать, о необходимости перепроверять полученную от посторонних лиц информацию, куда обращаться, в случае контакта с преступниками и т. п.);

- увеличение количества профильных специалистов в рядах правоохранительных органов (т. е. лиц, имеющих техническое образование и специальные знания в области науки и техники);

- использование инструментов для защиты от мошенников (например, антивирусное ПО, программы (услуги) по защите от спам звонков, предлагаемых операторами мобильной связи и (или) банковскими организациями);

- подготовка методик по исследованию мультимедийных данных, документов, носителей информации, хранящих следы преступной деятельности с использованием нейросетевых технологий (с целью их изучения и дальнейшего экспертного исследования);

- минимизация размещения в сети Интернет личной информации (так как ее сбор и анализ при помощи НС, позволяет преступникам планировать конкретные действия в отношении жертвы или их групп (родственники, коллеги);

- проведение исследований по применению НС для выявления использования последних и материалов (объектов), в которых они тем или иным образом были применены;

– обязать организации пометать информационные ресурсы (продукты, услуги и т. п.) в которых использовались нейросетевые технологии.

В заключении, хотелось бы отметить, что на современном временном периоде ИТ развиваются настолько стремительно, что практически невозможно спланировать (предположить, продумать) как или по какому пути пойдет это развитие. Тем более сложно спрогнозировать возможности нейросетевых технологий и ИИ в целом, их направления использования при совершении преступлений, однако это не должно останавливать поступательное движение в области превенции и борьбы с высокотехнологической преступностью.

Список литературы

1. МВД России [сайт]. URL: <https://мвд.пф/dejatelnost/statistics>.
2. Global Cybercrime Report : Which Countries Are Most at Risk in 2023? // Seon [сайт]. URL: <https://seon.io/resources/global-cybercrime-report/>.
3. Итоги года 2023 // JetCSIRT [сайт]. URL: https://jetcsirt.su/upload/godovoy_otchet_jet_2023.pdf.
4. Актуальные киберугрозы для организаций: итоги 2023 года // Positive Technologies [сайт]. URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-data>.
5. Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F (2024) Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS ONE 19(4): e0297312. <https://doi.org/10.1371/journal.pone.0297312> [статья]. URL: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0297312>.
6. Cost of a Data Breach Report 2023. URL: <https://www.ibm.com/downloads/cos/E3G53MBP>.
7. Богословский С. Н. Области применения искусственных нейронных сетей и перспективы их развития // Политематический сетевой научный журнал Кубанского государственного аграрного университета. 2007. № 27. С. 228–238.
8. Львов Ф. А. Типы и применение нейронных сетей // Кронос: естественные и технические науки. 2019. № 2 (24). С. 25–31.
9. Казьмин О. Ю., Симонина О. А. Использование нейронных сетей для решения задачи оптимизации электромагнитной обстановки в сетях радиодоступа // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 25–37.
10. Земинов М. А. Изучение работы нейронных сетей: нейронные сети основы, использование нейронных сетей в экономике // Гуманитарные науки в современном вузе: вчера, сегодня, завтра : сборник научных трудов / под ред. С. И. Буганиева, А. С. Манина. – СПб. : Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2019. С. 880–885.
11. Астафьев А. И., Четвериков С. Ф. Применение нейронной сети с направленной активацией нейронных элементов для оценки эффективности лечения гепатита // Надежность и качество : сборник научных трудов. Т. 2. 2016. С. 281–283.
12. Жмуровский К. В. Нейронные сети и как они работают: основные виды и этапы разработки нейронных сетей // Современные тенденции и инновации в науке и производстве : сборник научных трудов. Междуреченск : Кузбасский

государственный технический университет имени Т.Ф. Горбачева, 2023. С. 417.1–417.3.

13. Петросов Д. А. Моделирование искусственных нейронных сетей с использованием математического аппарата теории сетей Петри // Перспективы науки. 2020. № 12 (135). С. 92–95.

14. Смирнов В. М., Агакий Д. А. Использование нейронных сетей при расследовании противоправных деяний // Тенденции развития науки и образования. 2023. № 97-12. С. 105–107.

15. Мулдашев Р. Н., Холопова Е. Н. Использование цифровых профилей личности и нейронных сетей при выявлении и расследовании преступлений // Эксперт-криминалист. 2023. № 4. С. 26–28.

16. Ганжа М. В. Применение нейронных сетей в новых подходах к превенции преступлений // Уголовная политика и культура противодействия преступности : сборник научных трудов. Краснодар : Краснодарский университет МВД России, 2023. С. 375–379.

17. Петрова В. Ю. Прогнозирование преступлений, связанных с легализацией преступных доходов и применением нейронных сетей // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы : сборник статей. М. : Академия управления МВД России, 2018. С. 144–148.

18. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_115625/.

19. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/.

20. Московская межрегиональная транспортная прокуратура [сайт]. URL: <https://epp.genproc.gov.ru/web/mmtп/activity/legal-education/explain?item=69345532>.

21. Приволжская транспортная прокуратура [сайт]. URL: <https://epp.genproc.gov.ru/web/ptп/activity/legal-education/explain?item=73071748>.

22. Побегайло А. Э. Нейронные сети как средство совершения преступления: уголовно-правовая и криминологическая характеристика // Проблемы противодействия киберпреступности : сборник научных трудов. М. : Московская академия Следственного комитета Российской Федерации, 2023. С. 168–172.

23. Тирранен В. А. Преступления с использованием искусственного интеллекта // Развитие территорий. 2019. № 3 (17). С. 10–13.

24. Ерахтина Е. А., Тирранен В. А. Преступления, совершаемые с использованием искусственного интеллекта: проблемы квалификации и расследования // Вестник Сибирского юридического института МВД России. 2019. № 2 (35). С. 36–41.

25. Масечкин И. Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10. № 3. С. 461–476.

Чеканов И. Р.¹,

*аспирант кафедры информационных технологий,
искусственного интеллекта и общественно-социальных
технологий цифрового общества
Российского государственного социального университета*

Краев И. В.²,

*студент кафедры информационных технологий,
искусственного интеллекта и общественно-социальных
технологий цифрового общества
Российского государственного социального университета*

Молоканова Б. Б.³,

*студент кафедры информационных технологий,
искусственного интеллекта и общественно-социальных
технологий цифрового общества
Российского государственного социального университета*

ИСПОЛЬЗОВАНИЕ ГРАФОВЫХ СТРУКТУР ДЛЯ ВИЗУАЛИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном мире информационная безопасность (ИБ) становится одним из ключевых аспектов деятельности организаций и государства. В связи с активным развитием технологий и увеличением объема нормативных и законодательных актов, эффективный анализ и их применение становится все более затруднительной, но при этом первостепенно значимой задачей.

Для специалистов в области информационной безопасности актуальным вопросом является анализ и эффективное применение обширной базы нормативных и законодательных документов. Данные о правовых нормах и требованиях в области информационной безопасности необходимы для выполнения установленных и регламентированных процедур в процессе обеспечения защиты информации.

Предложенный метод группировки и использования графовых структур для систематизации, упорядочения и визуализации документов в области информационной безопасности позволяет организовать документы, отразить связи между элементами и в результате упростить процесс работы специалистов и руководителей структурных подразделений области ИБ.

Результаты исследования могут быть использованы для построения базы данных (БД) экспертных информационно-аналитических систем (ЭИАС), что значительно улучшит работу специалистов и повысит эффективность управления информационной безопасностью.

¹ © Чеканов И. Р., 2024.

² © Краев И. В., 2024.

³ © Молоканова Б. Б., 2024.

Целью данного исследования является разработка метода группировки и использования графовых структур для систематизации, упорядочения и визуализации документов в области информационной безопасности.

Для достижения цели исследования сформулированы следующие задачи:

1. Провести анализ существующих подходов к систематизации данных в области информационной безопасности.
2. Предложить подход к группировке и использованию графовых структур для организации информации в базе данных.

В процессе исследования будет использовано комбинирование методов анализа и синтеза, а также статистический и компьютерное моделирование. Будет проведено сравнительное исследование различных методов систематизации и визуализации данных, для определения наиболее эффективного подхода. В дальнейшем будет создан прототип информационно-аналитической системы на основе разработанного метода, и проведена апробация на реальных данных. Также будет проведено исследование эффективности и практической ценности метода с помощью сравнительного анализа результатов работы системы.

Инструменты работы с данными

При работе с документами в области ИБ специалисты часто обращаются к различным инструментам. Например, справочными системами, перечнями и другими открытыми данными.

Справочно-правовые системы, такие как «КонсультантПлюс», «Гарант» и др., являются одним из наиболее широко известных и активно применяемых инструментов данного типа [1]. Они позволяют осуществлять точный поиск необходимой информации на основе актуализируемой базы данных и предоставлять широкий набор документов. Однако недостатком справочных систем является отсутствие структурированного подхода к анализу документов.

Перечни документов, такие как «Справочник законодательства Российской Федерации в области информационной безопасности» [2], предоставляют практическую полноту и актуальность информации. Они помогают ориентироваться в нормативных актах, но могут быть неудобными для поиска документов по содержанию из-за ограничения организации в виде списка наименований.

Карта законодательства в области информационной безопасности отражает иерархию законов и нормативных актов, что помогает легко находить связи между ними [3]. Однако у карты законодательства также есть определенные недостатки, относящиеся к возможностям поиска и ориентирования в законодательстве.

Итак, для эффективной работы со справочными системами, перечнями документов и картой законодательства в области информационной безопасности необходимо учитывать их преимущества и недостатки, чтобы организовать наиболее удобный и комплексный подход для решения поставленной задачи.

Анализ данных

Определение подхода в структуризации данных зависит от выявления объема и специфик данных. Подобное исследование в области информационной безопасности является сложной задачей, требующей анализа и отбора соответствующих документов законодательной и нормативной базы Российской Федерации.

Согласно проведенному исследованию [4] количество документов данной области составляет порядка 383 шт.

На основе результатов, определения основных юридических групп документов и выявления ключевых семантических составляющих элементов базы данных, можно заключить, что документы отражают различные специфики, направления и области деятельности специалистов в области ИБ. Обобщение семантических данных и группирование документов может содержать уникальные правила, требования и рекомендации, направленные на обеспечение безопасности информации в конкретных сферах деятельности.

Структурирование данных

Опираясь на анализ результатов научных работ, отобранные ключевые семантические данные и перечень документов, можно определить структуру групп и подгрупп для дальнейшей структуризации:

1. «Информация» (54 документа):
 - 1.1. Информация ограниченного доступа.
 - 1.2. Общедоступная информация.
 - 1.3. Информация, доступ к которой не может быть ограничен.
2. «Защита информации» (131 документ):
 - 2.1. Физическая защита.
 - 2.2. Аппаратная защита.
 - 2.3. Программная защита.
 - 2.4. Организационная защита.
 - 2.5. Психологическая защита.
 - 2.6. Правовая защита.
3. «Аудит» (27 документов):
 - 3.1. Аттестация аппаратно-программных комплексов.
 - 3.2. Внутренний аудит.
 - 3.3. Внешний аудит.
4. «Контроль» (91 документ):
 - 4.1. Контроль доступа.
 - 4.2. Контроль сети.
 - 4.3. Контроль политик и процедур.
 - 4.4. Контроль событий.
 - 4.5. Контроль защиты информации.
5. «Управление» (54 документа):
 - 5.1. Управление рисками.
 - 5.2. Управление программами безопасности.
 - 5.3. Управление ресурсами.
 - 5.4. Управление персоналом.
 - 5.5. Управление инцидентами.
6. «Угрозы» (91 документ):
 - 6.1. Модель угроз.
 - 6.2. Модель нарушителя.
 - 6.3. Вредоносное программное обеспечение.
 - 6.4. Сетевые атаки.

Количество указанных документов определялось путем поиска наименований категорий и подкатегорий составленных групп. Следует отметить, что документы могут относиться к нескольким категориям. На основе данной особенности формируются связи между документами.

Построение графовых структур

Отдельным вопросом является преобразование подготовленного материала под визуализируемые объекты.

Структурирование и представление групп позволяет пользователям ориентироваться на обобщенные понятия в области информационной безопасности и находить требуемые документы Российской Федерации.

При построении графовых структур для перечня групп в области информационной безопасности, каждая подгруппа будет представлена в виде объекта круговой формы, обозначаемой в соответствии с номерами подпунктов структуры, а связи между элементами групп и подгрупп – линиями.

Например, связи основных групп можно представить следующим образом (рис.).

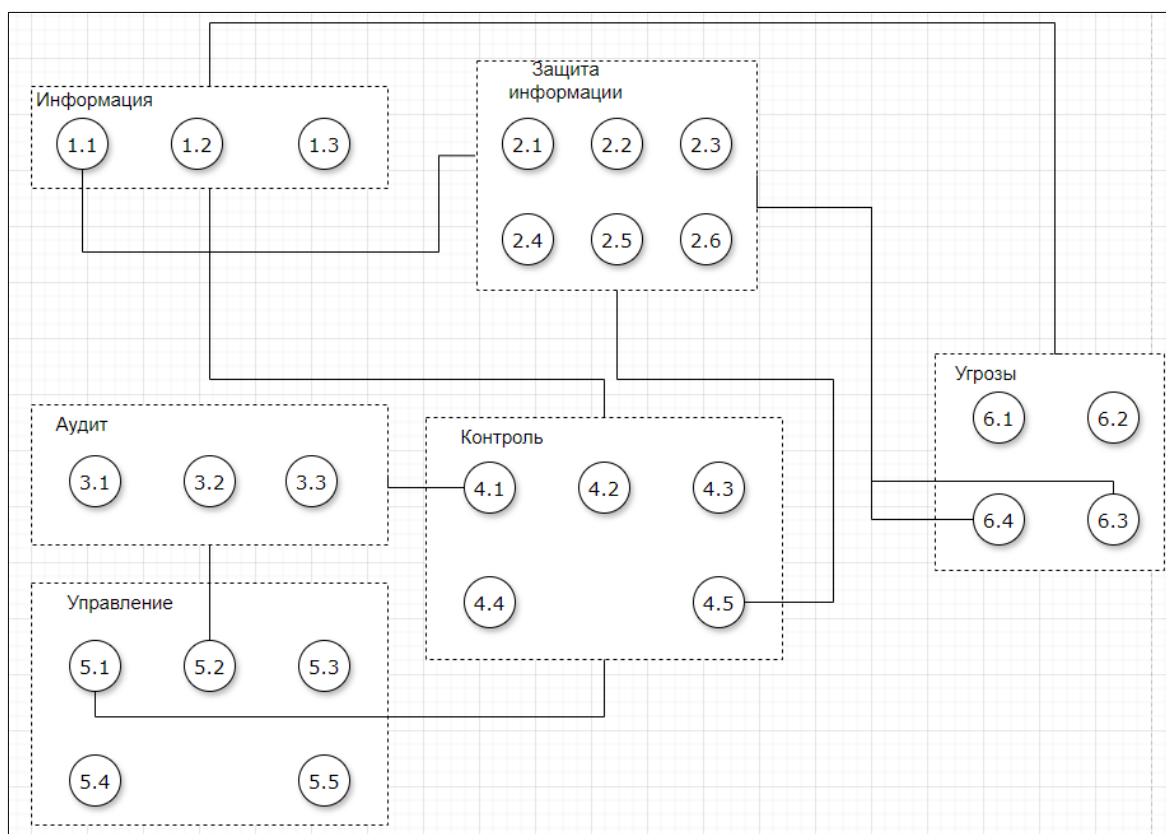


Рис. Графовая структуризация

1. «Информация»:

Связана с:

- «Защита информации»;
- «Контроль»;
- «Угрозы».

2. «Защита информации»:

Связана с:

- «Информация» (подблок «Информация ограниченного доступа»);
- «Контроль» (подблок «Контроль защиты информации»);
- «Угрозы» (подблок «Вредоносное программное обеспечение»).

3. «Аудит»:

Связан с:

- «Контроль» (подблок «Контроль доступа»);
- «Управление» (подблок «Управление программами безопасности»).

4. «Контроль»:

Связан с:

- «Защита информации» (подблок «Контроль защиты информации»);
- «Управление» (подблок «Управление рисками»).

5. «Управление»:

Связан с:

- «Контроль» (подблок «Управление рисками»).

6. «Угрозы»:

Связан с:

- «Защита информации» (подблок «Вредоносное программное обеспечение»).

Из анализа взаимосвязей можно сделать вывод о том, что каждая группа занимает определенную роль в обеспечении безопасности информации. Полученная структура позволяет отразить целостную картину взаимосвязей групп и подгрупп выявленных направлений в области ИБ.

Таким образом, графовая структуризация взаимосвязей между блоками является ключевым элементом для разработки реляционных таблиц базы данных и отражает особенность взаимодействия частных подгрупп и целых групп документов.

В ходе проведенного исследования анализ используемых инструментов для работы с документами в области ИБ отразил отсутствие и высокую актуальность структурированности документов в области информационной безопасности, что позволило применить метод группировки и использования графовых структур для систематизации, упорядочения и визуализации элементов БД. Применяемый подход позволит организовать информацию в группы, отразить связи между элементами реляционных таблиц БД.

Результаты исследования привели к структуризации данных законодательной и нормативной базы Российской Федерации в области информационной безопасности и определению ключевых взаимосвязей групп и подгрупп элементов.

Дальнейшее развитие данного метода может привести к созданию более сложных связей документов в области ИБ и модернизации разработанной экспертной информационно-аналитической системы [5], способствующей более эффективному анализу и управлению информационной безопасностью.

Список литературы

1. Современные тенденции в развитии коммерческих компьютерных справочно-правовых систем / [В. В. Филатов и др.] // Журнал прикладных исследований. 2022. № 6. URL: <https://cyberleninka.ru/article/n/sovremennye-tendentsii-v-razvitii-kommercheskih-kompyuternyh-spravочно-pravovyh-sistem>.
2. Справочник законодательства Российской Федерации в области информационной безопасности (версия 04.04.2024) // Хабр–2024. URL: <https://habr.com/ru/post/432466/>.
3. Базовая карта законодательства Российской Федерации по защите информации и как ей пользоваться // Хабр–2024. URL: <https://habr.com/ru/companies/bastion/articles/595215/>.
4. Чеканов И. Р., Краснов А. Е. Анализ семантических элементов базы данных экспертной системы для работы с законодательными и нормативными документами в области информационной безопасности // Проблемы управления безопасностью сложных систем : сборник научных трудов / под общ. ред. А. О. Калашникова, В. В. Кульбы. М. : Институт проблем управления имени В.А. Трапезникова РАН, 2022. С. 221–225.
5. Свидетельство о государственной регистрации программы для ЭВМ № 2023667310 Российская Федерация. Фемида : № 2023665111 : заявл. 19.07.2023 : опубл. 14.08.2023

Чубанова Е. И.¹,
*студент юридического факультета
Российской таможенной академии*

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

История регулирования искусственного интеллекта (ИИ) начинает свой отсчет с 1942 г. и выработки трех законов робототехники Айзека Азимова [1]:

1. Робот не может своими действиями или бездействием причинять вред человеку.

2. Робот должен выполнять приказ человека, если они не противоречат первому закону.

3. Робот должен защищать самого себя, пока такая защита не противоречит первому или второму законам.

Эти «законы» научной фантастики не могут считаться ни нормами, ни правовыми принципами.

Однако они играют важную роль для правового регулирования, поскольку Айзек Азимов – первый, кто выразил идею возможности установления правил поведения не только для людей и предложил прогрессивную концепцию человекоориентированного подхода к регулированию ИИ. Международное сообщество едино в стремлении обеспечить соблюдение прав человека путем установления эффективного правового поля для ИИ, однако стратегии его развития отличаются на европейском и американском континентах [3, с. 40]. Следует отметить, что правильный выбор стратегии и регуляторного подхода помогает сбалансировать преимущества и риски и добиться цели правового регулирования.

Стоит согласиться с профессором Дэвидом Эдельманом, что очевидна необходимость правового регулирования ИИ, ведь человечеству уже известно о предупреждениях и дефектах наносящих или способных наносить ущерб при использовании. Зато неочевиден ответ на вопрос: «как регулировать?». В одном из выпусков Washington Post профессор отметил, что важно регулировать технологии ИИ «такими, как они есть», т. е. так, как его действительно используют и решать практические вопросы разработки и применения, а не как явление, оторванное от контекста [1].

По этому поводу другой профессор Томас Вишмейер, анализируя особенности сферы ИИ, в частности неумолимую скорость технологических изменений, развитие новых сфер деятельности и бизнес-моделей, а также изменения в обществе, связанные с каждой из них, считает, что регуляторные нормы должны соответствовать балансу таких критериев как определенность, четкость и упругость.

С одной стороны, сфера ИИ должна определять правила поведения, чтобы отвечать на существующие риски, однако в то же время не должна быть слишком ограничительной и сдерживать развитие технологий, с другой быть достаточно

¹ © Чубанова Е. И., 2024.

адаптивной к динамическому развитию технологий. Это мнение отражает всю сложность обеспечения эффективной правовой регламентации ИИ. Профессор Оксфордского университета Кристофер Деккер выделяет два подхода к правовому регулированию – нормативный (rule based) и целевой (goal based) [2].

Нормативный подход подразумевает установление четких правил поведения, общеобязательных предписаний, подробных инструкций для уполномоченных органов. Целевое регулирование состоит в установлении принципов, стандартов с целью достижения результатов правового регулирования. Этот подход не определяет четкие функции и задачи субъектам права, он стимулирует их действовать с целью достижения определенных целей.

Виртуализация части жизнедеятельности человека неизбежна, а виртуальным миром и повседневной жизнью в ближайшем будущем полностью сможет заниматься искусственный интеллект, более осознанный, чем человек. ИИ как электронная личность, по мнению ученого, может быть наделен способностью осознавать общественную опасность своего действия или бездействия и их последствий, управлять своим поведением, поэтому вполне может быть признан субъектом преступления.

Однако такие изменения станут реальными лишь при условии переработки всей системы криминального права.

Ф. Коста и А. Каррано отмечают, что проблемы защиты интеллектуальной собственности в контексте применения искусственного интеллекта в основном связаны с двумя аспектами: обеспечение свободы действий при использовании искусственного интеллекта без нарушения интеллектуальных прав третьих лиц и защита инвестиций в исследовании и разработке в сфере использования искусственного интеллекта [1].

Итак, учитывая комплексность понятия и динамичность развития технологий ИИ, а также с учетом высоких рисков отдельных технологий можно предложить поэтапную концепцию правового регулирования.

I этап. Стратегический. Он предусматривает применение целевого подхода – определение принципов и стандартов правового регулирования. Принципы регулирования искусственного интеллекта обеспечат системность, предотвратят неопределенность, непоследовательность законодательных органов в регулировании ИИ и будут стимулировать инновационное развитие технологий. Именно такие преимущества целевого подхода к регулированию ИИ выразил главный директор по технологиям США Майкл Крациос [4, с. 81].

Несмотря на критику «принципиального регулирования» из-за его общности и неконкретности стоит согласиться с мнением Линн Паркер, заместителя главного директора по технологиям США.

Она считает, что принципы ИИ необходимо определять слишком широко, чтобы охватить все технологии ИИ и одновременно оставить дискрецию каждому ведомству создавать нормы для конкретного сектора и технологии.

Важным аспектом целевого регулирования является создание механизмов контроля за их соблюдением. Это ответ на критику о «вялости» целевого регулирования. Например, в США федеральные ведомства обязаны подавать

в Управление научно-технической политики Белого дома меморандумы, в которых обосновывают соответствие определенного нормативного акта определенным принципам. Такой механизм позволяет Управлению Белого дома, не имея нормативной функции, осуществлять надзор и координацию за регуляторными органами. Зато в ЕС огромное количество рекомендаций, предложений, стратегий имеет характер «мягкого права» [2].

Определение принципов правового регулирования можно приравнять к установлению «регуляторного решета», которое просеивает и отсеивает нормативно-правовые акты, не соответствующие государственной политике в сфере ИИ. Это контроль качества. Именно так охарактеризовал значение «принципиального регулирования» Р. Дэвид Эдельман, политик и ученый, директор Проекта по технологиям, экономике и национальной безопасности Массачусетского технологического института [1].

II этап. Нормативный. Определив индикаторы качества и введя механизмы контроля можно переходить к следующему уровню регулирования. Принятие законодательных актов, которые учитывают особенности и риски конкретных технологий, определение уполномоченных органов и их функций.

В контексте применения нормативного подхода регулирования, стоит согласиться с мнением профессора Томаса Вишмеера о возможности применения действующего законодательства к регулированию ИИ [2]. В частности он считает, что применение технологий ИИ в разного рода общественных отношениях обуславливает возможность частичного регулирования и ИИ соответствующими нормами гражданского, хозяйственного, уголовного и международного права без их «диджитализации», однако для полноценного обеспечения правового поля в сфере ИИ необходимо специальное законодательство. Стоит учесть мнение профессора Оксфордского университета Кристофера Деккера о необходимости применения нормативного подхода к технологиям с высокими рисками [4, с. 80].

Поэтому параллельно с внедрением стратегического этапа необходимо принять нормативные акты, регулирующие технологии систем автономного вооружения. В этой сфере необходима точность считает Томас Метцингер, профессор философии Университета Майнца и член Экспертной группы по вопросам ИИ [1]. Он критикует европейский Кодекс этических принципов из-за отсутствия четкой позиции относительно использования автономного летального оружия - запрещено. В окончательном тексте применение таких смертоносных технологий определяется как «критическая проблема». Такой поэтапный процесс регулирования обеспечит системность, скоординированность действий различных органов.

Предварительно определенная система принципов предотвратит риск чрезмерного регулирования отрасли, а также будет заполнять пробелы нормативного регулирования (которые обязательно будут возникать в связи с динамикой развития технологий ИИ).

Таким образом, можно сделать вывод, что на практике «чистые» версии подходов к правопониманию отношений с ИИ почти не существуют, обычно это «гибридные» подходы, сочетающие элементы обоих с превалированием первого или второго. Поэтому, указывая на нормативный подход, будем понимать, что

предусматривает примат нормативного регулирования над целевым. Далее рассмотрим существующие тенденции, сложности и модели правосубъектности ИИ. Перечислим используемые подходы и тенденции по вопросу наделения юнита ИИ правосубъектностью.

Список литературы

1. Искусственный интеллект и право: есть контакт? URL: <https://www.garant.ru/news/1401154/>.
2. Путин заявил о необходимости цифровой трансформации России. URL: <https://tass.ru/ekonomika/10172635>.
3. Родикова В. А. Искусственный интеллект vs судебское усмотрение: доверять нельзя проверять. Перспективы и риски автоматизации судебной практики // Вестник арбитражной практики. 2023. № 3. С. 37–50.
4. Соменков С. А. Искусственный интеллект: от объекта к субъекту? // Вестник Университета имени О.А. Кутафина. 2019. № 2 (54). С. 78–89.

Чурин Р. А.¹,

*главный эксперт отдела компьютерных
и радиотехнических экспертиз
управления экспертиз цифровой и речевой информации
Экспертно-криминалистического центра МВД России,
преподаватель кафедры информационной безопасности
учебно-научного комплекса информационных технологий
Московского университета
МВД России имени В.Я. Кикотя*

ОСОБЕННОСТИ ИССЛЕДОВАНИЯ НОВЕЙШИХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Исключение человека из трудоемких или опасных операций позволяет повысить безопасность, удешевить и ускорить технологические процессы. Специальная военная операция, начавшаяся в 2022 г., продемонстрировала всему миру актуальность дронов и по факту стала триггером для начала научно-технической революции в сфере беспилотных и роботизированных систем. Не согласиться или не заметить это уже невозможно.

С этим прогрессом беспилотные летательные аппараты (БПЛА) надежно закрепились как объект криминалистического исследования. Ежедневно назначаются экспертизы по фактам их целевого применения, отрабатываются материалы, где еще не взлетевший дрон является орудием совершения противоправных действий.

Чаще всего БПЛА представляют из себя специальный аппарат, отдельные элементы которого или сам корпус создают подъемную силу, присутствует силовая установка, а также электронная начинка, отвечающая за получение информации, управление полетом и бортовыми системами. Необходимо обратить внимание, что в новейших дронах современные технологии и материалы все чаще отходят в сторону, уступая место наиболее быстрому и дешевому процессу производства, например, это поверхности из пенопласта и использование сантехнических изделий в качестве основы летательного аппарата.

В отличие от наружных частей электронная начинка новейших дронов претерпела множество кардинальных изменений. Она по-прежнему может быть как централизованной, когда за управление всех систем отвечает один контроллер, так и децентрализованной, когда имеется несколько самостоятельных бортовых систем.

В электронных системах БПЛА может содержаться следующая информация:

- полетные данные (маршрут летательного аппарата);
- журнал команд управления (логирование полученных управляющих команд);
- сведения о местоположении (точка запуска, расположение оператора, «домашняя» точка, цель);

¹ © Чурин Р. А., 2024.

- информация, полученная в ходе полета (видео-, фото-, термография, спектрограмма радиообстановки, полетная информация и др.);
- данные транспондера или радиолокационного ответчика (в некоторых случаях передают в эфир бортовой номер, заводской номер транспондера, высоту полета, скорость и географические координаты);
- информация, формируемая электронными блоками силовой установки (серийные и заводские номера, комплектация, дата сборки или программирования, периоды использования, диагностические коды неисправностей и т. д.).

Наиболее часто встречаются следующие полетные контроллеры БПЛА:

1. Специализированные контроллеры на базе «ArduPilot».

Универсальные контроллеры, применяемые для всех типов беспилотных аппаратов (летательные вертолетного, коптерного и самолетного типов, надводные, подводные, наземные, комбинированные и даже стационарные системы поддержки дронов). Сам по себе «ArduPilot» - система управления беспилотными аппаратами с открытым программным кодом. В основе этих контроллеров чаще всего «STM32», но могут встречаться контроллеры «Arduino», одноплатники на основе «Intel», «Qualcomm» и др. (рис. 1).



Рис. 1. Специализированные контроллеры на базе «ArduPilot»

Наиболее эффективным для получения криминалистической информации из контроллеров «ArduPilot» является программное обеспечение «MissionPlanner», также могут применяться программы «QGround Control», «Matlab» и другие.

2. Полетные контроллеры на базе «Raspberry Pi» и его аналогах (рис. 2).



Рис. 2. Полетные контроллеры на базе «Raspberry Pi»

«Raspberry Pi» – одноплатный компьютер на аппаратной платформе ARM v6 – v8. Изначально разрабатывался британской компанией «Raspberry Pi Foundation» как бюджетная система для обучения информатике и робототехнике, однако сегодня находит повсеместное применение в качестве основы вспомогательных систем (домашние сервера, медиа центры, контроллеры управления умным домом и т. д.). Использует установленную на внешний накопитель информации (USB-флеш-накопитель или карту памяти) операционную систему Linux (чаще всего Debian и Raspberry Pi OS). Кроме того, получили распространение специализированные прошивки, позволяющие использовать «Raspberry Pi» в качестве полетного контроллера. В этом случае накопитель информации может отсутствовать, а все данные дрон получает однократно после включения, либо управляется дистанционно.

Необходимо отметить, что «Raspberry Pi» может применяться на борту БПЛА для обеспечения вспомогательных функций (например, навигация или обработка и трансляция видеосигнала) и не являться управляющим элементом.

Для общего анализа информации наиболее эффективен «Magnet Axiom», при этом надо учитывать различные форматы хранения координат местоположения.

3. Полетные контроллеры на базе «ESP32» (рис. 3).

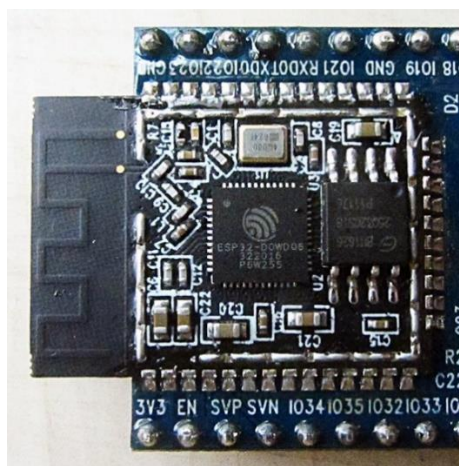
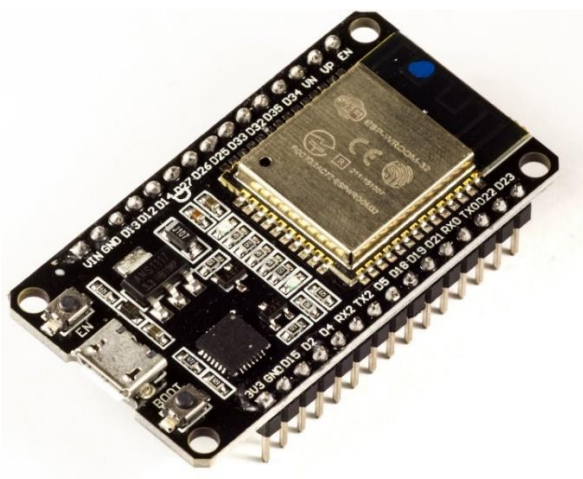


Рис. 3. Полетные контроллеры на базе «ESP32»

«ESP32» – серия недорогих микропроцессоров с малым энергопотреблением. Выпускаются фирмой Espressif Systems, КНР. Отличаются наличием интегрированных контроллеров радиосвязи (Wi-Fi, Bluetooth, Thread). Эти одноплатные компьютеры китайского производства являются прямым наследником ESP8266, ставшим популярным в качестве альтернативы Arduino. Чаще всего их можно встретить в системах умного дома, приборах учета или детских электронных конструкторах.

В беспилотниках такие контроллеры стали популярны благодаря своей низкой стоимости, а также простой системе программирования. Как правило используются в паре с хорошими приемниками. В целом они показали свою низкую эффективность и сегодня вероятность повстречаться с дроном, управляемым ESP32 стремиться к нулю.

4. Специализированные полетные контроллеры на платформе STM32 (рис. 4).

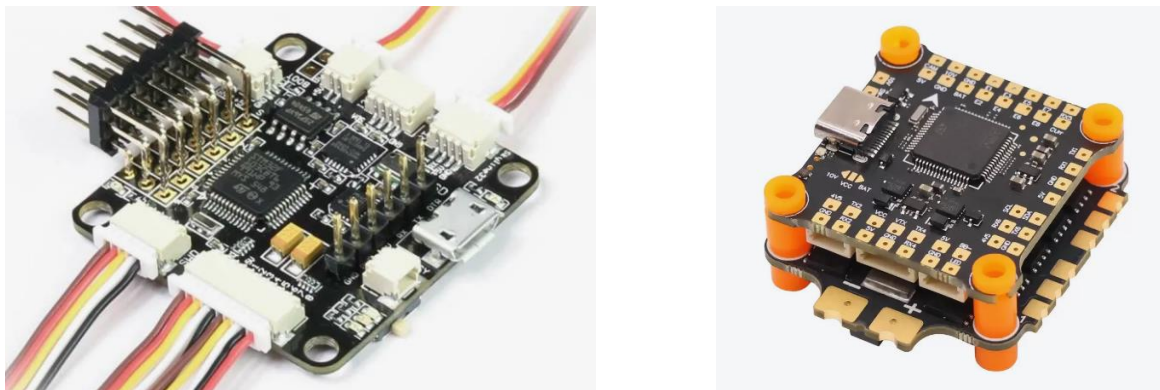


Рис. 4. Специализированные полетные контроллеры на платформе STM32

Производители таких контроллеров развиваются с огромной скоростью и демонстрируют новые модели с периодичностью в несколько месяцев, что обычно не свойственно для изготовителей электроники. Такие контроллеры наиболее распространены в FPV-дронах. Особенностью их аппаратной реализации является размещение полетного задания в оперативной памяти. БПЛА с таким полетным контроллером содержит только загрузчик (bootloader), а полетную информацию получает при подключении пульта дистанционного управления или смартфона. Соответственно получение полетных данных в рамках экспертизы невозможно.

5. Полетные контроллеры БПЛА марки DJI (рис. 5).

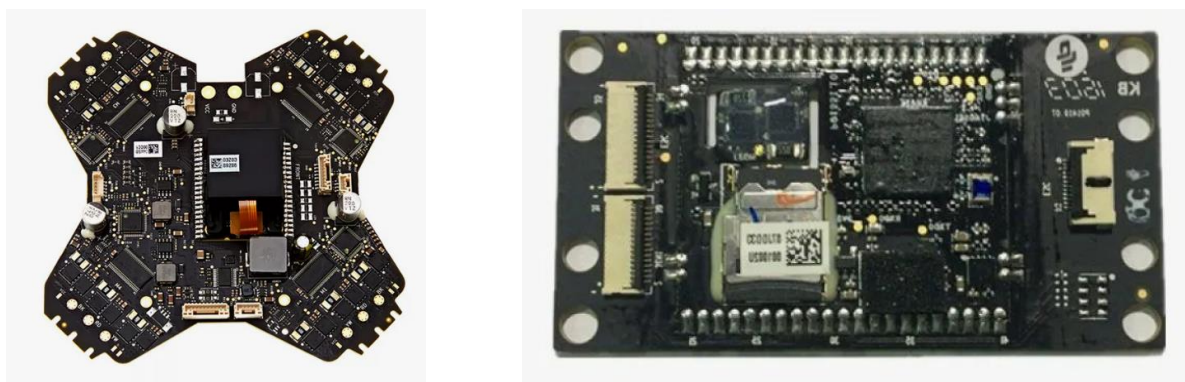


Рис. 5. Полетные контроллеры БПЛА марки DJI

Производятся китайской частной компанией «SZ DJI Technology Co., Ltd», являющейся основным новатором в сфере летающих дронов. Для извлечения информации из контроллеров БПЛА «DJI» производителем предусмотрено программное обеспечение «DJI Assistant 2». Анализ извлеченной информации можно осуществлять с помощью ПО «Мобильный криминалист», «UFED Physical Analyzer» и другие. Стоит отметить, что при определенных настройках БПЛА информация при извлечении будет шифроваться. Решение для обхода шифрования в настоящее время не найдено.

Помимо полетных контроллеров значимую информацию, могут содержать пульты дистанционного управления (далее – ПДУ), подключенные к ним смартфоны, а также карты памяти, установленные в летательных аппаратах.

На основе проведенного анализа и опыта криминалистического исследования БПЛА, можно выделить пять типовых вопросов, выносимых перед экспертом:

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. В большой степени все эти задачи решает судебная радиотехническая экспертиза. Сегодня большинство экспертно-криминалистических подразделений в системе МВД России занимаются таким видом экспертиз. Региональные подразделения оборудованы специализированной радиотехнической лабораторией – комплекс для исследования радиоэлектронных устройств «Удовольствие» (ЗАО «РНИЭЦ», г. Санкт-Петербург).

Отдельно стоит указать на необходимость соблюдения мер личной безопасности при исследовании БПЛА: они могут содержать взрывоопасные вещества (неразорвавшиеся боеприпасы, элементы самоликвидации, мины-ловушки и т. д.); ядовитое топливо, а также средства радиоэлектронной борьбы, уровень сигнала которых превышает предельно допустимые нормы.

Таким образом, в связи с увеличением количества случаев применения БПЛА в криминальных целях, необходимо продолжить анализ их представления в качестве объектов экспертиз, а также изучить вопрос оснащения экспертно-криминалистических подразделений системы МВД России специализированным оборудованием. Необходима разработка методических рекомендаций по исследованию БПЛА для использования при производстве радиотехнических экспертиз и исследований.

Список литературы

1. Авиация : энциклопедия / гл. ред. Г. П. Свищёв. М. : Большая Российская энциклопедия, 1994.
2. Завалов О. А., Маслов А. Д. Современные винтокрылые беспилотные летательные аппараты : учебное пособие. М. : МАИ-Принт, 2008.
3. Мартин Д. Дроны: первый иллюстрированный путеводитель по БПЛА. М. : Эксмо, 2018.
4. Шеваль В. В. Беспилотные летательные аппараты как носители оборудования комплексных систем наблюдения / под ред. М. Н. Красильщикова. М. : МАИ-Принт, 2010.

5. Методика исследования объектов радиотехнической экспертизы : методика / [В. М. Щербак и др.]. М. : Экспертно-криминалистический центр МВД России, 2019.
6. Чурин Р. А. Особенности исследования беспилотных летательных аппаратов // Информационные технологии в деятельности органов внутренних дел : сборник научных трудов. М., 2023. С. 51–54.

Чурина С. Р.¹,

бизнес-аналитик отдела развития систем менеджмента

АО «Концерн “Калашников”»,

магистрант кафедры

«Системный анализ и управление»

Ижевского государственного технического университета

имени М.Т. Калашникова

ПРИМЕНЕНИЕ НОРМ КОНТРОЛЯ К БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ

Проведение осмотра самолета – критически важный аспект для обеспечения безопасности полётов и продления срока службы воздушного судна. Регулярные проверки помогают выявить потенциальные проблемы на ранней стадии, предотвратить возможные аварии и отказы. Это также помогает поддерживать высокую эффективность и надежность самолета, что напрямую влияет на комфорт и безопасность пассажиров.

Большинство разработанных в авиации мер контроля могут быть приняты с небольшими правками для беспилотных летательных аппаратов (БПЛА). Рассмотрим основные методы проверки самолетов на земле, затем сравним их с методами проверки БПЛА.

Виды проверки авиационных судов:

1. Транзитная проверка (transit check).

Одна из самых простых проверок которая выполняется регулярно. Суть проверки заключается в визуальном осмотре судна на наличие механических повреждений таких как царапины, вмятины, трещины. При осмотре проверяется весь самолет и все его видимые конструкции. Осмотр судна совершают и техники, и капитан перед вылетом. В случае выявления отклонений при проведении данной проверки все нарушения устраняются на месте, если устранить дефект на месте не является возможным, командир воздушного судна и авиакомпания принимают решение о смене самолета.

2. Ежедневный технический осмотр.

Данный вид проверки выполняется один раз в 24–36 часов. Так же, как и в предыдущем пункте проводится внешняя проверка самолета на наличие механических повреждений, а также происходит проверка уровня всех жидкостей в системах и аварийного оборудования. Данную проверку проводят только техники. Если в ходе проверки выявили нарушения, то судно отправляют на тех обслуживание для устранения несоответствий.

3. Еженедельный технический осмотр.

Данный вид контроля выполняется один раз в 7–10 дней, занимает примерно пять часов времени. На данном этапе помимо внешней проверки самолета на наличие механических повреждений, проверяются:

¹ © Чурина С. Р., 2024.

- технические жидкости, которые доливают, либо заменяют при необходимости;

- электронные бортовые устройства на работоспособность.

В случае обнаружения несоответствия, судно отправляют на станцию технического осмотра до устранения нарушений.

Так как самолет устройство, состоящее из множества частей, визуальный контроль – это начальный уровень проверки судна. Далее проводятся более серьезные проверки самолета и всех его систем с применением специальных приборов.

4. A-check.

Данная проверка проводится каждые 500–800 часов налета, в зависимости от возраста самолета. Данный вид осмотра занимает от 10 до 50 часов, при этом происходит проверка:

- конструкций самолета для выявления каких-либо коррозий, деформаций, отсутствующих частей или повреждений;

- светотехнического оборудования;

- гидравлической системы;

- системы кондиционирования воздуха;

- системы управления закрылками;

- тормозов и стояночной системы.

Проверка судна может проводиться раньше или позже установленных пяти-сот часов налета. Решение зависит от конкретной модели, условий эксплуатации, а также его возраста. Выявленные отклонения сразу устраняются.

5. B-check.

Данная проверка проводится каждые три-шесть месяцев, в зависимости от количества проверок A-check и от возраста судна. В среднем B-check занимает 150–180 человеко-часов, это около трех дней, при этом проводятся проверки, устраняются неисправности.

6. C-check.

Проверка судна осуществляется примерно каждые два года, но может происходить и раньше, в зависимости от модели и возраста самолета. Происходит осмотр, проверка и, при необходимости, замена всех компонентов и систем самолета. По длительности проверка занимает не более трех недель, это около 600 человеко-часов. Все неисправности устраняются на месте.

7. D-check.

Самая длительная и энергоемкая проверка, которая затрагивает все устройства самолета. При D-check происходит полный разбор судна, замена некоторых частей самолета. Сам самолет проверяется разными видами дефектоскопии на наличие трещин, либо усталостных напряжений. Периодичность данной проверки каждые 6–12 лет, а длительность самого осмотра и ремонта может длиться три месяца.

Благодаря проведению подобных проверок пассажиры и экипаж могут быть уверены в работоспособности и безопасности самолетов. Что касается БПЛА, то данные методы могут быть применимы, однако длительность проверок будет

намного меньше. Разберемся подробнее и сравним методы проверок для беспилотных летательных аппаратов и самолетов в табл.

Таблица

Сравнение методов проверки

	Самолет	БПЛА
Транзитная	Визуальный осмотр на наличие повреждений	Визуальный осмотр на наличие повреждение и каких-либо загрязнений
Ежедневная	Визуальный осмотр на наличие повреждение, проверка всех технических жидкостей	Визуальный осмотр на наличие повреждений и каких-либо загрязнений. Чистка дрона
Еженедельная	Визуальный осмотр на наличие повреждение, проверка и доливка всех технических жидкостей	Визуальный осмотр на наличие повреждений и каких-либо загрязнений. Чистка дрона. Проверка всех деталей и узлов
A-check	500–800 часов налета. Проверка всех конструкций	50 часов налета. Осмотр всех конструкций
B-check	3–6 месяцев. Проверка всех конструкций. При необходимости замена некоторых частей	2 месяца. Осмотр всех конструкций, чистка загрязнений, проверка аккумуляторных батарей. При необходимости, замена некоторых узлов, обновление ПО
C-check	2 года. Происходит осмотр, проверка и, при необходимости, замена всех компонентов и систем самолета	3 месяца. Осмотр всех конструкций, чистка загрязнений. Проверка крепления камер, а также проверка самих камер. Проверка пульта ДУ
D-check	6–12 лет. Полный разбор судна, замена некоторых частей самолета	12 месяцев. Осмотр всех конструкций, чистка загрязнений. Замена узлов крепления пропеллеров, обновление ПО, замена аккумуляторный батарей

Проверка самолётов и БПЛА имеет ряд общих аспектов, таких как проверка технического состояния, контроль за исправностью систем и механизмов, а также обеспечение безопасности полетов. Однако есть и существенные различия.

Самолеты обычно проходят более тщательную и глубокую проверку, поскольку они предназначены для перевозки пассажиров и грузов на большие расстояния. Эта проверка включает в себя не только визуальный осмотр, но и использование специализированного оборудования для диагностики состояния всех систем самолета. Кроме того, самолеты должны соответствовать строгим стандартам безопасности и регулярно проходить сертификацию.

В то же время, БПЛА используются для выполнения различных задач, включая мониторинг, наблюдение, доставку грузов и т. д. Их проверка может быть менее строгой, поскольку они не перевозят людей и не требуют такой же степени безопасности. Тем не менее, проверка БПЛА также важна для обеспечения их надежности и эффективности работы.

Еще одно различие заключается в том, что проверка самолетов обычно проводится в специально оборудованных ангарах или на аэродромах, тогда как проверка БПЛА может проводиться в любом удобном месте, специализированная наземная инфраструктура не требуется. Более того, если для обслуживания самолета необходимо специально обученная команда из нескольких человек, то техническими проверками БПЛА может заниматься подготовленный техник или сам пилот.

Таким образом, хотя проверка самолетов и БПЛА имеет общие цели и задачи, она осуществляется с разной степенью глубины и строгости в зависимости от типа воздушного судна и его предназначения.

Список литературы

1. Киселев Д. Ю., Макаровский И. М. Неразрушающие методы контроля технического состояния воздушных судов. Самара : Издательство Самарского университета, 2017.
2. Ведерников Ю. В. Основы теории структурной оптимизации систем контроля и управления беспилотными летательными аппаратами. СПб. : Политехника, 2022.
3. Чурин Р. А. Особенности исследования беспилотных летательных аппаратов // Информационные технологии в деятельности органов внутренних дел : сборник научных статей. М., 2023. С. 51–54.

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
Научно-исследовательского института специальной техники
НПО «Специальная техника и связь» МВД России,
кандидат юридических наук*

ДВЕ СТОРОНЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ И ЭКСТРЕМИЗМУ

Терроризм и экстремизм как в России, так и в мировом масштабе по-прежнему остаются одними из остро стоящих перед государством проблемами. А происшедшие события 22 марта текущего года еще раз свидетельствуют об их актуальности.

За последние пять лет только в 2021 г. наблюдалось снижение числа преступлений террористического характера (–8,8 %). Последующий рост числа преступлений террористического характера (в 2022 г. – +4,5 % и в 2023 г. (+6,7 %, всего: 2 382), по словам директора ФСБ России А. Бортникова, обусловлен в основном «обострением ситуации в мире и ростом напряженности на рубежах России».

В части касающейся преступлений экстремистской направленности, то за тот же пятилетний период первые четыре года шел значительный рост их количества (+268 %) и лишь в 2023 г., несмотря на активные попытки «раскачивания» протестной активности ведущими средствами массовой информации Запада и США, пытающиеся оказывать радикализирующее воздействие на российскую молодежь и подростков, число преступлений экстремистской направленности снизилось (–14,4 %, всего: 1 340).

Активизация криминальной деятельности различных организаций деструктивного характера связывается, в том числе, с использованием огромного потенциала информационных ресурсов сети Интернет. Более половины преступлений экстремистской направленности (56,0 %; всего: 751; –8,3 %) в текущем году были совершены с использованием сети Интернет.

На фоне уменьшения киберпреступлений, связанных с публичными призывами к осуществлению экстремистской деятельности (ст. 280 УК РФ) и возбуждением ненависти либо вражды (ст. 282 УК РФ), заметно увеличилось количество публичных действий, направленных на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях (ст. 280.3 УК РФ) с 34 до 120 (+233,3 %) [4].

¹ © Шайдаев М. Ш., 2024.

Следует отметить, что одновременно с расширением сферы влияния в интернет-пространстве экстремистские и террористические организации быстро стали осваивать возможности стремительно развивающихся информационно-коммуникационных технологий, в том числе и технологий искусственного интеллекта (ИИ). В силу открытости и доступности, относительной дешевизны и простоты передачи программного обеспечения технологии ИИ в руках террористов и экстремистов признаются одной из угроз безопасности государства и общества.

Использование технологий искусственного интеллекта предоставляет экстремистским идеологам широкий спектр инструментария для осуществления целевого информационно-психологического воздействия как на отдельного человека, так единовременно на большие массы людей.

Так, генерированием посредством искусственного интеллекта ложной информации или ложной интерпретации существующего факта общественной или политической жизни в информационном пространстве можно спровоцировать целевые группы на неадекватную реакцию или определенные негативные действия, нарушающие общественный порядок.

Используя алгоритмы глубокого обучения можно осуществить целенаправленную трансформацию обычных, повседневных образов и превратить их в негативные образы, увеличивая эффективность воздействия на целевые аудитории.

Для привлечения новых сторонников в свои организации экстремистские идеологи используют отдельные склонности пользовательской аудитории, например, как доверие к позитивным новостям или медиаперсонам. Технологии искусственного интеллекта позволяют при необходимости продвинуть в медиапространстве любую новость или персону, придавая им особую ценность и важность за счет представления их в положительном свете и ежедневного навязывания пользователям, использование которых в дальнейшем облегчает идеологическую обработку и вербовку пользователей [6].

Создание с применением ИИ различного интерактивного программного обеспечения для общения с пользователями через социальные сети – еще одно направление внедрения технологий ИИ, которое не могло остаться вне поля зрения экстремистов, пытающихся их использовать в качестве интеллектуальных агентов для продвижения своих идей. Так называемые «веб-роботы», «социальные» или «чат-боты» в руках экстремистов уже пришли на смену людям-пропагандистов, вербовщиков и наёмных троллей. К примеру, обладающая большим опытом использования в своих психологических операциях механизмов социальной инженерии запрещенная в России организация «Исламское государство» еще в 2015 г. создала тысячи ботов в «Twitter» для пропаганды, сбора средств, вербовки и координации активных и потенциальных боевиков, а также для расширения своей аудитории среди активных пользователей существующих продуктов ИИ. Распространение упрощенных, недорогих или даже бесплатных ботов позволяет экстремистским организациям устанавливать аффективные связи с пользователями социальных сетей и мобилизовывать их на радикальные и насильственные действия [5].

Наряду с этим, даже создаваемые с благими намерениями для общения с пользователями через социальные сети боты могут стать объектом внимания

экстремистов, связанного со способностью ИИ к самообучению и запоминанию. Умышленно искажая данные, на основе которых проводится обучение, а именно навязывая «чат-боту» в процессе общения с ним деструктивный контент и радикальные взгляды, можно внести изменения в работу алгоритма, нацелив ИИ на пропаганду экстремистских идей. Так случилось с искусственным интеллектом «Тау», разработанным компанией Microsoft, который через непродолжительное время стала выдавать экстремистские утверждения [2].

Экстремисты для продвижения своей идеологии используют любые средства. Одно из них основывается на способности искусственного интеллекта путем анализа различных источников информации (блоги, статьи, форумы, опросы и т. д.) определять отношение автора текста к предмету, обсуждаемому в нем, основываясь на котором можно осуществлять целенаправленное манипулирование мнениями журналистов, блогеров и т. п., а также их аудитории [6].

Другим эффективным средством для осуществления своей деятельности экстремистами признаются так называемые технологии «фальшивых людей». Суть ее – в создании искусственным интеллектом поддельных видео-выступлений публичных политиков, деятелей бизнеса, культуры или представителей конфессиональных организаций, содержащих призывы к осуществлению экстремистских действий, с целью провоцирования напряженности. В основе указанной технологии лежит способность нейросети к обучению генерировать изображения людей, используя бесконечную коллекцию изображений реальных лиц. Добавляя сгенерированному изображению любые культурные и этнические особенности, эмоции и настроения, синтезируя в дальнейшем человеческое изображение и голос, создаются необходимые персонажи несуществующих или реальных людей. Причем, такие технологии позволяют создать любое поддельное видео, практически не отличающееся от реального. А, учитывая, что доверие к изображениям людей, созданных ИИ, иногда выше чем к изображениям реальных людей, то интерес экстремистов к технологиям «фальшивых людей» для манипулирования поведением больших целевых групп вполне очевиден [6]. Так, с помощью синтезированного видеобращения какого-нибудь кумира несовершеннолетних можно убедить их посетить подложное законное мероприятие с целью вовлечения их в массовые беспорядки [1].

Существенную опасность в руках экстремистов и террористов могут представлять системы предсказательной аналитики на основе больших данных с использованием ИИ. Такие системы путем обработки массивов данных СМИ, интернет-пространства и социальных сетей способны прогнозировать будущие события. Таким образом, заранее определив дату и место сбора массового мероприятия, террористы могут спланировать террористический акт во время его проведения [7].

Приведенные примеры применения искусственного интеллекта можно рассматривать как умышленное противоправное воздействие на человека. Кроме этого, существенную опасность представляет преднамеренное совершение ИИ общественно-опасных деяний.

Важным составляющим безопасности использования ИИ является недопущение утери контроля над ним, особенно ИИ, входящим в различные системы

управления. Подобные системы управления с элементами ИИ предназначены, например, для управления беспилотным транспортом (автомобильный транспорт, летательный аппарат, надводные и подводные аппараты) или отдельными производственными процессами.

В системах боевого управления искусственный интеллект заменяет функции, традиционно считающиеся прерогативой человека, как, например, анализ и оценка обстановки, распознавание целей в сложных боевых условиях, выдача команд на применение вооружения. Кроме того, рассматриваемые системы могут быть использованы для выполнения задач по оценке погодных, климатических и экологических условий, а в условиях ведения боевых действий – для выполнения разведывательных задач по прогнозированию и оценке уязвимостей в линиях обороны противника, оценке и выбору сил и средств на выполнение боевой задачи.

Таким образом, захват контроля над искусственным интеллектом с целью его переориентирования на совершение необходимых для террористов действий, может быть чреват тяжелыми последствиями, а в случае, например, с беспилотным транспортом он может быть использован для совершения террористических актов. В свою очередь, утеря контроля над системами управления производственными процессами может привести к технологическим авариям.

По мере совершенствования технологий ИИ очевиден рост спроса на его возможности со стороны экстремистских и террористических организаций, что требует принятия адекватных мер правоохранительными органами со стороны правоохранительной системы и в первую очередь по опережающим темпам внедрения новейших разработок в области технологий ИИ в оперативно-служебную деятельность.

Указанные разработки, основанные на способности ИИ за ограниченное время обрабатывать огромные массивы данных, могут быть использованы для автоматического сбора из социальных сетей, интернет-публикаций и иных источников в информационно-телекоммуникационных сетях информации, имеющей отношение к экстремистской деятельности. Проводя на основе поиска незаметных на первый взгляд связей и закономерностей анализ имеющейся информации, искусственный интеллект способен отграничить экстремистские материалы от неэкстремистских и идентифицировать признаки деятельности экстремистских групп, организаций, сообществ.

Распознавание ИИ экстремистских материалов, постов экстремистской направленности с последующей аутентификацией подлинности пользователя компьютера, позволит установить первоисточник информации экстремистского характера в информационно-коммуникационных сетях, а также местонахождение устройств, их передавших, а при помощи разработанных алгоритмов – ускорить процесс удаления публикаций, постов экстремистского характера. Подобные алгоритмы ИИ при выявлении пользователей, ранее замеченных в пропаганде экстремизма и терроризма, или вновь пытающихся открыть подобные аккаунты в сети, производят их автоматическую блокировку.

Представляет интерес опыт использования подобных технологий ИИ отдельными интернет-компаниями для противодействия распространению экстремистских материалов на своей платформе. Например, Компания Facebook¹ применяет ИИ для распознавания изображений, видеороликов и текстов экстремистского характера и определяет фейковые аккаунты, которые могут принадлежать экстремистам. Если система обнаруживает, что пользователь пытается загрузить в соцсеть контент, ранее отмеченный как «нежелательный», она автоматически блокирует загрузку. Используя алгоритмы «прочесывания», ИИ находит и удаляет «экстремистские и террористические сегменты» [8].

С использованием технологий ИИ заметно ускоряется обработка больших объемов видео-, фотоинформации в сети Интернет, что незаменимо в случае необходимости осуществления за короткое время предварительной обработки, анализа, обнаружения и распознавания образов с последующей идентификацией личностей, причастных к совершению преступлений экстремистского или террористического характера.

Используя свойство интернета, как источника информации о различной деятельности людей, организаций, технологии искусственного интеллекта способны путем анализа деятельности лиц, причастных к экстремистской деятельности, прогнозировать протестные акции или противоправные действия по экстремистским мотивам, а также при необходимости составлять психологические портреты лиц, склонных к совершению экстремистских преступлений.

Социальные сети являются источником обширной информации относительно интересов, увлечений, записей пользователей, фиксирующих показатели его поведенческой активности. Российские разработки искусственного интеллекта для психоанализа граждан по их соцсетям открывают широкие возможности по оценке личности и прогнозированию ее поведения без осуществления психологического тестирования, требующего его добровольного согласия». Полученная информация может быть полезна при выявлении и своевременном реагировании на разжигание национальной розни, вербовку или вовлечение, в первую очередь молодого поколения, как наиболее активных пользователей соцсетей, в экстремистскую деятельность [9]. Так, разработанное «Ростехом» на основе искусственного интеллекта программное обеспечение путем анализа данных в социальных сетях, а также сообщений в СМИ и других источниках информации позволит прогнозировать массовые беспорядки [10].

Разработчиками НИИ «Квант» создана интеллектуальная система «Авенир», которая, используя технологии глубокого машинного обучения, по заданным ключевым словам осуществляет мониторинг общественного мнения и протестных настроений в социальных сетях [11].

В сфере противодействия терроризму технологии ИИ также становятся все более востребованными и уже нашли свое применение при решении ряда задач.

Потеря контроля над беспилотным транспортом чаще всего связывается с возможными кибератаками на их аппаратно-программное обеспечение. Реше-

¹ Запрещена в России: принадлежит корпорации Meta, которая признана в России экстремистской.

ния безопасности, основанные на технологиях искусственного интеллекта, способны поднять на новый уровень защиту беспилотников от кибератак и попыток перехвата террористами управления ими для использования в своих целях.

С другой стороны, обеспечивая защиту беспилотного транспорта от несанкционированного вмешательства в их систему управления, большое внимание уделяется созданию высокоэффективных систем противодействия использованию в террористических целях самих беспилотников, как правило, беспилотных летательных аппаратов (БПЛА). Областью внедрения технологий ИИ становятся высокотехнологичные средства обнаружения, поражения и нейтрализации беспилотников.

На основе нейронных сетей создаются системы поиска операторов, управляющих БПЛА. ИИ, проанализировав поведение беспилотника в небе на основе данных положения солнца, рельефа, и других препятствий, обуславливающих траекторию полета, способен определить место запуска БПЛА.

В части касающейся систем нейтрализации БПЛА следует отметить применяемые уже системы принудительной посадки беспилотников, функционирующих на базе ИИ.

Ускоренное развитие систем противодействия беспилотникам, ставших в последние годы эффективным средством ведения боевых действий, чаще всего происходит во время военных конфликтов. Так, для защиты крупных территорий от беспилотных летательных аппаратов развитие получили специализированные средства глушителей каналов навигации беспилотников, в которых ИИ отвечает за автоматическое определение «свой-чужой» по ситуационным и поведенческим характеристикам объекта. Универсальность комплекса состоит в его самообучаемости для достижения максимально четкой идентификации беспилотников среди всех воздушных объектов.

Переходя в другую сферу применения ИИ, следует упомянуть о получивших широкое применение, в том числе в России, «умных» видеокамерах, идентифицирующих личность человека на предмет выявления потенциальных преступников. В московских системах видеонаблюдения используются нейросети, распознающие лицо человека путем сопоставления его внешности с фотографиями из базы. Если алгоритм считает, что выявлен преступник, полиция получает уведомление с его изображением, текущей локацией и личными данными. Обучив искусственный интеллект выявлять признаки наличия у человека оружия и намерения совершить теракт, система при обнаружении оружия в руках или сумке способна моментально оповестить полицию или автоматически заблокировать преступнику вход в здание [12].

В рамках расследования преступлений террористического характера, являющихся одним из наиболее сложных видов преступлений, в большинстве своем требуется оперативно и в кратчайшие сроки провести анализ большого объема информации. Применение ИИ в такой ситуации может не только ускорить процесс установления всех обстоятельств дела и розыска подозреваемых в преступлении, но и исключить возможные ошибки следствия [3].

Исследование возможностей технологий ИИ с целью последующего перехода к их внедрению для обеспечения служебных процессов является в последние годы приоритетным направлением деятельности и МВД России.

С 2023 г. началась реализация Плана (комплекса мероприятий) по внедрению технологий искусственного интеллекта в деятельность органов внутренних дел Российской Федерации на 2023–2025 гг., направленный на повышение эффективности оперативно-служебной деятельности подразделений МВД России за счет использования технологий ИИ.

В рамках выполнения указанного комплекса мероприятий предусматривается решение ряда задач, в том числе:

- анализ использования технологий ИИ в составе информационных систем и сервисов МВД России с целью выработки предложений по их внедрению в информационные системы и сервисы ИСОД МВД России;
- формирование наборов данных (датасетов) для обучения и тестирования нейросетевых моделей;
- сопровождение опытно-конструкторских работ, результаты которых используют технологии ИИ.

На сегодняшний день одной из таких выполняемых работ является создание сервиса информационно-аналитического обеспечения деятельности Ситуационного центра МВД России, отвечающий за информационно-аналитическое обеспечение решения задач управления силами и средствами органов внутренних дел в кризисных ситуациях. Создаваемый сервис позволит автоматизировать управленческую деятельность по реагированию на чрезвычайные обстоятельства и чрезвычайные ситуации, в том числе и массовые беспорядки, в которые могут перерасти при определенных условиях публичные и иные массовые мероприятия.

Применение нейронных сетей во входящих в состав сервиса подсистемах и модулях позволит обеспечивать моделирование оперативной обстановки и различных процессов оперативно-служебной деятельности с целью анализа различных вариантов их развития с целью выработки управленческого решения.

Таким образом, в складывающейся обстановке перерастания экстремизма и терроризма в высокотехнологичные угрозы обществу и государству внедрение технологий искусственного интеллекта в интересах правоохранительных органов и специальных служб приобретает существенное значение в повышении эффективности борьбы с указанными угрозами. Основанием для сосредоточения усилий специалистов и разработчиков в этом направлении служит Национальная стратегия развития ИИ на период до 2030 г.

Список литературы

1. Багмет А. М., Бычков В. В. Расследование массовых беспорядков, в том числе с участием несовершеннолетних, и вовлечения в них несовершеннолетних : учебное пособие. М. : Юнити-Дана, 2021.
2. Бычков В. В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-коммуникационных сетей, так и борьбы с ними // Вестник Московского университета МВД России. 2022 № 1. С. 60–65.
3. Гедгафов М. М. Роль искусственного интеллекта в противодействии терроризму // Экономические исследования. С. 91–95.

4. Комплексный анализ состояния преступности в Российской Федерации по итогам 2023 года и ожидаемые тенденции ее развития : аналитический обзор / [М. В. Гончарова и др.]. М. : Всероссийский научно-исследовательский институт МВД России, 2024. С. 37–45.

5. Матяшова Д. О. Злонамеренное использование искусственного интеллекта обсудили в рамках XIII международного IT-форума // Пролог: журнал о праве. 2022. № 2. С. 105–114.

6. Пашенцев Е. Н. Злонамеренное использование искусственного интеллекта: новые угрозы для международной информационно-психологической безопасности и пути их нейтрализации // Государственное управление. Электронный вестник. 2019. № 76. С. 279–303.

7. Искусственный интеллект как террорист: новые угрозы безопасности. URL: <https://ria.ru/20190618/1555644961.html>.

8. «Фейсбук»: искусственный интеллект против терроризма. URL: https://polit.ru/article/2017/06/18/fb_ii/.

9. Искусственный интеллект проведет психоанализ россиян по соцсетям. URL: <https://ruposters.ru/news/29-11-2021/iskusstvennii-intellekt-izuchit-rossiyan>.

10. В России разрабатывают искусственный интеллект для предупреждения массовых беспорядков. URL: <https://3dnews.ru/1054840/roste-rabotaet-nad-tehnologiy-pozvolyayushchey-predskazivat-massovie-besporyadki>.

11. ФСБ использует искусственный интеллект для анализа настроений в социальных сетях. URL: https://infostart.ru/journal/news/tekhnologii/fsb-ispolzuet-iskusstvennyy-intellekt-dlya-analiza-nastroeniy-v-sotsialnykh-setyakh_974258/.

12. Умное оружие и мониторинг соцсетей: сможет ли ИИ предотвращать теракты. URL: https://dzen.ru/a/EzK37_QLSxd8sG9r.

Шапкин С. В.¹,

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

Научный руководитель: **Полянская Е. П.,**

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

ПЕРСПЕКТИВЫ РАЗВИТИЯ КРИПТОВАЛЮТ И ИХ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

В последнее время распространение криптовалюты стало заметным явлением в сфере информационной безопасности. Использование криптовалют в качестве альтернативного средства оплаты и инвестирования привлекает внимание как частных лиц, так и компаний. Однако, вместе с увеличением интереса к криптовалютам возросли и угрозы для информационной безопасности. Киберпреступники используют различные методы для кражи криптовалюты, взлома криптобирж и мошенничества. Сегодня мы рассмотрим перспективы развития криптовалют и их влияние на информационную безопасность, а также основные угрозы, связанные с киберпреступностью, и способы защиты от них. Для начала определим, что такое криптовалюта. Криптовалюта – это разновидность цифровой валюты, которая не имеет физического воплощения и единого центра, который будет ее контролировать. Она работает в так называемой «цепочке блоков» или «блокчейн-цепочке передачи информации».

Появление криптовалют как инструментов обмена и инвестирования связано с перспективой их развития. Использование криптовалют может стать проще и эффективнее по мере развития технологии. Связь между блоками гарантируется тем, что каждый блок имеет свою хеш-сумму, а предыдущий блок – свою. Изменение информации в одном блоке приведет к изменению данных во всех последующих блоках. Вопросы информационной безопасности являются одной из многих проблем, связанных с развитием криптовалют. Поскольку все они происходят в цифровой среде, они уязвимы для кибератак. Существуют слабые места, которыми злоумышленник может воспользоваться, если захочет. Влияние криптовалют на информационную безопасность может быть, как положительным, так и отрицательным. С другой стороны, на развитие новых подходов к защите и обмену данными может повлиять использование криптовалют, растущая популярность привлекает внимание преступников, которые могут воспользоваться этими технологиями в своих целях.

Перспектива развития криптовалют. Это одно из самых перспективных направлений современной экономики. Наиболее характерной особенностью

¹ © Шапкин С. В., 2024.

криптовалют является отсутствие центрального органа управления, поскольку каждая транзакция происходит непосредственно между отправителем и получателем. Безопасность и анонимность транзакций обеспечиваются за счет децентрализации. Из этого вытекает что данное платежное средство имеет как положительные, так и отрицательные особенности.

Преимущества:

1. Финансовую информацию можно сохранить в тайне.
2. Конфиденциальность и анонимность являются важными факторами безопасности.
3. Транзакции с использованием криптовалют обрабатываются быстрее, чем традиционные способы оплаты.
4. Криптовалюты свободны от государственного вмешательства и цензуры из-за децентрализации.

Недостатки:

1. Стоимость монеты ничем не подкреплена и основана на доверии пользователя, что приводит к резким колебаниям курса.
2. Транзакции не могут быть отменены или скорректированы.
3. Все больше и больше людей начинают использовать криптовалюты в качестве платежного средства, разрабатываются новые технологии для улучшения использования криптовалют.

Влияние криптовалюты на информационную безопасность. Криптовалюты представляют собой уникальный набор проблем для информационной безопасности. Например анонимность, которая окружает транзакции криптовалют, является одной из них. Криптовалюты не привязаны к физическим или юридическим лицам, что затрудняет отслеживание происхождения мошеннической или преступной деятельности. Природа криптовалют затрудняет их регулирование и мониторинг. Это создает благоприятную почву для использования преступниками криптовалют в преступной деятельности. Цена криптовалют может затруднить принятие их в качестве оплаты предприятиями. Компании, прибыльность которых зависит от стабильных цен, подвергаются риску неопределенности, которая может повлиять на их прибыль.

Кибератаки на криптовалюту:

1. Sybil attack (Атака сибилл) – киберпреступник создает множество фальшивых аккаунтов для манипулирования сетью и проведения недобросовестных транзакций.
2. Double Spending (Двойное расходование) – киберпреступник отправляет одни и те же криптовалюты на два разных адреса одновременно, пытаясь потратить их дважды. Для успешного двойного расходования киберпреступник должен контролировать большинство вычислительной мощности сети.
3. Transaction Malleability (Изменение транзакции) – у киберпреступников есть возможность изменять данные в транзакциях до их включения в блокчейн, что может привести к ошибкам или дублированию транзакций.
4. Обналичивание средств через миксеры: для скрытия происхождения украденных средств, киберпреступники могут использовать миксеры (сервисы по смешиванию криптовалют), чтобы усложнить отслеживание транзакций.

5. Фишинг и мошеннические сайты: мошенники могут создавать фишинговые сайты или использовать фальшивые биржи криптовалют для кражи личных данных или средств у пользователей.

Это важная часть, требующая хорошего подхода и соблюдения элементарных требований безопасности, поэтому давайте разберемся в ней. Я составил список методов, которые пользователи могут использовать для защиты криптовалют:

1. Выбор безопасного кошелька. Вы можете использовать холодный кошелек для хранения криптовалют. Лучше всего выбрать кошелек с хорошей репутацией.

2. Создать надежный пароль. Не делитесь своим кошельком с незнакомцами, придумайте сложный пароль для доступа к нему.

3. 2FA – это двойная сертификация. Чтобы повысить безопасность от несанкционированного доступа, вам следует включить двухфакторную аутентификацию для вашего кошелька.

4. Регулярные обновления. Чтобы получить новейшую систему безопасности, установите обновления кошелька.

5. Создание резервных копий. Чтобы не потерять доступ к своим средствам, создавайте резервную копию своего кошелька и храните его в надежном месте.

6. Физическая безопасность. Рекомендуются хранить свое устройство и кошелек в надежном месте. Пользователь может повысить безопасность своего кошелька, следуя рекомендациям.

Перспективы развития криптовалют представляют собой уникальные возможности изменить финансовую систему и цифровую экономику в целом. Важно помнить о необходимости надежной защиты кошелька.

Список литературы

1. Косов М. Е. Функционирование рынка криптовалют: текущее состояние и проблемы развития // Вестник Удмуртского университета. 2019.

2. Свон М. Блокчейн: схема новой экономики / пер. с англ. М. : Олимп-Бизнес, 2021.

3. Терентьева О. И. Трансформация мировой валютной системы: будущее за криптовалютой // Вестник Московского университета. Серия 6 «Экономика». 2022. С. 15–19.

Шарай А. Е.¹,

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

*Научный руководитель: Калашикова А. А.,
преподаватель кафедры информатики и математики
Московского университета
МВД России имени В.Я. Кикотя*

ОЦЕНКА УРОВНЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СФЕРЕ ОБОРОТА ДЕЦЕНТРАЛИЗОВАННЫХ ФИНАНСОВЫХ АКТИВОВ

Первое дело о присвоении денег на бирже криптовалюты в России было закрыто в 2023 г. Субъектами данного правонарушения выступили: криптобиржа WEX, пользователи платформы и системный администратор компании, который в октябре 2018 г. заблокировал доступ к объединённым расчетным счетам и адресам криптовалютных кошельков, находившихся под контролем юридического лица, чье имя не указывается, и незаконно присвоил средства в размере трех миллиардов рублей. Преступление рассматривается не только в рамках уголовного, но и гражданского процесса, так как за пользователями остаётся право на подачу искового заявления в отношении ответчика.

Децентрализованные финансовые активы стали популярными не только среди профессиональных пользователей информационных технологий, но и среди людей, обладающих посредственными знаниями в этой области, благодаря возможности обмена, кредитования, инвестирования и получения доходов без участия посредников, в роли которых могут выступать государство, центральный или коммерческий банк, или же другое лицо. Однако, это свойство децентрализованных финансов используется не только в мирных целях, но и в преступных, включая кражу или даже финансирование террористических актов.

Пункт 10 ст. 4 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [1] запрещает использование ЦФА в процессе обмена на товары, работы или услуги (кроме внешнеторговых договоров между резидентами и нерезидентами). Данное ограничение позволяет избежать преступлений связанных с использованием цифровых финансов. Необходимость в регуляции этой сферы подобными (запрещающими) способами связана с недостаточностью возможности контроля и надзора государства в делах оборота криптовалюты, обоснованной самой сущностью децентрализованных систем.

¹ © Шарай А. Е., 2024.

Безусловно, введение ограничений защищает от возникновения возможных посягательств. Но в условиях санкций, наложенных на финансовый сектор, у российского бизнеса возникает острая необходимость в альтернативных способах расчета с международными партнерами. Данный фактор обуславливает процесс инвестирования в отечественные компании в том числе за счет использования цифровых активов, не ограниченных в трансфере. Именно поэтому необходимо создавать технические условия, определяющие конкурентоспособность России на мировой арене, а также определять рамки для использования децентрализованных финансовых активов путём вмешательства государства через законодательство.

Неизбежность интеграции децентрализованных ЦФА в деятельность хозяйствующих субъектов очевидна. Противодействие преступлениям в этой сфере должно осуществляться на профессиональной основе, что подразумевает не только юридический подход, но и технический, а также подготовку собственных кадров, обладающих соответствующими знаниями.

В 2023 г. на VIII заседании Межгосударственного совета по противодействию коррупции Генеральный прокурор Российской Федерации И. В. Краснов сообщил о первых запросах, направленных в иностранные органы, компетентные в вопросах цифровых активов и коррупции. По его словам, количество подобных интеграций возрастет. Он предложил обобщить практический опыт в оперативной и процессуальной деятельности правоохранительных органов в данной сфере. Была упомянута концепция создания единого поля и установления общих процедур для более эффективного сотрудничества.

Исходя из выше сказанного, можно сделать вывод, что для полноценного и безопасного функционирования технологий блокчейн в России необходимо разработать и принять соответствующую законодательную базу, обеспечить профессиональную подготовку кадров и использовать опыт иностранных специалистов, а также сотрудничать с ними в практических аспектах.

Список литературы

1. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: <http://www.consultant.ru/>.
2. Камышанова А. Е., Брилева А. Д. Правовое регулирование криптовалюты в России: проблемы и перспективы // Научные статьи по специальности «Право». URL: <https://cyberleninka.ru/article/n/pravovoe-regulirovanie-kriptovalyuty-v-rossii-problemy-i-perspektivy>.
3. Козлова Н. Закончено первое дело о присвоении денег на бирже криптовалюты // RG.RU. URL: <https://rg-ru.turbopages.org/rg.ru/s/2023/04/19/koshelki-vne-dostupa.html>.

Швырев Б. А.¹,

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

Ромашкин Т. Р.²,

заместитель командира взвода факультета подготовки
специалистов в области информационной безопасности
Московского университета
МВД России имени В.Я. Кикотя

Антонов А. С.³,

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

МОДЕЛЬ КАНАЛА УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ WI-FI

Наличие на объекте акустической разведки, беспроводной сети стандарта связи IEEE 802.11, может являться потенциальным техническим каналом утечки информации за счет размещения на объекте технических средств передачи информации, которое работает на этом же протоколе беспроводной связи.

Для исследования возможности существования канала утечки акустической информации за счет использования легальных беспроводных протоколов на защищаемом объекте проведены экспериментальные исследования.

В рамках исследования, возможных каналов утечки информации за счет использования легальных беспроводных протоколов, выполнены натурные измерения в безэховой экранированной камере (далее – БЭК) Московского университета МВД России имени В.Я. Кикотя радиосигнала от разработанного устройства, моделирующего микрофон в диапазоне частот Wi-Fi (рис. 1). Использование БЭК объясняется тем, что без него обеспечить радио тишину невозможно.

Условия проведения объектового исследования – осуществление возможности выявления потенциального ТКУИ за счет использования беспроводной связи стандарта IEEE 802.11.

Подготовленная для эксперимента модель микрофона состоит из модуля Wi-Fi ESP8266 с USB работающим на частоте 2,4 ГГц, микрофона и источника питания – внешнего аккумулятора.

¹ © Швырев Б. А., 2024.

² © Ромашкин Т. Р., 2024.

³ © Антонов А. С., 2024.

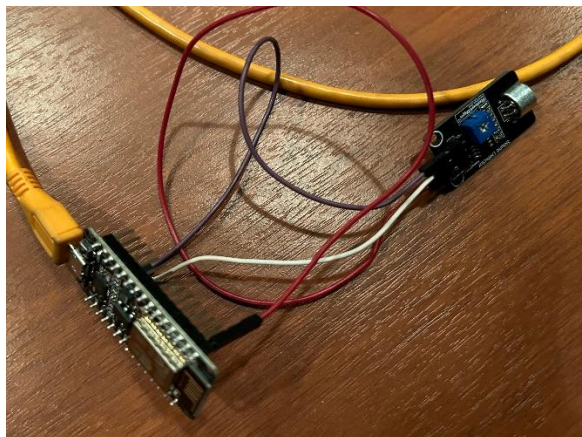
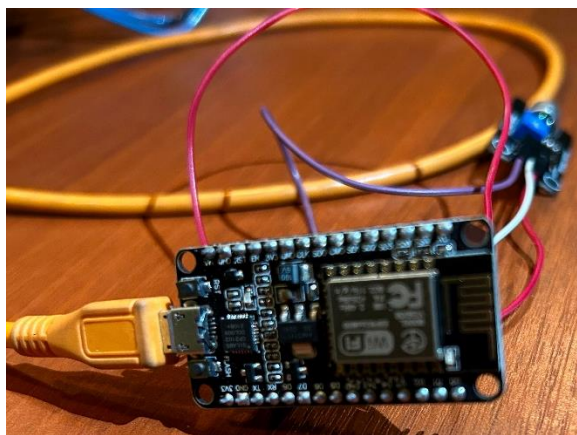


Рис. 1. Внешний вид собранной модели

Средства измерения, применяемые в рамках эксперимента: портативный анализатор спектра «Rohde&Schwarz FSH13», работающий в диапазоне частот от 9 кГц до 13,6 ГГц, со встроенным предусилителем и антенна «НБА-02», диапазон частот которой от 0,009 МГц до 2500 МГц.

Подготовительный этап исследования состоял из сборки модели, подключения внешнего источника питания, общей настройки всех устройств и проверки функционирования компонентов тестового стенда.

Последовательность эксперимента состояла из четырех этапов: проверка возможности передачи звукового сигнала через микрофон, размещенном в модели (рис. 2). Для этого использовался мобильный телефон с программным обеспечением, которое генерирует сложный импульсный звуковой сигнал в различной тональности и на компьютере, подключенном к модели по Wi-Fi, проверялась возможность передачи данного звукового сигнала (его уровень шума), который отображался в дБ на диаграмме (рис. 3).

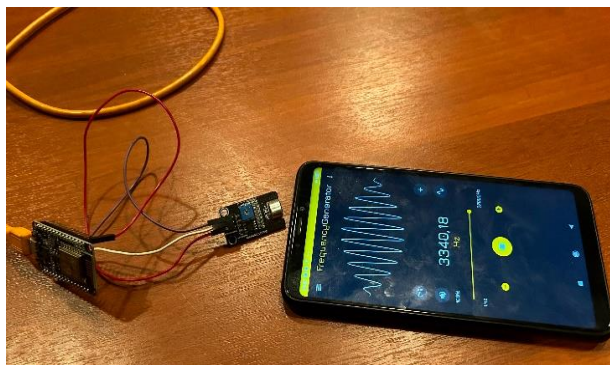


Рис. 2. Передача звукового сигнала через микрофон модели АР



Рис. 3. Результаты передачи звукового сигнала через микрофон модели АР, отображаемые на компьютере

В БЭЖ был помещен мобильный телефон, Wi-Fi которого был переведен в «режим модема». В этом режиме любое устройство с Wi-Fi модулем может подключиться к нему зная наименование SSID и пароль от модели (в том случае, если он установлен (назначен). Далее при помощи портативного анализатора спектра и измерительной антенны был получен следующий результат: спектр сигнала первого канала Wi-Fi, излучаемого мобильным телефоном (рис. 4).

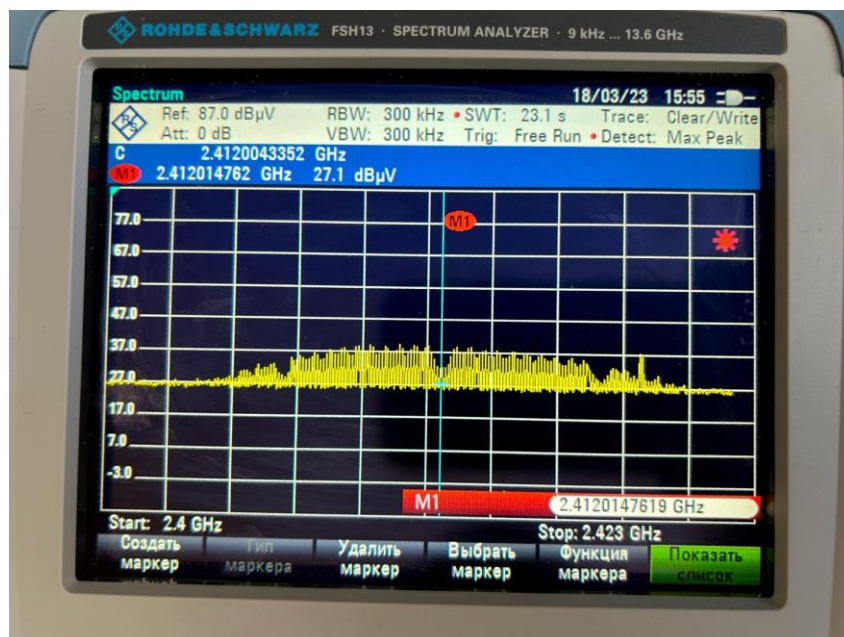


Рис. 4. Спектр сигнала Wi-Fi, излучаемого мобильным телефоном

Указанные результаты измерений отражают, что спектр передаваемых данных в первом канале достаточно широкий и определить, что в нем конкретно передается сложно, там может быть отправка и служебной информации между моделью и мобильным телефоном, аудио, видео и (или) иные данные.

В БЭК была помещена модель, настроенная в режим модема. К нему был подключен мобильный телефон, с которым модель обменивалась служебными данными. Результаты измерений спектра излучений следующие, представленные на рис. 5. На нем видно, что спектроанализатор показывает спектр излучений данного устройства как источник Wi-Fi сигнала (в диапазоне частот 2,412–2,418 ГГц), т. е. оно представляется легальным устройством и никак не скрывается.

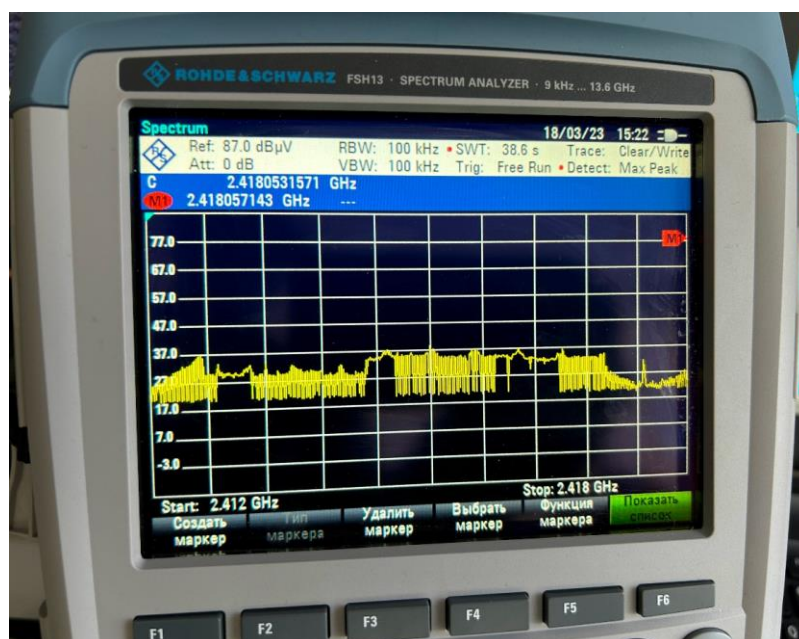


Рис. 5. Спектр сигнала модели AP, настроенной в режим модема

Исследуемая модель АР, переведена в режим устройства, подключенного к АР Wi-Fi, которым являлся мобильный телефон, функционирующим в режиме модема. Работает на первом канале частоты Wi-Fi 2,4 ГГц, где нижняя частота – 2,401 ГГц, а верхняя – 2,423 ГГц. Приемная антенна была установлена в непосредственной близости от модели АР, а мобильный телефон, к которому подключена данная АР расположен на большом удалении для исключения его воздействия, что позволяет отстроиться по мощности от сигнала мобильного телефона (рис. 6).



Рис. 6. Размещение антенны на тестовом стенде

Полученные в результате измерений, представлены на рис. 7.

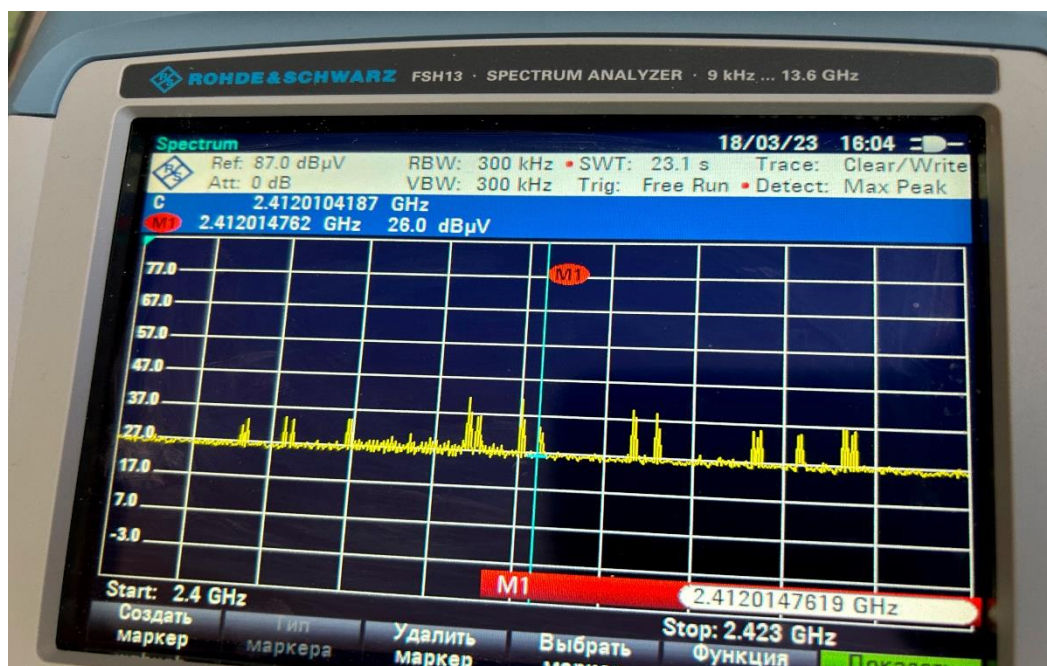


Рис. 7. Спектр сигнала модели АР, подключенного к телефону

Спектр модели значительно отличается от предыдущих измерений, величина гармоник, формируемых ее микрофоном значительно меньше всего уровня электромагнитного излучения, который создает мобильный телефон в режиме модема. Таким образом, модель очень сложно выявить в общем диапазоне, и она маскируется в легальных каналах Wi-Fi.

Необходимо отметить, что при помощи приложения, например, «Wi-Fi Analyzer» на базе ОС Андроид, исследуемая модель AP Wi-Fi не определяется, то есть оперативно подобным способом установить наличие данного устройства на объекте или рядом с ним невозможно.

Также предполагается, что злоумышленник может расположить рядом с объектом дополнительную Wi-Fi сеть, которая будет настроена соответствующим образом для сокрытия своим сигналом радиоизлучения, находящегося на целевом объекте.

Таким образом, наличие на защищаемом объекте Wi-Fi является угрозой информационной безопасности.

В заключении отметим, что выявить несанкционированное закладочное устройство, размещенное на защищаемом объекте и работающее на основе беспроводной связи стандарта IEEE 802.11 достаточно трудоемко. Для этого необходимо использовать специализированные технические средств поиска закладочных устройств, с меньшей эффективностью можно воспользоваться индикаторами электромагнитного поля и (или) нелинейным локатором.

Наличие на защищаемом объекте радиоизлучения диапазона Wi-Fi потенциально является угрозой безопасности. Разработанная модель устройства передачи акустической речевой информации за счет использования легальных протоколов беспроводных сетей подтвердила свою работоспособность и позволило смоделировать канал утечки информации, исследование которого необходимо продолжать для его оценки и выработке комплекса эффективных мер противодействия.

Список литературы

1. Зайцев А. П., Мещеряков Р. В., Шелупанов А. А. Технические средства и методы защиты информации : учебник для вузов. 7-е изд., испр. М. : Горячая Линия-Телеком, 2018.
2. Поршнев С. В., Беляев Д. О. Скрытые технические каналы утечки информации, обрабатываемой в средствах вычислительной техники: анализ действующей нормативно-методической базы, терминология // Вестник УрФО. Безопасность в информационной сфере. 2021. № 1 (39). С. 5–13.
3. Jared Newman and Michael Brown, Best water leak detectors for smart homes, TechHive, March 18, 2022.
4. Mike Prospero, Best water leak detectors in 2022, Tom's Guide, April 6, 2022.
5. Darwin, The Best of the Z-Wave Water Leak & Flood Sensors, Darwins-Den.com, March 7, 2018.
6. Diao W., Liu X., Zhou Z., Zhang K. Your voice assistant is mine: How to abuse speakers to steal information and control your phone; Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices; Scottsdale, AZ, USA. 3–7 November 2014. P. 63–74.
7. IEEE-SA, IEEE Standard for Ethernet, IEEE Standards Authority, 2012.

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

ВНЕДРЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В ПРАВООХРАНИТЕЛЬНУЮ ДЕЯТЕЛЬНОСТЬ ДЛЯ ОБЕСПЕЧЕНИЯ ПРОЗРАЧНОСТИ И ЦЕЛОСТНОСТИ ДАННЫХ

Компьютерные технологии нашли применение во всех сферах нашей жизни. Их роль особенно прослеживается в обеспечении передачи и обмена информацией, являющейся одной из главных ценностей в современном мире. Следовательно, возникает потребность в обеспечении безопасности личных данных, их защите и контроле доступа.

Ключевым инструментом в решении данной задачи могут стать блокчейн-технологии. Они представляют собой цепочку блоков с определенной информацией, использующую одноранговую сеть, доступную для подключения каждого человека. Кроме информации каждый блок содержит в себе свой идентификатор и идентификатор предыдущего блока. При изменении данных в каком-либо блоке будет изменен и его хеш, соответственно все следующие блоки станут недействительными.

Одна из характеристик блокчейн-технологии, делающие их привлекательными для применения в различных областях, – децентрализация. Традиционно управление данными и их хранение представляет собой централизованную систему. В случае с блокчейн-технологиями все наоборот – обработка информации осуществляется с помощью распределительной сети узлов. Данное свойство исключает необходимость наличия центрального контролирующего органа, обеспечивая следующие достоинства: повышенная надежность и устойчивость к атакам, отсутствие единой точки отказа, а также возможность достижения прозрачности и подлинности данных без необходимости доверия к центральному органу. Непрерывность цепочки блоков обеспечивает прозрачность и подлинность данных, так как все модификации блоков фиксируются в непрерывной последовательности. Данный принцип работы технологии особенно полезен в тех случаях, когда необходимо обеспечить надежную защиту данных от подделки.

Благодаря своим характеристикам, блокчейн может быть использован для создания систем согласования данных и их защиты от подделок, что может значительно облегчить работу правоохранительных органов и помочь при решении задач, поставленных перед ними.

¹ © Шикалова В. М., 2024.

В настоящее время существует ряд проблем, связанных с обеспечением прозрачности и целостности данных, а также с существующими методами их хранения и защиты. Они обусловлены их уязвимостью к кибератакам и несанкционированному доступу, что может стать причиной утраты или подверженности информации изменениям.

Блокчейн способен предложить решение данных проблем, однако использования одних только хешей недостаточно, так как современные компьютеры имеют большие мощности и способны вычислить многочисленное их количество в секунду, откуда появляется возможность значительно изменить блок и просто пересчитать хеши остальных составляющих цепи. Во избежание этого в блокчейне используется технология «Proof of Work» («Доказательство работы»), задача которой состоит в значительном замедлении создания новых блоков. Главными участниками алгоритма являются майнеры, работа которых обычно сводится к серии вычислений с перебором параметров для нахождения хеша, что позволяет обеспечить высокий уровень безопасности системы [1].

Применение блокчейн-технологий в работе правоохранительных органов можно рассмотреть в разных аспектах. За счет своих характеристик, они способны повлиять на такие процессы, как сбор и хранение доказательств, тем самым повышая прозрачность и эффективность работы, установление подлинности документов, борьбу с коррупцией, а также послужить основой организации учета судебных решений [2].

Внедрение блокчейна в работу правоохранительных органов способствует ряду инноваций в их деятельности. Использование смарт-контрактов – это программный код, представляющий собой цифровую версию обычного контракта, который самостоятельно контролирует выполнение условий и не требует участия сторон и посредников. Создание децентрализованной базы данных, способной обеспечить доступ к информации для всех участников системы. Также блокчейн-технологии можно использовать для развития системы идентификации, что включает в себя биометрические данные, распознавание голоса и т. д. [3].

Однако при интеграции блокчейн-технологий в правоохранительную деятельность могут возникнуть некоторые сложности. Первое, с чем можно столкнуться – необходимость больших единовременных затрат на разработку и внедрение, что может ограничить их использование в небольших подразделениях. За отсутствием достаточных знаний появляется потребность в обучении сотрудников и дальнейшем их расширении. Также не стоит забывать, что блокчейн – относительно новая технология, находящаяся в процессе развития, и она может иметь несовершенства и уязвимости.

Список литературы

1. Использование технологии блокчейна в правоохранительной деятельности / [И. И. Кирюшин и др.] // Полицейская деятельность. 2024. № 1. С. 27–41.
2. Антонян Е. А., Аминов И. И. Блокчейн-технологии в противодействии кибертерроризму. URL: <https://cyberleninka.ru/article/n/blokcheyn-tehnologii-v-protivodeystvii-kiberterrorizmu>.
3. Токолов А. В. Блокчейн-технология в обеспечении кибербезопасности государства. URL: <https://cyberleninka.ru/article/n/blokcheyn-tehnologiya-v-obespechenii-kiberbezopasnosti-gosudarstva>.

Шубина К. С.¹,

*преподаватель кафедры противодействия преступлениям
в сфере информационно-телекоммуникационных технологий
Московского университета
МВД России имени В.Я. Кикотя,
кандидат юридических наук*

ЭЛЕКТРОННЫЕ СРЕДСТВА СВЯЗИ, ИСПОЛЬЗУЕМЫЕ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ И СУДОВ

Процессы цифровизации и глобализации способствуют ежегодному увеличению количества интернет-пользователей. Согласно статистическим данным, представленным в отчете ООН «Мировые демографические перспективы», на январь 2024 г. число людей, проживающих на Земле, составляет 8,08 млрд, из них 5,61 млрд являются пользователями мобильных телефонов (с января 2023 г. количество пользователей выросло на 2,5 %). При этом около 5,35 млрд человек ежедневно используют в личных и профессиональных целях сеть Интернет [1]. Сложно представить современного человека без телефона, который уже давно перестал быть просто гаджетом.

Электронные средства связи активно используются в деятельности правоохранительных органов и судов. Стратегией развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, определен поэтапный переход государственных органов и органов местного самоуправления к использованию инфраструктуры электронного правительства [2]. Для судебной системы предусмотрено подключение к «электронному правосудию», в соответствии с которым стало возможным дистанционное участие граждан, т. е. с применением электронных средств связи, в арбитражном, административном, гражданском и уголовном судопроизводстве [3].

В законодательстве Российской Федерации понятие «электронные средства связи» отсутствует, однако в энциклопедии «Кругосвет» оно определяется как «техника передачи информации из одного места в другое в виде электрических сигналов, посылаемых по проводам, кабелю, оптоволоконным линиям или вообще без направляющих линий» [4].

В Федеральном законе от 7 июля 2003 г. № 126-ФЗ «О связи» содержится толкование таких терминов, как «линия связи», «сеть связи», «средства связи» и «электросвязь» [5]. Их анализ позволяет установить существенные признаки понятия «электронные средства связи» и дать следующее их определение применительно к уголовному судопроизводству – «электронные технические и программные средства государственных органов, осуществляющих предварительное расследование и рассмотрение уголовного дела по существу, обеспечивающие оперативное и качественное формирование, обработку, хранение, передачу и прием текстовой, числовой, графической, аудио-, видео- или иной информации

¹ © Шубина К. С., 2024.

без нарушения ее целостности, в одну или несколько точек связи посредством использования зашифрованных каналов» [6].

К используемым в деятельности правоохранительных органов и судов электронным технологиям связи относятся:

- факсимильная связь;
- телефонная связь;
- единая система информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России), включающая в себя сервис электронной почты, сервис электронного документооборота и т. д.;
- электронная почта;
- видео-конференц-связь (ВКС);
- электронные платформы, включенные в Единый реестр Минкомсвязи России, более известные как мессенджеры.

Впервые фотоэлектрическая факс-система была продемонстрирована А. Корном в 1902 г., спустя пол века Международным союзом электросвязи были разработаны и утверждены международные стандарты для факсимильной передачи информации, после чего она и получила широкое распространение. На сегодняшний день может показаться, что факсимильная связь – пережиток прошлого. Но это не совсем верно. Многие государственные органы используют данный вид связи, гарантирующий безопасную передачу данных без риска их утечки, среди них и территориальные органы внутренних дел.

Сотрудниками правоохранительных органов и судов в целях взаимодействия с участниками уголовного судопроизводства применяется телефонная связь, в том числе связь посредством мессенджеров. Например, для вызова на следственное действие. Однако предварительно следует выяснить удобна ли такая форма связи для лица, что подтверждается распиской «О разъяснении права на извещение посредством СМС и/или телефонограммы, а также на получение информации, связанной с рассмотрением дела в суде, на официальном сайте суда в сети Интернет» [7].

Кроме того, используя телефонную связь, следователь (дознатель) уведомляет адвокатское образование о необходимости предоставления защиты подозреваемому (обвиняемому). Нередко сотовая связь применяется для получения консультаций у экспертов (в частности, по вопросам, возникающим при назначении экспертиз).

В 2012 г. была утверждена концепция создания ИСОД МВД России, которая на сегодняшний день успешно функционирует. Данная система состоит из множества сервисов, интерес для данной статьи представляют: сервис электронной почты (СЭП), сервис электронного документооборота (СЭД), сервис видео-конференц-связи модернизированный (СВКС-м) и т. д.

Так следователь (дознатель), направляя запрос или же поручение о производстве отдельных следственных действий (оперативно-разыскных мероприятий) в другой территориальный орган, должен отдавать приоритет сервисам электронной почты и электронного документооборота. Это связано с тем, что за-

груженные документы регистрируются, следовательно их исполнение отслеживается. Однако в Следственном комитете Российской Федерации, ФСИН России, судах и других учреждениях сервисы ИСОД МВД России не используются, в связи с чем для направления запросов и истребования ответов применяется электронная почта.

Достоинствами сервиса электронного документооборота являются: обеспечение быстрого обмена документами между подразделениями МВД России, упрощение их поиска и процесса согласования.

Посредством сервиса электронной почты возможен обмен сообщениями не только с участниками и учреждениями, подключенными к ИСОД МВД России, но и пользователями сети Интернет, что позволяет делиться служебной и деловой корреспонденцией, получать обращения граждан и направлять запросы в различные организации. С помощью вкладки «Календарь» можно организовать свое рабочее время онлайн. Для этого необходимо просто выбрать дату и добавить событие (например, производство очной ставки). Посредством функции «добавить человека» можно пригласить определенное лицо на запланированное мероприятие, например, оперуполномоченного для сопровождения следственного действия. Онлайн планирование позволяет руководителю следственного органа (органа дознания) равномерно распределять нагрузку среди подчиненных.

Изначально СВКС-м был создан для обеспечения видеокоммуникации между сотрудниками МВД России всех регионов, в частности для организации и проведения совещаний.

Единственное нормативное определение видео-конференц-связи содержится в приказе Судебного Департамента при Верховном Суде Российской Федерации от 28 декабря 2015 г. № 401 «Об утверждении Регламента организации применения видео-конференц-связи в федеральных судах общей юрисдикции» [8]. Ранее это было объяснимо, так как данная технология использовалась только на судебных стадиях уголовного судопроизводства. Однако с внесением изменений в УПК РФ Федеральным законом от 30 декабря 2021 г. № 501-ФЗ, стало возможным применение систем ВКС при производстве допроса, очной ставки и опознания, то есть на стадии предварительного расследования [9]. Представляется, что ст. 5 УПК РФ должна быть дополнена определением термина «видео-конференц-связь».

В ч. 1 ст. 189.1 УПК РФ при производстве следственных действий предусмотрено использование систем ВКС только государственных органов, осуществляющих предварительное расследование. На сегодняшний день данным требованиям удовлетворяет лишь сервис ВКС-м ИСОД МВД России, который гарантирует безопасное соединение между подразделениями МВД России и исключает факт утечки информации.

Как известно, оборудованием видео-конференц-связи оснащены не только территориальные ОВД, но и СИЗО, места лишения свободы, лечебно-исправительные и лечебно-профилактические учреждения, туберкулезные и психиатрические больницы и т. д. В этой связи возникает вопрос: возможно ли дистанционное производство допроса, очной ставки, предъявления для опознания в одном

из указанных учреждений. По нашему мнению, ответ может быть положительным при выполнении следующих условий: неукоснительном соблюдении требований уголовно-процессуального законодательства; использовании сертифицированного оборудования ВКС, удовлетворяющего установленным стандартам. К такому оборудованию можно отнести:

- видеосвязь электронных платформ, включенных в Единый реестр Минкомсвязи российских программ для электронных вычислительных машин и баз данных;
- мобильную версию СВКС-м ИСОД МВД России.

Из соображений логики и безопасности мобильная версия данного сервиса должна быть разработана на базе Android. Устанавливая мобильную версию сервиса на служебное устройство, необходимо убедиться, что у него заблокирован доступ к сервисам Google (Google Play, Google Maps), вход осуществляется по логину и паролю, а данные о дате и времени входа регистрируются в системе.

В науке также рассматриваются проблемы подключения между системами видео-конференц-связи разных ведомств, связанные с отсутствием единых стандартов и протоколов связи (на данный момент не существует единого стандарта, который бы обеспечивал совместимость различных систем); различиями в аппаратном и программном обеспечении; нехваткой квалифицированных специалистов и проблемами с сетевым оборудованием. Пути их решения только предстоит найти, однако попытки уже предпринимаются.

Несмотря на требование уголовно-процессуального законодательства, касающееся использования систем ВКС только государственных органов, осуществляющих предварительное расследование, известны случаи применения в практической деятельности следователей (дознавателей) и судей видеосвязи электронных платформ (мессенджеров).

Перспективные российские аналоги зарубежных платформ (WhatsApp, Skype, Viber)¹ – это ISQ, Вконтакте (Vk), ТамТам. В России они используются редко по сравнению с другими странами, хотя развитие технологии ВКС началось еще в прошлом веке.

К электронным платформам российского производства, включенным в Единый реестр Минкомсвязи, относятся:

- Vinteo (№ 412);
- Видеоселектор (№ 751);
- Proffipsilon Video (PiVideo) (№ 1896).

Vinteo – российская разработка. Данная программа позволяет вести запись конференции, не требуя дополнительного лицензирования; поддерживает все открытые стандарты связи, в том числе H.323, SIP и WebRTC; оснащена функцией синхронного перевода и т. д.

ВКС *Vinteo* применяется для реализации проектов федерального и международного уровня. В государственном секторе посредством этой программы было выполнено более 200 проектов. 21 апреля 2020 г. Верховный Суд Российской

¹ Запрещены в России: принадлежат корпорации Meta, которая признана в России экстремистской.

Федерации впервые в нашей стране провел онлайн-заседания через веб-конференцию (для их организации применялась ВКС Vinteo).

В качестве достоинств платформы Vinteo разработчики выделяют:

- оперативность: программа позволяет быстро принимать решения за счет увеличения скорости обмена информацией;
- качество: программа обеспечивает высококачественный обмен информацией, исключая технические помехи;
- конфиденциальность: программа при передаче и получении данных шифрует их, тем самым обеспечивая безопасность;
- масштабируемость;
- простота использования: программа обладает простым и понятным интерфейсом.

Видеоселектор также является российской разработкой и используется для организации видеоконференций в ФНС России, Минобороны России, МСЦ РАН и т. д. Данная программа предлагает широкий спектр инструментов для онлайн-общения, в том числе приватные и групповые чаты, голосовые звонки и видеозвонки, а также видеоконференции. Преимуществами данного продукта являются:

- доступность: программа работает на различных устройствах и операционных системах, включая российские, и может быть использована через любой современный браузер;
- функциональность и удобство;
- высокое качество;
- безопасность: доступ к конференциям защищен, а передаваемые данные зашифрованы, что обеспечивает безопасность общения;
- масштабность: видеоселектор является широко используемой системой видео-конференц-связи в России, включая более чем 150 тыс. пользователей;
- экономия ресурсов: благодаря микшированию видеопотоков на сервере клиентские устройства и пропускная способность требуют минимальных ресурсов;
- совместимость: видеоселектор поддерживает сеансы видео-конференц-связи со многими производителями аппаратных ВКС.

Proffipsilon Video, также известный как PiVideo, считается одним из наиболее часто используемых и надежных сервисов для видеоконференций. Данный сервис предлагает множество функций, которые делают его привлекательным для компаний и организаций, в том числе государственных.

Одним из основных преимуществ этой программы является то, что она доступна на разных платформах, включая Windows, macOS, iOS и Android. Благодаря этому, пользователи могут оставаться на связи независимо от того, каким устройством они пользуются. Кроме того, у PiVideo высокое качество видео и звука, что обеспечивает комфортное и эффективное общение. К тому же она предоставляет ряд инструментов для совместной работы. Например, на конференциях можно использовать доски для рисования или делиться документами.

Безопасность также является важным аспектом этой программы. Все данные, передаваемые через этот сервис, шифруются, что защищает их от несанкционированного доступа. PiVideo также предлагает инструменты для обеспечения приватности, такие как отключение видео и аудио участников конференции.

Таким образом, использование электронных средств связи является необходимым для эффективного функционирования правоохранительных органов и судов. Их применение гарантирует:

- оперативную коммуникацию между правоохранительными министерствами и ведомствами;
- способствует эффективному распределению рабочего времени и ресурсов;
- обеспечивает безопасность участников уголовного судопроизводства.

Вместе с тем требуют своего решения ряд вопросов технического, организационного и правового характера.

Список литературы

1. Статистика интернета и соцсетей на 2024 год – цифры и тренды в мире и в России // WebCanape. URL: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2024-v-mire-i-v-rossii/?utm_referrer=https%3a%2f%2fyandex.ru%2f#3.
2. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Информационно-правовой портал «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/71570570/>.
3. Плахота К. С. Использование электронных средств связи в судебном разбирательстве по уголовным делам: современное состояние и перспективы // Вестник Дальневосточного юридического института МВД России. 2022. № 1 (58). С. 100–104.
4. Универсальная научно-популярная энциклопедия «Кругосвет». URL: https://www.krugosvet.ru/enc/nauka_i_tehnika/transport_i_svyaz/ELEKTRONNIE_SREDSTVA_SVYAZI.html.
5. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» // НПП «Гарант-сервис». URL: <https://base.garant.ru/186117/>.
6. Плахота К. С. Использование электронных средств связи в уголовном судопроизводстве) : автореф. дис. ... канд. юрид. наук. М., 2023.
7. Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 3 «О внесении изменений в некоторые постановления Пленума Верховного Суда Российской Федерации» // Официальный сайт Верховного Суда Российской Федерации. URL: <https://www.vsrp.ru/documents/own/8281/>.
8. Приказ Судебного Департамента при Верховном Суде Российской Федерации от 28 декабря 2015 г. № 401 «Об утверждении регламента организации применения видео-конференц-связи в федеральных судах общей юрисдикции» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_376566/.
9. Федеральный закон от 30 декабря 2021 г. № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» // НПП «Гарант-сервис». URL: <https://base.garant.ru/403333311/>.

Эрдниев А. С.¹,

начальник учебно-научного комплекса информационных технологий

Московского университета

МВД России имени В.Я. Кикотя,

кандидат педагогических наук

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Генезис понятия «информационная безопасность» в парадигме образовательного процесса. Информационная безопасность, как концептуальное направление подготовки кадров для органов внутренних дел определяется с позиции соответствующей национальной Доктрины [1], во главе угла которой стоит трактовка данного понятия, как «состояния защищенности от внутренних и внешних информационных угроз». Предикат ключевого определения через призму правоохранительной деятельности сводится к защите инфополя или инфосреды от внешнего деструктивного воздействия.

Вместе с тем заслуживает внимания культурологический подход к формулированию искомого понятия [2, с. 61]. Реалии цифрового общества предполагают расширение функционала «безопасности» от состояния защищенности информации к состоянию защиты от воздействия чуждой по отношению к субъекту инфопространства системы координат.

Подобное отношение к информационной безопасности, как к направлению подготовки кадров высшей квалификации определяет потребность к переходу подготовки специалистов по защите информации к специалистам по противодействию киберугрозам. Новое функциональное назначение специалиста диктует необходимость контекстного трактования кибербезопасности.

В исследовании дискурса информационной безопасности [3, с. 212], концепт кибербезопасности занимает подчиненную роль, выступая в качестве сущности, определяющей противоборство различных сторон за киберпространство. Применительно к правоохранительным органам данное определение позволяет сформулировать следующую семантику навыков специалиста: исследование информационных уязвимостей, анализ инфосреды, воздействие на деструктивное информационное пространство, профилактика деструктивного информационного воздействия. Таким образом пассивные навыки защиты информации дополняются навыками активного воздействия на внешнюю по отношению к защищаемому пространству информацию.

Реализация подобной парадигмы инфобезопасности в образовательном процессе определяет потребность в изменении подходов к подготовке квалифицированных специалистов для органов внутренних дел.

Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) 4-го поколения как новый педагогический потенциал. В сен-

¹ © Эрдниев А. С., 2024.

тябре 2025 г. планируется введение в действие новых ФГОС ВО. Для информационной безопасности подобные изменения могут оказаться концептуальными. С одной стороны это продиктовано новой номенклатурой укрупненной группы специальностей и направлений подготовки, с другой ФГОС ВО 4-го поколения ориентированы на формирование мировоззрения личности будущего квалифицированного специалиста, что предполагает увеличение количества часов для освоения гуманитарно-социальных дисциплин в счет уменьшения времени на подготовку технического специалиста.

Наличие потенциальных угроз для высшего образования в сфере информационной безопасности требует детального анализа сущности происходящих изменений. Одним из оснований, определяющих содержание образовательного процесса в новой системе координат, является законодательная парадигма, характеризующая сущность базового понятия в национальном правовом пространстве [4]. Важнейшей составляющей выступает ответственность юридических и физических лиц за необеспечение безопасности информации, а также необходимость выделения системы защиты информации в отдельную организационную структуру на уровне хозяйствующего субъекта. Данные обстоятельства определяют потребность наличия у квалифицированного специалиста компетенций связанных с критическим мышлением и организационно-распорядительными навыками, которые относятся к универсальным компетенциям. Отсюда следует, что наличие гуманитарно-социального компонента в подготовке кадров для сферы информационной безопасности продиктовано объективной необходимостью. Вместе с тем, гуманитарные знания не должны вступать в диссонанс с техническими, а обязаны быть гармонично имплементированы в образовательную подготовку.

Методологический подход к разработке ФГОС ВО [5] демонстрирует возможность рационального внедрения гуманитарного компонента, при этом позволяет выстроить системный подход к насыщению остальных элементов образовательной подготовки, направленных на формирование технических навыков. Важнейшим условием внедрения ФГОС ВО 4-го поколения является ориентация на формирование технического мировоззрения у специалиста, что обеспечивает потребность в насыщении техническими дисциплинами все этапы образовательной подготовки. В разрез с действующей системой подготовки кадров для органов внутренних дел, выступает необходимость насыщения первого года обучения не только профессиональным образовательным компонентом, основанном на профессиональном обучении по должности служащий «Полицейский», но и ориентация на фундаментальные знания в сфере технических наук таких, как: дискретная математика, дифференциальные уравнения, математический анализ и т. д.

Таким образом вырисовывается потребность в разработке профессионального компонента, связанного с выполнением функций сотрудника полиции, но в рациональной интеграции с техническим образованием, с сохранением равновесия по формируемым компетенциям.

Концепция подготовки специалистов по информационной безопасности для органов внутренних дел. Сформулированные методологические рамки позволяют определить сущность подготовки кадров в следующей системе координат:

образовательная подготовка должна быть нацелена на формирование навыков не только по защите информационного пространства, но и обеспечивать защиту от деструктивной информации; структура образовательного процесса должна соблюдать условие по гармонизации подготовки сотрудника полиции и специалиста, обладающего техническими компетенциями.

Безусловно, для определения содержания образовательного процесса необходима усовершенствованная компетентностная модель специалиста, учитывающая требования заказчиков в действующих реалиях [6, с. 117]. Профессиональные компетенции, как отражение функционального назначения квалифицированного специалиста позволяют определить содержательное наполнение образовательного процесса и детерминировать специализации подготовки под задачи конкретного подразделения органов внутренних дел, нуждающегося в специалистах того или иного профиля.

Эффективность подготовки кадров во многом обеспечивается рациональной последовательностью освоения необходимого набора профессиональных компетенций, а также выстраивания образовательного процесса не только с точки зрения практико-ориентированного обучения, но и формирования осознанного отношения к формируемым компетенциям. В этом случае следует обратить внимание на качественный подбор индикаторов оценки эффективности сформированности компетенций, при которых будущий квалифицированный специалист должен демонстрировать не столько наличие навыков «конвейерной работы», демонстрируя знания и умения выполнять отдельные функции, но и овладеть методом и технологией трудовой деятельности.

Важным условием эффективности организации образовательной подготовки является определение предметной области защиты. Бесспорны новые геополитические реалии, в которых актуальным становится концепция ментальных, когнитивных и смысловых войн [7]. Однако, следует вспомнить об основной смысловой функции сотрудника полиции – защите законных прав и интересов граждан. В этой деонтологической идеологии служителя правопорядка, субъект правоохраны не должен занимать одну из противоборствующих сторон, а должен обеспечивать защищенность национальных интересов. Рассматриваемый контекст напоминает о том, что военных и правоохранителей хоть и одна высшая цель – служение государству, но средства достижения цели различны.

Список литературы

1. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // НПП «Гарант-сервис». URL: <https://base.garant.ru/71556224/?ysclid=lvm2nynrxs10301940>.
2. Былевский П. Г. Разработка культурологической парадигмы информационной безопасности в контексте разрушения цифрового глобализма // Вестник Кемеровского государственного университета культуры и искусств. 2023. № 65. С. 54–65.

3. Ваничкина А. С. Концептуальная парадигма дискурса информационной безопасности // *Германистика 2021: nove et nova : сборник научных трудов*. М. : Московский государственный лингвистический университет, 2021. С. 209–213.
4. Гриценко Л. А. Изменение законодательной парадигмы в области информационной безопасности в России // *Молодой исследователь 2024 : сборник статей*. Пенза : Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. С. 71–73.
5. Мартынов В. Г., Душин А. В., Иванова А. Д. О методологическом подходе к разработке федеральных государственных образовательных стандартов высшего образования четвертого поколения в части универсальных компетенций // *Высшее образование сегодня*. 2023. № 3. С. 35–41.
6. Горбатов В. С., Эрдниев А. С. Совершенствование подготовки кадров по обеспечению безопасности информационной инфраструктуры органов внутренних дел // *Безопасность информационных технологий*. 2024. Т. 31. № 1. С. 100–119.
7. Овчинский А. С. Угрозы ментально-когнитивных смысловых войн // *Информационные технологии в деятельности органов внутренних дел : сборник научных трудов*. М. : Московский университет МВД России имени В.Я. Кикотя, 2023. С. 17–19.

Яковлева К. Ю.¹,

*адъюнкт факультета подготовки
научных и научно-педагогических кадров
Московского университета
МВД России имени В.Я. Кикотя*

*Научный руководитель: Сумин А. А.,
профессор кафедры уголовного процесса
Московского университета
МВД России имени В.Я. Кикотя,
доктор юридических наук, профессор*

ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ (КОМПЬЮТЕРНОЙ) МОДЕЛИ В СЛЕДСТВЕННЫХ ДЕЙСТВИЯХ, ПРОВЕРКЕ И ОЦЕНКЕ ДОКАЗАТЕЛЬСТВ

Компьютерное (электронное) моделирование открывает возможности представления контента (содержания) электронной информации, который может использоваться в уголовно-процессуальном доказывании.

Как правильно было отмечено О. В. Химичевой и А. А. Суминым, «деятельность государственных органов предполагается изменить за счет использования данных в электронном виде и внедрения информационных технологий» [4, с. 254].

Следовательно, функционирование такой информационной технологии, как «компьютерное (электронное) моделирование», создает электронную модель (компьютерную модель), под которой здесь и далее понимается следующее: модель, выполненная в компьютерной (вычислительной) среде и представляющая собой совокупность данных и программного кода, необходимого для работы с данными. Для применения компьютерной модели в процессе моделирования необходимо использовать программное обеспечение компьютерного моделирования и вычислительной техники [1].

Соглашаясь с выводом О. В. Мичуриной о том, что «на данный момент реализовано достаточно мер, позволяющих следователю и дознавателю применять информационные технологии для производства следственных и иных процессуальных действий» [3, с. 121], приводим подтверждающие примеры такого применения: использование беспилотного летательного аппарата и средств вычислительной техники при осмотре места происшествия, для подготовки к проверке показаний на месте позволяет осуществлять лазерное 3D-сканирование географического пространства и объектов, а результатом является электронная (компьютерная) модель, или электронная 3D-модель. По результату функционирования информационной технологии, например, к протоколу осмотра места происшествия электронная (компьютерная) модель, находящаяся на электронном носителе информации, будет приобщена в качестве приложения к доказательству.

¹ © Яковлева К. Ю., 2024.

Также, использование электронной 3D-модели позволит визуализировать и существенно улучшить степень обоснованности выводов эксперта и в уголовном судопроизводстве, а это, в свою очередь, объективно явится дополнительной гарантией корректной оценки следователем (дознавателем) и судом указанных выводов.

С. В. Зуевым и Л. Н. Масленниковой предлагают видеомоделирование в уголовном процессе, под которым понимают «воссоздание на основе доказательств, имеющих в материалах уголовного дела, с помощью анимации, симуляции или технологии виртуальной реальности имеющего значение для уголовного дела обстоятельства или события и представление его результатов в видеографической форме» [2, с. 196].

Указанные обстоятельства и терминологические аспекты позволили представить возможности применения электронной (компьютерной) модели, или электронной 3D-модели в следственных действиях, в проверке и оценке доказательств:

1. Создание электронной модели на основе доказательств по уголовному делу ч. 2 ст. 74 УПК РФ:

- электронная 3D-модель одного доказательства (например, создание электронной 3D-модели с целью анализа показаний подозреваемого на наличие противоречий в показаниях, данных в ходе допроса подозреваемого);

- электронная модель всех собранных доказательств по уголовному делу (например, создание электронной модели с целью анализа показаний подозреваемого данных в ходе допроса подозреваемого, а потом в ходе очной ставки, также на наличие противоречий);

- электронная 3D-модель как инструмент получения вещественного доказательства или иного документа (например, установление механизмов совершения преступления на основе реалистичных математических параметров, заложенных в создание данной модели).

2. Применение электронной (компьютерной) модели, или электронной 3D-модели для проведения следственных действий:

- проверка показаний на месте путем использования электронной 3D-модели в качестве инструмента создания реконструкции для проведения данного следственного действия;

- следственный эксперимент путем использования электронной 3D-модели, которая позволит проверить возможность слышать, видеть или реально воспринимать объекты, а данная модель позволит воспроизвести реалистичные условия с сохранением реалистичных параметров;

- в тех местах, где производство следственных действий создает опасность для жизни и здоровья участвующих в них лиц, а использование электронной 3D-модели в следственном действии обеспечит необходимую безопасность. Такое предложение позволит исключить данное условие общих правил производства следственных действий в ч. 4 ст. 164 УПК РФ.

3. Проверка и оценка доказательств с помощью электронной (компьютерной) модели, или электронной 3D-модели:

– создание электронной 3D-модели с реалистичными параметрами, позволяющими проверять показания свидетеля. Например, согласно позиции С. В. Зуева и Л. Н. Масленниковой, в возможности «свидетеля наблюдать определенные обстоятельства в конкретной географической точке, проверки возможности движения пули по определенной траектории и другое» [2, с. 196].

При использовании в уголовно-процессуальном доказывании электронной 3D-модели возрастает важность такого участника уголовного судопроизводства, как специалист. Его специальные знания могут примениться, как в производстве исследования по вынесенному постановлению следователя (дознателя), так и при подготовке и участии в следственных действиях (например, осуществление с помощью электронной 3D-модели реконструкции места происшествия и для целей других следственных действий).

Таким образом, системное представление применения электронной (компьютерной) модели, или электронной 3D-модели позволяет показать ее возрастающее значение в уголовно-процессуальном доказывании. Однако требуется дальнейшая теоретическая и правовая проработка использования такой информационной технологии, как электронное (компьютерное) моделирование.

Предлагается исследовать особенности проведения проверки показаний на месте и следственного эксперимента путем использования электронной 3D-модели. В связи с этим потребуются соответствующие законодательные изменения.

Список литературы

1. ГОСТ Р 57700.37–2021. Национальный стандарт Российской Федерации. Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения : утвержден и введен в действие Приказом Росстандарта от 16 сентября 2021 г. № 979-ст. М. : ФГБУ «РСТ», 2021.
2. Высокотехнологичный уголовный процесс : монография / под ред. С. В. Зуева, Л. Н. Масленниковой. М., 2023.
3. Мичурина О. В. Обеспечение уголовно-процессуальной деятельности информационными технологиями // Противодействие преступлениям в сфере информационно-телекоммуникационных технологий : сборник научных трудов / сост. А. В. Константинов. М. : Московский университет МВД России имени В.Я. Кикотя, 2023. С. 117–121.
4. Сумин А. А., Химичева О. В. Некоторые вопросы, связанные с цифровизацией материалов уголовного дела // Современные проблемы уголовного процесса: пути решения : сборник научных трудов / под общ. ред. А. Ю. Терехова. Уфа, 2022. С. 253–258.

Ярмак К. В.¹,

начальник управления учебно-методической работы

Московского университета

МВД России имени В.Я. Кикотя,

кандидат юридических наук, доцент

ОБ ОПЫТЕ ПРОВЕДЕНИЯ ОЛИМПИАДЫ ШКОЛЬНИКОВ «УНИВЕРСИТЕТ ЦИФРОВОЙ ПОЛИЦИИ» ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фундаментальные и прикладные направления развития естественнонаучных знаний в цифровой трансформации правоохранительных органов в целом направлены на повышение эффективности и оперативности их работы, расширение возможностей противодействия преступлениям, а также выведения процессов предварительного расследования или проведения судебных экспертиз на качественно новый уровень. В настоящей статье нами предпринята попытка рассмотрения одного из направлений развития естественнонаучных компетенций у сотрудников правоохранительных органов на этапе их профессиональной подготовки, которая играет важную роль в обеспечении эффективности работы правоохранительных органов.

Как известно, подготовка кадров для органов внутренних дел представлена широкой многоуровневой системой, выстроенной по нескольким направлениям, и реализуется в различных формах. К таким формам относим обучение на базе суворовских военных училищ МВД России по основным образовательным программам, которые объединены с комплексом общеразвивающих элементов, с целью подготовки детей к военной или полицейской службе. Также к базовому уровню относится и профессиональное обучение по программам профессиональной подготовки лиц, принятых на службу в ОВД. Базовая форма подготовки специалистов заключается в реализации образовательных программ среднего профессионального образования (подготовка специалистов среднего звена) или образовательных программ высшего образования. Кроме того ведомственная система подготовки кадров предусматривает создание условий для совершенствования имеющихся или приобретения новых компетенций действующими сотрудниками в рамках освоения программ переподготовки или повышения квалификации. Специфической формой получения и поддержания необходимых служебных компетенций является функционирование в МВД России системы подготовки сотрудников по месту их службы в формате профессиональной служебной и физической подготовки.

Безусловно, наиболее важной и системообразующей формой качественной подготовки полицейских кадров является реализация образовательных программ высшего образования. И от того, какого уровня предварительной подготовки образовательные организации получают кандидатов на обучение, зависит, как скоро и на каком уровне будут сформированы профессиональные компетенции выпускника. Представляется, что помимо профориентационных мероприятий

¹ © Ярмак К. В., 2024.

и репутационного статуса вуза существенным фактором формирования конкурсной ситуации в рамках приемной кампании могут служить проводимые на собственной базе олимпиады школьников.

Олимпиадное движение в России в настоящее время обрело очень важное значение в самоопределении образовательной траектории большинства школьников. Начинаясь в прошлом столетии с московских предметных олимпиад, эта форма оценивания способностей молодежи развилась до целого движения, привлекающего ежегодно сотни тысяч учащихся общеобразовательных школ [4].

Считаем, что именно по направлению естественнонаучных дисциплин проведение олимпиад школьников может иметь наибольшую значимость, что играет важную роль в подготовке технических специалистов для МВД России. Олимпиада создает условия для выявления и поощрения молодых талантливых школьников и учащихся средних специальных образовательных организаций, проявляющих интерес к научным и техническим дисциплинам, которые в дальнейшем могут стать обучающимися ведомственного университета.

В целях стимулирования интереса к деятельности Министерства внутренних дел Российской Федерации среди учащихся старших классов школ, популяризации полицейских профессий и государственной службы в целом, актуализации деятельности по обеспечению безопасности информационных технологий в правоохранительной сфере, пропаганды правовых и технических знаний, руководство Московского университета МВД России имени В.Я. Кикотя выступило с инициативой организации на своей базе в 2023–2024 учебном году первой олимпиады школьников по информационной безопасности.

При разработке наименования олимпиады за основу был взят уже существующий в Университете образовательный проект «Университет цифровой полиции» и одноименная образовательная платформа [3].

Еще в августе 2023 г. на оперативном совещании у начальника Университета был утвержден комплекс мероприятий, включающий в себя мероприятия по правовому, организационному и методическому обеспечению Олимпиады. Во исполнение Комплекса мероприятий была проделана большая организационная работа. На основании решения Ученого совета приказом Университета утверждено Положение об олимпиаде школьников «Университет цифровой полиции» в федеральном государственном казенном образовательном учреждении высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя». Также приказом Университета утверждены составы организационного комитета и методической комиссии.

Одной из ключевых задач, стоящих перед организационным комитетом, являлось налаживание тесного взаимодействия со всеми Управлениями (Главными управлениями) МВД России всех регионов Российской Федерации, образовательными организациями МВД России, а также Департаментами образования города Москвы и Московской области. Одновременно были направлены в адрес ЭКЦ МВД России, УБК МВД России, БСТМ МВД России, ФКУ НПО «СтиС» МВД России, ГИАЦ МВД России, ДИТСиЗИ МВД России письма с приглашением к сотрудничеству в Олимпиаде школьников в качестве соорганизаторов. Именно указанные подразделения являются основными заказчикамиготавливаемых по техническим специальностям профессиональных кадров. В резуль-

тате плодотворной работы удалось достичь согласия на открытие дистанционных площадок проведения заключительного очного этапа олимпиады в ряде регионов, покрыв при этом большую часть России: от Санкт-Петербурга на западе до Сахалина на востоке, от Салехарда на севере до Республики Северная Осетия – Алания на юге.

Методической комиссией был сформирован банк вопросов для дистанционного проведения отборочного этапа олимпиады. Вопросы по общеобразовательным предметам: «Информатика и ИКТ», «Математика» и «Физика». Банк вопросов состоял из 75 задач различной степени сложности. Задания олимпиады имеют творческий характер и повышенный уровень сложности. Не маловажное значение уделено форме подачи олимпиадных заданий. Так, их содержание должно отличаться от школьных и, одновременно, быть связано со спецификой полицейской деятельности. Отдельные авторы уже обращали внимание на тот факт, что подобные задачи при хорошей логике рассуждений могут быть решены без наличия глубоких знаний предмета, но большинство всё-таки требуют серьезных знаний и большого труда. И те, и другие варианты, должны помогать школьникам воспринимать естествонаучные дисциплины привлекательными [1].

В установленном порядке обеспечено функционирование специализированного раздела официального сайта Московского университета МВД России имени В.Я. Кикотя (<https://мосу.мвд.рф/>), посвященного олимпиаде, где размещены необходимые документы и новостная лента.

Структура олимпиады предполагает классическое деление на отборочный и заключительный этапы. По итогам проведенной электронной регистрации участников олимпиады зарегистрировалось более 900 обучающихся 10–11 классов, а также первых-вторых курсов колледжей и техникумов. География зарегистрированных участников охватила 53 региона Российской Федерации.

В отборочном этапе, проведенном с применением дистанционных технологий (Moodle) приняли участие и показали свои результаты 416 участников, из них 330 – набрали минимальное количество баллов и получили именные сертификаты об участии в олимпиаде.

Для проведения в очном формате заключительного этапа олимпиады утвержден состав жюри, включающий в себя квалифицированных сотрудников Университета из числа руководителей кафедр учебно-научного комплекса информационных технологий, а также сотрудников подразделений – соорганизаторов олимпиады. Заключительный этап Олимпиады представляет собой разработку и защиту проектов по направлениям в области защиты информации и актуальным тематикам, связанным с цифровой трансформацией деятельности правоохранительных органов. На основании рейтинговых таблиц финалистами олимпиады стало 22 участника из 10 регионов Российской Федерации. В заключительном этапе смогли принять участие 15 участников из девяти регионов Российской Федерации. Два участника воспользовались возможностью открытых дистанционных площадок и осуществляли защиту своего проекта из г. Чита и г. Самара.

Конкурсанты при подготовке и защите проектов демонстрировали творческие способности и углубленные знания в области технических наук. Наибольший интерес и соответствующую высокую оценку у членов жюри получили проекты, связанные с разработкой авторских идей в области робототехники на

службе полиции, криптографической защиты информации, облачных вычислений, дополненной реальности в правоохранительной деятельности. Победителем Первой олимпиады школьников «Университет цифровой полиции» по информационной безопасности признан обучающийся 10 класса МБОУ СОШ № 1 г. Александров Владимирской области Илья Черноглазов, представивший проект «Применение 3D-технологий для изъятия следов подошвы обуви».

По итогам проведения рассматриваемого мероприятия нами сделаны определенные выводы о значении олимпиад школьников в подготовке технических специалистов МВД России. В первую очередь, олимпиада позволяет выявить школьников, демонстрирующих выдающиеся способности в технических дисциплинах и одновременно проявляющих интерес к службе в органах внутренних дел. Такие талантливые школьники должны получать определённые преференции при поступлении в ведомственные образовательные организации для дальнейшего развития своих способностей в рамках образовательных программ высшего образования, в том числе ориентированных на подготовку к работе в МВД России. Сами олимпиадные задания направлены на развитие аналитического мышления, логики, а также практических навыков, которые могут быть полезными при выборе профессии в МВД России. В конечном счете, участие и тем более победа в олимпиаде является мощным мотивационным фактором для школьников, способствующим повышению их интереса к естественным наукам и их использованию в работе полиции.

Таким образом, олимпиады школьников – это не только проверка знаний и умений, но и инструмент поиска и поддержки талантливой молодежи, которая готова в будущем стать настоящими профессионалами в своей области [2]. Это отличная возможность показать свое мастерство, найти новых единомышленников и вдохновиться на дальнейшие достижения. Считаем, что олимпиады школьников, являясь инструментом воспитания научного и критического мышления, стимулируют развитие науки и образования в целом, а также помогают молодым людям сориентироваться на своем профессиональном пути в частности.

Список литературы

1. Математические олимпиады как средство развития познавательной активности школьников / [Е. Н. Бажанова и др.] // Вестник МГПУ. Серия: Информатика и информатизация образования. 2023. № 4 (66). С. 78–93.
2. Самойлова И. В. Олимпиады школьников в аспекте психологического благополучия ребенка // Управление качеством образования: теория и практика эффективного администрирования. 2022. № 3. С. 81–86.
3. Свидетельство о государственной регистрации программы для ЭВМ № 2023665116 Российская Федерация. Образовательная платформа «Университет цифровой полиции» : № 2023663948 : заявл. 03.07.2023 : опубл. 12.07.2023 / [К. В. Ярмаки др.] ; заявитель Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя».
4. Тищенко А. А. Из истории становления предметных олимпиад естественнонаучного цикла в СССР // Наука и школа. 2023. № 4. С. 145–150.