СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Московская академия Следственного комитета имени А.Я. Сухарева

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

материалы II Международной научно-практической конференции

(Москва, 26 апреля 2024 г.)

Москва, 2024

УДК 343.98
ББК 67.5
С 56

С 56 **Проблемы противодействия киберпреступности**: материалы II Международной научно-практической конференции (Москва, 26 апреля 2024 года) / Под общ. ред. О.Ю. Антонова, Э.Б. Хатова. М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2024. – 146 с.

Сборник сформирован по материалам, представленным на II Международную научно-практическую конференцию «Проблемы противодействия киберпреступности», проведенную Московской академией Следственного комитета имени А.Я. Сухарева 26 апреля 2024 года.

Материалы конференции, посвященные актуальным проблемам противодействия киберпреступности, могут представлять интерес для ученых, преподавателей, студентов и аспирантов юридических факультетов и вузов, а также сотрудников правоохранительных органов.

II Международная научно-практическая конференция «Проблемы противодействия киберпреступности»

Во исполнение п. 5.3. Приказа Председателя Следственного комитета Российской Федерации от 30.01.2023 № 19 «Об организации работы по расследованию преступлений, совершенных с использованием информационно-коммуникационных технологий», 26.04.2024 в Московской академии Следственного комитета имени А.Я. Сухарева (далее – Академия) состоялась II Международная научно-практическая конференция «Проблемы противодействия киберпреступности».

В мероприятии очно и дистанционно приняли участие свыше 100 ученых-криминалистов, сотрудников Следственного комитета России и других правоохранительных органов, представители и руководство компаний-разработчиков высокотехнологичной криминалистической техники и программного обеспечения раскрытия и расследования преступлений.

Конференция была представлена научными школами Московского государственного юридического университета имени О.Е. Кутафина, Московского университета МВД России имени В.Я. Кикотя, Академии управления МВД России, Всероссийского государственного университета юстиции, Высшей школы экономики.

Активное участие в работе пленарного заседания и секционной работе форума приняли сотрудники Следственного комитета Республики Беларусь, представители Института повышения квалификации и переподготовки Следственного комитета Республики Беларусь, Правоохранительной академии

Республики Узбекистан; Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан; Всероссийского научно-исследовательского института МВД России; Российского государственного университета правосудия; Санкт-Петербургской Академии СК России; «МИРЭА – Российский технологический университет» и других вузов страны, а также сотрудники Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации, следственных органов Следственного комитета России, ученые, аспиранты ведущих российских вузов, профессорско-преподавательский состав и обучающиеся Академии.

В ходе работы двух секции дискуссионное поле конференции было образовано проблемными вопросами международного и зарубежного опыта борьбы с киберпреступлениями, уголовно-правовой и криминологической характеристики киберпреступлений, в том числе в контексте обеспечения национальной безопасности и реализации уголовной политики, уголовно-процессуальных и криминалистических особенностей производства следственных и иных процессуальных действий, а также использования специальных знаний при расследовании киберпреступлений; расследования преступлений, совершаемых с использованием высоких технологий в сфере экономики, и пути их решения; взаимодействия следственных органов и оперативно-розыскных подразделений в досудебном производстве по материалам и уголовным делам о киберпреступлениях, международного сотрудничества в сфере уголовного судопроизводства по уголовным делам о киберпреступлениях, а также положительным опытом организации обучения сотрудников следственных органов методике расследования киберпреступлений

и применению информационно-коммуникационных технологий при расследовании преступлений.

Высококвалифицированный состав участников форума позволил реализовать комплексный подход к анализу поставленных вопросов, предложить действенные организационно-управленческие, законотворческие, тактико-криминалистические, технические и иные предложения по совершенствованию мер, направленных на противодействие киберпреступности, наметить перспективы дальнейшего взаимодействия и сотрудничества всех заинтересованных сторон.

Резолюция
II Международной научно-практической конференции «Проблемы противодействия киберпреступности»

Участники конференции выразили общую обеспокоенность существующим уровнем киберпреступности. На сегодняшний день крайне актуальны вопросы расследования такого вида криминальных деяний, составляющих треть от общего количества регистрируемых на территории нашей страны преступлений, 75 % которых, к сожалению, остаются нераскрытыми.

Заслушав и обсудив доклады и сообщения, участники Конференции отмечают необходимость:

1. совершенствования уголовного, уголовно-процессуального законодательства, законов об оперативно-розыскной деятельности, о печати, средствах массовой информации с целью повышения эффективности защиты жизни, здоровья, прав и законных интересов граждан России от преступных посягательств, совершенных с использованием сети «Интернет», мобильной телефонии и с учетом тенденций развития современных цифровых финансовых технологий;
2. систематизации судебной практики и выработки единых подходов при квалификации таких новых видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий как публичное распространение заведомо ложной информации о деятельности российских Вооруженных Сил, госорганов, добровольческих формирований и их дискредитация;
3. изучения (обобщения) практического опыта работы криминалистов (следователей-криминалистов) подразделений военных следственных органов Следственного комитета Российской Федерации, работающих в зоне СВО, в том числе по тактике получения, предварительного исследования, документирования и использования криминалистически значимой цифровой информации из памяти компьютерных устройств беспилотных транспортных средств;
4. развития технологий искусственного интеллекта в решении задач выявления, фиксирования и исследования следов преступлений, совершенных с использованием информационных технологий, а также прогнозирования и предупреждения таких преступных проявлений на стадии приготовления.
5. активизации деятельности по повышению квалификации и обучению сотрудников правоохранительных органов цифровым компетенциям в области предупреждения, раскрытия и расследования киберпреступлений.

А.И. Алиев

Технические аспекты деанонимизации пользователя, использующего криптовалюту при совершении преступления

Аннотация. В статье обсуждаются технические аспекты деанонимизации пользователя, использующего криптовалюту для совершения преступления. Нами рассматриваются различные методы и инструменты, которые могут быть использованы для выявления и идентификации таких пользователей. Автором также анализируются возможности обхода мер безопасности и предлагаются рекомендации по улучшению процессов деанонимизации в целях борьбы с преступностью.

***Ключевые слова*:** криптовалюта, цифровая валюта, деанонимизация, преступление.

Развитие информационно-телекоммуникационных технологий привело к тому, что преступность по всему миру обрела цифровой вид, в связи с чем огромное количество преступлений совершается с использование данных технологий, что также не обошло стороной и экономику. Относительно новым явлением в экономике является появление криптовалюты, которая обрела огромную популярность у злоумышленников, в связи с высоким уровнем анонимности данного рода активов.

Говоря об обороте криптовалюты нельзя не обратить внимание на то что ранее, до 2021 года криптовалюта никак не регулировалась государством, но с принятием Федерального закона №259-ФЗ «О цифровых финансовых активах и цифровой валюте[1]» криптовалюта в Российской Федерации законодательно урегулирована в связи, и признана средством платежа.

За 2023 год, согласно отчету Министерства внутренних дел Российской Федерации, совершено 1 947 161 преступлений, из которых 676 951 совершены с использованием информационно-телекоммуникационных технологий, что составляет 29,7 % от общего числа преступлений[2] (рис. 1). Согласно данной информации, можно сделать вывод о том, что цифровой мир является огромным простором для совершения преступлений, а также для сохранения анонимности лица, совершившего преступление.

[1] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».
[2] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2023 года. URL: https://мвд.рф/reports/item/47055751/ (дата обращения 24.02.2024).

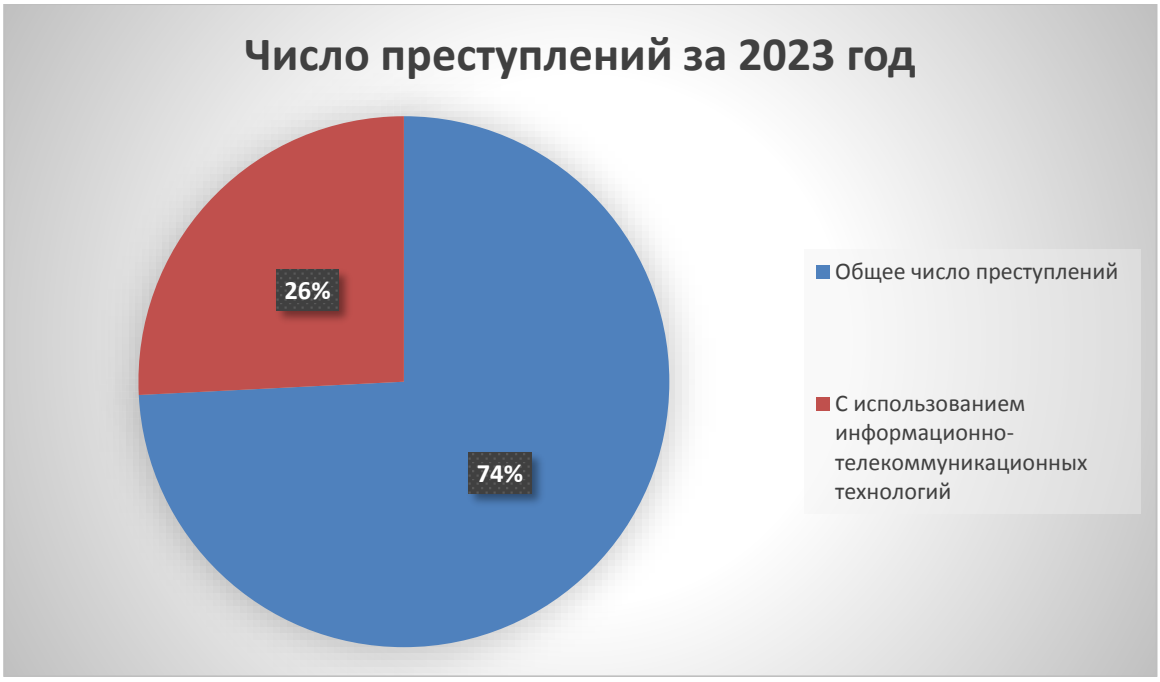


Рис. 1. Количество совершенных преступлений в Российской Федерации в процентном соотношении

Производство по делам, в которых фигурирует криптовалюта осложняются тем, что многие следователи не располагают информацией о том, каким образом возможно установить личность лица, который использует криптовалюту. Анонимность пользователя использующего криптовалюту функционирует за счет действия технологии «блокчейн», зарождение которой началось в 1970-х годах, тогда американским криптографом Ральфом Мерклом было разработано хэш дерево, технология систематизации данных в блоках, позже в 1991 году была сформулирована первая концепция технологии «блокчейн», но признания данная концепция не получила, так как сильно опередила свое время и только лишь в 2008 году человек под псевдонимом Сатоши Накамото, представил свою криптовалюту, функционирующую на основе технологии блокчейн – BitCoin[1].

Основными особенностями блокчейна являются:

Децентрализация – информация о действиях на основе данной технологии не хранится на одном сервере, она распределена между всеми участниками сети.

Взаимосвязь между блоками – каждый последующий блок, хранящий в себе информацию о чем-либо, в нашем случае о транзакциях криптовалюты, связан с предыдущим и таким образом образует цепочку блоков, откуда и название blockchain, что с английского переводится как цепочка блоков. При этом для создания каждого нового блока необходимо решить сложную математическую задачу.

Все транзакции, проведенные при помощи данной технологии, являются открытыми, то есть все участники сети могут их увидеть.

[1] Что такое блокчейн: понятия принципы, особенности технологии. Tangem team. URL: https://tangem.com/ru/blog/post/what-is-a-blockchain/ (дата обращения: 10.05.2024)

Исходя из чего мы можем сделать вывод о том, что «блокчейн», представляет собой книгу учета, в которой сведения заносятся с использование криптографии и их невозможно подменить.

Так по мнению Судницына А.Б. и Молокова В.В., использования уязвимости блокчейна, контроль за несколькими узлами данной сети позволит получить достаточно сведений для уточнения источники транзакции и глубокий анализ общедоступных сведений данной системы позволяет провести большое количество аналитической работы с целью установления источника транзакции[1].

В данном направлении в Российской Федерации государственными и частными организациями проводится большой объем работы. Так компания Шард представляет большой спектр услуг, направленных на установление владельцев криптокошельков, отслеживание транзакций, ими же разработано программное обеспечение позволяющее решать большой спектр аналитических задач[2], также Росфинмониторингом разработано программное обеспечение «Прозрачный блокчейн», которое позволяет проводить аналитическую работу с криптокошельками, отслеживать транзакции, произведенные с использованием криптокошелька, конечной целью которой является установление фактического владельца криптокошелька[3].

По мнению Ю.В. Гаврилина и И.С. Бедерова, принадлежность криптовалюты определенному лицу устанавливается на основании следующих фактов:

– владение приватным ключом доступа к криптовалютному кошельку, позволяющему совершать операции с находящейся в нем криптовалютой;

– указание адреса криптовалютного кошелька для приема платежей на странице в социальной сети, в переписке посредством сервиса мгновенных сообщений (мессенджеров), записи в блоге, сообщении на форуме или на сайте;

– указание сведений о личности в соответствии с правилами функционирования криптовалютной биржи или обменника[4]. С чем мы полностью согласны, так как практически все методы идентификации владельца криптовалюты сводятся к вышеперечисленным.

Анализ блокчейна: анализ транзакций в блокчейне может помочь идентифицировать пользователей, особенно если они используют один и тот же адрес для нескольких транзакций или переводят большие суммы.

1. Методы социальной инженерии: аледователь при производстве следственных действий, а именно использовать методы социальной инженерии, для сбора личной информации о пользователях криптовалют.

---

[1] Судницын А.Б, Молоков В.В. Отдельные возможности получения и использования сведений об операциях с криптовалютой при раскрытии и расследовании преступлений // Вестник Восточно-Сибирского института МВД России. 2019, № 2 (89). С. 213–221.

[2] Шард – платформа по безопасности цифровых активов. URL: https://shard.ru/

[3] Официальный сайт Федеральной службы по финансовому мониторингу. URL: https://fedsfm.ru/activity/informational-systems/pb-gos-modul

[4] Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды академии МВД России. 2021, № 4 (60). С. 101−108.

2. Анализ сетевого трафика: анализ сетевого трафика может помочь идентифицировать IP-адреса, используемые для транзакций криптовалют, и связать их с реальными людьми. Сетевой трафик – это данные, передаваемые через сеть, такие как IP-адреса, MAC-адреса и данные о передаче пакетов, анализ сетевого трафика может помочь идентифицировать пользователей, совершающих преступления, путем анализа данных о передаче пакетов, связанных с преступной деятельностью. Например, если преступник использует один и тот же IP-адрес для нескольких транзакций, связанных с преступной деятельностью, это может помочь идентифицировать его. Кроме того, анализ сетевого трафика может помочь идентифицировать обменные площадки, которые используются преступниками для отмывания денег.

3. Использование информации из открытых источников: следователь может использовать информацию из открытых источников, таких как социальные сети или форумы, для сбора личной информации о пользователях криптовалют.

4. Государственное регулирование: некоторые страны требуют от обменных площадок и кошельков криптовалют проводить проверку личности своих клиентов, что может помочь идентифицировать пользователей.

В заключении хотелось бы отметить, что каждый из перечисленных, что несмотря на то, что криптовалюты предназначены для обеспечения анонимности и конфиденциальности транзакций, существует несколько технических методов, которые могут быть использованы для деанонимизации пользователей, совершающих преступления. Анализ блокчейна, анализ сетевого трафика, использование информации из открытых источников и использование методов машинного обучения являются некоторыми из наиболее распространенных методов деанонимизации.

Однако каждый из этих методов имеет свои преимущества и недостатки, и их эффективность может зависеть от конкретной ситуации и типа криптовалюты, которую использует преступник. Поэтому важно продолжать исследования в области деанонимизации пользователей криптовалют при совершении преступлений, чтобы разработать более эффективные и надежные методы.

А.Н. Антропов

Способы анонимизации трафика в сети интернет, механизмы противодействия анонимизации и их перспективы

Аннотация. Анонимизация трафика является одним из способов защиты конфиденциальности пользователей в сети Интернет. Существует несколько способов анонимизации трафика – Tor, VPN, прокси-серверов и другие технологий. Каждый из этих способов имеет свои преимущества и недостатки, которые подробно рассматриваются в статье. Однако, анонимизация трафика также может быть использована для совершения преступлений в сети Интернет, что вызывает необходимость в разработке механизмов противодействия анонимизации. В статье рассматриваются различные подходы к противодействию анонимизации, такие как анализ трафика, блокировки доступа к анонимизаторам, использование систем глубокого обучения и другие.

***Ключевые слова*:** Интернет, средства шифрования, социальные сети, мессенджеры, блокировка.

На момент две тысячи двадцать третьего года общая численность Российской Федерации составляет коло 144,7 млн человек, согласно данных Росстата с учетом Всероссийской переписи населения 2020 года. Интернет-пользователями являются 127,6 млн человек, что составляет 88,18 % проникновение интернета в социальное общество в России[1]. Исходя из данных цифр и соотношения в процентной составляющей имеем возможность сделать вывод причины интеграции преступлений в информационно-телекоммуникационную сеть Интернет – развита широкая и бюджетная доступность компьютерно-технического оснащения для совершения преступлений в сети.

Сеть Интернет предоставляет возможность способствующие совершения большинства преступлений, в силу ряда обстоятельств, в число которых следует включить:

1. Анонимность: Интернет предоставляет преступникам возможность совершать противозаконные действия, сохраняя при этом анонимность. Это делает сложнее их обнаружение и привлечение к ответственности.
2. Глобальный охват: Интернет не имеет географических границ, что позволяет злоумышленникам действовать из любой точки мира. Это затрудняет сотрудничество между правоохранительными органами разных стран и усложняет процесс преследования.
3. Техническая сложность: Многие киберпреступления требуют специальных технических знаний для их раскрытия и расследования. Не все правоохранительные органы обладают необходимыми ресурсами и навыками для борьбы с этим типом преступлений.

[1]Digital 2023: статистика аудитории интернета и соцсетей в России. URL: https://www.prstudent.ru/research/digital-2023-statistika-auditorii-interneta-i-socsetej-v-rossii (дата обращения 14.02.2024).

4. Отсутствие четких законов: в некоторых случаях законодательство не может эффективно реагировать на новые типы киберпреступлений, потому что они постоянно эволюционируют и меняются. Это может привести к тому, что преступники остаются безнаказанными.

5. Масштабы: Огромное количество пользователей и транзакций в Интернете делает сложным мониторинг и обнаружение преступной деятельности. Преступники могут использовать автоматизированные инструменты для массовых атак, что увеличивает масштабы преступности.

6. Низкое восприятие риска: Многие пользователи Интернета недооценивают риски, связанные с кибербезопасностью, и не принимают необходимых мер защиты. Это делает их лёгкой целью для преступников.

7. Как отмечают исследователи социологических наук наиболее подверженной категорией экстремизма является молодежь до 30 лет, что также подтверждается изученной нами судебной практикой (указать количество изученных приговоров), средний возраст осужденных к наказанию или в отношении которых вынесен штраф составляет XX лет.

Прежде чем начать обсуждение сервисов анонимизации считаем нужным уделить внимание сетевой услуге – хостинг. Данная услуга позволяет размещать сайты и приложения в интернете, обеспечивая их доступность и работоспособность[1]. Хостинг подразделяется на выделенный и виртуальный. Виртуальный хостинг представляет собой один выделенный физический сервер, на котором располагаются множество веб-сайтов, а также используется с целью реализации функционала виртуальной анонимизации. Под выделенным

Принимая во внимание сокрытие информационных следов с использованием средств анонимизации, требуется выделить средства, обеспечивающие анонимность пользователей сети Интернет, к которым следует отнести[2]:

1. VPN-сервисы (Virtual Private Network или виртуальная частная сеть) – общее название технологий, которые позволяют устанавливать одно или несколько сетевых соединений поверх другой сети. Данная технология используется для различных целей, например для создания частных сетей, обход ограничений доступа к контенту, анонимность и конфиденциальность в сети, а также улучшения качества подключения.

Данное соединение представляет собой так называемый «туннель» между компьютером пользователя и сервером, где данные шифруются каждым узлом до их передачи через этот «туннель». После подключению к данному виду сервиса, производится идентификация вашей сети и выполняет аутентификацию, сравнивая введенный пароль с данными в своей базе данных. В результате прохождения успешной авторизации VPN предоставляет вам права на выполнение определенных действий, например серфинг в интернете. После установления соединения, трафик (от англ. Traffic – движение. Также есть менее

[1]Хостинг: варианты, сравнения, пользовательская статистика. URL: https://habr.com/ru/companies/ruvds/articles/443522/ (дата обращения 08.03.2024).

[2]Алейников Д.П., Зык А.В. Современные технологии анонимизации в сети Интернет // Образование и право. 2021. № 7. С. 223–224.

популярный вариант написания «Bandwidth» - пропускная способность) начинает движение между вашим компьютером и сервером в зашифрованном виде[1].

Зашифрованность прежде заключается в том, что VPN-сервис изменяет IP-адрес вашего технического средства на свой собственный. Таким образом все данные передаются к внешним ресурсам, которые вы, соответственно, запрашиваете с VPN-сервиса.

В криминалистических целях следует отметить, что не вся информация, передаваемая через VPN-соединение, шифруется. Каждый провайдер VPN имеет свои технологические характеристики способов и уровней шифрования, политику хранения логов (от англ. Log – текстовый файл, на который автоматически сохраняются/записываются важные сведения о работе системы или программы), что способствует образованию информационному следу на сервере. Также нужно учитывать подход VPN-провайдера с третьими лицами, в нашем случае с правоохранительными органами, по факту предоставлению информации. Соответственно в случае отсутствия хранения логов на сервере, то информационный след блекнет.

2. Прокси-сервера – компьютерная система или программа, которая выступает в качестве посредника между клиентом (компьютером пользователя) и сервером, предоставляющим требуемые ресурсы (сайты, файлы и т.д.). Когда пользователь отправляет запрос на получение ресурса, этот запрос проходит через прокси-сервер, который, в свою очередь, передает его серверу, предоставляющему ресурс, и получает ответ от него. После этого прокси-сервер передает ответ пользователю.

Прокси-серверы используются для различных целей, таких как обеспечение безопасности, конфиденциальности и анонимности в сети Интернет, а также для кэширования и фильтрации контента. Они могут быть локальными или удаленными, бесплатными или платными, и могут иметь различные функции и настройки в зависимости от потребностей пользователей.

Одним из основных преимуществ использования прокси-серверов является то, что они позволяют пользователям скрыть свой IP-адрес и местоположение, что может быть полезно для защиты конфиденциальности и безопасности в сети Интернет. Кроме того, прокси-серверы могут использоваться для обхода географических ограничений и цензуры в сети Интернет, а также для ускорения доступа к ресурсам за счет кэширования.

В целом, прокси-серверы являются полезным инструментом для обеспечения безопасности и конфиденциальности в сети Интернет, однако их использование требует осторожности и понимания того, как они работают и какие риски могут быть связаны с их использованием. Среди рисков следует выделить: риск использования ненадежных прокси-серверов, то есть используемые злоумышленниками для сбора личных данных пользователей; рис утечки

[1]Газин Д.М., Тибалов Н.П., Поначугин А.В. Актуальность использования VPN-сервисов в России в условиях мировой нестабильности // Международный научно-исследовательский журнал. - 2023. - №2 (128).

конфиденциальной информации; риск уменьшения скорости соединения; риск блокировки доступа к ресурсам; риск нарушения законов.

3. SSH-туннели – метод передачи сетевого трафика через защищенное SSH-соединение. SSH (Secure Shell) – это протокол, который обеспечивает безопасное соединение между клиентом и сервером, используя шифрование и аутентификацию.

SSH-туннелирование позволяет перенаправлять сетевой трафик с одного компьютера на другой, используя SSH-соединение в качестве туннеля. Это может быть полезно для обеспечения безопасности и конфиденциальности при передаче конфиденциальной информации по сети, а также для обхода ограничений и цензуры в сети Интернет.

Существует два основных типа SSH-туннелирования: локальное и удаленное. Локальное туннелирование используется для перенаправления трафика с локального компьютера на удаленный сервер через SSH-соединение. Удаленное туннелирование используется для перенаправления трафика с удаленного сервера на локальный компьютер через SSH-соединение.

SSH-туннелирование может быть настроено с помощью командной строки или с использованием специальных программ, таких как PuTTY. Для настройки SSH-туннелирования необходимо иметь доступ к SSH-серверу и знать его IP-адрес и порт.

В целом, SSH-туннелирование является полезным инструментом для обеспечения безопасности и конфиденциальности при передаче конфиденциальной информации по сети, а также для обхода ограничений и цензуры в сети Интернет. Однако его использование требует определенных знаний и навыков, и его эффективность зависит от надежности и безопасности используемого SSH-соединения.

4. Tor – сеть анонимных прокси-серверов, которая используется для обеспечения конфиденциальности и безопасности в сети Интернет. Tor позволяет пользователям скрыть свой IP-адрес и местоположение, что может быть полезно для защиты конфиденциальности и безопасности в сети Интернет.

Однако, как и любое другое технологическое средство, Tor может быть использовано с различными целями, включая распространение негативной информации. Некоторые пользователи Tor могут использовать сеть для распространения негативной информации, например, для кибербуллинга, клеветы или распространения фейковых новостей.

Однако, следует помнить, что использование Tor с целью распространения негативной информации является неэтичным и противоречит принципам конфиденциальности и безопасности, на которых основана сеть Tor. Большинство пользователей Tor используют сеть для законных целей, таких как защита конфиденциальности и безопасности в сети Интернет, и не поддерживают использование сети для распространения негативной информации.

В целом, Tor является полезным инструментом для обеспечения конфиденциальности и безопасности в сети Интернет, однако его использование

требует ответственности и соблюдения этических норм. Люди, которые используют Tor с целью распространения негативной информации, должны понимать, что их действия могут причинить вред другим людям и подлежат уголовному преследованию.

Наиболее популярным сервисом является именно VPN-сервисы, которые позволяют формировать обезличивание вашего устройства, посредством сокрытия информации о посещенных веб-сайтах, используемых в браузере, местоположении. В настоящее временя это особенно полезно во время блокировки доступа к определенным сайтам, таким как Youtube, WhatsApp, сервисы VPN позволяет обойти подобные ограничения и получить доступ к привычным социальным сетям.

По факту изучения Google Play (виртуальный магазин бесплатных, а также платных приложений, игр и сервисов) можно выделить наиболее популярные VPN-сервисы, а именно:

1. VPN (Stolitomson VPN).
2. VPN от Planet VPN.
3. VPN Proxy Master: Super VPN.
4. Turbo VPN.
5. AdGuard VPN.

Не малой популярностью среди пользователей социальных сетей являются прокси-сервера, о которых говорили ранее. Большой фурор в их использовании возник при ограничении доступа на территории к мессенджеру Telegram после обращения Роскомнадзора в Таганский суд г. Москвы с иском о его блокировки из-за отказа компании предоставлять ФСБ ключи шифрования, необходимые для кодирования сообщений пользователей, 13 апреля 2018 года суд заблокировал доступ к мессенджеру. [1]

Прежде чем выяснять последствия ограничения доступа, мы отметим, что мотивом для данного решения стали утверждения ФСБ, на фоне спора Роскомнадзора и Telegram, об использовании данного мессенджера террористами в России в целях межличностной связи и своими кураторами из-за границы. Также резонансным стало дело террориста-смертника и его кураторов, использовавших данную программу во всех стадиях подготовки теракта в метро Санкт-Петербурга 03.04.2017 на перегоне между станциями «Технологический институт» и «Сенная площадь», посредством взрыва неустановленного, на тот момент, взрывного устройства[2]. После данного события представительство ФСБ направило основателю Telegram Павлу Дурову запросы на предоставление информации для декодирования сообщений в отношении шести номеров. В следствии отсутствия ответа на направленный запрос, Роскомнадзор обратился в Таганский суд Москвы с иском о блокировке мессенджера, и 13.04.2018

[1]История блокировки мессенджера Telegram в России. РИА Новости. URL: https://ria.ru/20200618/1573145082.html (дата обращения: 23.03.2024).

[2]По поручению Председателя СК России уголовное дело по факту взрыва в метро Санкт-Петербурга принято к производству Главным управлением по расследованию особо важных дел. URL: https://sledcom.ru/news/item/1113066/ (дата обращения: 23.03.2024).

произошла блокировка доступа к мессенджеру по всей территории Российской Федерации.

Данная блокировка показала, насколько неэффективны подобные решения во время процветания программного оборудования, поскольку наличие прокси-сервера позволяет обходить подобные ограничения. В частности, после ограничения доступа к Telegram были выпущены обновления с опцией SOCKS (прокси-сервер), предоставляемая посредством нескольких ботов: @socks5_bot; @proxy_socks5_bot; @ShadowSocks_bot[1]. Подобные «прокси» изменяют IP-адрес, к которому обращается только клиент Telegram, зашифровывает весь трафик. Соответственно инструкции по обходу различных блокировок, шифрованию трафика являются общедоступными.

Учитывая ранее рассмотренные средства анонимизации следует обозначить, что большая часть преступных деяний, в виде распространения негативного контента в сети, совершается в интернет-платформах, закрепляющих за каждым лицом идентифицирующий номер (ID – англ. Data name, identifier — опознаватель), аналог паспорта в сети Интернет, привязывающийся к устройству, посредством которого был осуществлен вход в социальную сеть. Подобная идентифицирующая информация способствует изобличению лица, опубликовавшего подобный контент.

Механизмы противодействия анонимизации направлены на то, чтобы предотвратить использование технологий анонимизации трафика для совершения преступлений в сети Интернет. Ниже приведены некоторые из механизмов протяфыцйфиводействия анонимизации и их перспективы[2].

1. **Анализ трафика**: один из наиболее распространенных методов противодействия анонимизации заключается в анализе трафика, проходящего через сеть. Этот метод позволяет выявить необычные шаблоны поведения, которые могут указывать на использование технологий анонимизации. Например, анализ трафика может выявить тот факт, что несколько пользователей входят в сеть с одного и того же IP-адреса, что может указывать на использование сети Tor.

2. **Идентификация пользователей по их поведению в сети**: этот метод заключается в сборе информации о поведении пользователей в сети, такой как частота посещений сайтов, продолжительность сеансов, выбор сайтов и т.д. Эта информация может быть использована для идентификации пользователей, даже если они используют технологии анонимизации.

3. **Блокировка доступа к анонимизаторам**: некоторые организации и государственные структуры блокируют доступ к известным анонимизаторам, таким как сеть Tor или VPN-сервисы. Этот метод может быть эффективным для предотвращения доступа к определенным ресурсам, но он не всегда эффективен

[1]Прокси для Telegram, настройка и подключение на ПК, Android и iOS. URL: https://dzen.ru/a/YKzYL-cWmgiB3ufr (дата обращения: 27.03.2024).

[2]Родвилина В.А., Родвилин И.П., Коломинов В.В. Проблемы противодействия использования анонимности в сети интернет в преступных целях // Криминалистика: вчера, сегодня, завтра. 2021. №4 (20). С. 68–73.

для блокировки всех видов анонимизации трафика. Реализация на уровне правовых законодательных актов имеет начало в 2017 году. В период данного года Указом Президента Российской Федерации от 09.05.2017 № 203 была принята Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 гг. в целях противодействия «цифровой» преступности». Также с 01.11.2017 вступает в законную силу Федеральный закон от 29.07.2017 № 276-ФЗ[1], запрещающий не сами анонимайзеры как технические средства, а лишь те VPN-сервисы, которые откажутся блокировать доступ к запрещенным сайтам.

4. **Использование систем глубокого обучения (искусственный интеллект)**: системы глубокого обучения могут быть использованы для анализа больших объемов данных, собранных из сети, и выявления необычных шаблонов поведения, которые могут указывать на использование технологий анонимизации. Этот метод может быть эффективным для выявления новых видов анонимизации трафика, которые еще не известны.

5. **Сотрудничество между организациями**: противодействие анонимизации требует сотрудничества между различными организациями, такими как провайдеры услуг Интернет, правоохранительные органы и другие. Совместными усилиями можно достичь более эффективного противодействия анонимизации трафика посредством

В целом, перспективы развития механизмов противодействия анонимизации связаны с развитием технологий анонимизации трафика. По мере появления новых технологий анонимизации появляются и новые методы противодействия. Однако, следует помнить, что противодействие анонимизации должно соблюдать баланс между защитой конфиденциальности пользователей и предотвращением совершения преступлений в сети Интернет.

Р.И. Бардачевский

О направлениях повышения профессиональной подготовки следователей в области информационных технологий и кибербезопасности

Аннотация. В приведенной статье автор на основе собственной практики и научных исследований описывает ряд направлений профессиональной подготовки следователей в области информационных технологий и кибербезопасности.

Ключевые слова: противодействие киберпреступности, подготовка следователей.

[1]Федеральный закон от 29.07.2017 № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации».

Согласно классическому определению, криминалистика является наукой, исследующей закономерности механизма преступления, возникновения информации о преступлении и его участниках, закономерностях собирания, исследования, оценки и использования доказательств и основанных на познании этих закономерностей специальных методах и средствах судебного исследования и предотвращения преступлений.[1] Функции криминалистики предполагают изучение специфики самого преступного деяния, как объекта криминалистического познания с учетом закономерностей его совершения, раскрытия и расследования.

Тем самым, познающий обстоятельства совершенного в киберпространстве преступного деяния следователь обязан обладать знаниями о механизмах таких преступлений, закономерностях возникновения и собирания их следов.

Для реализации таких задач криминалистического исследования компьютерной информации, средств ее обработки и защиты В.Б. Вехов выделяет следующие направления в предлагаемой им теории:

1. Криминалистическое учение о компьютерной информации;
2. Криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей;
3. Криминалистическое использование компьютерной информации, средств ее обработки и защиты[2].

Эти направления определяют необходимый для следователя объем знаний, применяемый при расследовании киберпреступлений, отражающихся в электронных цифровых следах.

В свою очередь, на основании анализа механизма следообразования в компьютерных системах предлагается рассмотреть классификацию электронно-цифровых следов, в качестве основания которой будет фигурировать степень опосредованности воздействия пользователя на компьютерную систему: следы непосредственные и опосредованные.

Под непосредственными следами будут подразумеваться электронно-цифровые следы, имеющие прямую (непосредственную) связь с причиной (целью) воздействия пользователя на компьютерную систему. В качестве таких следов выступают компьютерные данные, образованные пользователем посредством устройств ввода (клавиатура, микрофон, светочувствительная матрица и пр.), скопированные (перемещённые) файлы, почтовые отправления, переписка с использованием мессенджеров, история запросов Интернет-браузера, журнал вызовов, записи в прикладных базах данных и пр. Указанные следы могут быть как локальными (то есть находящимися непосредственно на носителе, который может быть изъят и подвержен аналитическому

[1] Криминалистика: учебник / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская; под ред. Р.С. Белкина. М.: Норма, 2008. С. 41.

[2] Вехов В.Б. Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики: сб. трудов участников междунар. науч.-практич. конф. Ростов н/Д., 2017. С. 41.

исследованию), так и удалёнными (находящимися на ресурсе, доступ к которому обеспечивается с применением средств телекоммуникации, т.е. канала связи).

В качестве опосредованных следов рассматриваются электронно-цифровые следы, не имеющие прямой связи с причиной (целью) воздействия пользователя на компьютерную систему, но инициированные этим воздействием, обусловленные особенностями функционирования системного программного обеспечения, стандартами форматов файлов и протоколов передачи данных. К таким следам относятся записи в файлах журналирования системных событий, файлах реестра операционной системы, метаданные пользовательских файлов (например, EXIF), записи служебных баз данных, таблиц размещения файлов и пр.[1]

Знания о следах и механизмах следообразования формируют направленность интеллектуальной деятельности следователя на правильное познание закономерностей собирания, исследования, оценки и использования соответствующих доказательств.

В свою очередь, необходимость поиска и применения адекватных мер противодействия киберпреступности, защиты информационной инфраструктуры обуславливают пристальное внимание общества к качеству подготовки специалистов по противодействию киберпреступлениям.

К необходимым компетенциям современные исследователи обоснованно относят:

1) Фундаментальные знания в области информационных технологий и кибербезопасности:

– архитектура и организация функционирования ЭВМ;

– современные вычислительные системы и сети связи, сетевые технологии;

– администрирование современных операционных систем;

– администрирование баз данных;

– работа с большими данными;

– системы искусственного интеллекта;

– средства мониторинга информационных сетей;

– уязвимости современных программных и аппаратно-программных средств.

2) Общие методы и средства обеспечения информационной безопасности:

- защищенные сетевые технологии глобального, корпоративного и локального назначения;

– математические аспекты защиты информации, криптографии, стеганографии, крипто и стегоанализа;

– способы и средства разработки защищенных приложений;

– системотехника и схемотехническое проектирование аппаратных средств информационной безопасности;

– построение и функционирование электронных платежных систем.

3) Понимание технологий реализации угроз информационной безопасности:

– программирование в современных операционных средах;

[1] Себякин А.Г. Тактика использования знаний в области компьютерной техники // Сер. Библиотека криминалиста. Москва, 2023. С. 17.

– анализ алгоритмов;
– реверс-инжиниринг программных текстов;
– атаки на электронные платежные системы;
– поиск следов и методы расследования киберпреступлений в кредитно-финансовой сфере.

4) Понимание принципов управления бизнесом и обеспечения его информационной безопасности:
– гражданско-правовые отношения;
– основы управления предприятием и организацией;
– описание бизнес-процессов;
– основные бизнес-процессы банка;
– нормативная база Центрального банка Российской Федерации;
– нормативно-правовая база информационной безопасности;
– автоматизированные системы обработки, хранения и передачи информации с учетом уровней и критериев безопасности.

5) Понимание принципов управления рисками:
– международные стандарты управления рисками и информационной безопасности;
– Базельские стандарты;
– теория вероятностей и математическая статистика;
– теория игр;
– оценка экономической эффективности[1].

Таким образом, приведенные направления являются одними из базовых для подготовки следователей, специализирующихся в расследовании киберпреступлений.

А.М. Гапанович

О борьбе с киберпреступностью в Республике Беларусь

Аннотация. В статье раскрываются подходы к термину «киберпреступление», анализируется законодательство Республики Беларусь, регламентирующее ответственность за преступления против компьютерной безопасности, приводятся данные официальной статистики состояния киберпреступности в республике, а также меры, предпринимаемые Следственным комитетом по борьбе с этим явлением.

***Ключевые слова*:** киберпреступность, компьютерная безопасность, кибербезопасность, легализация преступных доходов, финансирование терроризма, киберцентр, Следственный комитет, Институт Следственного комитета.

[1] Шеремет И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. № 5 (18). С. 3–7.

Быстрое развитие в современном мире информационно-телекоммуникационных технологий привело к интенсивному внедрению электронных (цифровых) устройств в повседневную жизнь каждого человека, что в свою очередь повлекло возникновение и широкое распространение такого явления как киберпреступность (киберпреступление).

Сам термин «киберпреступность» стал применяться в зарубежной печати в начале 1960-х гг., когда были установлены первые случаи правонарушений, совершенных с использованием электронно-вычислительных машин (ЭВМ). В 1990-е гг. интеллектуальный потенциал молодых людей стал все чаще проявляться в стремлении обогатиться путем незаконного снятия (перевода) денежных средств с использованием электронных технологий. Первое высокотехнологичное преступление на территории нашей республики было зарегистрировано 20 ноября 1998 г., когда, внедрив в программное обеспечение «компьютера-жертвы» вредоносную программу типа «троянский конь» под названием Back Orifice, обвиняемый осуществил несанкционированный доступ к сетевым реквизитам пользователей сети Интернет из числа клиентов крупнейшего в Беларуси столичного сервис-провайдера[1].

Что же такое киберпреступление (киберпреступность)? Единых подходов к данному определению нет, хотя оно активно используется и в доктрине, и на практике. Даже в принятом международном правовом акте, посвященном киберпреступности – Будапештской конвенции о киберпреступности (далее – Конвенция), единства нет, т. к. в ее тексте происходит подмена понятий – термин «киберпреступление» заменяется термином «компьютерное преступление». При этом Конвенция содержит обширное перечисление преступлений относимых к киберпреступлениям – противозаконный доступ к компьютерной системе; неправомерный перехват компьютерных данных; воздействие на компьютерные данные; противозаконное использование компьютерных устройств, программ, паролей, кодов доступа и иных подобных данных; мошенничество с использованием компьютерных технологий; правонарушения, связанные с производством и распространением детской порнографии; правонарушения, связанные с нарушением авторского права и смежных прав[2]. Таким образом Конвенцией к числу киберпреступлений отнесены многие преступления, при совершении которых используется компьютерная техника.

По мнению Лаборатории Касперского (далее – Лаборатория) киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. К ней Лаборатория относит: мошенничество с использованием электронной почты и интернета; кражу цифровой личности (хищение и

[1] Полещук Д.Г. Становление и развитие уголовно-правовой охраны информационной безопасности. URL: http://ncpi.gov.by/document/?regnum=U02300728 (дата обращения 03.04.2024).

[2] Конвенция о компьютерных преступлениях. URL: https://rm.coe.int/1680081580 (дата обращения 03.04.2024).

использование личных данных); кражу данных платежных карт и другой финансовой информации; хищение и перепродажу корпоративных данных; кибершантаж (вымогательство денег под угрозой атаки); атаки с использованием программ-вымогателей; криптоджекинг (майнинг криптовалют с использованием чужих ресурсов); кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным); нарушение работы систем с целью компрометации сети; нарушение авторских прав; онлайн-торговлю запрещенными товарами; домогательства; изготовление или хранение детской порнографии[1].

Сотрудники государственного учреждения "Научно-практический центр проблем укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь" В.В. Белокопытов и В.М. Филиппенков к киберпреступлению относят правонарушение, непосредственно связанное с использованием компьютерных технологий и сети Интернет, включающий в себя распространение вирусов, нелегальную загрузку файлов, а также кражу персональной информации, например информации по банковским счетам[2].

М. Герке полагает, что термин киберпреступление имеет довольно широкое значение, к нему может быть отнесено любое преступление, совершенное в электронной среде, т. е. действие посредством компьютера, которое является незаконным и которое может быть совершено при помощи глобальных электронных сетей[3] .

Д.В. Грибанов считает, что понятие киберпреступление может объединить такие понятия, как интернет-преступление, а также компьютерное преступление и связанное с компьютером преступление, совершаемые с использованием компьютерных (электронных) сетей или в так называемом кибернетическом пространстве[4].

М.С. Абламейко называет киберпреступлениями общественно опасные деяния, которые совершаются с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете[5].

Более определенно данный вопрос регулирует законодательство Республики Беларусь. Так, согласно ст. 8 Концепции информационной безопасности Республики Беларусь к киберпреступлениям отнесены исключительно предусмотренные Уголовным кодексом Республики Беларусь (далее – УК)

---

[1] Что такое киберпреступность? Защита от киберпреступности. URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime?ysclid=lutxa8a3wi453780484 (дата обращения 04.04.2024).

[2] Белокопытов В.В., Филиппенков В.М. Особенности совершения и предупреждения киберпреступлений (Часть 1) // КонсультантПлюс. Беларусь: ООО «ЮрСпектр». Минск, 2024.

[3] Герке М. Понимание киберпреступности: Руководство для развивающихся стран. URL: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html (дата обращения 04.04.2024).

[4] Грибанов Д.В. Кибернетический терроризм: новая угроза общественной безопасности // Российский юридический журнал. 2004. № 4. С. 75–78.

[5] Абламейко М.С. Правовая защита от кибератак и действия Республики Беларусь // Юридический журнал. Минск: Минский институт управления, 2008. № 3. С. 70–78.

преступления против **информационной безопасности** (Раздел XII, Глава 31 УК)[1].

Необходимо отметить, что в 2021 г. в соответствии с внесенными в УК изменениями и дополнениями название указанных раздела и главы изложены в новой редакции, называются и содержат преступления против **компьютерной безопасности** (ст. ст. 349-355 УК), диспозиции статей которых существенно обновились. К ним законодателем отнесены следующие пять составов преступлений (ст. ст. 351, 353 К исключены): несанкционированный доступ к компьютерной информации (ст. 349 УК); уничтожение, блокирование или модификация компьютерной информации (ст. 350 УК); неправомерное завладение компьютерной информацией (ст. 352 УК); разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354 УК); нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК). Специфичность названных составов преступлений обусловлена особенностями их предмета – компьютерная программа, система, сеть или информация.

Кратко и в общем характеризуя преступления против компьютерной безопасности необходимо согласиться с М.А. Дубко, который отмечает следующее. Деяние при совершении преступлений против компьютерной безопасности проявляется в активном поведении субъекта. Большинство составов являются материальными, поэтому общественно опасные последствия выступают обязательным признаком объективной стороны таких преступлений, который подлежит установлению. Указанные преступления считаются оконченными с момента наступления общественно опасных последствий, указанных в статье. Законодательное определение преступных последствий в диспозициях статей главы 31 УК определяется через оценочные признаки в виде существенного вреда или тяжких последствий, которые устанавливаются органом, ведущим уголовный процесс, в каждом конкретном случае на основе фактических обстоятельств дела[2].

На состоявшемся 18 декабря 2019 г. заседании Президиума Верховного Суда Республики Беларусь, посвященном практике рассмотрения судами уголовных дел о преступлениях против информационной (компьютерной) безопасности отмечалось, что за истекшие к тому моменту шесть лет обвинительные приговоры по рассматриваемой категории уголовных дел постановлены в отношении всего 114 лиц. При анализе судебной практики очевидной стала проблема терминологии. Понятийный аппарат достаточно сложный и требует наличия как элементарных, так и специальных знаний в области информационных технологий. Большинство ошибок, которые допускались судами при рассмотрении дел данной категории, обусловлено недостаточным

[1] Постановление Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь». URL: http://ncpi.gov.by/document/?regnum=p219s0001&q_id=10493884 (дата обращения 05.04.2024).

[2] Барков А.В. Уголовное право: учеб. пособие / А. В. Барков [и др.] ; под ред. А. Л. Савенка, А. В. Шидловского, К. С. Захилько. Минск: БГУ, 2023. С. 529–530.

уровнем технических знаний в сфере компьютерных технологий. Выходом из ситуации определено развитие специализации судей по данной категории дел, повышение уровня их технических и технологических знаний, совершенствование законодательства в этой сфере[1].

Одним из проблемных вопросов противодействия киберпреступлениям является высокая степень их латентности. По причине излишней доверчивости, банальной невнимательности, неосведомленности о способах совершения такого рода преступлений, а в некоторых случаях из-за личной меркантильности многие наши соотечественники становятся жертвами преступников, при этом некоторые из них и вовсе не сообщают о произошедшем в правоохранительные органы.

Юридические лица также иногда предпочитают решать возникающие проблемы без участия правоохранительных органов. Должностные лица пострадавших организаций опасаются, что убытки от расследования киберпреступления могут оказаться выше суммы причиненного ущерба. Поскольку правоохранительные органы, как правило, изымают на срок до двух месяцев сервер для производства судебной экспертизы, это может привести к проблемам в деятельности юридического лица. Кроме того, организация опасается подрыва репутации, а также выявления в процессе расследования различных правонарушений в работе самой пострадавшей компании[2].

Следует отметить, что по сложившейся практике термин киберпреступления интерпретируется гораздо шире и охватывает не только преступления, предусмотренные главой 31 УК, но и входит в совокупность с экономическими преступлениями (предпринимательская деятельность, осуществляемая без лицензии (ст. 233 УК), уклонение от уплаты налогов, сборов (ст. 243 УК), включает преступления связанные с хищениями, в том числе мошенничество (ст. 209 УК), вымогательство (ст. 208 УК), хищение имущества путем модификации компьютерной информации (ст. 212 УК), а также затрагивает преступления связанные с незаконным оборотом наркотиков (ст. 328 УК) и ряд других.

В качестве подтверждения серьезности положения дел в республике с киберпреступностью следует привести некоторые сведения статистики. Согласно данным Национального статистического комитета Республики Беларусь о социально-экономическом положении республики в 2022 г. в сравнении с предыдущими годами число зарегистрированных хищений имущества путем модификации компьютерной информации (ст. 212 УК) и преступлений против компьютерной безопасности (ст. ст. 349-355 УК), при сравнении 2010 г. и 2022 г. возросло более чем в 5 раз и соответственно составило 2 523 и 13 541 преступление. При этом количество осужденных по приговорам судов, вступившим в законную силу, в эти годы изменилось не так

[1] Президиум Верховного Суда Республики Беларусь принял постановление о практике рассмотрения судами уголовных дел о преступлениях против информационной безопасности (глава 31 УК). URL: https://www.court.gov.by/ru/justice/press_office/3c1d6c901c0c456e.html (дата обращения 08.04.2024).

[2] Никитин Ю.А. Преступления против информационной безопасности (Часть 1): противодействие и квалификация // КонсультантПлюс. Беларусь / ООО «ЮрСпектр». – Минск, 2024.

существенно и составило 953 и 1205 лиц, соответственно[1]. Это свидетельствует о наличии существенных проблем у правоприменителей при раскрытии и расследовании названных видов преступлений. Таким образом, киберпреступления чаще всего остаются нераскрытыми. Как показывает следственная практика, из года в год предварительное расследование по большинству уголовных дел о таких преступлениях приостанавливалось в связи с неустановлением лица, подлежащего привлечению в качестве обвиняемого.

На состоявшемся 16 февраля 2024 г. заседании коллегии Следственного комитета Республики Беларусь (далее – СК) с подведением итогов работы следственного ведомства за 2023 г. отмечено, что по сравнению с 2022 г. в 2023 г. общий уровень преступности снизился на 3,5 % и составил немногим более 85 тысяч преступлений. Одновременно с этим отмечается рост тяжких и особо тяжких преступлений – за счет повышения уровня киберпреступности. Так, доля киберпреступности составила 21,5 % от общего числа зарегистрированных в 2023 г. преступлений, что сопоставимо с количеством совершенных в этом году краж. В 2022 г. уровень киберпреступности в общей структуре преступлений составлял 16,5 %. Председатель СК Д.Ю. Гора обратил внимание, что в отношении белорусов киберпреступники в основном работают из-за границы, преимущественно с территории Украины. Во взаимодействии с Министерством внутренних дел Республики Беларусь (далее – МВД) в прошлом году пресечена деятельность трех крупнейших скам-групп, численностью более 50 лиц, члены которых за три года совершили более 20 тысяч хищений с банковских карт белорусов. По данной категории дел потерпевшим вернули более 39 миллионов белорусских рублей. Была пресечена деятельность крупнейшего теневого криптообменника, годовой оборот, которого составил около 40 миллионов долларов США[2].

Анализ практики расследования киберпреступлений, свидетельствует, что для вывода похищаемых денежных средств, а также иного полученного преступным путем дохода преступники используют банковские платежные карточки и банковские счета, открытые в банковских учреждениях Республики Беларусь. При этом платежные инструменты они приобретают на теневом рынке в сети Интернет, либо получают от «подставных» граждан (так называемых «дропов» и «дроповодов»), которые из корыстных побуждений оформляют на себя банковские платежные карты, а затем распространяют их реквизиты и аутентификационные данные. Для нелегального транзита и вывода денежных средств преступники также незаконно используют финансовые инструменты, получив к ним доступ удаленно с помощью специальных вредоносных программных средств, в результате взлома учетной записи, используемой для авторизации межбанковской системы идентификации, неавторизованные «p2p-

[1]Статистический ежегодник, 2023. URL: https://belstat.gov.by/upload/iblock /0a7/lk1zigmat2 zbcwvo3ljrfm1tow2f5zd2.pdf) (дата обращения 09.04.2024).

[2] Следственным комитетом на заседании коллегии подведены итоги работы за прошлый год. URL: https://sk.gov.by/ru/news-ru/view/sledstvennym-komitetom-na-zasedanii-kollegii-podvedeny-itogi-raboty-za-proshlyj-god-13446/ (дата обращения 08.04.2024).

переводы» и т. д.[1]. Здесь следует отметить, что «дропов», согласившихся за легкие деньги открыть на свое имя банковские пластиковые карточки, иные платежные инструменты и средства платежа и осуществить их сбыт, а равно распространивших их реквизиты либо аутентификационные данные ждет уголовная ответственность за незаконный оборот данных средств и инструментов платежа (ст. 222 УК) с наказанием вплоть до 10 лет лишения свободы в случае совершения указанных действий повторно, организованной группой либо в особо крупном размере.

Международный опыт показывает, что при отмывании доходов от киберпреступлений характерным является использование следующих механизмов: использование счетов, открытых по утраченным документам или на подставных лиц; использование фиктивных (транзитных) предприятий; проведения цепи финансовых операций через несколько банковских счетов с помощью удаленного доступа; использования наличных на последнем этапе цепи финансовых операций; использования альтернативных платежных систем (электронные платежи), как национальных, так и международных; покупка электронных денег и использование систем платежей через электронные кошельки; конвертация незаконных доходов в товары путем приобретения последних посредством сети интернет. Это отчасти подтверждает и национальная следственная практика. В схемах получения и (или) легализации преступных доходов чаще всего использовались такие продукты банковской системы, как банковские переводы (во всех группах предикатных преступлений) и банковские платежные карточки (мошенничества, преступления, связанные с использованием информационных технологий). Таким образом, киберпреступления представляют высокую степень угрозы в области легализации преступных доходов и финансирования терроризма, в связи с чем в целях предотвращения легализации преступных доходов должны рассматриваться в качестве предикатных по отношению к ним[2].

С принятием Указа Президента Республики Беларусь от 29 августа 2023 г. № 269 «О мерах по противодействию несанкционированным платежным операциям» (далее – Указ № 269) у следователей появилась возможность оперативно блокировать движение денежных средств по банковскому счету и электронных денег на электронных кошельках, тем самым своевременно защищать интересы лиц, которым в результате преступной деятельности причиняется ущерб, защищать права потребителей финансовых услуг на платежном рынке, пресекать совершение преступлений, делая невозможным осуществление несанкционированных платежных операций.

---

[1] Мотолько А.Ф. Об отдельных аспектах использования автоматизированной системы обработки инцидентов в рамках обеспечения противодействия преступности // Основные направления совершенствования системы национальной безопасности: материалы II Международной научно-практической конференции (Минск, 17 ноября 2023 года). Минск: СтройМедиаПроект, 2023. С. 360–363.

[2] Дубко М.А. Киберпреступность: риски и угрозы отмывания преступных доходов. URL: http://ncpi.gov.by/document/?regnum=u02200198&q_id=10560658 (дата обращения 09.04.2024).

Указом № 269 определены полномочия Национального банка Республики Беларусь, поставщиков платежных услуг и правоохранительных органов в сфере противодействия несанкционированным (инцидентам) и попыткам их совершения, регламентирован порядок информационного взаимодействия по обмену сведениями об инцидентах посредством Автоматизированной системы обработки инцидентов Национального банка (далее – АСОИ). АСОИ осуществляются получение, обработка, накопление и хранение информации о совершенных операциях либо попытках совершения несанкционированных переводов денежных средств (электронных денег), фактах или попытках мошенничества в банковском секторе, а также о нарушениях безопасности и защиты информации, в том числе компьютерных атаках, направленных на объект информационной инфраструктуры, которые могут привести к случаям и попыткам осуществления несанкционированных переводов денежных средств и электронных денег.

Согласно Указу № 269 следователи наделены правом получать информацию об инцидентах из АСОИ и оперативно предоставлять посредством нее такие сведения поставщикам платежных услуг и Национальному банку. Кроме этого, СК уполномочен принимать решения о приостановлении на срок до 10 суток расходные операций по банковскому счету или электронному кошельку пользователей платежных услуг, являющихся участником инцидента, в отношении которого имеется подозрение об участии в совершении противоправных деяний. В последующем от органа уголовного преследования требуется принятие иных уголовно-процессуальных мер в отношении денег, заблокированных на счетах, т. к. мера по приостановлению по ним расходных операций является временной.

В целях формирования в республике единообразной правоприменительной практики на начальном этапе реализации Указа № 269 в Генеральной прокуратуре Республики Беларусь 27 февраля 2024 года проведено заседание межведомственной рабочей группы в рамках которого изучен и одобрен к использованию с 1 марта 2024 года, разработанный СК и МВД алгоритм взаимодействия их территориальных подразделений, которым регламентируется порядок действий сотрудников криминальной милиции и следователей при рассмотрении заявлений или сообщений о преступлениях, а также проведения процессуальных действий, требующих санкционирования прокурором или его заместителем.

Большинство кибератак совершается преступниками с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров, компьютерной системы или сетей из строя из иных личных или политических мотивов.

В целях повышения уровня защиты национальной информационной структуры от внешних и внутренних угроз Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» в республике предписано создать национальную систему обеспечения кибербезопасности. Государственным органом, осуществляющим координацию деятельности

других государственных органов и иных организаций по ее созданию и функционированию, обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры, определен Оперативно-аналитический центр при Президенте Республики Беларусь в структуре которого создан Национальный центр кибербезопасности (далее – НЦК). К полномочиям НЦК отнесено:

- взаимодействие с центрами кибербезопасности, в том числе осуществление сбора, обработки, анализа и обобщения информации, поступающей из этих центров, формирование и ведение общереспубликанской базы данных о киберинцидентах;
- координация и реализация мероприятий по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов на объектах информационной инфраструктуры, реагированию на такие киберинциденты;
- осуществление автоматизированных сбора, обработки, накопления, систематизации и хранения данных о кибербезопасности объектов информационной инфраструктуры, направленных на обнаружение, предотвращение и минимизацию последствий кибератак и вызванных ими киберинцидентов на указанных объектах, реагирование на такие киберинциденты;
- оказание методической и практической помощи государственным органам и иным организациям в вопросах обеспечения кибербезопасности принадлежащих им объектов информационной инфраструктуры;
- проведение учений по действиям при возникновении киберинцидентов на объектах информационной инфраструктуры, разработка программ и методик проведения этих учений, сценариев реагирования на кибератаки;
- организация проведения аналитических и научных исследований в области обеспечения кибербезопасности, при необходимости распространение результатов таких исследований, в том числе в средствах массовой информации.

Для реализации функции реагирования на киберинциденты в составе НЦК создана и функционирует национальная команда реагирования на киберинциденты (CERT.BY), которая взаимодействует по данным вопросам:

- на международном (межгосударственном) уровне – с форумом команд реагирования на компьютерные инциденты (FIRST);
- на национальном уровне – с командами реагирования на киберинциденты центров кибербезопасности[1].

Сами же центры обеспечения кибербезопасности и реагирования на киберинциденты (далее – киберцентры) предстоит создать в 2024-2025 гг. в государственных органах и иных организациях перечень которых определен постановлением Совета Министров Республики Беларусь от 23 февраля 2024 г. № 120 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40». Киберцентры также могут создаваться и организациями, имеющими лицензии на деятельность по технической или криптографической

[1] Указ Президента Республики Беларусь от 14.02.2023 № 40 «О кибербезопасности». URL: http://ncpi.gov.by/document/?regnum=p32300040&q_id=10560221 (дата обращения 10.04.2024).

защите информации в части составляющих данный вид деятельности работ по проектированию, созданию, аудиту систем информационной безопасности критически важных объектов информатизации.

Для эффективного противодействия организованной киберпреступности в середине 2022 г. в структуре СК было создано новое подразделение – главное управление цифрового развития предварительного следствия, сотрудники которого основную свою деятельность сконцентрировали на решении трех основных задач. Во-первых, это установление и задержание руководящего звена преступной группировки. Во-вторых, выявление и устранение цифровых средств совершения преступлений – фишинговых ресурсов, скомпроментированных банковских карт, сим-карт, других инструментов преступлений. В СК на сегодня выработан эффективный алгоритм оперативной блокировки фишинговых ресурсов – в течение нескольких часов с момента их выявления. В-третьих, пресечение деятельности белорусских пособников – «дропов», «дроповодов», которые за деньги на системной основе снабжают группировки банковскими картами, сим-картами для использования при совершении преступлений. За последний год СК выявлена и пресечена деятельность нескольких групп пособников («дропов») численностью в пределах 100 и более лиц, действовавших на территории разных областей страны.

В последнее время наблюдается тенденция роста киберпреступлений с использованием фейкового контента, созданного в том числе при помощи программ искусственного интеллекта. Регистрируется большое количество мошеннической рекламы псевдоинвестиционных компаний, которые призывают белорусов онлайн вкладывать деньги или криптовалюту под большие проценты. Для усыпления бдительности потенциальных жертв мошенники действуют якобы от имени крупных белорусских и российских компаний – «Беларуськалий», «Белнефтехим», «Белэнерго», «Газпром» и пр. Создается и распространяется посредством социальных сетей поддельная видеореклама якобы с участием видных белорусских и зарубежных общественных и политических деятелей, смонтированным голосом которых призывают к передаче всех своих сбережений преступникам. В связи с этим сейчас проводится активная работа над выработкой эффективных мер противодействия мошенническому контенту, распространяемому через социальные сети и интернет-рекламу[1].

Необходимо отметить, что ведущая роль в формировании у следователей знаний, умений и навыков в сфере досудебного уголовного производства, в том числе по уголовным делам о киберпреступлениях, отведена учреждению образования «Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь» (далее – Институт), созданному в системе СК в соответствии с Указом Президента Республики Беларусь от 25

[1] Андрей Мотолько: механизм оперативной блокировки похищенных денежных средств заработает в начале года. URL: https://sk.gov.by/ru/news-ru/view/andrej-motolko-mexanizm-operativnoj-blokirovki-poxischennyx-denezhnyx-sredstv-zarabotaet-v-nachale-goda-13215/ (дата обращения 11.04.2024).

июня 2020 г. № 244 «О создании учреждения образования», начавшему свою деятельность в 2021 году.

В целях повышения цифровой грамотности следователей и удовлетворения потребности СК в обучении сотрудников тактике и методике расследования преступлений, совершенных с использованием высоких технологий, работе со специализированными программным обеспечением, научно-техническими средствами и криминалистической техникой в декабре 2022 г. в Институте создана и функционирует кафедра обеспечения цифрового развития предварительного следствия.

На базе Института реализуются образовательные программы дополнительного образования взрослых в сфере досудебного уголовного производства, проводятся учебные занятия по образовательным программам повышения квалификации «Собирание и использование компьютерной информации при расследовании преступлений», «Противодействие преступлениям, совершенным в сфере высоких технологий» и пр.

Уникальной современной образовательной киберплощадкой для следователей страны стал открытый в 2023 г. криминалистический полигон следственного ведомства, аналогов которому нет ни в Беларуси, ни в странах ближнего зарубежья. Высокотехнологический полигон представлен рядом локаций, в том числе локацией «квартира киберпреступника», которые, при необходимости, легко модернизируются. Основной методикой проведения занятий на учебном полигоне являются кейс-технологии. Так в локации «квартира киберпреступника» уже запрограммированы интерактивные задания, например проведение осмотра места происшествия, обыска и пр. Ознакомиться с учебным кейсом легко и быстро: достаточно воспользоваться личным мобильным телефоном – навести сканер на QR-код, размещенный у входа в локацию.

В силу того, что на передовой деятельности СК – обеспечение информационной безопасности и успешное расследование киберпреступлений, ведомственное учреждение образования осуществляет серьезную работу в сфере научно-методического обеспечения службы правоохранителей. Так, в январе 2023 г. состоялось знаковое событие, прошла презентация первого подготовленного Институтом учебного пособия «Компьютерная информация в следственной деятельности: собирание, оценка, использование», которое было высоко оценено Министерством образования Республики Беларуси и получило соответствующий гриф. Подтверждением актуальности и востребованности пособия стали награды, полученные изданием в 2023 г. в Республике Беларусь (приз имени В.Д. Спасовича в номинации «Следствие» (Министерство юстиции), диплом II степени Национального конкурса «Искусство книги» в номинации «Учебник нового столетия» (Министерство информации) и Российской Федерации (I-е место Международного конкурса на лучшее издание по проблемам совершенствования дополнительного профессионального образования (Всероссийский институт повышения квалификации сотрудников Министерства внутренних дел), I-е место в номинации «Криминалистика»

Всероссийского конкурса с международным участием на лучшее учебное (научное) издание (Санкт-Петербургская академия Следственного комитета).

В текущем году Институтом запланировано проведение специализированного курса повышения квалификации по вопросам раскрытия и расследования преступлений, связанных с оборотом виртуальных платежных средств и цифровых финансовых активов, а также коллективом авторов ведется работа над учебным пособием «Особенности расследования киберпреступлений, совершенных организованной преступной скам-группой».

Кроме этого, Институт в установленном порядке в рамках своей компетенции осуществляет международное сотрудничество в сфере подготовки, переподготовки и повышения квалификации кадров для СК, иных военизированных организаций и правоохранительных органов иностранных государств, научной деятельности и информационного обмена. Примером такой работы является состоявшаяся 11 апреля 2024 г. в г. Минске международная научно-практическая конференция «Противодействие преступлениям с использованием цифровых активов», организатором которой выступили СК и Институт. В обсуждении методов борьбы с киберпреступностью приняли участие представители Росфинмониторинга, Следственного комитета и Министерства внутренних дел России, сотрудники агентства по финансовому мониторингу Республики Казахстан, научно-методического центра цифровой криминалистики правоохранительной академии Республики Узбекистан, а всего более 100 экспертов в сфере борьбы с киберпреступностью.

Подытожив, отметим, что реализуемый СК совместно с иными заинтересованными ведомствами комплекс мер в целом позволил сдержать рост киберпреступности, установить кто и откуда атакует, какой преступный инструментарий использует. Это позволяет с оптимизмом смотреть в будущее с целью сделать невозможным совершение киберпреступлений в отношении граждан и юридических лиц, находящихся на территории Республики Беларусь.

М.Б. Киселев

Противодействие распространению фейков о деятельности российских Вооруженных Сил, добровольческих формирований, государственных органов и их дискредитации в условиях специальной военной операции

Аннотация. В статье рассматриваются вопросы уголовно-правового противодействия распространению заведомо ложной информации о деятельности российских Вооруженных Сил, добровольческих формирований и государственных органов по защите интересов страны, ее граждан, поддержанию международного мира и безопасности, а также их дискредитации, приведена практика следственных органов Следственного комитета Российской Федерации по борьбе с данными преступными проявлениями, высказаны предложения о целесообразности дачи Верховным Судом Российской

Федерации разъяснений по вопросам квалификации преступлений, предусмотренных ст. 207^3 и 280^3 УК РФ, подготовки в целях унификации подходов к правовой оценке соответствующих деяний обзора материалов судебной практики.

Ключевые слова: национальная безопасность, специальная военная операция, Вооруженные Силы Российской Федерации, добровольческие формирования, государственные органы Российской Федерации, информационно-телекоммуникационные технологии, распространение заведомо ложной информации, дискредитация, фейки.

Как справедливо отмечается в юридической литературе происходящие в современном информационном мире события глобального масштаба, неизбежно влекут активизацию киберпреступников, рост и появление новых видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий[1].

Не является в этом отношении исключением и геополитический конфликт России и коллективного Запада, вступивший в острую фазу с началом специальной военной операции на Украине, в условиях проведения которой российское государство испытывает не только политическое, экономическое, дипломатическое, военное, но и беспрецедентное информационное воздействие. Западные СМИ, социальные сети, мессенджеры и иные Интернет-ресурсы наводнила заведомо ложная и дискредитирующая информация о целях и задачах специальной военной операции, деятельности российских Вооруженных Сил и государственных органов, которую охотно тиражируют оппозиционно настроенные к действующей российской власти и проводимой внешней и внутренней политике страны граждане.

При этом нельзя не согласиться с мнением о том, что современное общество характеризуется снижением статуса истинных ценностей и подменой духовных устремлений личности потребительскими инстинктами толпы, что детерминирует его приверженность к безумному и недостоверному контенту, мгновенно распространяемому в медиасфере, и чем неправдоподобнее фейковая информация, тем более действенное влияние она оказывает на массовое сознание[2].

Распространение фейковой и дискредитирующей информации о деятельности российских Вооруженных Сил и государственных органов помимо подрыва их авторитета, нарушения прав граждан на объективную информацию направлено на формирование и радикализацию в стране протестных настроений, может привести к дестабилизации социально-политической обстановки и в условиях продолжающейся специальной военной

[1] Коимшиди Г.Ф., Саркисян А.Ж. Прогноз динамики IT-преступности в Российской Федерации на 2023 год // Расследование преступлений: проблемы и пути их решения. 2023. № 1. С. 76.

[2] Кушхов Х.Л., Мухтаров Д.Д. О потенциале фейков в современных информационных войнах // Журнал прикладных исследований. 2022. № 6. С. 82.

операции представляет серьезную угрозу для национальной безопасности Российской Федерации[1].

В этой связи следует отметить, что российский законодатель своевременно и оперативно отреагировал на возникшие угрозы, дополнив в марте 2022 года УК РФ статьями 207[3] и 280[3], установившими уголовную ответственность за дискредитацию Вооруженных Сил и распространение дезинформации об их деятельности[2], и расширив впоследствии действие этих норм в отношении посягательств на информацию об исполнении государственными органами своих полномочий за рубежом в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности, оказании Вооруженным Силам и войскам Национальной гвардии Российской Федерации содействия добровольческими формированиями[3].

Учитывая высокую степень общественной опасности рассматриваемых посягательств для личности, общества и государства, противодействие фейкам о действиях российских военных, представителей госорганов, добровольцев и их дискредитации в условиях продолжающейся специальной военной операции является для органов правопорядка приоритетным направлением деятельности, в которой ключевая роль с учетом компетенции отведена Следственному комитету Российской Федерации (далее – Следственный комитет).

В этой связи в Следственном комитете незамедлительно приняты необходимые меры, направленные на предотвращение массового распространения недостоверной и дискредитирующей информации о российской армии. В следственных органах ведомства организовано взаимодействие на данном направлении деятельности с органами прокуратуры, МВД и ФСБ России. В целях выявления ложных (фейковых) материалов, информации, дискредитирующей руководство страны, воинские формирования,

---

[1] См. подробнее: Бугера Н.Н., Лихолетов А.А., Лихолетов Е.А. Публичное распространение заведомо ложной информации о деятельности Вооруженных Сил Российской Федерации: некоторые вопросы толкования уголовного закона // Вестник Волгоградской академии МВД России. 2022. №2 (61). С 25 – 30; Ермолович Я.Н. Введена уголовная ответственность за фейки о Вооруженных Силах Российской Федерации (научно-практический комментарий к Федеральному закону «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» от 4 марта 2022 г. № 32-ФЗ) // Право в Вооруженных Силах – Военно-правовое обозрение. 2022. № 4. С. 74–85; Кибальник А.Г. Уголовная ответственность за распространение фейков об использовании Вооруженных Сил РФ. Как применять новую норму УК // Уголовный процесс. 2022. № 5. С. 63–64.

[2] Федеральный закон от 04.03.2022 № 32-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» // СПС «Консультант Плюс».

[3] Федеральные законы от 25.03.2022 № 63-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 150 и 151 Уголовно-процессуального кодекса Российской Федерации», от 18.03.2023 № 58-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», от 25.12.2023 № 641-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СПС «Консультант Плюс».

федеральные государственные органы и патриотически настроенных общественных деятелей, осуществляется круглосуточный мониторинг средств массовой информации, социальных сетей и других Интернет-ресурсов. В ходе данной работы изучаются публикации общественных деятелей, представителей оппозиционных движений, наиболее активных представителей антироссийской идеологии, налажено постоянное взаимодействие со средствами массовой информации, освещающими проведение специальной военной операции.

Выявляемым фактам размещения недостоверных сведений дается надлежащая правовая оценка, при наличии оснований незамедлительно возбуждаются и расследуются уголовные дела, инициируются мероприятия по ограничению доступа к информационным ресурсам, распространяющим фейки.

Так, уже 16.03.2022 в следственном управлении Следственного комитета по Томской области по результатам рассмотрения материалов регионального управления ФСБ России возбуждено уголовное дело по ч. 1 ст. 207^3 УК РФ в отношении жительницы ЗАТО г. Северск, которая в период с 04.03.2022 по 15.03.2022 размещала в одном из мессенджеров под видом достоверных сведений заведомо ложную информацию об использовании российских Вооруженных Сил в ходе специальной военной операции, якобы получая ее от очевидцев с мест событий, происходящих на территории Украины и республик Донбасса[1].

При этом в ходе проводимого в следственных органах ведомства мониторинга средств массовой информации анализируется и иностранная пресса на предмет выявления фактов распространения недостоверной информации на территории зарубежных государств, совершения действий по формированию у иностранных граждан ложных представлений о проводимой Вооруженными Силами Российской Федерации специальной военной операции на Украине, русофобских настроений.

К примеру, в апреле 2022 года в Главном следственном управлении Следственного комитета возбуждено по п. «б, в» ч. 2 ст. 207^3 УК РФ и расследуется уголовное дело в отношении неустановленных лиц, которые в марте 2022 года разместили в информационных изданиях западных стран, в том числе таких как «CNN», «BBC News», заведомо ложную информацию о якобы совершенных российской армией авиационных бомбовых ударах по зданиям городской больницы № 3 (роддома) и драматического театра в г. Мариуполе Донецкой Народной Республики, повлекших гибель и ранения мирных граждан[2].

Всего с момента введения уголовной ответственности за рассматриваемые деяния за 2022 – 2023 гг. следователями Следственного комитета возбуждено 303 уголовных дела по признакам преступлений, предусмотренных ст. 207^3 УК РФ,

---

[1] Двое жителей Томской области подозреваются в публичном распространении заведомо ложной информации об использовании ВС РФ. URL: www.tvtomsk.ru/news/75304-severchanka-podozrevaetsja-v-publichnom-rasprostranenii-zavedomo-lozhnoj-informacii-ob-ispolzovanii-vs-rf.html (дата обращения: 12.04.2024).

[2] ТАСС: СК РФ возбудил дело о фейках о ВС России после украинской провокации в Буче. URL: http://sledcom.ru/press/smi/item/1675053/ (дата обращения: 12.04.2024).

и 99 дел о совершении деяний, предусмотренных ст. 280[3] УК РФ, а по результатам проведенных расследований в суд направлено 147 дел о распространении заведомо ложных сведений (70 – в 2022 году и 77 – в 2023 году) в отношении 149 лиц и 55 дел о дискредитации российских военных, добровольцев и госорганов (6 – в 2022 году и 49 – в 2023 году) в отношении 60 лиц[1].

К примеру, по результатам рассмотрения оконченного в Главном следственном управлении Следственного комитета уголовного дела судом признан виновным в совершении преступления, предусмотренного п. «д» ч. 2 ст. 207[3] УК РФ, и осужден к лишению свободы на срок 8 лет с лишением права заниматься деятельностью, связанной с администрированием сайтов сети Интернет, сроком на 4 года известный журналист Невзоров (признан иностранным агентом), который будучи длительное время несогласным с внешней и внутренней политикой России, испытывая неприязнь к действующей власти, государственным органам, ведомствам и учреждениям Российской Федерации, в том числе Вооруженным Силам, последовательно 09.03.2022, 16.03.2022, 03.04.2022 и 06.04.2022 размещал на Интернет-ресурсах доступные неограниченному кругу лиц публикации и видеоматериалы, содержащие заведомо ложные сведения об обстрелах российскими военными городской больницы № 3 (роддома) в г. Мариуполе Донецкой Народной Республики, убийствах мирного населения в г. Буча Киевской области Украины, сопровождая публикации фейковыми фотографиями, достоверно зная, что их источниками являлись украинские СМИ, а достоверность официально опровергнута Минобороны России[2].

В следственном управлении Следственного комитета по Кировской области завершено расследование уголовного дела по обвинению в совершении преступления, предусмотренного ч. 2 ст. 280[3] УК РФ, Владимирова, который 17.08.2023 в г. Кирове, испытывая стойкую неприязнь к Вооруженным Силам Российской Федерации и органам государственной власти в связи с проведением специальной военной операции, по мотивам политической ненависти и вражды, при помощи источника открытого пламени поджог содержащую символику российских Вооруженных Сил палатку мобильного пункта отбора на военную службу по контракту, принадлежащую ФКУ «Военный комиссариат Кировской области», осуществил на свой мобильный телефон видеосъемку процесса ее горения и распространил соответствующую видеозапись среди своих знакомых в мессенджере WhatsApp.

По результатам судебного рассмотрения дела Владимиров признан виновным совершении инкриминируемого преступления и осужден к 2 годам лишения свободы с отбыванием в исправительной колонии общего режима с лишением

[1] Статистические сведения Следственного комитета Российской Федерации за 2022 – 2023 годы. URL: http://sledcom.ru (дата обращения: 12.04.2024).

[2] Приговор Басманного районного суда г. Москвы от 01.02.2023 по делу № 01-0152/2023 // Официальный сайт Басманного районного суда г. Москвы. URL: mos-gorsud.ru/rs/basmannyj/search (дата обращения 12.04.2024).

права заниматься деятельностью, связанной с администрированием сайтов в сети Интернет, сроком на 2 года[1].

В Главном следственном управлении Следственного комитета окончено уголовное дело по обвинению по п. «б» ч. 2 ст. 207^3 УК РФ гражданина Колумбии Хиральдо Сарая, обеспечившего совместно с иными иностранцами в составе организованной группы за получаемое из-за рубежа денежное вознаграждение, техническую подготовку и скрытное размещение в одном из торговых центров г. Москвы мобильных устройств, через которые путем удаленного подключения посредством сети Интернет, производилась массовая рассылка текстовых сообщений, адресованных абонентам российских операторов сотовой связи (всего распространено более 7 тыс. сообщений) с ложной информацией об использовании Вооруженных Сил Российской Федерации в ходе специальной военной операции. Приговором суда подсудимый осужден к 5 годам 2 месяцам лишения свободы с отбыванием наказания в колонии общего режима[2].

В профилактических целях в следственных органах ведомства организовано регулярное освещение в СМИ результатов следственной работы, при этом акцентируется внимание на неотвратимости наказания за совершение преступлений рассматриваемой категории, на системной основе используются формы прямого взаимодействия с общественностью, в том числе такие как проведение круглых столов, лекций и бесед в образовательных учреждениях и трудовых коллективах.

Активная деятельность следственных органов Следственного комитета по выявлению и расследованию фейков о деятельности российских военных, представителей госорганов, добровольцев и их дискредитации, примеры назначения судом достаточно сурового наказания за совершение рассматриваемых деяний, безусловно должны «остудить пыл» фейкометов из числа так называемых «ревнителей свободы слова» и «несогласных со спецоперацией».

Вместе с тем в целях общей превенции важнейшее значение имеет не суровость назначаемого за совершение преступлений наказания, а обеспечение неотвратимости ответственности за содеянное, правильность квалификации совершенных деяний. И в этой связи необходимо отметить, что в ходе складывающейся правоприменительной практики возникают вопросы, связанные:

1) с толкованием используемых в ст. 207^3, 280^3 УК РФ весьма общих, оценочных терминов и формулировок, таких как «заведомо ложная информация», «публичное распространение», «публичные действия»,

[1] Приговор Октябрьского районного суда г. Кирова от 07.12.2023 по делу № 1-623/23 (12302330022000029) // Официальный сайт Октябрьского районного суда г. Кирова. URL: oktyabrsky.kir.sudrf.ru / modules.php (дата обращения 12.04.2024).

[2] В Москве вынесен приговор по уголовному делу о распространении ложной информации о проведении специальной военной операции // URL: http://sledcom.ru/news/item/1792708/ (дата обращения: 12.04.2024).

«публичные призывы», «дискредитация», «под видом достоверных сообщений», что может повлечь случаи квалификации деяний во многом по принципу «на усмотрение правоприменителя»;

2) возможными сложностями в отдельных случаях разграничения уголовно-наказуемой дискредитации от критики действий отдельных должностных лиц, органов военного управления, или деятельности органов государственной власти;

3) конкуренцией норм и необходимостью разграничения деяний, подлежащих квалификации по ст. 207^3 и 280^3 УК РФ;

4) отсутствием четких критериев определения «тяжкие последствия» для целей ч. 3 ст. 207^3 УК РФ, что может повлечь сложности установления прямой причинной связи между фактом распространения информации и наступлением общественно опасных последствий;

5) ограничением рамок усмотрения правоприменителя детальным, исчерпывающим перечнем последствий, необходимых для квалификации деяния по ч. 2 ст. 280^3 УК РФ.

Во избежание ошибок в правоприменительной практике как уже ранее неоднократно отмечалось[1] представляются необходимыми дача Верховным Судом Российской Федерации соответствующих разъяснений по квалификации рассматриваемых преступных деяний, подготовка обзора материалов судебной практики, а также научно-практическое осмысление обозначенной проблематики.

И.Б. Коновалов

Приемлемость использования цифровых доказательств, полученных методами ОСИНТ, при расследовании экономических преступлений

Аннотация. Настоящая статья ставит своей целью исследование приемлемости использования цифровых доказательств, полученных методами ОСИНТ, в процессе расследования экономических преступлений. Для достижения данной цели рассматриваются нормативно-правовое регулирование применения таких доказательств, особенности использования ОСИНТ-методов, проведен анализ ряда процессуальных аспектов их использования, а также

[1] См. подробнее: Киселев М.Б. Уголовно-правовая охрана национальной безопасности Российской Федерации в информационном пространстве в условиях специальной военной операции // Правовой вектор конституционного развития России (к 30-летию со дня принятия Конституции Российской Федерации): сборник научных трудов Всероссийской научно-практической конференции, 14 декабря 2023 г. / Сост. С.О. Харламов. М.: Московский университет МВД России имени В.Я. Кикотя, 2024. С. 50 – 55; Пичугин С.А. Уголовная ответственность за деяние, предусмотренное статьей 207.3 УК РФ: вопросы регламентации и правоприменения // Отечественные и мировые проблемы уголовно-правовой науки. 2023. № 3. Т. 8. С. 61.

выработаны рекомендации по совершенствованию правового регулирования и правоприменения в данной области.

Ключевые слова: информационные технологии, ОСИНТ, цифровые доказательства, экономические преступления.

Развитие информационных технологий и их проникновение во все сферы общественной жизни оказывают существенное влияние на характер современной преступности. Экономические и финансовые преступления все чаще совершаются с использованием различных высокотехнологичных средств, что значительно усложняет их выявление и доказывание. В этих условиях цифровые доказательства, такие как электронные документы, записи коммуникаций, транзакционные данные и иная электронная информация, приобретают особую важность при расследовании экономических преступлений[1].

Одним из эффективных инструментов получения таких цифровых доказательств являются методы ОСИНТ (OSINT – Open Source Intelligence, также именуемая интернет разведкой). Использование открытых источников информации, включая сеть Интернет, социальные медиа, публичные базы данных и другие общедоступные ресурсы, предоставляет следователям и экспертам дополнительные возможности для сбора доказательственной информации, релевантной расследуемым экономическим преступлениям[2][3]. Применение ОСИНТ-методов позволяет восполнить пробелы в традиционных источниках доказательств и выявить значимые цифровые следы противоправной деятельности.

В Узбекистане основные положения применения электронных (цифровых) доказательств содержатся в Уголовно-процессуальном кодексе Республики Узбекистан[4] и Законе «Об электронном документообороте»[5]. Согласно узбекскому законодательству, электронные документы, записи, данные и иная цифровая информация могут быть признаны доказательствами по уголовным делам при условии соблюдения требований к их фиксации, изъятию и исследованию.

Цифровые (электронные) доказательства определяются как информация в электронно-цифровой форме, имеющая значение для установления обстоятельств уголовного дела. К ним относятся:

---

[1] Номоконов В.А., Тропина Т.Л. Киберпреступность: тенденции и проблемы противодействия // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 28–36.

[2] Волеводз А.Г. Противодействие киберпреступности: правовые основы международного сотрудничества. М.: Юрлитинформ, 2014. 352 с.

[3] Сафронов Б.А., Решняк М.Г. Современные тенденции преступности, связанной с использованием информационных технологий // Российский следователь. 2016. № 13. С. 32–37.

[4] Уголовно-процессуальный кодекс Республики Узбекистан от 22.09.1994 г. № 2012-XII (в редакции Закона РУз. от 27 февраля 2024 года № ЗРУ-915 – Национальная база данных законодательства, 28.02.2024 г. № 03/24/915/0160).

[5] Закон Республики Узбекистан «Об электронном документообороте» от 29.04.2004 г. № 611-II // (СЗ РУз., 2004 г., № 20, ст. 230)

- электронные документы (текстовые файлы, таблицы, графики и пр.);
- аудио- и видеозаписи;
- сведения об электронных платежах и финансовых транзакциях;
- данные с электронных устройств (смартфонов, компьютеров, серверов и т.д.);
- информация из сетей передачи данных и социальных медиа.

Ключевыми принципами использования цифровых доказательств в уголовном судопроизводстве являются допустимость, достоверность и относимость, соблюдение которых обеспечивается посредством строгого процессуального порядка работы с цифровыми доказательствами, проведения судебных экспертиз и оценки доказательств судом.

Исходя из того, что методы ОСИНТ представляют собой комплекс аналитических приемов, ориентированных на сбор, обработку и анализ информации, доступной из общедоступных источников, применение их в контексте расследования экономических преступлений, расширяет возможности следователей и экспертов при проведении действий, направленных на установление обстоятельств дела. При этом используемые сеть Интернет (веб-сайты, социальные сети, форумы, блоги), публичные базы данных и реестры, средства массовой информации, а также специализированные информационно-аналитические ресурсы, позволяют получать различные виды цифровых доказательств, включая электронные документы и переписку, сведения о финансовых операциях и платежах, данные с мобильных устройств и компьютеров, информацию из социальных сетей и иных онлайн-источников.

Работа с цифровыми данными, полученными с использованием ОСИНТ-методов, требует строгого соблюдения процессуальных правил их фиксации и изъятия. Это включает документирование процесса поиска, сбора и копирования информации, обеспечение целостности и неизменности электронных доказательств, изъятие и упаковку носителей информации с соблюдением правил обращения, а также процессуальное оформление результатов такой деятельности. Надлежащее процессуальное оформление цифровых доказательств, полученных из открытых источников, является ключевым условием для обеспечения их допустимости в уголовном судопроизводстве.

Вместе с тем вопрос процессуального закрепления доказательств, связанных с открытыми данными сложен и имеет ряд проблем:

1. Постоянное изменение параметра релевантности выдаваемых стандартными поисковыми системами информации;

2. Затруднено получение одинакового результата, при использовании одинаковых запросов в разные промежутки времени, по причине изменчивой природы сети Интернет и открытых данных.

В странах Евросоюза, а также в США, Канаде и Южной Корее, следователи сами используют данные из открытых источников, в то время как на территории Узбекистана, для закрепления полученных доказательств должно быть предоставлено экспертное заключение. Вместе с тем использование ОСИНТ в оперативно-розыскной деятельности допустимо для установления первичных

данных, которые в дальнейшем будут подтверждены посредством государственных баз данных и архивных выписок.

Так, например, полученные через поисковые системы копии документов, проиндексированных данными поисковыми системами[1], позволяет получить сведения, которые могут составлять государственную, коммерческую, банковскую или иную тайну, не нарушая законодательство страны, так как публикация документа или нарушение регламента его хранения имело место со стороны его правообладателя.

Такая практика расширяет возможности правоохранительных органов для сбора цифровых доказательств, особенно по финансовым и экономическим делам. Например, информация из социальных сетей, финансовых порталов, корпоративных сайтов и других общедоступных ресурсов часто используется для установления фактических обстоятельств преступления.

Вместе с тем, применение доказательств, полученных с помощью ОСИНТ сопряжено с определенными проблемами. Одной из ключевых является обеспечение их допустимости и достоверности. Суды в зарубежных странах уделяют пристальное внимание вопросам процессуального оформления, целостности и источника происхождения цифровых данных, полученных из открытых источников. Нередки случаи, когда такие доказательства признаются недопустимыми ввиду нарушений при их фиксации и изъятии.

Проведенный анализ показывает, что применение методов интернет разведки в процессе расследования экономических преступлений имеет как значительные преимущества, так и определенные сложности процессуального характера. С одной стороны, цифровые доказательства, полученные из открытых онлайн-источников, позволяют следователям и экспертам восполнить пробелы в традиционных доказательствах и установить ранее неизвестные фактические обстоятельства дела. Особенно это актуально для финансовых и корпоративных преступлений, где цифровые следы зачастую имеют решающее значение. С другой стороны, их использование сопряжено с рядом проблем, связанных с обеспечением допустимости и достоверности в уголовном судопроизводстве.

Для преодоления выявленных проблем представляется целесообразной разработка детальных методических рекомендаций по порядку работы с цифровыми доказательствами, полученными из открытых источников. Такие рекомендации должны содержать четкие требования к процессуальному оформлению всех этапов использования данных интернет-разведки: от поиска и сбора информации до ее приобщения к материалам уголовного дела.

Особое внимание следует уделить вопросам обеспечения целостности и неизменности электронных доказательств, а также их экспертному исследованию для подтверждения подлинности и достоверности. Кроме того, необходимо совершенствовать законодательство в части регулирования использования цифровых доказательств, в том числе полученных с применением методов ОСИНТ, с учетом специфики их природы и динамичности информационной среды.

[1] Gardner, B., Long, J. & Brown, J. (2011) Google hacking for penetration testers (Vol. 2). Elsevier.

Только комплексный подход к решению обозначенных вопросов позволит эффективно использовать такие доказательства при расследовании экономических преступлений.

В.Д. Коцюба

Международный опыт использования программ прикладного программирования в борьбе с отмыванием доходов, полученных преступным путем, и финансированием терроризма

Аннотация. Автор изучает возможность использования интерфейса прикладного программирования при модернизации практик противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма. Делается анализ международного опыта реализации данного инструмента Подразделениями финансовых разведок других стран.

Ключевые слова: ПОД/ФТ, ФАТФ, финтех, новые технологии, программы прикладного программирования, международный банкинг.

Рекомендации Группы разработки финансовых мер по борьбе с отмыванием денег (ФАТФ) содержат отдельную рекомендацию по включению новых технологий в национальную финансовую систему (Рекомендация 15). Она предписывает финансовым организациям проводить анализ рисков отмывания доходов, полученных преступным путем, и финансирования терроризма (ОД/ФТ) до запуска технологических продуктов и передовой деловой практики, включая использование новых или развивающихся технологий и недавно появившихся механизмов их передачи. Сравнительно недавно Группой был выпущен отчет о ключевых вопросах имплементации Рек.15[1], где указывается на неблагоприятное состояние реализации данной Рекомендации юрисдикциями-членами ФАТФ.

Влияние на текущее положение оказало большое число использования программ-вымогателей, даже не смотря на их замедление темпа разработки в 2023 году.

Попробуйте представить механизм, включающий в себя программный код и успешно подобранный чувствительный инструментарий. Такой механизм принято называть интерфейсом прикладного программирования (Application Programming Interface (API). API — это тип программного обеспечения, которое позволяет различным приложениям подключаться и взаимодействовать друг с другом. Интерфейс прикладного программирования также часто используется для предоставления платежных услуг, например, при приеме пожертвований через веб-сайты. Эксперты группы по виртуальным активам и цифровой

[1] Status of implementation of Recommendation 15 by FATF Members and Jurisdictions with Materially Important VASP Activity. URL: www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf.

трансформации ФАТФ назвали API одним из наиболее используемых и актуальных решений для выявления угроз и рисков ОД/ФТ.

Полезность данной программы для выявления ОД/ФТ заключается в возможности, к примеру, соединить программное обеспечение для идентификации клиентов (например, программа «Знай своего клиента») с инструментами мониторинга или инструментами идентификации рисков и угроз с профилями рисков клиентов (программа надлежащей проверки клиента), чтобы генерировать оповещения или изменять классификацию рисков по мере необходимости. Программа позволяет быстрее интегрировать различные взаимосвязанные инструменты и базы данных, что особенно актуально, поскольку одной из самых сложных задач для многих финансовых учреждений является интеграция множества различных и зачастую комплексных систем.

Преимущества интерфейса прикладного программирования:

повышение согласованности между традиционными банковскими данными и отказ от разрозненных систем с фрагментированной структурой;

повышение автоматизации процессов, позволяющих оптимизировать ресурсы баз данных, конечные выводы идентификации и мониторинга;

предоставление полных данных, определяющих более полный профиль рисков новых клиентов, например, в процессе регистрации пользователей.

Также API имеет большую ценность для государственного сектора, так как позволяет получить доступ к реестрам финансовых учреждений и обеспечивает возможность проведения постоянного мониторинга изменений в финансовой системе.

Применение интерфейса прикладного программирования на практике.

Наличные деньги все еще являются средством платежа и их трансграничное перемещение признается ФАТФ источником высокого риска[1]. Это осложняет расследование, поскольку отправитель и получатель находятся в разных странах, и это требует взаимодействия и координации разных регуляторов и правоохранительных органов.

Для решения этой проблемы подразделением финансовой разведки (ПФР) Туниса (CTAF) в январе 2021 года была запущена платформа «Ганнибал» которая постоянно контролирует физическое трансграничное перемещение валюты[2]. Платформа «Ганнибал», созданная при использовании технологии блокчейн (blockchain), является результатом сотрудничества и координации между правоохранительными органами (Министерством внутренних дел и Таможней), банками, почтой и обменными пунктами. Платформа «Ганнибал» направлена на распознавание и оценку национальных рисков отмывания денег и финансирования терроризма, связанных с физическим трансграничным перемещением валюты.

Эта технология соединяет базы данных заинтересованных сторон (Министерства внутренних дел, таможни, банков, почтовых отделений,

[1] Guidance for Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet- Based Payment Services. FATF/OECD. June, 2013.

[2] Hannibal Platform. URL: https://ctaf.gov.tn/data/uploads/pdf/6036f1504b6ed5.73786894.pdf.

обменных пунктов и ПФР Туниса) и гарантирует прозрачность и достоверность информации. Интерфейс прикладного программирования позволяет соответствующим ведомствам получать в режиме реального времени данные об объемах ввоза иностранной валюты и всех связанных с ней банковских операциях. Программа отслеживает таможенное декларирование и конечную точку перемещения валюты. Полученная информация с помощью заданных алгоритмов оценивает риски и угрозы, а также, по мере необходимости, преобразовывает полученные материалы в разведданные.

Платформа позволяет властям Туниса принимать соответствующие превентивные меры для снижения национальных рисков отмывания денег и финансирования терроризма, связанных с физической трансграничной транспортировкой валюты.

В целях оптимизации процессов в антиотмывочном контуре необходимо выстраивать государственно-частное партнерство, целью которых будет являться предоставление финансовой информации, позволяющей своевременно выявлять и пресекать риски ОД/ФТ. В этой связи интересным представляется опыт индийских коллег по созданию платформы IndiaStack[1].

IndiaStack — это набор АР-интерфейсов, которые позволяют государству и частному сектору использовать уникальную цифровую инфраструктуру для решения проблем, связанных с предоставлением услуг бесконтактной и безналичной оплаты.

IndiaStack предоставляет четыре различных технологических уровня, включая универсальную биометрическую цифровую идентификацию, единый интерфейс для всех банковских счетов страны, безопасный способ обмена данными и возможность свободного перемещения записей цифровых удостоверений личности, устраняя необходимость сбора и хранения бумажных документов.

Эта инфраструктура включает в себя Aadhaar (глобальная система проверки биометрической идентификации), eKYC, eSign, DigiLocker (оцифровка личных документов) и UPI (Единый платежный интерфейс) — инструменты, которые способствуют упорядоченному росту открытого цифрового банкинга в стране.

Помимо упрощения внутренних процедур, API облегчают координацию заинтересованных ведомств.

Использование API-интерфейсов надзорными органами в сочетании с финансовой аналитикой может повысить эффективность практики отчетности и качество надзора за рисками. Рассматриваемый инструмент позволяет надзорным органам обрабатывать историю транзакций в сочетании со свежими данными и создавать автоматизированные отчеты для дальнейшего использования в работе.

Прерогатива финансовых институтов – это своевременное и качественное оказание услуг. Согласно европейским стандартам мгновенных межбанковских платежей (SEPA SCT Inst.) срок перевода денежных средств между клиентами

[1] Является ли индийская IndiaStak сильнейшей финтех платформой? URL: https://ajuniorvc.com/india-stack-fintech-unicorn-upi-aadhar-explained-case-study-global/.

должен составлять не более 10 секунд[1]. С точки зрения ПОД/ФТ мгновенная скорость перевода создает новые правила банковского мониторинга. В связи с «временной ограниченностью» банки могут некачественно проводить НПК, в частности, анализировать санкционные списки.

Вытекающей из этого проблемой также является слепое следование рекомендациям. Из-за большого массива данных осуществление банковского комплаенса происходит по траектории «идентификация пользователя - характер операции» и при малейшем недочете со стороны финансового учреждения отменяется транзакция, пользователь заносится в список «подозрительных клиентов» или применяется де-рискинг. Такие действия банка оправдывают желание обезопасить себя от применения санкций (например, отзыв лицензии) со стороны регулятора.

Интерфейс прикладного программирования считается наилучшим решением перечисленных выше проблем. Системы API позволяют банкам мгновенно сверять данные клиента, проводить НПК и оценивать поле «подозрительной деятельности», включая риски и угрозы совершения транзакций.

В последнее время на площадке ФАТФ поднимаются вопросы цифровой идентификации личности и возможные возникающие угрозы и риски ОД/ФТ. Отражением этой тенденции становится распространение процедур удаленной идентификации, то есть установления личности без физического присутствия. Новые решения весьма разнообразны — это использование биометрии (Индия), проверка сведений через государственные (Нигерия, Мексика) и частные (Великобритания) базы данных, видеоидентификация (Испания, Швейцария, Эстония). Инструментарий API позволяет совмещать базы хранения биометрических данных и программ идентификации клиента, что позволяет осуществить своевременную и достоверную НПК[2].

Подводя итоги, необходимо отметить, что цель легализации доходов осталась неизменной, поменялись способы и инструменты совершения такого преступления. С развитием информационных технологий ландроматы отошли от прачечных и салонов красоты и стали использовать перепродажу наличности туристическим агентствам, анонимные пожертвования и оплату обучения в частных школах, «теневую» инкассацию через фирмы-однодневки, карусельные обналичивания денежных средств.

Стоит обратить внимание на тот факт, что финансовая активность ландроматов и террористов не всегда отличается от активности законопослушных граждан. Согласно отчету ФАТФ о возникающих угрозах финансирования терроризма[3] власти Саудовской Аравии проанализировали

---

[1] SEPA Instant Credit Transfer (SCTinst) scheme Rulebook, (2017). URL: europeanpaymentscouncil.eu

[2] Достов В.Л., Негляд Г.Ю., Шуст П.М. Влияние финансовых технологий на практику борьбы с отмыванием денег и финансированием терроризма // Финансовые исследования. 2018. № 4 (61). С. 44.

[3] The Emerging Terrorist Financing Risks report. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Emerging-Terrorist-Financing-Risks.pdf.coredownload.pdf.

счета 1150 человек, которые посещали Сирию и Ирак для осуществления незаконной деятельности. По итогам было выявлено, что совершаемые ими транзакции были характерны уровню их дохода.

Поэтому с целью минимизации риска ОД/ФТ технологии API призваны детально и мгновенно перерабатывать информацию о клиентах и совершаемых ими транзакций, заданные алгоритмы позволяют хранить в облачных сервисах полученные материалы, которые могут стать разведданными при необходимости и осуществлять незамедлительное сообщение о подозрительной транзакции регулятору.

И.А. Кубасов
А.В. Кирюхин

Разработка моделей машинного обучения для раскрытия и расследования киберпреступлений

Аннотация. В данной статье исследуются возможности применения моделей машинного обучения, которые в современных условиях цифровой трансформации правоохранительных органов становятся одним из эффективных инструментов противодействия киберпреступности. Предложены перспективные направления разработки и применения моделей машинного обучения для повышения эффективности раскрытия и расследования киберпреступлений.

***Ключевые слова*:** модели машинного обучения, искусственный интеллект, киберпреступления, киберпреступники, деятельность правоохранительных органов.

Современная цифровая трансформация правоохранительных органов осуществляется на основе широкого внедрения и развития информационных технологий, а также выработки управленческих решений на основе данных, которые приобретает цифровой вид. При этом стремительно развивающиеся информационные технологии значительно изменяют и структуру преступности, создавая сложные новые задачи перед правоохранительными органами в противодействии киберпреступности[1]. Так, по данными статистики в 2014 году было зарегистрировано 11 тыс. преступлений использованием информационно-телекоммуникационных технологий (далее – ИТТ), а в 2023 году – 677 тыс. (+6054.54 %)[2]. Доля преступлений, с использованием ИТТ в 2023 году составила 35% из общего числа совершённых преступлений.

[1] Минбалеев А. В. Проблемы использования искусственного интеллекта в противодействии киберпреступности // Вестник Южно-Уральского государственного университета. Серия: Право. 2020. Т.20, № 4. С. 116-120. DOI 10.14529/law200420.

[2] Основы кибербезопасности: Учебник / А. В. Бецков, Б. А. Торопов, И. А. Кубасов [и др.]. – Москва: Академия управления МВД России, 2023. – 108 с.

Развитие инновационных технологий таких как искусственный интеллект, интернет вещей, блокчейн и др., привело к появлению новых видов преступлений с использованием ИТТ, например, таких как:

1) криптоджекинг – это несанкционированное использование ресурсов устройств (компьютеров, смартфонов, планшетов или даже серверов) для добычи криптовалюты;

2) атаки с использованием искусственного интеллекта (далее – ИИ) – преступники используют ИИ для автоматизации создания вредоносного программного обеспечения и разработки алгоритмов, позволяющих обходить существующие системы обеспечения информационной безопасности;

3) использование технологии Deep fake для создания убедительных поддельных аудио и видео материалов с целью дезинформации, манипуляции и осуществления мошеннических действий;

4) атаки на основе интернета вещей - атак характерен несанкционированный доступ к информации, нарушение работоспособности системы;

5) атаки с помощью программ-вымогателей на критическую информационную инфраструктуру – такие атаки влекут за собой нарушения работоспособности системы, финансовые потери и ущерб для репутации организаций.

Следует подчеркнуть, что в дополнение к международному сотрудничеству в сфере противодействия киберпреступности возникла потребность также на государственном уровне выработать единое определение понятия «киберпреступность» и разработать комплексные методы криминалистического расследования таких дел, в том числе с использованием специальных знаний и новых технологий, таких как машинное обучение, представляющее собой направление искусственного интеллекта, сосредоточенное на создании систем, которые обучаются и развиваются на основе получаемых ими данных[1].

Согласно Концепции технологического развития на период до 2030 года[2] применение технологий ИИ способствует улучшению производительности и значительному расширению возможностей для создания инновационных продуктов и сервисов, оказывающих существенное влияние на развитие государства. Применяя модели машинного обучения, сотрудники правоохранительных органов могут раскрыть сложные преступные схемы и оперативно реагировать на них, предвосхитить и нейтрализовать кибератаки. Интеграция алгоритмов машинного обучения в раскрытие и расследование киберпреступлений не только открывает возможности для противодействия изощренным современным киберпреступлениям, но и решить ряд проблемных вопросов, которые возникают у сотрудников правоохранительных органов при расследовании киберпреступлений. Это следующие проблемные вопросы.

[1] Кубасов И.А. Разработка методов ДНК-фенотипирования для расследования и раскрытия преступлений // Вестник Воронежского института МВД России. 2022. № 2. С. 166-172.

[2] Распоряжение Правительства Российской Федерации от 20.05.2023г. №1315-р «Концепция технологического развития на период до 2030 года».

1. Большой объем структурированных и неструктурированных данных из различных источников, необходимых для сбора и анализа при раскрытии и расследовании киберпреступлений. Модели машинное обучение позволяют автоматизировать процесс сбора и анализа данных, выявляя закономерности и сокращая временные ресурсы для раскрытия и расследования киберпреступлений.

2. Сложность раскрытия и расследования разных видов киберпреступлений, обусловленная постоянным совершенствованием и развитием методов и способов совершения киберпреступлений.

3. Скрытая активность и анонимность совершения киберпреступлений. Применение моделей машинного обучения позволяют оперативно выявлять «аномалии» в данных, что особенно важно в случаях использования киберпреступниками новых методов мошенничества или несанкционированного доступа.

Далее предлагаем перспективные направления разработки и применения моделей машинного обучения для повышения эффективности раскрытия и расследования киберпреступлений.

1. Разработка моделей машинного обучения для анализа цифровых следов, оставленных киберпреступниками. На первом этапе данной разработки необходимо осуществить автоматический сбор цифровых данных из различных источников информации (серверные логи, история браузера, журналы событий и т.д.). На втором этапе - «очистить» данные (устранить ошибки и нерелевантную информацию). На третьем этапе – непосредственно проанализировать данные и установить корреляции (взаимосвязи между различными событиями и участниками) данных из разных источников. На четвертом этапе – синтез управленческого решения. Такой подход предоставит более полное представление о киберпреступлении и поможет в сборе доказательств[1].

2. Разработка моделей машинного обучения для идентификации и анализа подозрительных действий, связанные с киберпреступлениями, путем мониторинга и анализа поведенческих паттернов пользователей и систем. На первом этапе данной разработки следует искусственную нейронную сеть обучить на основе больших объемов данных, чтобы распознавать «аномалии» (отклонения от нормы), которые могут указывать на совершение киберпреступления. На втором этапе – установить корреляцию «аномалий» с другими данными, например, с данными, содержащимися в базах правоохранительных органов, для подтверждения или опровержения подозрений, что в конечном итоге позволит правоохранительным органам более оперативно реагировать на киберпреступления[2].

---

[1] Иванов А.И., Кубасов И.А., Самокутяев А.М. Тестирование больших нейронных сетей на малых выборках // Надежность и качество сложных систем. 2020. № 3(31). С. 72-79. DOI: 10.21685/2307-4205-2020-3-9.

[2] Иванов А. И., Кубасов И. А. Сильный искусственный интеллект: повышение качества нейросетевых решений с переходом к обработке входных данных большого объема //

3. Разработка моделей машинного обучения для текстового анализа и обработки естественного языка в контексте раскрытия и расследования киберпреступлений. На первом этапе данной разработки следует искусственную нейронную сеть обучить автоматически обрабатывать огромные объемы текстовых данных на разных языках, такие как электронные письма, сообщения в мессенджерах и документы, выявляя ключевые слова и фразы, указывающие на незаконную деятельность. На втором этапе - анализ эмоциональной окраски сообщений, возможно связанных с угрозами или прессингом, а также распознавание контекстуальных связей между различными сообщениями, понимание скрытых взаимодействий и связей между лицами. На третьем этапе - извлечение персональных данных из текстов, что может быть критически важно для идентификации киберпреступников, а также автоматическое создание сводок из больших текстовых массивов, что значительно ускоряет процесс расследования, предоставляя сотрудникам правоохранительных органов содержательные отчеты.

4. Разработка моделей машинного обучения для идентификации IP-адресов и устройств - источников кибератак, а также связанных с ними сетевых узлов. На первом этапе данной разработки следует искусственную нейронную сеть обучить мониторить трафик в реальном времени и отслеживать перемещение данных между устройствами/сетями. На втором этапе – анализ данных с автоматизацией сопоставления IP-адресов с конкретными пользователями и устройствами для идентификации киберпреступника. На третьем этапе – синтез управленческого решения, в том числе выработка предложений по более эффективной тактике защиты от вероятных кибератак.

В заключении, хотелось бы заметить, что киберпреступники крайне быстро адаптируются к новым реалиям борьбы с ними, используя современные достижения науки и техники. Все это обязывает сотрудников правоохранительных органов иметь в арсенале эффективные инструменты для противодействия киберпреступности. Адаптивность моделей машинного обучения, применяемых при раскрытии и расследовании киберпреступлений, должна обеспечить своевременное обновление и адекватное реагирование на новые киберугрозы. Используя новые данные, модели машинного обучения позволяют прогнозировать и нейтрализовать потенциальные атаки, улучшая обнаружение «аномалий» данных. Такая способность к быстрому и точному реагированию делает машинное обучение незаменимым инструментом для правоохранительных органов при раскрытии и расследовании киберпреступлений.

Киберпреступность уже давно стала проблемой международного уровня, решение которой требует консолидации усилий с применением современных достижений в сфере информационных-телекоммуникационных технологий.

Надежность и качество сложных систем. 2021. №1 (33). С. 9-16. DOI 10.21685/2307-4205-2021-1-1.

А.Ю. Любавский

Повышение эффективности поиска криптокошельков на машинных носителях информации

Аннотация. В статье приведен сравнительный анализ методов поиска информации о криптовалютных кошельках на машинных носителях информации.

***Ключевые слова*:** криптовалютные кошельки, технология блокчейн, многопоточное сканирование, операционная система, машинный носитель информации.

Сегодня развитие научно-технического прогресса привело к тому, что привычные финансовые активы (наличные деньги, вклады, вложения в ценные бумаги и т.д.) постепенно начинают замещаться замещаются цифровыми финансовыми активами (ЦФА), которые на сегодняшний день успешно интегрировались в экономику[1], а также криптовалютой.

С момента появления биткойна в 2009 году количество различных криптовалют сейчас составляет 6 тыс. разновидностей. Отношение к указанным активам у населения различное, но уже ряде стран криптовалюту наряду с государственными денежными знаками используют как средство оплаты.

Принципиальный признаком криптовалюты является применение технологии блокчейн. Данная технология представляет собой цепочку из блоков с записями транзакций, которые связаны между собой и защищаются с использованием криптографии. При этом каждый блок содержит свой собственный уникальный криптографический идентификатор, который указывает (связывает) его с предыдущим блоком цепи. После добавления в блокчейн, блоки уже невозможно изменить без потери данных о всей последующей цепи, что незамедлительно дает другим пользователям знать, что было совершено стороннее вмешательство в обход правил. Это дает возможность просто отказать в использовании модифицированной версии цепочки (потому что без признания модифицированного блока со стороны большинства участников процесса он бесполезен) и продолжать работать с исходной ветвью. Электронные криптовалютные кошельки могут быть привязаны к блокчейну, чтобы гарантировать, что их баланс соответствует действительности, а новые транзакции проверяются с помощью данных в цепочке блоков для гарантии того, что каждая из них — настоящая и была произведена криптовалютой, которая реально принадлежит плательщику (или его кошельку).

С одной стороны, такой подход обеспечивает безопасность производимых транзакций (взаимных расчетов). С другой стороны, идентифицировать

[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» (с изменениями и дополнениями).

отправителей и получателей указанных активов становится затруднительным для правоохранительных органов.

Именно за счет указанных выше технологических решений данный актив стал популярен в преступных кругах. Криптовалюту используют при сбыте наркотических веществ, террористические организации, хаккеры, вымогатели и мошенники и т.д.

Для хранения криптовалютных активов применяются различные программно-аппаратные средства:

- десктопные приложения, которые устанавливаются на персональные компьютеры пользователей (рис. 1);

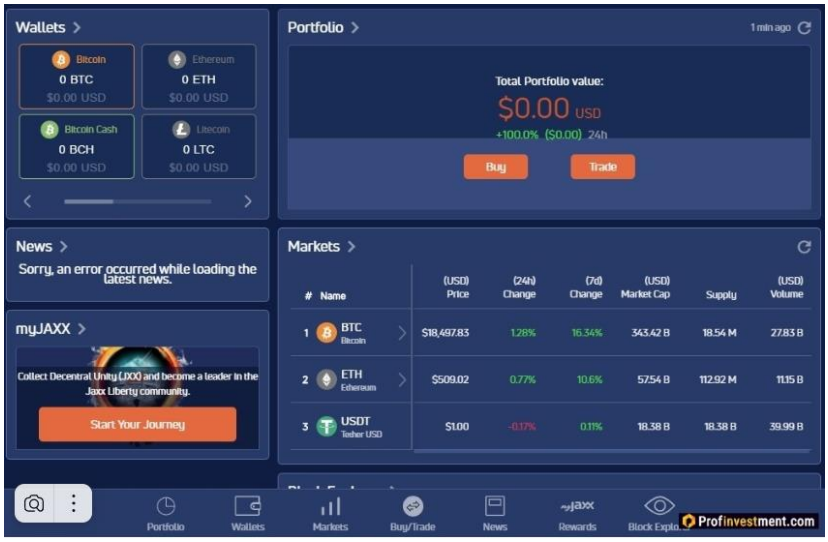


Рис. 1. Пример десктопного криптокошелька

- мобильные приложения, аналогичные предыдущим приложениям, за исключением того, что устанавливаются на мобильные устройства (рис. 2);

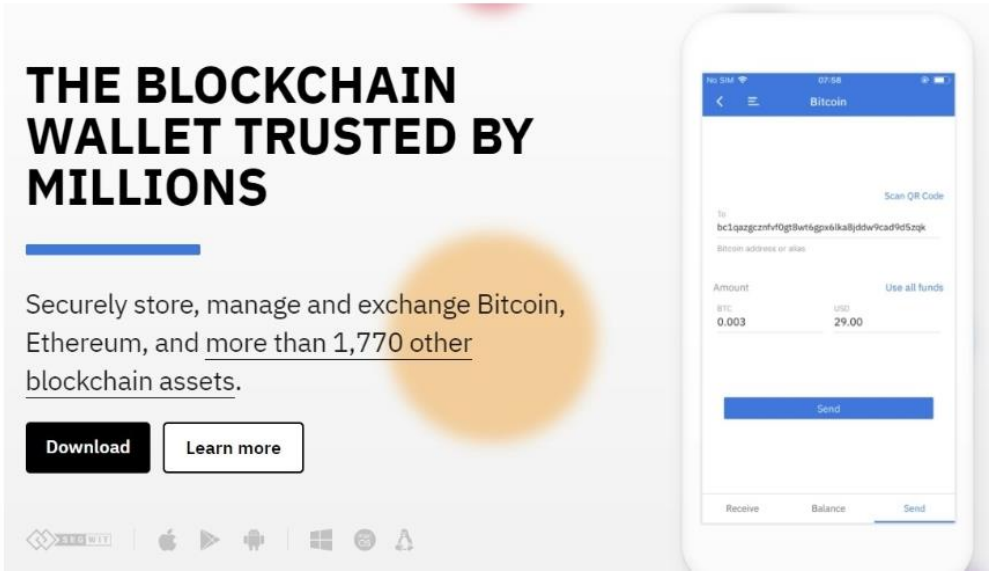


Рис. 2. Пример мобильного криптокошелька

- онлайн-кошельки работают по принципу обычного сайта, и пользователь может с помощью логина и пароля войти в аккаунт с любого устройства, на котором есть выход в интернет (рис. 3);

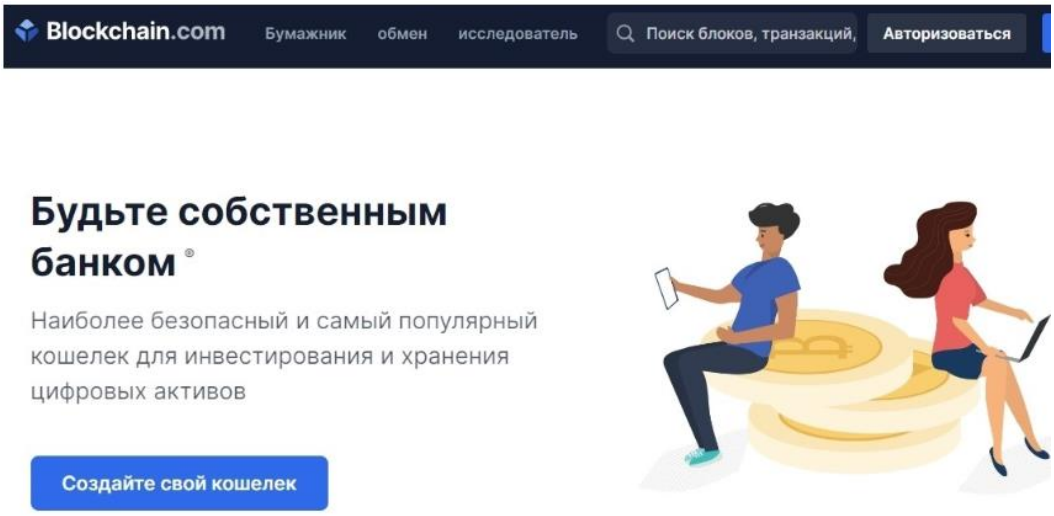


Рис. 3. Пример онлайн-криптокошелька

- аппаратные кошельки в формате физических устройств, подключаемые к компьютеру через USB-разъем. Чаще всего устройство оснащено дисплеем, где отображается основная информация. Обеспечивает холодное хранение приватных ключей в строго автономной среде (рис. 4).

Рис. 4. Пример онлайн-криптокошелька

- в текстовом виде является разновидностью холодного криптокошелька. При таком способе хранения владелец сохраняет ключи криптокошелька в файле на персональном компьютере, либо на бумажном носителе информации в виде строки символов.

Наличие криптовалютных активов у подозреваемых возможно выявить путем таких процессуальных действий как осмотр или обыск за исключением последнего метода, так как при последнем способе хранения существует

достаточное количество приемов, позволяющих скрыть указанный файл с ключами криптокошелька в файловой системе персонального компьютера.

Файлы и документы в ходе проведения осмотра содержимого персонального компьютера можно осуществлять по средством встроенного функционала операционных систем (встроенная система поиска в файловой системе), либо специализированных программ, таких как «Архивариус 3000», «Ищейка проф Deluxe» и другие аналоги. Вместе с тем, для того чтобы выявить файлы, в которых содержатся строки, содержащие ключи криптокошельков необходимо для поиска ввести последовательность символов в точности повторяющих ключ криптокошелька.

Если обратить свое внимание ключ криптокошелька представляет собой чередующуюся последовательность цифр, английских букв, и символов: «0x6F358447262b8623DAF4af99D153714Df326e0fa». Кроме этого, подобная последовательность может храниться в виде растровых изображений (скрин с экрана, цифровая фотография). Таким образом, вероятность выявления нахождения электронных файлов с ключами криптокошельков становится минимальной, либо потребует большое количество временных ресурсов для последовательного просмотра содержимого всех файлов, хранящихся на машинном носителе информации. Справедливо отметить тот факт, что уверенные пользователи персонального компьютера способны изменить расширение искомого электронного файла, что сводит вероятность обнаружения ключей криптокошелька к минимуму.

Приведенные факты привели к постановке научно-практической задачи по разработке программы, позволяющей выявлять на машинных носителях информации записи, по своему виду аналогичные ключам криптокошельков.

Ранее коллективом авторов была разработана программа, позволяющая осуществлять поиск на машинном носителе информации файлы как текстовые, так и графические, содержащие в себе искомые слова и фразы в режиме многопоточного сканирования файловой системы[1]. Для решения научно-практической задачи поставленной в настоящей статье была произведена модификация программного кода.

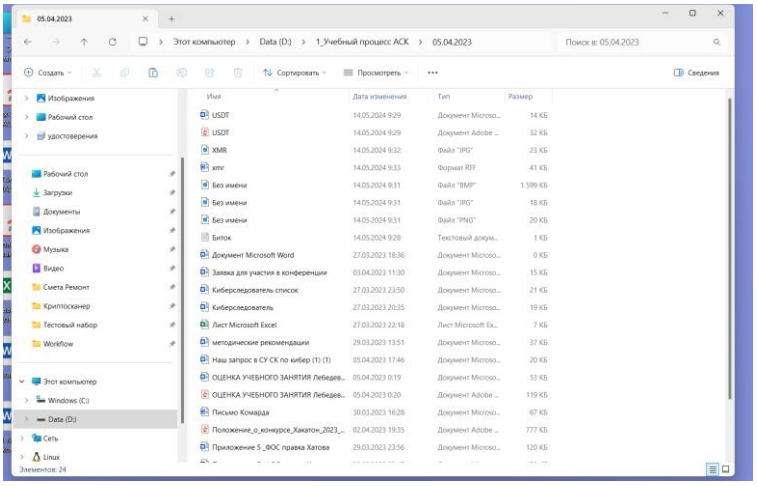
На первом этапе был разработан генератор последовательностей из чисел, символов и английских букв различного регистра. Далее многопоточный режим сканирования файловой системы выявляет указанную последовательность в электронных документах.

Кроме этого отмечаем, что ввиду того, что у существующих криптовалют алгоритмы построения уникального ключа отличаются, одновременно набор символов логически не взаимосвязан, что сводит вероятность ложных срабатываний на файлы, написанные латиницей, стремиться к нулю. Для

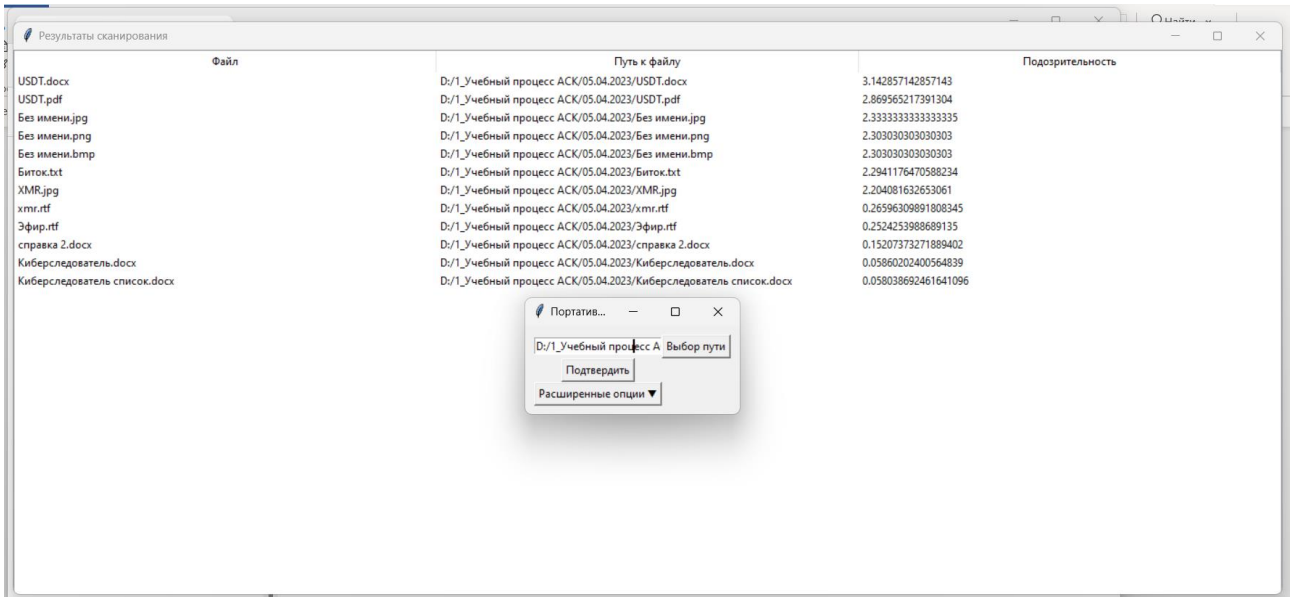
[1] Любавский А.Ю., Семененко В.А., Хатов Э.Б. Свидетельство о государственной регистрации программы для ЭВМ № 2023666767 Российская Федерация: № 2023664802: заявл. 12.07.2023; опубл. 04.08.2023.

повышения быстродействия программы для выявления строк аналогичных ключу от криптокошелька достаточно выявить комбинацию из 5 символов, причем для исключения ложных срабатыванием осуществляется проверка предыдущего и последующего знака (включая пробелы).

Таким образом, на языке программирования Python разработана программа, осуществляющая в многопоточном режиме параллельный перебор символов в документе, записывающая в отдельное окно список файлов содержащих в себе последовательности символов аналогичных ключам криптокошельков (Рис. 5 А, Б).



А



Б

Рис. 5. А – папка с помещенным в нее в нее тестовым набором файлов с ключами криптокошельков. Б – результат работы программы

Для проверки работоспособности разработанной программы в файловую систему помещены файлы различных форматов, содержащих в себе ключи криптокошельков различных валют. Результат обнаружения файлов составил

100%, причем как в текстовом формате так и в графическом и формате служебных файлов операционной системы с расширением bat.

В результате проведенных исследований был разработан инструмент, позволяющий оптимизировать процесс осмотра содержимого машинных носителей информации при расследовании уголовных дел, в которых фигурируют операции с криптовалютой в условиях нечеткого поиска. Наборы символов, выявленных в файлах в ходе осмотра с применением разработанной программы достаточно проверить существующими в сети Интернет эксплорерами блокчейна.

П.В. Меджевитдин

Современные возможности судебной компьютерно-технической экспертизы в борьбе с киберпреступностью

Аннотация. Статья посвящена современным возможностям судебной компьютерно-технической экспертизы по делам о киберпреступлениях. Автор дает краткий сравнительный анализ специализированных программных комплексов для производства компьютерно-технических экспертиз, а также дает оценку их применения, в том числе при экспертизе нестандартных объектов криминалистического исследования.

Ключевые слова: киберпреступность, компьютерно-техническая, экспертиза, программно-аппаратный комплекс.

Компьютерно-техническая экспертиза, как отдельный вид, возникла в России во второй половине 90-х годов. Юридический статус получен в 2000 году постановлением Правительства Российской Федерации. Введена в перечень экспертиз приказом Минюста в 2003 году.

При этом первый семинар экспертов компьютерно-технического направления был проведен ЭКЦ МВД России в 2001 году в Краснодаре, первые стажировки экспертов по соответствующему профилю начали проводиться Министерством юстиции и ЭКЦ МВД России также в 2001 году.

В настоящее время в судебно-экспертном центре Следственного комитета Российской Федерации (ЭКЦ СКР) отделом компьютерно-технических исследований и экспертами соответствующего профиля в регионах выполняются следующие экспертизы:

- компьютерно-техническая экспертиза, разделяемая на следующие подвиды:
- компьютерная экспертиза – компьютеры от серверов до встроенных систем, отдельные носители информации (жесткие диски, компакт-диски, устройства флеш-памяти), электронные документы, виртуальные объекты;
- экспертиза компьютерной сети – сетевое оборудование, передаваемая по сети информация;

- экспертиза мобильных устройств – мобильные телефоны, планшеты, часы и фитнес-браслеты, другие носимые «гаджеты»;

- фотовидеотехническая экспертиза – камеры и видеорегистраторы, фотографии, видеозаписи;

- информационно-аналитическая экспертиза – экспертиза баз данных и сопоставление больших объемов информации, поиск в них различных закономерностей.

Следует отметить, что в настоящее время эксперты, выполняющие компьютерно-технические экспертизы, имеются не только в центральном аппарате, но и в следующих регионах: г. Санкт-Петербурге, г. Симферополе, г. Казани, г. Ессентуки, г. Красноярске, г. Хабаровске, г. Благовещенске, г. Воронеже, г. Иркутске, г. Кемерово, г. Нижнем Новогороде, г. Новосибирске, г. Омске, г. Барнауле, и г. Екатеринбурге.

При этом именно в Следственном комитете впервые в России (еще в 2014 году) выделили информационно-аналитическую экспертизу в отдельное направление (внесена Минюстом в перечень экспертиз только в 2020 году).

В большинстве своем, в ЭКЦ СКР удалось собрать наиболее грамотных экспертов данного направления. Во многих случаях дополнительные и повторные экспертизы, выполненные нашими специалистами, позволяют получить результаты там, где их не смогли добиться специалисты других ведомств. Также часто поступают обращения из других ведомств с просьбой о возможности проведения компьютерно-технических экспертиз нашими специалистами по наиболее сложным и резонансным делам.

Сотрудниками отдела постоянно проводятся апробации вновь разрабатываемого отечественного программного обеспечения (далее – ПО) по линии компьютерно-технической экспертизы, в результате чего разработчики отечественных программ имеют возможность их совершенствовать.

В целях совершенствования следственной деятельности, руководство и сотрудники отдела постоянно выступают с лекциями о современных возможностях компьютерно-технической экспертизы перед слушателями курсов повышения квалификации, проводимых на базе Московской Академии Следственного комитета Российской Федерации им. А.Я Сухарева, а также на различных семинарах и выставках.

В связи с постоянно увеличивающимся количеством объектов, поступающих на компьютерно-техническое исследование, а также необходимостью ускорения получения результатов при их исследовании в настоящее время в ЭКЦ СКР применяются два способа работы с этими объектами – в рамках осмотра и в рамках экспертизы (исследования).

Осмотр позволяет, при большом количестве изъятых объектов, провести быстрое первоначальное исследование, отсортировав объекты на важные и не интересующие следствие, а также оперативно получить нужную информацию.

Однако при использовании осмотра как основного инструмента работы возникает ряд проблем.

Во-первых производство осмотра не должно длиться более одного дня, так как осмотр возможен только в присутствии понятых, либо с полной фото/видеофиксацией всего процесса осмотра. При этом только извлечение информации из мобильного телефона Apple Iphone с объемом памяти в 512 Гб может длиться более суток, и процесс извлечения технически не может быть прерван.

Во-вторых осмотр, как процессуальное действие, не предполагает самого процесса исследования – т.е. в рамках осмотра неправомерен, например, процесс восстановления информации.

В третьих, как нам представляется, по существу отсутствуют процессуальные основания для изменения внешнего вида или внутреннего содержания объекта – т.е. невозможно проводить работы по восстановлению работоспособности объекта, подбору пароля. Фактически, неправомерно даже само извлечение информации из мобильных телефонов, так как в этом случае экспертное программное обеспечение первоначально производит внедрение в «память» телефона специальной «программы-агента», с помощью которой в дальнейшем и производится извлечение информации.

Таким образом, во многих случаях проведение осмотра является только первоначальным действием, что во многих случаях просто невозможно. В связи с чем, приходится исследовать объекты в рамках экспертизы (исследования).

При общей характеристике компьютерно-технической экспертизы следует учитывать определенные внешние факторы, которые существенно влияют на производство экспертных исследований. Это в первую очередь необыкновенно быстрый прогресс научных достижений в области информационных технологий, а также постепенная изоляция Российской Федерации от остального мира.

Еще совсем недавно граница между компьютерами и электронно-бытовыми устройствами была очерчена довольно четко. Сейчас мобильные телефоны способны фотографировать и запоминать сотни изображений и нести определенный набор сервисных программ, фотоаппарат и видеокамера становятся периферийным устройством компьютера, некоторые фитнес-браслеты, часы и игровые приставки обладают громадными программными возможностями, мало уступающими компьютерным системам. Мультимедийные системы автомобилей, по сути, являются персональными компьютерами с возможностью выхода в Интернет. С каждым годом граница между компьютерными и некоторыми электронно-бытовыми устройствами стирается. Чайники подключаются по Wi-Fi к телефонам, а холодильники выходят в Интернет.

Емкости носителей информации также выросли в несколько раз. Увеличенная мощность процессоров устройств позволяет повсеместно внедрять парольную защиту и шифрование информационного содержимого.

Еще недавно для исследования мобильных телефонов были актуальны методы J-Tag и Chip-OFF, однако в настоящее время, в связи с полным шифрованием данных, а также тем, что ключ шифрования находится в процессоре мобильного

телефона, методы больше не используются и приходится прилагать все возможные усилия для восстановления работоспособности изъятых телефонов.

При использовании в мобильном телефоне числового пароля длительностью 6 символов подбор необходимой комбинации может затянуться на 4 – 6 месяцев.

При этом методическое обеспечение этого вида деятельности безнадежно отстает. Приходится учитывать, что многие ГОСТы, на положения которых эксперту приходится опираться при проведении исследований, устарели, т.к. разрабатывались в период, когда указанных проблем не существовало.

Доступные специализированные программные комплексы для производства компьютерно-технических экспертиз в настоящее время или не покрывают всех потребностей при производстве экспертиз или устарели. Наиболее часто используются:

- Forensic assistant (отечественное ПО, устарело);
- Encase (зарубежное ПО, устарело);
- FTK (зарубежное ПО);
- Belkasoft (отечественно-зарубежное ПО);
- X-Ways (зарубежное ПО);
- Magnet (зарубежное ПО);
- Amped (зарубежное ПО);
- Эскиз В (отечественное ПО);
- Зверобой, Следопыт, Октопус (отечественное ПО);
- UFED (зарубежное ПО);
- PC-3000 (отечественное ПО);
- Мобильный криминалист (отечественное ПО);
- Passware (зарубежное ПО);
- Elcomsoft (отечественное ПО);
- X- Ray (зарубежное ПО).

С помощью указанного программного обеспечения хорошо решаются задачи:

- поисковые задачи, связанные с обнаружением текстовых и графических файлов;
- контекстный поиск;
- выявление интернет-истории;
- выявление интернет-переписки.

Однако их практическое применение выявило следующие проблемы:

- Forensic assistant – по мнению специалистов – устарел и результативно работает только в тех случаях, если удалены атрибуты всех директорий, которые необходимо исследовать;
- Encase, FTK – возникают сложности с локализацией, игнорируются либо не обнаруживаются многие типы пользовательских файлов и интернет-мессенджеров;
- Belkasoft – по нашему мнению, эффективен только для поисковых задач, обнаружения интернет-истории и интернет-переписки, игнорирует либо не обнаруживает многие типы интернет-мессенджеров;

- X-Ways – часто встречаются затруднения с локализацией, недостаточный уровень восстановления файлов.
- UFED, Мобильный криминалист, X-Ray – исходя из нашего опыта, работали только с ограниченным перечнем мобильных устройств.
- Зачастую не обнаруживается (не исследуется) указанным программным обеспечением:
- зашифрованные (криптоконтейнеры);
- заархивированные с паролем файлы;
- файлы с измененным расширением;
- удаленные файлы, которые не были восстановлены (в первую очередь текстовые файлы).
- Нашими сотрудниками отмечаются явные проблемы с обнаружением (исследованием) указанным программным обеспечением:
- Tor Browser;
- Lotus Notes (особенно с паролем для доступа);
- Microsoft Exchange Server;
- Microsoft Office для Mac OS;
- Radmin;
- Team Viewer;
- Punto Switcher (в режиме логгирования использования клавиатуры).

Нами перечислены только типичные задачи и проблемы компьютерно-технической экспертизы. Однако имеются еще и необычные объекты или необычные задачи), которые также не могут быть исполнены с помощью указанного программного обеспечения: и необычные задачи КТЭ:

- обнаружение перечисленных выше объектов;
- обнаружение следов использования перечисленных выше программ;
- подбор программного обеспечения для интерпретации информации.
- Необычные объекты КТЭ:
- «умные часы»;
- фитнес-браслеты и трекеры;
- GPS-навигаторы и эхолоты;
- блоки АБС и подушки безопасности авто;
- комбинированные устройства и устройства, камуфлированные под устройства другого вида;
- поврежденные «обычные» объекты.

При этом даже с изъятием таких объектов на месте происшествия может возникнуть ряд проблем, так как они могут быть камуфлированы под другие объекты.

С 2004 года (момента появления первого специализированного ПО для производства компьютерно-технических экспертиз) неоднократно проводилось тестирование на предмет того, что лучше справится с задачами исследования – указанное специализированное ПО, либо большое количество мелких утилит, каждая из которых способна решать те или иные узкие задачи. По нашему

мнению, в этом состязании с большим преимуществом победили отдельные утилиты.

Таким образом, следователям необходимо понимать, что возможности специалиста в процессе производства экспертиз в текущей ситуации достаточно ограничены, так как он может обнаружить и интерпретировать далеко не всю информацию, имеющуюся на носителе.

Вместе с тем, высококлассный эксперт отличается от рядового коллеги тем, что сначала должен обнаружить все данные, которые остались от работы пользователя, интересующего следствие, а затем подобрать необходимое программное обеспечение для извлечения и интерпретации этих данных.

При этом необходимо учитывать, что киберпреступники – как правило наиболее подготовленные лица, обладающие специальными навыками в сфере высоких технологий, использующие передовые средства, методы и программы в своей деятельности. Поэтому производство экспертиз по кибепреступлениям с уверенностью можно рассматривать как одну из наиболее сложных задач, решение которых раскрывает возможности компьютерно-технических экспертиз, способствуя их постоянному совершенствованию.

И.Н. Озеров
К.И. Озеров

Некоторые вопросы специально-технического обеспечения раскрытия и расследования киберпреступлений в особых условиях

Аннотация. В статье рассмотрены проблемные вопросы, касающиеся использования специальной техники при раскрытии преступлений, правильной организации информационного обеспечения сотрудников, которые осуществляют оперативно-розыскную деятельность. Затронуты проблемы специально-технического обеспечения раскрытия и расследования киберпреступлений в особых условиях инструментарием по сбору и закреплению электронной информации имеющей важное значение для осуществления эффективного документирования преступлений в IT-сфере и их использования как специальных знаний. Обозначены сферы на которые посягают киберпреступники и вопросы взаимодействия следователей с оперативными подразделениями.

***Ключевые слова*:** взаимодействие, киберпреступления, особые условия.

Разнообразие сфер и способов совершения преступлений, субъектов преступления и организационно-структурным усложнением криминализации характеризуют масштабы современной преступности сегодня и не столько ее количество, сколько качественный рост. Распространенность изменяет конфигурацию всей системы современной преступной деятельности, которая

сместилась в интернет.[1] Преступность в значительной мере смещается в виртуальное пространство, в результате чего происходит изменение ее структуры, когда традиционные преступления вытесняются киберпреступностью.

В Стратегии национальной безопасности Российской Федерации к числу главных стратегических угроз национальной безопасности, в частности, отнесены появление новых форм противоправной деятельности с использованием информационных, коммуникационных и высоких технологий[2]. В Доктрине информационной безопасности[3] указано, что информационные технологии с течением времени приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства.

В этой связи российские ученые стали обращать пристальное внимание на активизацию использования информационно-телекоммуникационных сетей для совершения различных преступлений. Вместе с тем специализированные научные исследования в данной области проводятся сравнительно редко и, как правило, имеют узкую направленность, тогда как выделенная проблема имеет комплексный характер и требует системного подхода к ее решению[4]. При этом законодатель также с запозданием реагирует на видоизменения преступности, в том числе на новые способы совершения преступлений, обусловленные развитием информационных технологий и на развитие методов и средств борьбы с нею.

На четырнадцатом конгрессе ООН по предупреждению преступности и уголовному правосудию «Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению» (Киото, Япония 20–27 апреля 2020 г.) рассмотрен вопрос о «современных тенденциях в области преступности, последние изменения и новые решения, в частности использование современных технологий как средства совершения преступлений и инструмента борьбы с преступностью», при этом была подчеркнута необходимость обеспечения использования «технической помощи в предупреждении всех форм преступности и борьбе с

[1]Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению. Материалы четырнадцатого конгресса ООН по предупреждению преступности и уголовному правосудию (Киото, Япония 20–27 апреля 2020 г.). URL: https://www.unodc.org/documents/ congress//About/information (дата обращения: 15.07.2021).

[2] Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31 июля 2021 г. № 400) // Собрание законодательства РФ. 2021. № 27. Ст. 535.

[3] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[4] Иванцов С.В., Бадамшин С.К. Преступления террористической направленности: особенности международноправовой регламентации // Вестник Московского университета МВД России. 2019. № 2. С. 131–135.

ними… и новые и появляющиеся формы преступности».[1] Для этого предлагается осуществлять всеобъемлющие меры реагирования в области предупреждения киберпреступности и уголовного правосудия, в том числе принимать необходимые законодательные и иные меры для эффективного предупреждения новых, появляющихся и видоизменяющихся форм преступности и борьбы с ними на национальном, региональном и международном уровнях.

При этом методы, средства противодействия и фиксации киберпреступлений не всегда сопряжены с использованием специальных программ. Требуется знание и умение применения «старой» апробированной специальной техники, стоящей на вооружении правоохранительных органов, являющихся субъектами раскрытия и расследования киберпреступлений. Особенно актуальным данный вопрос становится в особых условиях, когда иными способами не возможно провести фиксацию действий киберпреступников.

На законодательном уровне, к сожалению, отчетливой классификации специальной техники не закреплено. Проанализировав литературу, посвященную этому вопросу, можно определить следующее: 1) специальные технические средства для выявления скрытой информации, поисковые приборы и приборы негласного наблюдения; 2) специальные технические средства для фиксации обнаруженной информации; 3) специальные технические средства для информационного обеспечения; 4) организационно вспомогательные специальные технические средства; 5) специальные технические средства создания условий, способствующих возникновению информации заданного вида[2].

Учитывая развитие науки и техники на сегодняшний день, в арсенал правоохранительных органов поступают все более современные спецсредства, которые позволяют решать даже самые сложные задачи. Разнообразие данных средств обуславливается широким спектром задач, которые ставятся перед сотрудниками правоохранительных органов в различных ситуациях, в том числе при проведении различных следственных действий в особых условиях.

Специализированное оборудование, используемое субъектами раскрытия и расследования киберпреступлений играет ключевую роль в выполнении ряда критически важных задач. Основные цели включают в себя идентификацию и фиксацию действий лиц, подозреваемых или изучаемых на предмет участия в незаконных активностях или правонарушениях. Дополнительно такая техника направлена на предоставление условий, благоприятствующих как формированию доказательств преступлений, так и раннему выявлению нарушений закона на первоначальных этапах их возникновения. Важным

[1] Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению. Материалы четырнадцатого конгресса ООН по предупреждению преступности и уголовному правосудию (Киото, Япония 20–27 апреля 2020 г.). URL: https://www.unodc.org/documents/congress//About/information (дата обращения: 15.07.2021).

[2] Князева А. Е., Новикова А. О. Проблемные вопросы использования технических средств в оперативно-разыскной деятельности // Деятельность оперативных подразделений: теория и практика. 2021. С. 100–103.

аспектом является обнаружение и прекращение использования противозаконных коммуникационных средств и механизмов радиотехнического наблюдения со стороны преступников. Эффективная реализация оперативно-розыскных мероприятий целенаправленно способствует идентификации и дальнейшему задержанию лиц, совершивших преступления и скрывающихся от предварительного расследования. Своевременное прибытие оперативных сотрудников, следователей и экспертов на места происшествия обеспечивает создание подходящих условий для их работы, что является завершающим этапом в цепочке задач, решаемых с помощью служебного оборудования.[1]

Подводя итог следует констатировать, что действия киберпреступников становятся все более агрессивными, они умеют тщательно скрывать следы, сохранять свою анонимность, заранее продумывают свое поведение так, чтобы осложнить правоохранительным органам сбор доказательств и избежать установленной законом ответственности. Кроме того, необходимо иметь ввиду, что зачастую, арсенал киберпреступников оснащен намного лучше, чем у правоохранительных органов. При совершении киберпреступлений применяются методы конспирации, а именно шифрование данных. Указанное свидетельствует о правовой и фактической сложности доказывания по таким делам.

Особые же условия только затрудняют методы противодействия киберпреступности, в связи с чем, борьба с киберпреступностью должна быть согласованной и единой. Для этого важно следователю взаимодействовать с оперативными подразделениями для успешного противодействия киберпреступности.

Специализированное оборудование, используемое субъектами раскрытия и расследования киберпреступлений играет ключевую роль в выполнении ряда критически важных задач и их эффективная реализация целенаправленно способствует идентификации и дальнейшему задержанию лиц, совершивших преступления и скрывающихся от предварительного расследования.

Список литературы

1. Озеров К.И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2021. № 1 (89). С. 167–171.

2. Озеров К.И. Мошеннические действия с применением информационно-телекоммуникационных технологий в сфере мобильных интернет-приложений // Юридический вестник Самарского университета. 2021. Т. 7. № 2. С. 133–137.

3. Озеров И.Н., Озеров К.И. Способы совершения мошенничества с использованием информационно-телекоммуникационных технологий в период

[1] Красненко Ю.В. Некоторые аспекты использования технических средств субъектами раскрытия и расследования преступлений // Проблемы правоохранительной деятельности. 2020. №. 2. С. 51–55.

коронавирусной инфекции // Проблемы правоохранительной деятельности. 2020. № 4. С. 32–35.

4. Тимофеев С.В. Проблемы проведения оперативно-розыскных мероприятий в сети darknet // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития: Материалы Международной научно-практической конференции, Москва, 17 октября 2019 г. / Под общей редакцией А.М. Багмета. М.: Московская академия Следственного комитета Российской Федерации, 2019. С. 572–576.

5. Самоделкин А.С., Тимофеев С.В. Современные методы выявления и раскрытия преступлений, совершаемых с использованием цифровых технологий // Вестник Восточно-Сибирского института МВД России. 2022. № 2(101). С. 206–215.

6. Тимофеев С.В., Иванова М.Д. Особенности реализации полномочий субъектами оперативно-разыскной деятельности при осуществлении взаимодействия с организаторами распространения информации в сети Интернет // Научный дайджест Восточно-Сибирского института МВД России. 2023. № 3(21). С. 37–45.

А.Э. Побегайло

Актуальные проблемы противодействия использованию нейронных сетей и искусственного интеллекта как средству совершения преступления

Аннотация. Использование нейросетей при совершении преступлений ставит перед правоохранительными органами ряд новых задач. В статье кратко рассматриваются дискуссионные вопросы определения средства совершения преступления, типология нейронных сетей, основные преступные деяния, которые возможно совершить с их использованием, и предлагаются подходы к закреплению их как квалифицирующего признака.

Ключевые слова: нейронные сети, вопросы квалификации преступлений, киберпреступления, киберпреступность.

В уголовном законодательстве отсутствует закрепленное нормативно понятие средства совершения преступления, при этом доктринальное понимание способа совершения преступления разрабатывалось уже как дореволюционными, так и советскими правоведами. Тем не менее, бурный рост информационно-телекоммуникационных технологий, включая нейронные сети и искусственный интеллект, требует анализа и возможной переоценки данного понятия.

Определения средства совершения преступления в науке уголовного права разнятся. Г.Н. Борзенков определял его как «материальные предметы, орудия, используемые преступником для совершения преступления»[1]. В.Н. Кудрявцев

[1] Борзенков Г.Н. Ответственность за мошенничество. М.: Юрид. лит., 1971. С. 65.

понимал под ним «такие вещи, которые используются преступником для воздействия на объект (предмет) преступления (деньги при даче взятки, оружие при убийстве, автомашина при наезде на пешехода и т. П.)»[1].

Цифровизация, появление и развитие киберпреступлений ставят перед учеными новые задачи по определению вредоносных компьютерных программ, иной компьютерной информации, а равно нейронных сетей. Большинство авторов относят вредоносные компьютерные программы именно к средству совершения преступления[2]. Ряд авторов относит их к орудиям совершения преступления[3]. Отдельные авторы относят вредоносные компьютерные программы и иную компьютерную информацию исключительно к предмету преступления[4]. Часть авторов придерживаются сбалансированного подхода и относят указанные понятия как к средствам, так и к орудиям, в зависимости от их вида, предмета посягательства, и наступивших преступных последствий5. Мы придерживаемся мнения, что вредоносные компьютерные программы и иная компьютерная информация относятся к средствам совершения преступления, поскольку орудия, в устоявшейся судебной практике и доктрине6, являются предметами материального мира, предназначенными, в частности, для физического воздействия на предмет преступления7.

Представляется, что нейронная сеть также является прежде всего средством совершения преступления, и лишь в случае использования вредоносных компьютерных программ или иной компьютерной информации в целях неправомерного воздействия на компьютерную информацию, используемую нейросетью для создания различного содержимого и являющейся ее частью, – предметом преступления.

Нейронная сеть – это математическая модель, построенная на принципах структуры и функциональных аспектов биологических нейронных сетей. Она состоит из взаимосвязанных искусственных нейронов, которые обрабатывают информацию и преобразуют ее с помощью распределенного и параллельного

---

[1] Кудрявцев В.Н. Объективная сторона преступления. М.: Госюриздат, 1960. С. 75.

[2] См. напр.: Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2 (9). С. 43–46; Воробьев В.В. Вредоносные компьютерные программы в уголовном законодательстве Российской Федерации // Путеводитель предпринимателя. 2015. № 26. С. 92–100.

[3] См. напр.: Гребенкин Ф. Б., Коврижных Л. А. Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ // Вестник гуманитарного образования. 2017. № 2. С. 71–77.

[4] См. напр.: Галушин П.В., Лапина Е.А. Иная вредоносная компьютерная информация как предмет преступления, предусмотренного статьей 273 УК РФ // Научный компонент. 2020. № 1 (5). С. 61–67.

[5] См. напр.: Попов А.Н. Преступления в сфере компьютерной информации: учебное пособие. СПб: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. С. 23.

[6] См, напр.: Бюллетень Верховного Суда РСФСР. 1975. № 6. С. 14.

[7] Побегайло А.Э. Борьба с киберпреступностью: учебное пособие. М.: Университет прокуратуры Российской Федерации", 2018. С. 57.

подхода. Искусственные нейроны в нейронной сети могут обрабатывать информацию одновременно и независимо друг от друга, что позволяет сети быстро адаптироваться и обучаться на больших объемах данных.

Теоретическая разработка алгоритмов нейронных сетей началась в 1940-х гг. XX в. Перцептрон, нейронная сеть первого поколения, был изобретен Ф. Розенблаттом в 1958[1]. Тем не менее, ряд задач был невыполним для нейронных сетей первого поколения, а их развитие ограничивалось недостаточной мощностью электронно-вычислительного оборудования той эпохи. Бурный рост вычислительных мощностей 1990-х и удешевление электронных компонентов в 2000-х гг. являлись одними из основных факторов развития самих нейронных сетей и интереса к ним.

Нейросетевые архитектуры обычно подразделяют на ряд поколений (эпох).

К первому поколению относятся простейшие нейронные сети прямого распространения (feedforward neural network), такие как перцептрон и многослойный перцептрон (MLP). Они могут решать базовые задачи классификации и регрессии.

Второе поколение – рекуррентные нейронные сети (RNN) LSTM и GRU. Такие архитектуры позволяют обрабатывать последовательные данные и проводить моделирование долгосрочных зависимостей, что позволило ученым существенно продвинуться в обработке такими нейросетями естественного языка.

Сверхточные нейронные сети (CNN) относятся к третьему поколению, используются, прежде всего, в области компьютерного зрения (computer vision, CV). С их помощью возможно эффективное извлечение иерархических признаков из визуальных данных, тем самым успешной выполняя задачи распознавания образов.

Нейросетевые архитектуры, основанные на механизме внимания (attention), а также трансформеры (transformers) относятся к четвертому поколению. Такие архитектуры эффективно обрабатывают и создают текстовую информацию, распознают изображения и могут выполнять ряд иных задач. К ним относятся BERT, GPT и им подобных. Одной из самых известных нейронных сетей на базе GPT является ChatGPT, разработанная компанией OpenAI. Помимо ChatGPT, на архитектуре генеративных предварительно обученных трансформеров также существуют модели Claude (компания Anthropic AI), Gemini (Google), Grok (X.AI) и ряд других, в том числе свободно распространяемых (такие как LlaMA (Meta AI), Mistral (Mistral AI) и др.).

Существует также еще ряд архитектур и типов нейронных сетей, такие как, например, генеративно-состязательные сети (generative adversarial networks, GAN), позволяющие, например, увеличивать разрешение цифровых изображений и создавать т.н. «глубокие подделки» («дипфейки»). В современных архитектурах нейросетей часто используются т.н. «слои» –

[1] Гафаров Ф.М., Галимянов А.Ф. Искусственные нейронные сети и приложения: учеб. пособие. Казань: Изд-во Казан. ун-та, 2018. С. 10.

отдельные нейронные сети различных типов, соединенные воедино, для выполнения различных задач.

На настоящий момент в российском уголовном законодательстве не имеется ни понятия или определения нейронных сетей, ни генерируемого ими содержимого. При этом они уже могут быть использованы для совершения следующих преступных деяний.

Создания реалистичных поддельных видео-, фото- или аудиозаписей (дипфейков), включая синтезированные голоса для имитации реальных людей, которые могут быть использованы для клеветы, мошенничества, а равно вымогательства (ст. 128.1, 159, 163 УК РФ).

Создания заведомо ложной информации с целью ввода в заблуждение общественности, запугивания ее, усиления расовой, национальной или иной розни, а равно доверия к источникам информации и государственным институтам (ст. 207, 207.1, 207.2, 207.3 УК РФ).

Создания порнографического содержимого (включая изображения несовершеннолетних) с помощью нейронных сетей в целях травли, дискредитации или нарушения законов о защите авторских прав (ст. 146, 242, 242.1 УК РФ).

Создания вредоносного программного обеспечения. Также нейросети могут использоваться упрощения поиска уязвимостей в программном обеспечении и создания специализированных атак на конкретные цели (ст. 273 УК РФ).

Создания материалов, пропагандирующих терроризм, диверсионные или экстремистские идеи, включая создание манипулятивного видео- или аудио-контента (ст. 205.2, 280, 280.1, 280.4, 281.1, 281.3, 282 УК РФ).

Также необходимо выделить возможность использования нейросети для автономного и быстрого анализа ряда независимых баз данных, незаконно попавших в руки злоумышленников, содержащих персональные и иные конфиденциальные данные. На основе таких данных нейросеть может достаточно быстро составить отчет о лицах, в отношении которых планируются преступные посягательства, например, мошеннические действия.

К проблемам квалификации преступлений, совершенных с использованием нейронных сетей, можно отнести относительную автономность нейронной сети, что при определенных сценариях применения может привести к тому, что пользователь не контролирует распространяемую ею информацию, не имеет прямого умысла по отношению к каким-либо действиям.

Помимо этого, в законе не нашел отражения и признак повышенной опасности нейронной сети. При использовании Интернета общественную опасность несет, прежде всего, признак публичности, а при использовании нейросети, на наш взгляд – признак доступности. До появления и распространения нейросетей с удобным пользовательским интерфейсом, например, создание поддельных фото-, видео- и аудиозаписей требовало специальных познаний в соответствующем программном обеспечении, то с использованием нейросетей познаний требуется значительно меньше.

При этом представляется неправильным причисление нейросети к вредоносному программному обеспечению. Нейросеть не может считаться заранее вредоносной, если только не была специально создана с помощью обучения на исходных кодах вредоносного программного обеспечения, но на настоящий момент таких нейросетей в общем доступе нет.

Как уголовно-правовое понятие «вредоносная компьютерная программа», так и «иная компьютерная информация» неотделимы от признака заведомости, когда при создании, использовании или распространении программа или иная компьютерная информация заранее направлены на указанные в законе преступные последствия[1].

При этом практически любую из существующих типов нейронных сетей к такой информации отнести нельзя, т. К. при их создании инженеры не предполагали достижения целей, перечисленных в ч. 1 ст. 273 УК РФ.

Представляется, что необходимо предложить следующие пути регулирования нейросети как средства совершения преступления: 1) внести в текст соответствующих статей УК РФ, квалифицирующего признака «…с использованием нейронной сети», по признаку доступности, увеличивающей общественную опасность деяния; 2) внести «…с использованием нейронной сети» как конститутивного признака ст. 273 и 274.1 УК РФ, поскольку для совершения данных преступлений, субъект в любом случае должен уже иметь специальные познания; 3) внести признак «с использованием нейронной сети, а равно искусственного интеллекта» в ст. 63 УК РФ в качестве одного из отягчающих обстоятельств; 4) дополнить указанное Постановление Пленума Верховного Суда от 15.12.2022 № 37 понятием нейронной сети как «математической модели, построенной на принципах структуры и функциональных аспектов биологических нейронных сетей, способной к созданию, использованию и распространению цифровой информации, включая текстовую информацию, видеозаписи, цифровые изображения, исполняемый код».

[1] См. п. 8 Постановления Пленума Верховного Суда РФ от 15.12.2022 № 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» // СПС «КонсультантПлюс».

И.С. Поляков

Современные возможности программного обеспечения поиска и анализа криминалистически значимой информации в информационно-телекоммуникационных сетях

Аннотация. В настоящей работе рассматриваются современные виды программного обеспечения, направленные на поиск, обнаружение, сбор и анализ электронных следов в информационно-телекоммуникационных сетях, в частности в сети «Интернет». Фактически они представляют собой инструментарий OSINT (разведки по открытым источникам) как способа познания об интересующем лице, факте или событии.

Ключевые слова: OSINT, Интернет, информационно-телекоммуникационная сеть, программное обеспечение, электронные следы.

Актуальность рассмотрения Интернет-ресурсов как следообразующих и следовоспринимаемых объектов обусловлена неуклонно возрастающей статистикой преступной деятельности в информационно-телекоммуникационных сетях. Согласно данным ГИАЦ МВД России только за январь-март 2024 года зарегистрировано 179,2 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий (ИТС) или в сфере компьютерной информации, что на 17,6 % выше, чем за аналогичный период в 2023 году (152,4 тыс.)[1]. 5 лет назад рассматриваемый показатель не превышал 56 тыс. уголовно-наказуемых деяний[2]. 10 лет назад число подобных преступлений не достигало даже тысячи (844)[3].

Изучение следователем огромного массива данных, содержащихся в ИТС Интернет, может быть существенно облегчено с помощью соответствующего программного обеспечения (ПО) по поиску, обнаружению, сбору и анализу т.н. электронных следов[4]. В данном исследовании кратко освещен существующий инструментарий (отдельные модули и библиотеки) в России и за рубежом.

Многие иностранные ученые, в частности из Республики Беларусь, Республики Индия, Исламской Республики Пакистан, Китайской Народной Республики, Соединенных Штатов Америки, отмечают, что одной из самых полных библиотек является проект Kali Linux, созданный Мати Ахарони и

[1] Состояние преступности в России за январь-март 2024 года. МВД России. URL: https://мвд.рф/reports/item/49477631/ (дата обращения: 01.04.2024).

[2] Состояние преступности в России за январь-март 2019 года. МВД России. URL: https://мвд.рф/reports/item/16523390/ (дата обращения: 01.04.2024).

[3] Состояние преступности в России за январь-март 2014 года. МВД России. URL: https://мвд.рф/upload/site1/document_file/ulsqsrGCng.pdf (дата обращения: 01.04.2024).

[4] Под ними предлагается понимать цифровой результат социального взаимодействия лица с помощью соответствующих инструментов, а равно форму документации поведения отдельного лица в виртуальном пространстве.

Максом Мозером в 2013 году[1]. Он включает в себя такие утилиты по сбору информации, представляющие интерес для следствия, как:

- Maltego, Recon-ng, MassMine – приложения для скачивания и архивирования данных, в частности рабочие электронные почты по домену компании, аккаунты в социальных сетях, восстановленные пароли к ним, учетные записи, под которыми зарегистрированы лица, связанные контакты, IP-адреса[2] с выстраиванием запрошенной информации в логическую цепочку;
- OSRFramework – набор библиотек для выполнения задач по проверке имен пользователей, исследования утечек данных, извлечения по частотным выражениям с визуализацией запросов из веб-приложений;
- SpiderFoot – инструмент с открытым исходным кодом для автоматизированного поиска сведений по поисковым системам;
- the Harvester – утилита для сбора электронных адресов, доменных имен[3], виртуальных хостов и открытых портов[4];
- Nmap – инструмент для обнаружения открытых портов и запущенных на нем службах, приложениях и их установленных номерах версий, хостов, IP- и MAC-адреса[5];
- Jhon the Ripper – программа для взлома паролей методом автоматического перебора;

[1] Qureshi, S., He J., Qureshi, S.S., Yhu, N., Rajputt, F.A., Ullah F., Nayir, A., Wajahat, A. (2022) Browser Forensics: Extracting Evidence from Browser Using Kali Linux and Parrot OS Forensics Tools. *International Journal of Network Security*, no. 24 (3), pp. 557–572; Дерюгин Р.А. Использование «разведки» по открытым источникам (OSINT) для получения криминалистически значимой информации из сети Интернет // Борьба с преступностью: теория и практика: тезисы докладов XI Международной научно-практической конференции (Могилев, 7 апреля 2023 г.). Могилев: Могилев. институт МВД, 2023. С. 424–428, Santoshi, D., Pulgam, N., Mane Vanita. Analzsis and Simulation of Kali Linux Digital Forensic Tools. *SSRN*. URL: https://ssrn.com/abstract=4111750 (accessed 01.04.2024), Grundy, B.J. The Law Enforcement and Forensic Examiners Introduction to Linux: A Comprehensive Practitioner's Guide to Linux as a Digital Forensics Platform (2023) *Linux*. URL: https://linuxleo.com/Docs/LinuxLeo_4.97.pdf (accessed 01.04.2024) и Поликарпов Е.С. Основы компьютерной разведки: учебное пособие. М.: Московский университет МВД России им. В.Я. Кикотя, 2020. С. 57.

[2] Уникальный идентификатор устройства в электронной (компьютерной) сети, состоящий из номера сети и номера узла, определяющий сетевое соединение. Он описывает, как осуществлено подключение.

[3] Идентификация конкретной части электронной (компьютерной) сети.

[4] Нужны для обращения из информационно-телекоммуникационной сети «Интернет» к компьютеру.

[5] Уникальный идентификатор, определяющий устройство при выходе в компьютерную сеть – аппаратный или физический адрес. Он описывает непосредственно само устройство.

- xplico – программа для анализа Интернет-трафика (извлечение электронных писем (протоколы POP3, IMAP и SMTP), все содержимое HTTP[1], вызовы VoIP[2] по протоколам FTP, TFTP).

В части анализа социальных сетей представляется интерес сопоставление таких инструментов, как CacheBack, EnCase Forensic и Internet Evidence Finder по критериям: анализ истории (список посещенных веб-сайтов), кэш браузера, Интернет-сессии и чаты социальных сетей/записи в них. По мнению новозеландских криминалистов, первые два показали отличные результаты, хотя и ограниченно анализируют информацию при использовании веб-браузера Safari[3]. Перечисленные программные обеспечения позволяют комплексно сканировать активность пользователя в веб-браузерах Internet Explorer, Firefox, Google Chrome, Opera, Safari, однако стоит отметить, что EnCase Forensic также охватывает веб-браузер Chromium и изучает не только цифровые следы, но и всю систему осматриваемого устройства[4].

Подобные программы позволяют получать данные о социально-психологическом портрете личности преступника (вредные привычки, увлечения, нездоровые пристрастия, эмоциональное состояние, круг общения, интересы и убеждения), идентификаторах устройств, используемых ресурсах (электронные кошельки, сервисы различных видов услуг), сопоставлять лица с учетом возможных вымышленных личностей и имен (по регистрационным данным) и их действия, устанавливать связи с группировками и организациями (подписки на идеологические и пропагандистские каналы, группы и сообщества) в ИТС Интернет.

Существуют специализированные утилиты для извлечения данных под конкретные браузеры или группы браузеров по типу Dumpzilla — изучение файлов cookie (посещений), истории загрузок, сохраненных закладок для веб-браузеров Firefox, Iceweasel, Seamonkey компании Mozilla Corporation. Поисковые запросы также могут быть значимой для следствия информацией. В пример можно взять как отечественную, так и зарубежную практику. Во-первых, американское дело Брайана Уолша, против которого выдвинуты обвинения в убийстве собственной жены. На планшете его сына была обнаружена следующая история запросов в поисковой системе Google в течение нескольких дней после пропажи Аны Уолш: через сколько времени тело начинает пахнуть; как остановить разложение тела; как связать тело; 10 способов избавиться от трупа,

---

[1] Протокол передачи гипертекста — получения данных клиентом сервиса электронной (компьютерной) сети. Он способствует безопасному установлению запросов между серверами через элементы: адрес хоста, метод, версия и путь до конкретного файла на сайте (URI), а также ответов: статус, заголовки и содержание (ошибки).

[2] Технология передачи голоса через IP-протокол.

[3] Cusack, B., Son, J.(2012) Evidence examination tools for social networks. 10th Australian Digital Forensics Conference, Novotel Langley Hotel, Perth, Western Australia. 3-5 December 2012. Edith Cowan University Research Online. URL: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1108&context=adf (accessed 01.04.2024).

[4] Akhbal E., Günes F., Akbal A. Digital forensic analyses of web browser records // Journal of Software. 2016. № 11 (7). P. 631-637.

если очень нужно; через сколько времени можно наследовать после пропажи лица; можно ли выкинуть части тела; что делать формальдегид, как долго сохраняется ДНК; можно ли по останкам установить личность; расчленение и лучше способы избавиться от тела; как отмыть кровь с деревянного пола; люминал для определения крови; что случится, если положить части тела в аммиак; лучше выкинуть или постирать вещи с места происшествия; ножовка как лучший инструмент для расчленения; можно ли вменить убийство без тела; можно ли установить личность по сломанному зубу; что происходит с волосами у умершего; какова скорость разложения трупа в пластиковом пакете в сравнении с тем, что в лесу; может ли пищевая сода заставить тело хорошо пахнуть[1].

Во-вторых, косвенным доказательством виновности сотрудника компании по уголовному делу (из собственной практики) выступали поисковые запросы лица с компьютера жены об ответственности за несанкционированный доступ к охраняемой законом компьютерной информации и за разглашение таких данных, а также подробное изучение судебной практики, совпадавшие хронологически с моментом совершения преступление.

В рамках соответствующего консорциума Национальный институт юстиции США предоставил финансирование нескольким университетам для анализа электронных следов, в частности Университету Род-Айленда, а также Университету Пердью для разработки программ по анализу глобальной компьютерной сети. Например, специалистами из первого университета разработано ПО DeepPatrol. Он разбивает видеоролики на картинки в режиме реального времени, анализирует их, используя детектор лиц и соответствующие классификаторы по определению пола, возраста, исходя из баз характерных черт, при помощи общедоступной сверточной нейронной сети компании Yahoo OpenNSFW. Используются базы данных IMDB-Wiki (Википедии), APPA-Real, RedLight (Центра цифровой криминалистики и кибербезопасности Университета Род-Айленда), NPDI и правоохранительных органов для обнаружения порнографических материалов в автоматизированном виде[2].

Учеными из второго университета разработано ПО «FileTSAR» — механизм выборочной реконструкции (восстановления) нескольких типов данных объемом до 100 ГБ, включая документы, изображения, аудио-, видеозаписи, электронную почту (на основе SMTP, IMAP, IMP) и сеансы VoIP для компьютерных сетей с возможностью ведения журнала важных данных. В настоящее время FileTSAR лицензирован 120 государствами и внедрен, как минимум, в 30 из них, включая 308-й батальон военной разведки и полицию Федеративной Республики Нигерия, подразделение по борьбе с киберпреступностью Португалии, офис шерифа

[1] Brian Walshe's Shocking Google Searches After His Wife Went Missing // NBC. URL: https://www.nbcboston.com/news/local/heres-what-brian-walshes-google-searches-included-after-his-wife-went-missing/2948147/ (дата обращения: 01.04.2024).

[2] Vega, M.A. (2022) DeepPatrol: Finding Illicit Videos for Law Enforcement. U.S. Office of Justice Programs. URL: https://www.ojp.gov/pdffiles1/nij/grants/254636.pdf (accessed 01.04.2024).

округа Грант (штат Висконсин, США) и Королевский военно-морской флот Великобритании[1].

Архитектура ПО FileTSAR может быть представлена следующим образом:

- коллектор собирает сведения об Интернет-трафике (содержание и статистику по использованию) в бинарном виде и сохраняет его в хранилище;
- классификатор распределяет данные для анализа по источнику и протоколу;
- анализатор рассматривает метаданные для установления пояса времени, пользователей и содержание файлов;
- визуализатор выявляет модели поведения, повторения и динамику, отражая, сортируя данные на улики, следы и возможные доказательства[2].

Из российских программных обеспечений отдельного внимания заслуживает платформа по безопасности цифровых активов «Шард» — совокупность программ для ЭВМ Explorer-API и Risk-API, позволяющих искать, собирать и анализировать общедоступные данные, касающиеся криптовалюты[3], смарт-контрактов, NFT-токенов и операций с ними, из блокчейнов и иных доступных источников информации. Она является достойным аналогом ПО Crystal нидерландской компании Crystal Intelligence.

Таким образом, существует ряд комплексных систем, которые автоматизировано ищут, собирают и анализируют информацию из открытых источников, как отечественного, так и зарубежного происхождения. Многообразие функционала иностранных ПО, которые существенно облегают расследование преступлений, требует разработку и внедрение российских аналогов в работу правоохранительных органов. Фактически они являются инструментами такого феномена, как OSINT, и могут быть представлены в виде схемы следующим образом.

---

[1] Novak, M. (2021) Improving the Collection of Digital Evidence. U.S. Office of Justice Programs. URL: https://nij.ojp.gov/topics/articles/improving-collection-digital-evidence (accessed 01.04.2024).

[2] Hansen A.R., Siegfried-Spellar K.C., Lee S., Chowdhiry S.S., Abraham N., Springer J., Yang B., Rogers M. File Toolkit for Selective Analysis & Reconstruction (FileTSAR) for Large-Scale Networks. *IEEE International Conference on Big Data* (Seattle, 10-13 Dec. 2018). IEEE: USA, 2018. P. 3059–3065.

[3] Предоставляются данные об электронных кошельках, участвовавших в транзакциях, время совершения трансакций, их хеш, риски криптовалютного адреса, индикаторы подозрительной активности, топ контрагентов по уровню риска, финансовую сводку.

Рис. 1. Функционал разведки по открытым источникам

Так, например, с помощью IP-адреса возможно установить адресное пространство государства, интернет-провайдера, часовой пояс, операционную систему компьютерного устройства, номер автономной системы, владельца и использующиеся им диапазоны. MAC-адреса имеют бóльшую значимость в контексте роутеров и модемов, нежели мобильных телефонов, поскольку у современных моделей при каждом новом подключении к сети присваивается случайный (подменный) MAC-адрес в целях информационной безопасности. Доменное имя также позволяет установить страну, регистрационные данные компании либо лица, в том числе имя владельца, используемые контактные данные, принадлежность к регистратору, даты регистрации и ее окончание, информацию об IP-адресах, используемые способы оплаты для его аренды, что способствует установлению криминалистически значимой информации.

Впоследствии полученные сведения можно проанализировать с помощью открытых источников по типу сервисов «2ip» и «whois». Даже при использовании VPN (технологий по маскировке IP-адреса пользователя и шифровании данных) возможно установить диапазон цепочки IP-адресов и, следовательно, какой компании они принадлежат для последующего запроса о данных лица, арендовавшего IP-адреса.

Сведения, полученные посредством OSINT, позволяют оперативно выдвигать и проверять версии, планировать соответствующие следственные действия и организовывать проведение мероприятий при расследовании не только преступлений, совершенных с использованием ИТС, но и иных уголовно-наказуемых деяний.

Д.А. Рыжиков

Отдельные проблемные вопросы цифровизации деятельности органов внутренних дел Российской Федерации

Аннотация. Статья посвящена проблемам обеспечения различных подразделений органов внутренних дел, возникающих при переходе к цифровому формату их деятельности. В публикации уточняются текущие направления технического и технологического совершенствования и предлагаются приоритетные и актуальные задачи, подлежащие решению в условиях глобального переоснащения Министерства внутренних дел. Вместе с тем, автором оцениваются перспективы реализации на практике предлагаемых решений и обосновывается необходимость применения программных, аппаратных и аппаратно-программных средств, предназначенных для взаимодействия подразделений МВД России на внутри- и межведомственном уровне с целью повышения уровня обеспечения раскрытия и расследования преступлений.

Ключевые слова: цифровизация деятельности органов внутренних дел, технологии «цифровых двойников», цифровая трансформация, научно-технический прогресс, нормативное регулирование и стандартизация нейросети.

Современная научно-техническая деятельность МВД России основывается на положениях Концепции научно-технической политики МВД России до 2030 года и предусматривает увеличение уровня научности и технологичности внедряемых в деятельность подразделений Министерства внутренних дел Российской Федерации современных достижений в сфере информационных технологий.

Цифровизация, как наиболее значимый тренд научно-технического прогресса, сегодня прочно занимает свои позиции в развитии общества и государства от момента внедрения достижений в сфере информационных технологий в быт граждан до реализации государственных программ развития средств обеспечения государственной безопасности.

И если в области обеспечения жизнедеятельности рядовых граждан наблюдается некоторая «избыточность», из-за чего результаты научно-технического прогресса разработчиками «придерживаются» для получения максимально возможной прибыли, то применительно к запросам обеспечения деятельности государственных органов в последние годы наметилась общая тенденция «нехватки ресурсов», затрагивающей, в том числе, значительные сферы деятельности подразделений Министерства внутренних дел Российской Федерации.

Такая негативная тенденция обусловлена спецификой осуществляемого подразделениями органов внутренних дел функционала, его сложностью, многозадачностью и закрытостью, но, вместе с тем еще, и сложностью государственного управления в области развития специализированного

информационно-технологического обеспечения деятельности подразделений МВД России, нехваткой научного и обслуживающего персонала, а также отсутствием должного методического и нормативного регулирования.

Преступное сообщество в современных условиях, необремененное выше озвученными проблемами, применяет в своей деятельности наиболее технологические и продвинутые средства (технические, программные и технологические), достигая порой весьма значительных результатов. При этом органы внутренних дел, зачастую и к сожалению, отстают в уровне своего оснащения, обеспечения, и находятся в рядах «догоняющих научно-технический прогресс». Во многом из-за этого увеличивается время решения актуальных задач, возникающих в рамках противодействии или раскрытия и расследования преступлений, либо исполнителями формируются результаты, неприменимые для достижения поставленных целей и применения их в качестве доказательств.

С учетом этих обстоятельств, руководством Российской Федерации и Министерства внутренних дел уделено значительное внимание не только текущим мероприятиям, направленным на повышение уровня цифровизации деятельности подразделений органов внутренних дел, но и перспективным направлениям развития обеспеченности правоохранительной деятельности государства, учитывающей повышение эффективности применения МВД России современных информационных технологий. Отражена эта деятельность в таких нормативных актах, как Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы», Указ Президента Российской Федерации от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации», приказ МВД России от 28.04.2023 № 260 «Об организации научной и научно-технической деятельности в системе МВД России», а также в Концепции использования искусственного интеллекта в деятельности подразделений МВД России на период до 2030 года и Концепции научного обеспечения деятельности органов внутренних дел Российской Федерации на период до 2030 года и других актах.

С учетом имеющегося нормативного регулирования направлений развития научно-технического развития, для МВД России, помимо разработки и внедрения новых, модернизации и развития имеющихся технологий «больших данных» и технологий искусственного интеллекта, в настоящее время видится актуальным и необходимым совершенствование:

- перспективных сетей передачи данных;
- аппаратно-программного обеспечения деятельности и управления деятельностью исполнителей и руководителей подразделений Министерства;
- межведомственного взаимодействия на основе новейших информационно-технических разработок;
- единой системы информационно-аналитического обеспечения деятельности МВД России;

- информационно-аналитической системы поддержки принятия решений сотрудниками МВД РФ;
- навигационного и геоинформационного обеспечения подразделений МВД России;
- специализированных робототехнических систем.

Результатом такой кропотливой целенаправленной работы станет постепенное формирование облика полицейского будущего, определяемого прежде всего функциональным многообразием, спецификой деятельности различных подразделений Министерства, а также особенностью нормативного регулирования этой деятельности.

Как показывает практический опыт, достижение озвученного конечного результата – развитие информационно-технической составляющей деятельности МВД России в целом, возможно только посредством решения большого круга частных, специализированных задач каждого из подразделений Министерства внутренних дел РФ.

Вместе с тем, в настоящее время, мы можем лишь констатировать приоритетные и актуальные задачи, подлежащие решению. И если рассматривать информационно-техническое развитие хотя бы в десятилетней перспективе, то наиболее значимым и необходимым видится внедрение следующих новшеств.

На основе имеющегося в Министерстве внутренних дел научно-технического потенциала необходимо создать ресурс (программный робот), обеспечивающий распознавание речи заявителя, преобразование ее в текстовый документ, формирование приоритетной классификации получаемых дежурными частями данных по направлениям деятельности подразделений ОВД, с последующим сопряжением полученных результатов с сервисом СОДЧ. Внедрение такой системы позволит сформировать не только краткосрочную («горячую») базу данных, обеспечивающую их постоянную обработку для формирования оперативного анализа и исключения дублируемой информации. Как нам видится, реализация данного предложения позволит повысить уровень обеспечения актуального для разработки и внедрения единого информационного пространства ситуационного управления всем силами и средствами территориальных органов МВД России, а также в значительной мере обеспечит снижение нагрузки сотрудников дежурных частей с одновременным повышением уровня оперативности реагирования на сообщения граждан. В дальнесрочной же перспективе, применение формируемой базы данных, обеспечит высокую репрезентативность прогнозирования и профилактики преступной деятельности на региональном и районном уровнях.

Крайне важным является вопрос необходимости разработки для всех служб МВД России, обеспечивающих раскрытие и расследование преступлений, средств автоматического поиска по ведомственным информационным базам данных, реализуемого посредством единой поисковой формы. В настоящее же время поиск представляющей для следствия и оперативных подразделений информации осуществляется в каждом сервисе обособленно, посредством своей

унифицированной формы, ввиду чего временные затраты на проверку даже одного лица весьма и весьма существенны.

Перспектива внедрения данного инструмента видится в повышении уровня оперативности и объективности принимаемых управленческих решений при проведении проверочных и оперативных мероприятий и следственных действий в рамках раскрытия и расследования преступлений.

Актуальным такой инструмент будет и для организации деятельности Министерства в сфере миграционной политики государства. Когда для принятия окончательного решения, за счет сокращения процедур оперативной проверки лица, предполагается уменьшение время аналитической обработки информационного массива разных баз данных в отношении проверяемого лица. При этом следует учитывать, что в настоящее время также отсутствует единая база судебных решений в отношении граждан по условным срокам, т.е. отсутствует информация, инструмент, необходимый и важный для принятия решения в отношении подозреваемых лиц для исключения рецидива или попытки преступника скрыться, уйти от ответственности.

Тут же, видится целесообразным рассмотреть необходимость разработки и мобильной версии такого инструмента, позволяющего посредством реализации квалифицированного (защищенного) удаленного доступа подключиться к ведомственным информационным базам данных заинтересованных уполномоченных лиц. Интересным данное решение будет, как минимум, для следственно-оперативных групп и групп немедленного реагирования, позволяющим в оперативном режиме осуществлять проверочные мероприятия подозреваемых лиц на причастность к совершению преступлений.

Для обеспечения оперативных подразделений, на базе стоящих на снабжении органов внутренних дел информационно-аналитических систем, видится перспективным разработка сервиса (сервиса-интегратора) ИСОД, позволяющего проведение анализа социальных сетей различных Интернет-ресурсов и мессенджеров. При этом варианты исполнения данного инструмента возможна как в стационарном, так и в мобильном видах.

Колоссальными темпами в настоящее время развивается сфера гражданского применения беспилотных робототехнических систем. Перспектива применения таких систем и средств в деятельности подразделений Министерства внутренних дел вполне себе очевидна. Расширение сферы применения такого инструмента обеспечения правоохранительной деятельности, наряду с повышением оперативности получения объективной фактической информации о ситуации на определенном участке местности, позволит в значительной мере сократить необходимость задействования «живой силы», личного состава и средств, например, при организации мер по охране общественного порядка в местах массового скопления людей, или при организации службы подразделениями ППС и ГИБДД.

На примере последней службы возможна разработка специализированного комплекса для производства осмотров мест ДТП, зарегистрированного как средство измерения и включающего: специализированное программное

обеспечение, беспилотный летательный аппарат и портативное средство формирования графической подписи или электронной подписи на основе отпечатка пальца. Посредством БПЛА, снабженного водонепроницаемым и ударопрочным сенсорным пультом управления с предустановленным программным управлением, обеспечивалась бы съемка места ДТП с верхней точки. На основе полученного снимка, программное обеспечение формировало бы схему места ДТП, которая, вместе с протоколом осмотра, подписывалась бы графической электронной или электронной подписью и направлялась посредством взаимодействия с порталом государственных услуг в личный кабинет или на электронную почту участникам ДТП, а также страховым службам.

Аналогичное средство видится перспективным и для производства осмотров мест происшествия, только в этом случае, если говорить уж о совсем фантастическом, то считаем возможным и необходимым проработать вопрос поэтапной реализации идеи создания автоматизированного беспилотного средства обеспечения производства осмотров мест происшествия, позволяющего формировать 3D-модель места преступления и осуществлять поиск, обнаружение и фиксацию следов преступления (обуви, следов рук и других кожных покровов человека, следов выстрела), фиксацию их расположения и взаиморасположения, загрузку полученных электронных следов в ведомственные базы данных, их обработку, анализ, и передачу полученных результатов сотрудникам дежурной следственно-оперативной группы для принятия управленческих решений, немедленного реагирования и раскрытия преступления «по горячим следам».

Это незначительный перечень предложений может и видится в качестве «фантастического» функционала, но в большей своей части он реализуем при правильном поэтапном подходе, основанном на полноценном внутри- и межведомственном взаимодействии. И если рассматривать возможности формирования 3D-модели, то тут уже можно говорить о перспективе расширения сферы её применения, например, для проведения повторного осмотра места происшествия без выезда на место СОГ (когда такой выезд затруднен или невозможен, либо в его первоначальное «содержание» уже привнесены изменения), для проведения следственного эксперимента, проверки показаний на месте, а также при проведении следствия судом для демонстрации отдельных событий преступления или самого места преступления в момент его осмотра в качестве модели подтверждающей интересующую суд информации.

Очевидно, что применение такого инструмента было бы незаменимо при производстве следственного осмотра в рамках проведения специальной военной операции или в условиях военных действий на территории республики Сирия, когда осложнен реальный выезд следственно-оперативной группы на место совершения преступлений или в места организации провокационных действий и действий, дискредитирующих армию Российской Федерации.

Интересным видится внедрение программных средств, обеспечивающих проведение электронного экспертного эксперимента в рамках производства

сложных и дорогостоящих экспертных исследований. Такое решение в значительной мере может сократить производственные затраты на формирование материально-технического обеспечение натурных экспериментов. Да, не везде такое решение сейчас применимо, но расширять области применения специальных программных средств крайне необходимо.

Видится перспективным и следующее. Разработка и внедрение в образовательный процесс систем, основанных на технологиях «цифрового двойника», реализуемых посредством метода имитационного моделирования, на наш взгляд, позволит в значительной мере повысить качественные характеристики формирования высококвалифицированного кадрового потенциала. Перспектива такого подхода при разработке учебного материала определяется комплексностью его реализации. Имитационное моделирование позволяет в полной мере отразить (имитировать) реальные условия и «рабочую» динамику профессиональной деятельности специалиста (следователя, дознавателя, сотрудника дежурной части и т.д.) во всем её многообразии личностных, служебных, социальных связей); отразить возможные содержания и формы совместной профессиональной деятельности за счет вовлечения в познавательную деятельность нескольких участников, распределения их ролей (полномочий, интересов и т.д.) и средств обеспечения их деятельности; имитировать диалоговое общение, в котором заложено необходимое условие для достижения учебных целей (в виде диалога или дискуссии с максимальным участием и взаимодействием всех обучаемых).

В настоящее время отдельные предложения видятся несерьезными или невозможными к реализации, однако, на наш взгляд, все озвученные решения вполне себе жизнеспособны при поэтапном решении (реализации) небольших стандартных задач, направленных на достижение глобальной цели. То есть нужна последовательная реализация научной и научно-технической политики Министерства во взаимодействии всех заинтересованных подразделений, с привлечением стороннего научного и технического потенциала.

Только комплексный, многосторонний подход, учитывающий различные, иной раз противоположные, по сути, научные и практические точки зрения позволит в конечном итоге реализовать «фантастические» задумки.

Вместе с тем оценивая перспективу цифровизации деятельности подразделений МВД России, нельзя не обратить внимание на отсутствие достаточного нормативного и правового регулирования внедрения и применения современных технических и программных средств обеспечения деятельности органов внутренних дел. Как показывает практика внедрения средств обеспечения деятельности различных подразделений Министерства внутренних дел, особо чувствительно нормативный пробел проявляется в рамках организации раскрытия и расследования преступлений, при реализации мер соблюдения процессуальных норм обеспечения производства следственных и иных действий.

И если рассматривать наши, озвученные предложения развития сферы обеспечения деятельности МВД России, в рамках цифровизации, то здесь

наиболее значимой проблемой является отсутствие должного регулирования единого подхода в оценке имеющегося, внедряемого нового или разрабатываемого на перспективу программного обеспечения.

Нормативное регулирование применения и оценка применения технических средств обеспечения организации раскрытия и расследования преступлений, контроля и охраны общественных мест или мест массового скопления людей пресыщена различными техническими условиями, регламентами, стандартами, методическими рекомендациями и правовыми документами, применительно же к программному обеспечению, развивающемуся семимильными шагами, нормотворчество относится весьма и весьма осторожно, хотя проблемная тенденция сформировалась не сегодня.

Многие из озвученных и предлагаемых к разработке предложений, предполагают применение различных технологий на основе искусственного интеллекта (компьютерное зрение, прогнозная аналитика, распознавание речи, периферийные вычисления, нейросети и т. д.). И если взять, те же нейросети, то здесь также не обходится без проблем.

В настоящее время существует множество различных методов оценки нейросетей, например, методы проверки однородности связных выборок или проверки гипотезы нормальности распределения, используют различные метрики и показатели, однако единого нормативно ведомственного документа в МВД России в настоящее время нет. По мнению многих специалистов, такого документа в принципе не может быть, т.к. это определяется прежде всего функционалом, реализуемым конкретным решением и конкретной нейросетью во вполне определенной области знаний. Но вместе с тем каждая область применения различных технических и программных средств обладает своей индивидуальностью, своим «регламентом». В современных условиях, без выверенного, нормативно определенного метода или способа найти, определить, использовать или интерпретировать результаты, можно, но бывает весьма трудно провести сравнение или обеспечить контроль и определить качество работы какой-то системы.

Стремительное развитие технологий искусственного интеллекта спровоцировало необходимость принятия норм, регламентирующих его использование в медицинской сфере. Учитывая это, для регулирования применения сервисов искусственного интеллекта в медицине в 2022-2024 годах уже разработаны 11 ГОСТов, а в текущее время в активной фазе разработки находятся еще два.

Например, разработанный стандарт для тестирования искусственного интеллекта не имеет аналогов в мире, и он устанавливает требования для каждого процесса жизненного цикла систем искусственного интеллекта, регулирует безопасное проектирование и техническое обслуживание систем искусственного интеллекта в клинической медицине и применим как разработчиками сервисов искусственного интеллекта и сотрудниками лабораторий при технических испытаниях, так и специалистами медицинских организаций в клинических испытаниях. По мнению специалистов этой сферы и разработчиков указанных

нормативных документов, использование стандартов обеспечит внедрение только проверенных, надежных решений в практическую медицину, поможет в разработке новых нейросетей и тестировании существующих[1].

Учитывая, что проверка работоспособности нейросети представляет собой сложный и длительный процесс действий, разработка стандарта, за счет применения методики последовательных операций для оценки нейросетей в соответствии с определенным сценарием действий, помимо сокращения затрачиваемого временного ресурса, позволит обеспечить справедливое и точное определение эффективности нейросетей, их качества и надежности.

Тем самым, вполне очевидна актуальность и необходимость разработки своего ведомственного стандарта и для правоохранительных органов. Решение вопроса нормативного регулирования, стандартизации требований для каждого процесса жизненного цикла систем искусственного интеллекта, применяемых для реализации задач правоохранительных органов позволит во многом сформировать благоприятные условия для создания надежных, проверенных, контролируемых программных решений, чем обеспечит уверенный рост темпов цифровизации деятельности Министерства внутренних дел в целом.

Подводя итоги, хочется отметить, что для полноценного развития сферы обеспечения деятельности органов внутренних дел следует учитывать не только современные технологии, программные и технические средства, но нормативное регулирование их применения. Только комплексный поэтапный подход к решению возникающих задач позволит достичь желаемых результатов, позволяющих решить задачи безопасности государства и общества.

Список литературы

1. Адамова А.А., Бецков А.В. Проблемы информатизации и информационной безопасности цифровых производств // Информатизация и информационная безопасность правоохранительных органов. Сборник трудов Международной научно-практической конференции. Москва, 2023. С. 7–14.

2. Курносенко А.Е., Шахнов В.А. Цифровая трансформация при подготовке производства изделий электроники // Автоматизация. Современные технологии. 2021. Т. 75. № 2. С. 51–56.

3. Шахнов В.А., Курносенко А.Е. Моделирование цифрового производства электронной аппаратуры в рамках концепции «Индустрия 5.0» // Цифровая трансформация промышленности: тенденции, управление, стратегии. Материалы I Международной научно-практической конференции (Екатеринбург, 11 октября 2019 г.) / Ответств. ред. В.В. Акбердина. Екатеринбург: Институт экономики Уральского отделения РАН, 2019. С. 585–594.

[1] Нейросеть в медицине теперь по ГОСТу – URL: https://niioz.ru/news/neyroset-v-meditsine-teper-po-gostu/ (дата обращения 25.04.2024)

Т.А. Сааков

Судебно-диагностическое исследование демографических характеристик личности по письменных речевым следам: понятие и криминалистическая значимость

Аннотация. В статье рассматриваются различные подходы к понятию «демографические характеристики автора», на основе анализа литературы автор обосновано к приходит к выводу о группе характеристик личности, относящихся к демографическим характеристикам автора. На основе анализа следственно-судебной практики автор обосновано приходит к выводу, что в эпоху цифровизации криминалистическая значимость установления демографических характеристик личности заключается в получении необходимой ориентирующей информации, позволяющей на первоначальному этапе расследования выйти из состояния «энтропии».

Ключевые слова: демографические характеристики автора, цифровые следы, диагностические исследование, криминалистическая значимость, судебная автороведческая экспертиза.

Особую актуальность установление демографических характеристик личности по письменным речевым следам приобретает в нынешних условиях цифровизации современного общества[1]. Это в первую очередь обусловливается тем, что с каждым годом возрастает количество преступлений, совершаемых при помощи использования информационно-телекоммуникационных технологий, включая сеть Интернет[2]. Например, по таким составам преступлений как ст.110 УК РФ, ст.110.1 УК РФ, ст.110.2 УК РФ, ст.119 УК РФ, ст. 120 УК РФ, ст.126 УК РФ, ст.163 УК РФ, ст. 207 УК РФ, ст. 205.1 УК РФ, ст. 205.2 УК РФ[3]. При этом следует отметить, что данный перечень составов преступлений, совершаемых с использованием компьютерно-опосредованных технологий, является далеко не исчерпывающим.

Во многом сложности при расследовании таких преступлений, как показывает анализ следственной и судебной практики, возникают из-за того, что личность преступника зачастую в веб-пространстве конспирируется, создавая себе вымышленный образ, не соответствующий реальному, вследствие чего

[1] См., например: Сааков Т.А. Актуальность установления демографических характеристик автора в целях розыска лиц по признакам письменной речи // Теория и практика судебной экспертизы в современных условиях: материалы VII Международной научно-практической конференции. М.: Проспект, 2019. С. 428–433.

[2] Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2019. №5 (57). С. 33.

[3] Уголовный кодекс Российской Федерации [Электронный ресурс] / федер. закон от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. РФ 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. РФ 5 июня 1996 г.: офиц. текст: по состоянию на 18 фев. 2020 г.: ввод. Федер. законом от 13 июня 1996 г. № 63-ФЗ.

получение полноценной и достоверной криминалистически значимой информации как в розыскных, так и в доказательственных целях вызывает немало сложностей у правоприменителей. На данное обстоятельство также указывает О.В. Танимов, который отмечает, что «В связи с развитием сети Интернет появляется проблема так называемой «виртуальной» личности, которую весьма трудно привлечь к ответственности за возможные противоправные деяния, совершаемые в сети»[1]. Однако при этом остаются цифровые следы, которые как отмечает А.И. Семикаленова, несут в себе значимую для следствия информацию, которая делится на основную (звук, текст, изображение) и дополнительную, позволяющую судить о способе, времени, создании, распространении и редактировании основной информации[2]. Исходя из сказанного следует, что основная информация в цифровых следах состоит преимущественно из вербальных компонентов.

Е.И. Галяшина отмечает, что «В условиях внедрения в информационное пространство компьютерно-опосредованных средств коммуникации <…> речевые действия выделяются в особые группы совершения правонарушений по способу их совершения, посредством слова или по предмету преступного посягательства в отношении слова — как продукта словотворчества»[3]. На данное обстоятельство также указывает А.В. Громова: «Рост «речевых» преступлений (клевета, угроза, вымогательство, экстремизм и др.), развитие каналов передачи информации (сотовая связь, интернет, различные средства аудио- и видеозаписи) актуализируют потребность правоохранительных органов в разработке соответствующего современным реалиям экспертно-криминалистического обеспечения»[4]. В этой связи существенное значение приобретают возможности судебно-диагностического исследования демографических характеристик личности по письменным речевым следам, так как результаты данного исследования расширяют потенцию органов дознания и следствия в получении розыскной и доказательственной информации о личности.

Получение криминалистически значимой информации органами дознания и следствия о свойствах личности преступника, в частности, о его демографических характеристиках, имеет первоочередное значение при расследовании и раскрытии преступлений. На данное обстоятельство, например, указывал М.В. Салтевский, который отмечал, что «Познание события преступления осуществляется через исследование, прежде всего, человека —

---

[1] Танимов О.В. Проблемы виртуальной личности в сети Интернет // Мониторинг правоприменения. 2012. № 4. С. 57.

[2] Семикаленова А.И. Цифровые следы: назначение и производство экспертиз / А. И. Семикаленова // Вестник Университета имени О.Е. Кутафина. 2019. №5. С. 117.

[3] Галяшина Е.И. Речевые следы как объекты судебных экспертиз (в свете идей Р. С. Белкина) // Современное развитие криминалистики и судебной экспертизы как реализация идей Р.С. Белкина. Материалы Международной научно-практической конференции «К 95-летию со дня рождения ученого, педагога, публициста» (г. Москва, 22 — 23 ноября 2017 г.). М.: РГ-Пресс, 2018. С. 189.

[4] Громова А.В. К вопросу о диагностике гендерных характеристик автора криминалистически значимого анонимного или псевдонимного текста // Вестник ТГПУ. 2010. № 10 (138). С. 179.

подозреваемого, обвиняемого, потерпевшего, свидетеля, как обладающего максимальным количеством свойств, которые отображаясь вовне, образуют источники информации для розыска и отождествления»[1]. А.М. Зинин отмечает, что установление личности — «одна из наиболее сложных задач, возникающих на первичном этапе раскрытия преступления. Для её решения собираются и исследуются разнообразные данные, отображающие свойства, индивидуализирующие конкретного человека»[2].

Чтобы рассмотреть возможности судебно-диагностического исследования демографических характеристик личности по письменным речевым следам, изначально целесообразно определить, что включает в себя понятие «демографических характеристик личности». Для этого необходимо разобраться в том, что в науке обычно понимают под понятием «личность», чтобы определить, какие из характеристик личности относятся к демографическим.

Стоит отметить, что понятие «личность» трактуется весьма неоднозначно в научной литературе. Как среди социологов, психологов, так и среди юристов существует разное понимание того, что включает в себя данное понятие, какова его структура и что следует понимать под свойствами личности.

Так, например, Е.А. Антонян в своей монографии даёт следующее определение личности: «Личность представляет собой особое качество человека, приобретённое в социальной среде, и как явление выступает во внешне наблюдаемых особенностях социально значимой активности человека — её деятельности, поведения, отдельных поступках, образа жизни и т. д. Сущность личности заключается в особенностях психических свойств, детерминирующих социальную активность человека, и представляет собой единство биогенетических, социогенетических и персоногенетических свойств. Именно они определяют детерминацию развития человека под влиянием среды и наследственности»[3].

По мнению коллектива авторов Московского государственного университета, понятие структуры личности включает в себя четыре большие группы свойств: социальные, психические, психологические и биологические, при этом отмечается, что эти свойства отражаются как идеально, так и материально и используются для изучения личности в криминалистике[4]. В.Е. Корноухов определяет человека через его деятельность, которая может протекать по двум направлениям — внутреннему и внешнему. Свойства личности, по его мнению, отражаются в той или иной форме деятельности индивида. Между личностью и деятельностью существуют определённые виды связи, которые имеют важное

---

[1] Салтевский М.В. Следы человека и приемы их использования для получения информации о преступнике и обстоятельствах преступления: лекция. Киев: НИ и РИО Киевской высшей школы МВД СССР им. Ф. Э. Дзержинского, 1983. С. 5.

[2] Зинин А. М. Габитоскопия и портретная экспертиза: курс лекций. М.: изд-во Моск. акад. МВД России, 2002. С. 16.

[3] Антонян Е. А. Личность рецидивиста: криминологическое и уголовно-исполнительное исследование: монография. М.: Моск. гос. юрид. ун-т. О. Е. Кутафина, 2013. С. 70–71.

[4]Криминалистика: учебник для вузов / В.Н. Герасимов, В.Я. Колдин, В.В. Крылов [и др.]; отв. редактор проф. Н. П. Яблоков. М.: изд-во БЕК, 1995. С. 22.

значение для раскрытия преступлений, так как их анализ важен в том отношении, что в деятельность составной частью входит способ совершения преступления, а также они могут быть положены в основу распознавания, то есть для отнесения личности к определённому классу преступников[1]. В. А. Жбанков подчеркивает, что «понятие «личность» включает в себя представление о социально значимых чертах человека, свойственных ему как отдельному индивиду»[2]. При этом учёный указывает: «сущность личности — персонификация общественных отношений, поэтому конкретная личность выражает свою общественную сущность в форме индивидуальности, которая выступает как её существенная характеристика, выражая способ бытия как субъекта самостоятельной деятельности. В этой связи личность социальна по своей сущности, но индивидуальна по способу своего существования»[3].

Исходя из вышеизложенного приходим к выводу, что свойства личности можно разделить на четыре большие группы: биологические, социальные, психические и психологические. Сразу оговоримся, что существует достаточно большое количество способов и средств, позволяющих получить криминалистически значимую информацию о свойствах личности, однако в настоящем исследовании нами будут рассматриваться возможности судебно-диагностического исследования письменных речевых следов в целях получения криминалистически значимой информации о демографических характеристиках личности.

В специальной литературе в области исследования устной и письменной речи для обозначения свойств личности используется понятие «языковая личность». Проведём анализ понятия «языковая личность».

Понятие языковой личности[4] было введено В. В. Виноградовым, который различал «коллективную языковую личность» и «индивидуальную языковую личность» и связывал изучение этих типов личности с языком художественной литературы. В рассуждениях В. В. Виноградова отмечается, что «социальное ищется в личностном через раскрытие всех структурных оболочек языковой личности»[5].

Следует отметить, что в языкознании существует множество подходов к определению понятия «языковая личность», например, в работах Г.Н. Беспамятновой, В. В. Воробьёва, Г. И. Богина[6] и ряда других авторов.

---

[1] Корноухов В.Е. Комплексное судебно-экспертное исследование свойств человека: монография. Красноярск: изд-во Краснояр. ун-та, 1982. С. 15–16.

[2] Жбанков, В. А. Развитие частной криминалистической теории о свойствах личности // Теория и практика судебной экспертизы (По материалам Криминалистических чтений, посвященных памяти заслуженного деятеля науки Российской Федерации, доктора юридических наук, профессора В.А. Снеткова): Сборник. М.: Экспертно-криминалистический центр МВД России. 2010. С. 47.

[3] Там же. С. 48.

[4] Виноградов В.В. О языке художественной литературы. М.: Гослитиздат, 1959. С. 122.

[5] Там же. С. 122.

[6] См., например: Беспамятнова Г.Н. Языковая личность телевизионного ведущего: дис. … канд. филолог. наук: 10.02.04. Воронеж, 1994. С. 19; Воробьев В.В. Языковая личность и

Проведя анализ имеющихся работ в области исследований «языковой личности», нам представляется наиболее удачным определение, приведённое в работе Ю. Н. Караулова. По его мнению, языковая личность — это «совокупность способностей и характеристик человека, обуславливающих создание и восприятие им речевых произведений (текстов), которые различаются: а) степенью структурно-языковой сложности, б) глубиной и точностью отражения действительности, в) определённой целевой направленностью»[1]. На данное обстоятельство также указывает Е. И. Горошко, которая отмечает, что «идея Ю. Н. Караулова о том, что за каждым текстом стоит языковая личность является одной из основополагающих для теоретического осмысления и обоснования неидентификационных исследований <…> будь то судебное автороведение, фоноскопия»[2].

Необходимо подчеркнуть, что понятие «языковая личность» связано с понятием «речевой портрет». Идея речевого портрета была выдвинута в середине 1960-х годов М. В. Пановым и в дальнейшем развивалась в криминалистическом автороведении С. М. Вулом и рядом других учёных[3]. Речевой портрет раскрывается посредством изучения анализа структуры языковой личности, рассматривающей различные языковые уровни, в которых проявляются особенности речи[4]. Исходя из этого, некоторые методические подходы к диагностике демографических характеристик личности по письменным речевым следам рассматриваются здесь на базе научных основ в области исследования речевого портрета личности.

Следует отметить, что С. М. Вул был одним из первых, кто для обозначения некоторых характеристик личности предложил понятие «социально-биографические характеристики»[5]. В последующем данное обозначение получило широкую практику применения, и на современном этапе нашло своё закрепление в методических рекомендациях Экспертно-криминалистического

национальная идея // Народное образование № 5, 1998. С. 25–30; Богин Г.И. Модель языковой личности в её отношении к разновидностям текста: дис. ... д-ра филолог. наук. Ленинград, 1984. 354 с.

[1] Караулов Ю.Н. Русский язык и языковая личность. М.: Наука, 1987. С. 3.

[2] Горошко Е.И. Судебно-автороведческая классификационная экспертиза. URL: http://www.textology.ru/article.aspx?aId=98 (дата обращения: 02.10.2024).

[3] Галяшина Е.И. Судебная автороведческая экспертиза и феноменология коммуникации в информационно-телекоммуникационной сети Интернет // Союз криминалистов и криминологов. 2018 (№ 3). С. 103.

[4] Алюнина О.Г. Понятие речевого портрета в современных лингвистических исследованиях // Лингвистика и лингводидактика на рубеже веков: теоретические и прикладные аспекты: материалы региональной научно-методической Интернет-конференции, посвящённой 10-летию факультета романо-германских языков. Ставрополь: изд-во СГУ, 2010. С. 107.

[5] Вул С.М. Общие положения методики решения вопросов о социально-биографических характеристиках автора документа // Современные проблемы судебной экспертизы и пути повышения эффективности деятельности судебно-экспертных учреждений в борьбе с преступностью: тезисы респ. науч. конф. Киев: НИИСЭ, 1983. С. 147–149.

центра МВД Российской Федерации[1]. Вместе с тем слово «биография» означает описание чьей-нибудь жизни[2]. Из этого следует, что понятие «социально-биографические характеристики личности» по своей сути является довольно широким, так данное понятие помимо демографических характеристик лица (пола, возраста, этнической принадлежности и т. д.) включает в себя место и год рождения человека, место его работы, адресные данные лица и т. п.

Наряду с этим заметим, что некоторые демографические характеристики личности могут не соответствовать социально-биографическим данным личности. Этому находим подтверждение в трудах М.В. Салтевского, который, ссылаясь на П.П. Цветкова, среди прочих рассматривал социальные свойства личности, в числе которых выделял персонографические – пол, возраст, национальность, место рождения, язык и другие, при этом он указывал, что «это установочные данные, они могут быть изменены умышленно либо искажены»[3].

Действительно, с данным утверждением сложно не согласиться. Оно очевидно и связано с тем, например, что место рождения, указанное в паспорте гражданина РФ, может не соответствовать его фактическому месту проживания, хотя документально эта информация может быть никак не закреплена. Также необходимо учесть, что биографические данные лица, которые в основном закреплены в официальных документах (свидетельство о рождении, паспорт и т. д.), зачастую искажаются злоумышленниками путём их подделки. Так, в соответствии со статистическими данным Главного информационно-аналитического центра МВД Российской Федерации только за январь-декабрь 2019 года было зарегистрировано 875 преступлений по делам о подделке, изготовлении или сбыте поддельных документов, государственных наград, штампов, печатей, бланков[4].

Исходя из изложенного выше считаем, что понятие «социально-биографические характеристики личности» по своей сути является более объёмным, чем «демографические характеристики личности», так как в ходе установления демографических характеристик личности могут быть диагностированы только некоторые из социально-биографических характеристик, которые могут в той или иной мере соответствовать или не соответствовать биографическим данным лица.

Наряду с вышесказанным важно обратить внимание на то, что в практике исследования устной речи используется понятие «обликовые характеристики», к которым относят: «пол, возраст, такие анатомо-физиологические

---

[1] Рубцова И.И., Ермолова Е.И., Безрукова В.И. Комплексная методика производства автороведческих экспертиз: методические рекомендации. М.: ЭКЦ МВД России, 2007. С. 36–77.

[2] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В. В. Виноградова. – 4-е изд., дополненное. – М.: ООО «ИТИ Технология», 2003. С. 48.

[3] Салтевский М.В. Указ. соч. С. 8–9.

[4] Официальный сайт Министерства внутренних дел РФ / ФКУ «Главный информационно-аналитический центр». URL: https://xn--b1aew.xn--p1ai/reports/item/19412450/ (дата обращения: 02.10.2024).

характеристики диктора как рост, вес, степень владения языком (на котором диктор говорит на исследуемой фонограмме), место длительного проживания и формирования речевых навыков, эмоциональное состояние, психофизиологическое состояние (отклонение от нормы, патологии), уровень образования и речевой культуры, социокультурный статус (социальная принадлежность, воспитание и т.п.)»[1].

Однако лексическое значение слова «облик» означает: «внешний вид, очертание, наружность»[2], что указывает на довольно широкий объём данного понятия. В этой связи Б. В. Жулинский, рассматривая проблемные аспекты установления анонимного автора по признакам письменной речи, отмечал, что «Термин «облик» не вполне отвечает смыслу слова, так как в результате анализа документа высказывается суждение о типо-характеристических данных человека, а не о его внешности»[3]. Действительно, с данным утверждением сложно не согласиться, так как на основе диагностического исследования письменного речевого следа, в котором отображается информация о речемыслительных навыках лица, можно создать речевой портрет личности.

Как отмечает Е. О. Бирюкова, «для речевого портрета определяющим является социальный уклон, т. е. подчеркивается важность того, к какой социальной группе принадлежит личность, что во многом определяет её индивидуальные свойства»[4]. Исходя из сказанного следует, что посредством диагностического исследования письменного речевого следа невозможно решить вопрос об облике человека, так как на основе данных, полученных по результатам исследования речемыслительных навыков индивида, отображённых в письменном речевом следе, создаётся речевой портрет личности, которая интересует оперативно-розыскные и/или следственные органы.

Более того, не во всех случаях демографические характеристики личности будут соответствовать в полной мере облику (внешнему виду) человека. Так, например, в условиях современной гендерной дисфории общества биологический пол личности, как демографический показатель, может быть мужским, в то время как сама личность может осознавать себя женщиной (трансгендерный переход)[5] — это может выражаться в одежде, причёске и даже пластических операциях, направленных на изменение своей внешности.

---

[1] Лебедева А.К. Судебно-экспертное исследование обликовых характеристик личности по фонограммам речи: правовые и методические аспекты: дис. … канд. юрид. наук: 12.00.12. М., 2017. С. 31.

[2] Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В. В. Виноградова. – 4-е изд., доп. – М.: ООО «ИТИ Технология», 2003. С. 430.

[3] Жулинский Б.В. Об использовании признаков письменной речи и почерка для установления автора анонимного текста // Криминалистика и судебная экспертиза. Респ. межд. Сборник. Выпуск 8. Киев: Изд. МВД УССР, 1971. С. 169.

[4] Бирюкова Е.О. Индивидуальный речевой портрет говорящего в телевизионном дискурсе // Вестник Череповецкого государственного университета. 2011. № 3 (31). С. 29.

[5] Ватсон Д.Б., Сайдль Х. Эволюция взглядов на гендерную идентичность: расстройство или «Новая» норма? // Российский психиатрический журнал. 2017. № 5. С. 33–39.

Для того чтобы определить, что включает в себя понятие демографические характеристики личности в рассматриваемом нами аспекте на данном этапе необходимо проанализировать лексическое значение слова «демография», чтобы понять, какие из характеристик личности можно отнести к демографическим.

В наши дни дискутируется определение предмета демографии как науки, что порождает неоднозначность при раскрытии лексического значения самого слова «демография». Понятие «демография» трактуется по-разному в зависимости от сферы его социального назначения. Так, например, в Экономическом словаре даётся следующее определение: *«ДЕМОГРАФИЯ (от греч. demos — народ и grapho — пишу) наука о народонаселении, изучающая изменение численности населения, рождаемость и смертность, миграцию, половозрастную структуру, национальный состав, географическое распределение и их зависимость от социально-экономических, исторических и других факторов»*[1]. В приведённом определении демография не затрагивает такие аспекты, как этническая и профессиональная принадлежность.

Большой толковый словарь по культурологии даёт несколько иное определение данному понятию: «*Демография — наука о народонаселении, его структуре (половозрастной, профессиональной, региональной, этнической) и динамике (рождаемость, смертность, миграции и т.д.)*»[2].

Если рассматривать лексическое значение слова «демография» с медицинской точки зрения, то, например, в Большом энциклопедическом словаре медицинских терминов встречается следующее определение: «*ДЕМОГРАФИЯ (demography) — изучение состава населения на национальной, региональной или локальной основе в соответствии с возрастом, полом, а также другими показателями, в том числе миграции и выживаемости. Эти данные используются в общественном здравоохранении для выявления специфических нужд и факторов риска в каждой отдельной области»*[3]. Как видно из приведённого определения, в медицинской сфере демография раскрывается с точки зрения того, какая часть населения является здоровой, а какая часть подвержена различным заболеваниям, каковы причины смертности народонаселения.

Отметим, что «С точки зрения теории следообразований речевой след – это информация, запечатлённая при помощи языка и посредством речевой деятельности в слове»[4]. Таким образом, обобщив различные подходы к

---

[1] Современный экономический словарь / Б. А. Райзебрг, Л. Ш. Лозовский, Е. Б. Стародубцева. – 6-е изд., перераб. и доп. – М.: ИНФРА-М, 2017. С. 96.

[2]Кононенко Б.И. Большой толковый словарь по культурологии. URL: https://dic.academic.ru/dic.nsf/enc_culture/1504/ (дата обращения: 02.10.2024).

[3] Медицинский словарь. URL: https://dic.academic.ru/dic.nsf/medic/2046 (дата обращения: 02.10.2024).

[4] Галяшина Е. И. Речевые следы как объекты судебных экспертиз (в свете идей Р. С. Белкина) // Современное развитие криминалистики и судебной экспертизы как реализация идей Р.С. Белкина. Материалы Международной научно-практической конференции «К 95-летию со дня рождения ученого, педагога, публициста» (г. Москва, 22–23 ноября 2017 г.). М.: РГ-Пресс, 2018. С. 189.

определению понятия «демография», приходим к выводу, что лексическое значение данного слова неоднозначно, в зависимости от сферы применения этого понятия его значение может быть разным, с учётом возможностей установления демографических характеристик личности посредством автороведческого судебно-диагностического исследования письменных речевых следов приходим к выводу, что к ним можно отнести такие характеристики, как:

— пол;
— возрастная группа;
— этническая принадлежность;
— территориальная принадлежность;
— уровень образования и речевой культуры;
— род занятий (хобби);
— профессиональная принадлежность;
— социальный статус[1].

М.Б. Садыков

Перспективы применения искусственного интеллекта для противодействия киберпреступлениям

Аннотация. В статье рассматриваются возможности применения искусственного интеллекта в сфере правоохранительной деятельности, в частности противодействия киберпреступности.

Вместе с тем, технология искусственного интеллекта в контексте использования в правоохранительной деятельности несет в себе и риски по аналогии с обоюдоострым мечом. В этой связи приведены следующие риски: предвзятое принятие решений, проблемы конфиденциальности, чрезмерная зависимость от технологий, возможность неправильного толкования, уязвимые места в системе безопасности, вытеснение рабочих мест, подотчетность и прозрачность, возможность злоупотребления, подрыв доверия, а также правовые и этические последствия.

В заключение отмечается, что, несмотря на многообещающие перспективы применения ИИ в правоохранительной сфере, связанные с ним риски требуют тщательного рассмотрения, регулирования и надзора.

***Ключевые слова*:** искусственный интеллект; правоприменение; риски; возможности; этика; регулирование; правоприменение; предвзятость; технология; киберпреступность.

Искусственный интеллект (далее - ИИ) и робототехника стали доминирующей силой в современном мире, привлекающей нас потенциалом для решения глубоких социальных проблем. Растущее мастерство искусственного интеллекта

[1] Сааков Т.А. К вопросу о понятии демографических характеристик автора в судебной автороведческой экспертизе // Язык. Право. Общество. Сборник статей V Международной научно-практической конференции. Пенза: изд-во ПГУ, 2018. С. 99–102.

в автономном выявлении подозрительных действий позволяет говорить о наступлении новой эры «умной» полиции. В некоторых регионах технологии уже превосходят людей в выявлении подобных действий. В тех случаях, когда такие передовые методы работы полиции оказываются эффективными, правоохранительным органам стоит взять их на вооружение[1].

Интеграция ИИ и робототехники в правоохранительную деятельность сопряжена как с преимуществами, так и с проблемами, требующими тщательно продуманной стратегии и распределения ресурсов[2]. Цель данной статьи - рассмотреть возможности и риски использования ИИ в правоохранительной сфере.

Рассмотрим изначально *возможности искусственного интеллекта в контексте правоохранительной деятельности*.

Правоохранительная деятельность – это деятельность, основанная на информации. Информация собирается, обрабатывается и используется для предотвращения или пресечения преступлений[3]. Для эффективной работы правоохранительных органов необходимо большое количество информации, или данных, о поведении людей, собранных из различных источников. В этой связи ИИ и робототехника вполне способны трансформировать правоохранительные органы, повысив эффективность сбора, анализа и обработки информации.

Можно даже предположить, что с увеличением числа датчиков и ростом объема больших данных правоохранительные органы уже в ближайшем будущем начнут в значительной степени полагаться на ИИ и робототехнику в борьбе с преступностью. Так, власти Китая усилили борьбу с преступлениями в сфере Web3 и искусственного интеллекта (ИИ) в связи с резким ростом числа правонарушений в этих двух секторах[4]. Расследование экономических и кибер-инцидентов уже сейчас сопряжено обработкой больших данных. В связи с чем, сотрудникам уже без помощи цифровых помощников сложно собрать и проанализировать все необходимые доказательства, особенно криптоактивы. А обработка ИИ электромагнитных волн Wi-FI роутера позволяет заглянуть в жилое помещение практически не оставляя следов.

Как именно ИИ и робототехника могут помочь правоохранителям в будущем для борьбы с киберпреступностью?

---

[1] Rademacher, T. (2020) Artificial intelligence and law enforcement. *Regulating artificial intelligence*. pp. 225–254.

[2]Artificial intelligence and robotics for law enforcement. (2019) *Interpol*: Unicri, Lyon: Turin. [Electronic resource] URL: https://www.europarl.europa.eu/cmsdata/196207/UNICRI%20-%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf (Access date: 08.10.2023).

[3] Гундаров А.В., Колесова Т.С., Максименко А.В. Международный опыт организации информационно-аналитической деятельности в правоохранительной системе // ЮП. 2017. № 1 (80). URL: https://cyberleninka.ru/article/n/mezhdunarodnyy-opyt-organizatsii-informatsionno-analiticheskoy-deyatelnosti-v-pravoohranitelnoy-sisteme (дата обращения: 09.10.2023).

[4] Chinese law enforcement ramps up monitoring of Web3, AI crimes. *Coingeek*: [Electronic resource] URL: https://coingeek.com/chinese-law-enforcement-ramps-up-monitoring-of-web3-ai-crimes/ (Access date: 07.10.2023).

Обнаружение и предотвращение угроз: Программы на основе искусственного интеллекта способны спонтанно анализировать огромные объемы данных. Эти данные затем используются для выявления закономерностей, а также потенциальных угроз кибербезопасности и других аномалий. Используя машинное обучение, эта система может выявить все, что кажется подозрительным, и помочь предотвратить потенциальную утечку данных еще быстрее и точнее, чем когда-либо прежде.

ИИ способен просматривать журналы безопасности и данные о событиях с целью обнаружения тенденций и сомнительных практик, которые могут быть проигнорированы аналитиками.

Анализ поведения: ИИ способен понять обычные действия пользователей в сетях и системах и отметить любое отклонение от шаблонов, сигнализирующее о потенциальной недобросовестной деятельности. Такая тактика позволяет не только еще точнее распознавать возможные угрозы внутри организаций, но и, что самое главное, занимать еще более проактивную позицию, чтобы остановить неизвестные, незнакомые, невиданные ранее типы вторжений и атак.

ИИ может использовать автоматизацию для реагирования на киберугрозы, позволяя быстро устранять атаки без участия человека. Это может означать принятие контрмер, выделение неисправных платформ и принятие мер по активной нейтрализации и предотвращению будущих угроз.

Аналитика кибербезопасности: Продвинутая аналитика на основе искусственного интеллекта может обеспечить глубокое понимание состояния кибербезопасности; она позволяет организациям распознавать уязвимые места, оценивать риски и продвигать свою борьбу с киберугрозами.

Выявление мошенничества в финансовой сфере и электронной коммерции завершается внедрением алгоритмов ИИ. Эти алгоритмы тщательно изучают данные о транзакциях и выявляют любые аномалии, которые могут содержаться в этих данных. Благодаря этому снижается количество ложных срабатываний и повышается точность выявления мошенничества.

Системы с искусственным интеллектом могут анализировать такие каналы связи, как электронные письма, сообщения и другие, чтобы обнаружить атаки социальной инженерии и фишинга. Система с искусственным интеллектом может добиться этого путем определения URL-адресов, контента или поведения, характерного для отправителя.

Улучшенная идентификация: ИИ может усовершенствовать методы установления личности людей за счет применения поведенческого анализа, биометрического распознавания, а также автоматического обнаружения аномалий, что позволит подтверждать личность людей гораздо точнее и безопаснее.

ИИ способен анализировать огромные объемы информации об угрозах из многочисленных источников. Это позволяет получить полезные сведения об угрозах, стратегиях и зарождающейся вялости, чтобы общество могло более эффективно противостоять киберугрозам.

Постоянно растущее использование киберпреступниками ИИ и стратегий машинного обучения усложняет необходимость уделять больше внимания разработке технологий ИИ для защиты от атак противника, которые обходят традиционную сетевую безопасность.

Защита конфиденциальности: Использование технологий ИИ, таких как дифференциальная конфиденциальность, позволяет защитить конфиденциальные данные путем деидентификации и объединения данных, сохраняя их суть для проведения анализа, что снижает риск утечки информации и раскрытия данных.

Непрерывное обучение: Ключевая черта, отличающая ИИ от традиционного ПО для обеспечения безопасности. Эти системы способны непрерывно учиться и совершенствоваться с течением времени. По мере того как они сталкиваются с новыми угрозами и анализируют прошлые инциденты, они становятся искусными в выявлении и смягчении последствий будущих атак.

Помощь в расследовании преступлений с помощью алгоритмов искусственного интеллекта

Использование алгоритмов искусственного интеллекта открывает широкие возможности для совершенствования рабочих процессов в правоохранительных органах. Используя передовые методы анализа данных и распознавания образов, эти алгоритмы помогают правоохранительным органам более эффективно и оперативно раскрывать преступления. Одной из ключевых областей, где алгоритмы искусственного интеллекта могут существенно повысить эффективность расследований, является анализ больших объемов цифровых доказательств. В связи с широким распространением цифровых устройств и онлайн-активности следователи часто сталкиваются с трудной задачей просеивания огромного количества данных. Алгоритмы искусственного интеллекта позволяют быстро обрабатывать и анализировать эти данные, выявляя ключевые закономерности и связи, которые в противном случае могли бы остаться незамеченными. Это не только экономит время следователей, но и повышает шансы на своевременное обнаружение важных улик. Кроме того, автоматизируя некоторые аспекты процесса расследования, алгоритмы искусственного интеллекта позволяют уменьшить количество человеческих ошибок и предвзятости, что ведет к более точному и объективному расследованию[1].

Ярким примером использования искусственного интеллекта в своей работе является полиция Эмирата Дубай. В структуре полиции есть специальное подразделение по искусственному интеллекту (General Department of Artificial Intelligence). В апреле 2022 года Исса Ибрагим Басаид, глава отдела приложений искусственного интеллекта и новых технологий в данном подразделении

[1] The Role of Artificial Intelligence in Law Enforcement. *LinkedIn* [Electronic resource]. URL: www.linkedin.com/pulse/role-artificial-intelligence-law-enforcement-chris-chiancone/?trk=article-ssr-frontend-pulse_more-articles_related-content-card (Access date: 09.10.2023).

полиции Дубая, включен в число 30 ведущих арабских экспертов региона в области ИИ по версии MIT Technology Review Arabia[1].

Вместе с тем, технология искусственного интеллекта в контексте использования в правоохранительной деятельности несет в себе и риски по аналогии с обоюдоострым мечом. Рассмотрим ***риски использования искусственного интеллекта в контексте использования в правоохранительной деятельности***.

Непредвзятое принятие решений: Системы искусственного интеллекта беспристрастны лишь настолько, насколько объективны данные, на которых они обучаются. Если исторические данные содержат предубеждения (ошибки), то ИИ может закрепить или даже усугубить эти предубеждения, что приведет к несправедливому отношению к определенным группам или лицам.

Проблемы конфиденциальности: Способность ИИ постоянно отслеживать, анализировать и хранить огромные объемы данных может нарушать права человека на неприкосновенность частной жизни. Например, технологии распознавания лиц могут использоваться без согласия, что приводит к необоснованной слежке.

Чрезмерная зависимость от технологий: слишком сильная зависимость от ИИ может привести к снижению значимости человеческой интуиции, суждений и контроля. Машины, несмотря на свои возможности, не обладают такими моральными принципами и пониманием контекста, как люди.

Возможность неправильного толкования: без надлежащего обучения или понимания функций ИИ сотрудники могут неверно интерпретировать его результаты, что может привести к неправильным или несправедливым действиям.

Уязвимые места в системе безопасности: как и любая другая технология, системы искусственного интеллекта могут быть взломаны или дестабилизированы. В связи с этим возникает проблема целостности данных и возможность подачи в систему ложной информации для введения правоохранительных органов в заблуждение.

Вытеснение рабочих мест: По мере того как ИИ берет на себя выполнение некоторых рутинных задач, приведет к сокращению рабочих мест в правоохранительных органах, что может привести к снижению уровня контроля и взаимодействия с людьми. Карта будущих профессий постоянно прогрессирует и пока не затрагивает творческие профессии. Но надолго ли?

Подотчетность и прозрачность: Процесс принятия решений ИИ, особенно в сложных алгоритмах, может быть трудно интерпретируемым. Такой "черный ящик" затрудняет привлечение системы к ответственности за свои решения или их оспаривание. Для ИИ интеллекта не составляет труда быстро просчитать входящие и выходящие сигналы, описать происходящий в черном ящике процесс

[1] Садыков М.Б. Внедрение автономных систем в Объединенных Арабских Эмиратах на примере полиции Дубая: правовые и технические аспекты // Технологии XXI века в юриспруденции. 2022. С. 162–173.

системой математических уравнений, что уже применяется некоторыми программами криптовалют для «взлома криптомикшеров».

Возможность злоупотребления: В неумелых руках возможности ИИ могут быть использованы не по назначению. Например, авторитарные режимы могут использовать слежку с помощью ИИ для подавления инакомыслия или преследования политических противников.

Подрыв доверия: если общественность почувствует, что ИИ в правоохранительных органах используется неправомерно или несправедливо, это может подорвать доверие к полиции и системе правосудия в целом.

Правовые и этические последствия: Использование ИИ может поставить под сомнение существующие правовые основы. В качестве примера можно привести вопросы о согласии, правах при проведении автоматизированных допросов и обоснованности доказательств, полученных с помощью ИИ, в суде.

Также важно углублять понимание и готовиться к риску злонамеренного использования ИИ преступными и террористическими группами, включая новые цифровые, физические, и политические атаки, особенно с использованием вычислительных возможностей квантовых компьютеров. Возможные варианты использования ИИ в злонамеренных целях включают кибератаки с использованием ИИ, распространение фальшивых новостей, а также инструменты для подмены лиц и подмены информации, которые манипулируют видео и ставят под угрозу доверие к ИИ, манипулируют видеозаписями и ставят под угрозу доверие к политическим деятелям или ставят под сомнение. Подмена лиц и голоса в видеороликах ставят под сомнение доверие к политическим деятелям или достоверность представленных в суде цифровых EXIF доказательств.

Согласно исследованиям V. Chiao, в последние годы учеными-правоведами написано много трудов, посвященных этическим последствиям использования искусственного интеллекта, машинного обучения, больших данных и прогностического программного обеспечения в контексте уголовного правосудия. Безусловно, предлагаемые технологии ИИ в области правоохранительной деятельности и правосудия существенно отличаются друг от друга. Однако, есть у них и общее: в итоге, все они предлагают предпринять те или иные меры (применение силы, определение меры пресечения, приговор суда и т.д.) через алгоритмическую обработку большого количества данных. В существующем подходе должностные лица принимают решения в соответствии с внутренним убеждением, где есть место морали, этике, праву. В этом и кроется его отличие от алгоритмического принятия решений.

V. Chiao предлагает их разделить на 3 группы: на вопросы справедливости, подотчетности и прозрачности[1]. Во-первых, если технология берет за основу массив информации, которые возможно уже в своем «сыром» виде предвзяты, то можем ли мы довериться такому ИИ? Во-вторых, кто будет нести ответственность за негативные последствия использования ИИ? В отличие от

[1] Chiao, V. (2019) Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice. *International Journal of Law in Context*, vol. 15, no. 2, pp. 126–139.

судей, присяжных, работников правоохранительных органов и т.д., спор с алгоритмом может показаться настолько же успешным, как спор со своим холодильником или тостером. Наконец, насколько для нас критично, что мы не знаем, как работает алгоритм, и, соответственно, что означает для нас незнание логики того, как ИИ пришел к тому или иному решению?

Несмотря на многообещающие перспективы применения ИИ в правоохранительной сфере, связанные с ним риски требуют тщательного рассмотрения, регулирования и надзора. Особенно с позиции норм права, которые сильно отстают от генерируемых возможностей ИИ. Баланс между потенциальными преимуществами и сопутствующими проблемами необходим для того, чтобы ИИ служил общественному благу, поддерживая принципы правосудия и справедливости, не нарушая права граждан.

А.Ж. Саркисян
Г.Ф. Коимшиди

IT-преступность в субъектах Российской Федерации по состоянию на 1 сентября 2024 г.

Аннотация. В статье представлены количество зарегистрированных IT-преступлений в Российской Федерации за 2019–2024 гг. Проведен ранжир значений криминальной нагрузки количества зарегистрированных IT-преступлений по субъектам Российской Федерации. Выявлено, какие субъекты Российской Федерации входят с криминальной нагрузкой выше среднего, среднего и ниже среднего.

***Ключевые слова*:** IT-преступления, криминальная нагрузка, децильный коэффициент.

По состоянию на 1 сентября 2024 г. в Российской Федерации за предыдущие 12 мес. было зарегистрировано 747 353 IT-преступлений (рис. 1). Это всего 38,5 % от всех зарегистрированных за этот период преступлений (1 915 780) в стране.

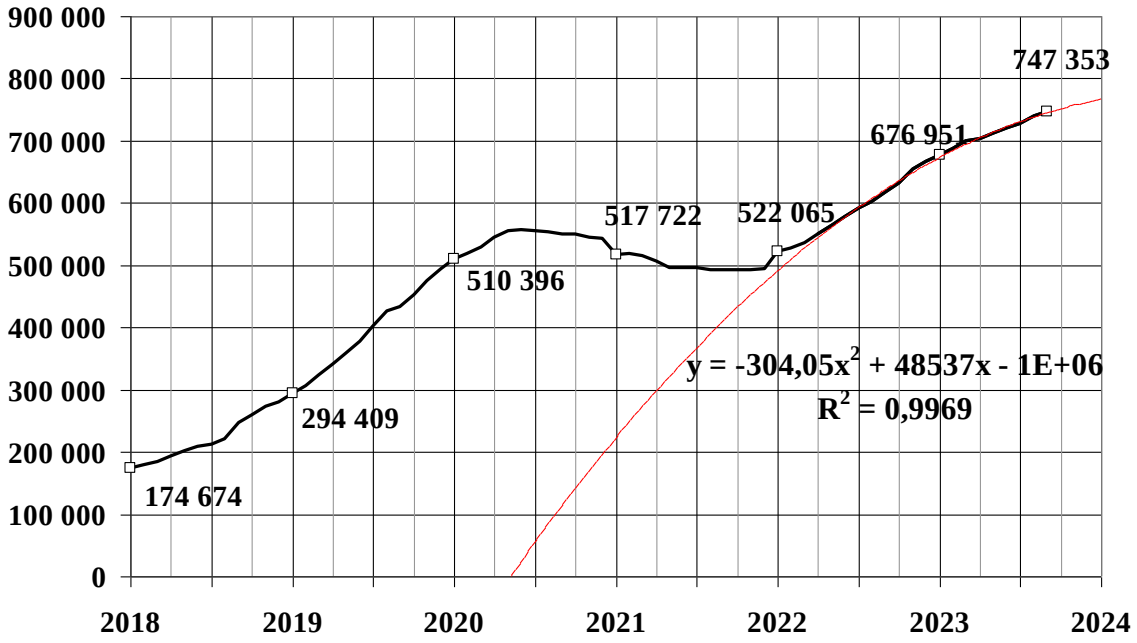


Рис. 1. Динамика количества зарегистрированных IT-преступлений в Российской Федерации. 2019–2024 гг.

По сравнению с 2023 г. (676 951) IT-преступность заметно увеличилась на 10,4 % (или на 70 402 преступления). А за шесть лет (с 2018 г. – 174 674 IT-преступлений) увеличилась более чем в четыре раза (4,3).

С апреля 2023 г. в динамике исследуемой преступности наблюдается параболический рост: ежемесячный прирост преступности увеличивается на 608,1 преступлений Надежность модели весьма высокая 99,7 %. Модель указывает на незначительное превалирование антикриминогенных факторов.

Почти каждое третье (32,6 %) IT-преступление зарегистрировано в одном из восьми субъектов Российской Федерации: каждое двенадцатое такое преступление (8,5 %) зарегистрировано в Москве; в республике Татарстан 4,6 %, в Красноярском крае – 4,5 %, в Санкт-Петербурге – 4,0 %, в Челябинской области – 3,1 %, в республике Башкортостан – 3,0 %, в Ростовской и Московской областях – по 2,5 %.

По состоянию на 1 сентября 2024 г. уровень IT-преступности (количество зарегистрированных за прошедшие 12 мес. IT-преступлений на 100 тыс. всего населения) увеличился по сравнению с аналогичным периодом прошлого года (АППГ) на 21,4 % или на 90,2 пункта и составил 511,7 преступлений на 100 тыс. населения страны (421,5 в АППГ).

Размах криминальной нагрузки на населения от IT-преступлений 124,5: от 19,2 в Чеченской республике до 1109,2 в Ненецком автономном округе. Средний уровень исследуемой преступности в субъектах Российской Федерации 504,5 IT-преступлений направленности на 100 тыс. населения. Стандартное (среднее) отклонение – 173,8.

В пятнадцати регионах страны с наибольшими значениями криминальной нагрузки от этих преступлений проживает 10 % населения страны (табл. 1).

Табл. 1

Субъекты Российской Федерации с наибольшими значениями криминальной нагрузки на населения *(проживает 10 % населения страны)*, 01.09.2024

Субъекты РФ	**Уровень**	**Субъекты РФ**	**Уровень**
Ненецкий АО	1109,2	Мурманская область	824,1
Новгородская область	953,7	Республика Коми	816,9
Республика Карелия	920,8	Республика Удмуртия	808,1
Кировская область	872,6	Псковская область	734,3
Томская область	855,0	Чукотский АО	719,5
Республика Татарстан	852,3	Алтайский край	712,6
Республика Марий Эл	841,1	Пермский край	711,9
Архангельская область	840,3	**Средняя нагрузка**	**825,4**

Криминальная нагрузки на население в группе от IT-преступности находится в интервале от 711,9 в Пермском крае до 1109,2 в Ненецком автономном округе. Средняя нагрузка в этой группе 824,4.

В пяти регионах страны с наименьшими значениями криминальной нагрузки и проживает 10 % населения страны: в Рязанской области (268,2), в Московской области (215,7), в республике Ингушетия (70,6), в республике Дагестан (53,96) и в Чеченской республике (19,2). Средняя нагрузка 157,0.

Соотношение этих средних – **децильный коэффициент**, характеризующий вариабельность субъектов Российской Федерации по криминальной нагрузке на население от IT-преступности – 5,3 нормальный.

Анализ субъектов Российской Федерации на статистическую однородность по уровню IT-преступности показал: в Ненецком автономном округе значения криминальной нагрузки на население от IT-преступлений настолько превышает средний показатель по всем регионам, что он нарушает статистическую однородность всей совокупности субъектов Российской Федерации по исследуемому.

Остальные (84) субъекта Российской Федерации по уровню IT-преступности составляют статистически однородную группу. Средняя криминальная нагрузка в группе 504,3 IT-преступлений на 100 тыс. населения; стандартное (среднее) отклонение 157,0

Типология субъектов Российской Федерации по криминальной нагрузке на население.

В **группе V (с высокой криминальной нагрузкой – больше среднего на два стандартных отклонения)** шесть субъектов Российской Федерации: Новгородская область (953,7 преступлений на 100 тыс. жителей области), республика Карелия (920,8), Кировская область (872,6), Томская область (855,0), республика Татарстан (852,3), республика Мари Эл (841,1) и Архангельская область (840,3). Средняя нагрузка 863,7. В группе проживает 8 874 532 жителя или 6,05 % всего населения страны.

В **группе IV (с криминальной нагрузкой выше среднего – больше среднего на одно стандартное отклонение)** одиннадцать субъектов Российской Федерации (табл. 2).

Табл. 2

Субъекты Российской Федерации, входящие в группу IV
(*с криминальной нагрузкой выше среднего*), 01.09.2024

Субъекты РФ	**Уровень**	**Субъекты РФ**	**Уровень**
Мурманская область	824,1	Пермский край	711,9
Республика Коми	816,9	Тверская область	704,1
Республика Удмуртия	808,1	Ямало-Ненецкий АО	690,6
Псковская область	734,3	Республика Мордовия	687,7
Чукотский АО	719,5	Челябинская область	687,6
Алтайский край	712,6	**Среднее значение**	724,9

Криминальная нагрузка в группе от 687,6 в Челябинской области до 824,1 в Мурманской области. Средняя нагрузка 724,9. В группе проживает 13 925 065 жителей или 9,49 % всего населения страны.

В **группе III (со средней криминальной нагрузкой – отличается от среднего не более чем на одно стандартное отклонение)** пятьдесят шесть субъектов Российской Федерации (табл. 3).

Криминальная нагрузка в группе от 379,0 в Ульяновской области до 669,1 в Костромской области. Средняя криминальная нагрузка 501,0. В группе проживает 104 523 568 жителей или 71,26 % всего населения страны.

В **группе II (с криминальной нагрузкой ниже среднего – меньше среднего на одно стандартное отклонение, но не более чем на два)** шесть субъектов Российской Федерации (табл. 4).

Криминальная нагрузка в группе от 379,0 в Ульяновской области до 669,1 в Костромской области. Средняя криминальная нагрузка 501,0. В группе проживает 104 523 568 жителей или 71,26 % всего населения страны.

В группе II (с криминальной нагрузкой ниже среднего – меньше среднего на одно стандартное отклонение, но не более чем на два) шесть субъектов Российской Федерации (табл. 4).

Криминальная нагрузка в группе от 268,2 в Рязанской области до 356,7 в республике Адыгея. Средняя криминальная нагрузка 151,0. В группе проживает 5 431 288 жителей или 3,70 % всего населения страны.

Табл. 3

Субъекты Российской Федерации, входящие в группу III
(*со средней криминальной нагрузкой*), 01.09.2024

Субъекты РФ	**Уровень**	**Субъекты РФ**	**Уровень**
Костромская область	669,1	Новосибирская область	521,3
Еврейская автономная область	661,6	Владимирская область	519,5
Курганская область	655,0	Пензенская область	514,8
Амурская область	648,4	Республика Крым	492,6
Сахалинская область	644,6	Москва	480,4
Красноярский край	636,9	Орловская область	474,8
Смоленская область	618,1	Республика Алтай	471,1
Камчатский край	615,3	Липецкая область	468,2
Магаданская область	613,4	Севастополь	455,2
Тюменская область	611,7	Ростовская область	449,8
Республика Хакасия	609,4	Нижегородская область	448,7
Хабаровский край	594,9	Иркутская область	448,4
Тамбовская область	592,0	Ивановская область	443,6
Забайкальский край	584,9	Саратовская область	443,5
Краснодарский край	576,2	Ленинградская область	440,8
Ханты-Мансийский АО	575,8	Карачаево-Черкесская республика	435,8
Республика Бурятия	571,3	Калужская область	433,1
Республика Башкортостан	553,7	Калининградская область	430,8
Волгоградская область	550,0	Воронежская область	426,5
Ярославская область	545,8	Астраханская область	419,1
Омская область	541,8	Оренбургская область	412,9
Курская область	539,0	Ставропольский край	406,8
Республика Северная Осетия Алания	536,4	Республика Калмыкия	404,2
Санкт-Петербург	535,6	Вологодская область	399,6
Приморский край	535,1	Свердловская область	386,4
Кемеровская область	534,3	Республика Саха (Якутия)	380,7
Чувашская республика	526,4	Белгородская область	380,6
Самарская область	522,8	Ульяновская область	379,0
		Среднее значение	**501,0**

Табл. 4

Субъекты Российской Федерации, входящие в группу II
(с криминальной нагрузкой ниже среднего), 01.09.2024

Субъекты РФ	**Уровень**	**Субъекты РФ**	**Уровень**
Республика Адыгея	356,7	Кабардино-Балкарская республика	297,3
Брянская область	352,5	Республика Тыва	276,9
Тульская область	348,1	Рязанская область	268,2
		Среднее значение	151,0

Группа I (с низкой криминальной нагрузкой – меньше среднего на два стандартных отклонения, но не более чем на три) четыре субъекта Российской Федерации: Московская область (215,7) и три республики Северного Кавказа – Ингушетия (70,6), Дагестан (53,9) и Чеченская республика (19,2). Средняя криминальная нагрузка 151,0. В группе проживает 13 922 298 жителей или 9,49 % всего населения страны.

Е.Н. Сиделёва

Судебная экономическая экспертиза в условиях информатизации и цифровизации современного общества

Аннотация. В статье рассматриваются особенности судебно-экспертного исследования экономических операций, находящихся в цифровой среде. На основании анализа следственно-судебной и экспертной практики автор обосновано приходит к выводу, что необходимо усовершенствовать законодательство и техническую базу для проведения экономических экспертиз в отношении экономических объектов из цифровой среды.

Ключевые слова: судебная экономическая экспертиза, расследование преступлений, экономические операции, цифровые следы.

В связи внедрением инновационных процессов в сферу судебно-экспертной деятельности необходима разработка и внедрение новых подходов к проведению экспертиз. Возросла необходимость обеспечения безопасности данных, ставших вещественными доказательствами в рамках расследования уголовных дел[1]. Все это подчеркивает необходимость качественной трансформации методов экспертизы, обновление материально-технической базы и повышение объема специальных знаний экспертов.

В условиях стремительно меняющейся мировой экономики и не менее быстрого развития высоких технологий, экономические преступления

[1] Неретина Н.С. Роль инновационных технологий в развитии судебной экспертологии // Вестник экономической безопасности. 2022. № 1. С. 147–150.

становятся все более сложными и масштабными. Кражи, мошенничество, вымогательство, коррупция, отмывание денег, финансовые пирамиды – это лишь малая часть широкого спектра преступлений, направленных на материальное обогащение преступника, которые сегодня активно развиваются и оказывают разрушительное влияние на экономическую стабильность и благополучие общества.

Овладев современными инструментами и методами в сфере информационных технологий, злоумышленники постоянно приспосабливаются к меняющимся условиям, от чего борьба с ними становится особенно сложной для правоохранительных органов и государства в целом. Экономические преступления имеют серьезные негативные последствия: они вызывают значительные финансовые потери граждан и организаций, подрывают доверие к системе бизнеса и государственных структур, а также создают непосильные трудности для экономического развития страны.

По данным Министерства внутренних дел Российской Федерации, в 2023 году каждое третье преступление совершалось с использованием высоких технологий. По состоянию на период январь-май 2024 года преступлений, совершенных с использованием информационно-телекоммуникационных технологий зарегистрировано на 16,5% больше по сравнению с январем-маем 2023 года.[1] Это говорит о том, что вместе с бесспорными преимуществами, которые принесла с собой цифровизация всех сфер нашей жизни, возникают и новые угрозы, связанные с правомерностью использования информации.

Эпоха стремительного развития цифровизации современного общества и активного распространения информационных взаимодействий среди субъектов экономико-правового пространства привела к тому, что традиционный вектор развития института судебной экспертизы стал неэффективным. В современном мире, где цифровизация охватывает все сферы жизни, возникли новые требования к объектам исследования и к судебным экспертизам в целом.

Исследование эксперта — уникальный процесс, в котором проявляются достижения различных наук, владение современными высокоэффективными методами исследования, специальные знания эксперта, его личный опыт.

Современные реалии требуют не только новых подходов к экспертизам, но и пересмотра методов их проведения к возможности применения инновационных технологий, что обосновывает необходимость качественной трансформации методов проведения экспертиз. Это, требует расширения набора базовых инструментов, используемых в рамках экспертного исследования, традиционные методы, такие как анализ и обработка документов теперь должны сочетаться с высокими технологиями, такими как анализ больших объемов данных с электронных носителей. Современные эксперты должны обладать не только профильным образованием, но и навыками работы с информационными базами данных, новейшими технологиями и были готовы к постоянному обучению и усовершенствованию своих навыков. Это позволит не только повысить качество

[1] Официальный сайт МВД России.URL: https://мвд.рф/reports/item/55225633/ (дата обращения: 20.06.2024).

проводимых экспертиз, но и обеспечить более эффективное расследование преступлений, что, в конечном итоге, будет способствовать повышению уровня правопорядка и безопасности в обществе.

Судебно-экономическая экспертиза является важным источником доказывания в звене судебной системы. Как самостоятельный источник доказательств в судебно-экономической экспертизе используются знания средств научного экономического анализа исходных данных, содержащихся в материалах, приобщенных к делу.

Судебно-экономическая экспертиза ставит перед собой задачу определения средствами экономического анализа признаков нарушения ведения финансово-хозяйственной деятельности и установление причиненного преступлением (правонарушением) ущерба. Это налагает соответствующие обязательства на эксперта-экономиста в выборе методов и методики исследования объектов.

Методами судебно-экономических экспертиз является совокупность приемов, используемых экспертом-экономистом при исследовании документов бухгалтерского и налогового учета, банковского кредитования и финансового анализа, управленческого учета, записей счетных регистров в совокупности с документами гражданско-правового характера и другими материалами дела, а также даче заключения по поставленным перед ним вопросам, входящим в его компетенцию.

Существенным признаком судебно-экономической экспертизы является методика экспертного исследования. Под методикой экспертизы принято понимать систему научно-обоснованных методов, приемов и технических средств, упорядоченных и целенаправленных для установления фактов, решения задач, относящихся к предмету экономической экспертизы и формирования обоснованных выводов.

В методиках судебно-экономической экспертизы методы структурированы, систематизированы и направлены на решение конкретных вопросов, входящих в предмет экспертизы. При научной разработке методик судебных экономических экспертиз учитывается специфика исследуемых объектов, характер извлекаемой из вещественных доказательств и других объектов информации.

Актуальность развития и совершенствования методов исследования судебной экономической экспертизы в условиях информатизации и цифровизации современного общества подтверждается постоянным применением общенаучных и частных судебно-экспертных теорий и учений, которые активно обсуждаются в научных кругах. В последние годы наблюдается развитие следующих ключевых направлений:

1. **Интеграция новых технологий**, включающих создание автоматизированных функциональных инструментов, повышающих эффективность и оптимизирующих работу эксперта, введение цифровых инструментов и методов анализа, а также разработку и адаптацию программных продуктов на основе Web-сервисов.

Интеграция новых технологий в судебно-экспертную деятельность значительно расширяет её возможности и повышает эффективность ключевых

направлений. Экспертам в области экономики необходимо постоянно совершенствовать и пополнять свой научно-технический арсенал, изучать современные и разрабатывать новые программные инструменты. Внедрение новых технологий качественно изменит судебно-экспертную деятельность и откроет большой потенциал для ее дальнейшего развития. Это, в свою очередь, не только расширит возможности, но и повысит достоверность и доказательственное значение заключений экспертов.

2. **Междисциплинарный подход**. Современные исследования всё чаще включают элементы из различных областей знаний, таких как криминалистика, IT- технологии, лингвистика и прочих.

Междисциплинарный подход в расследовании уголовных дел экономической направленности является ключевым для обеспечения точности и объективности результатов. Для полноты соответствия действий субъектов правовым нормам следствием дается правовая оценка выявленных нарушений. Экономическая экспертиза включает изучение материалов уголовного дела, анализ и исследование бухгалтерской и налоговой отчетности, кадровых документов, иных данных, относящихся к финансово-хозяйственной деятельности организации. На ряду с экономической экспертизой может проводится компьютерно-техническая экспертиза, экспертиза документов, почерковедческая, лингвистическая, строительно-техническая и другие.

Междисциплинарный подход позволяет объединить знания и методы из различных областей для более комплексного и точного анализа экономических преступлений.

3. **Повышение стандартов качества** в судебно-экспертной деятельности является важным критерием для обеспечения точности, надёжности и объективности экспертиз.

Процесс стандартизации в судебно-экспертной деятельности начался с выработки и принятия единых определений для применяемых в судебной экспертизе терминов, что представляет собой необходимую основу для осуществления эффективной деятельности по разработке единого научно-методического подхода в судебно-экспертной деятельности на основе внедрения единых механизмов валидации экспертных методик, аккредитации судебно-экспертных учреждений. Необходимым условием принятия в рамках проводимой стандартизации судебно-экспертной деятельности, наличие консенсуса представителей различных ведомств, определяющих путь внедрения единого научно-методического подхода в судебно-экспертную деятельность.

- Введение единых стандартов для проведения экспертиз экономической направленности помогает обеспечить прозрачность и сопоставимость результатов. Это включает разработку и применение национальных и международных стандартов.
- Обязательная аккредитация экспертных учреждений позволяет подтвердить их соответствие установленным стандартам качества. И включает в себя проверку компетентности экспертов-экономистов, соблюдение методик и процедур, а также наличие необходимого оборудования.

- Регулярное обучение и повышение квалификации экспертов экономической направленности способствует поддержанию высокого уровня профессионализма и актуальности знаний.
- Введение систем контроля качества, таких как внутренние и внешние аудиты, помогает выявлять и устранять недостатки в работе экспертных организаций.
- Ведение подробной документации и отчетности по проведённым экспертизам обеспечивает возможность проверки и повторного анализа результатов.

Эти меры способствуют повышению доверия к результатам судебных экспертиз экономической направленности и обеспечивают их использование в правоприменительной практике.

4. **Развитие частных теорий,** которые играют инновационную роль в решении задач, встающих в условиях информатизации и цифровизации современного общества.

Процесс формирования частных теорий новых родов и видов судебных экспертиз проходит те же этапы, что и развитие общей теории судебной экспертологии. На первом этапе происходит накопление эмпирического материала, отбор и заимствование из базовой науки методов и методик, которые могут быть использованы в производстве судебных экспертиз нового рода (вида). Этому, как правило, соответствует процесс дифференциации научного знания. На втором этапе конкретизируется, типизируются и систематизируются экспертные задачи, усиливается процесс интеграции научного знания при совершенствовании методов экспертного исследования и разработки экспертных методик. На третьем этапе происходит уточнение базовых понятий и создается целостная частная теория рода (вида) в общей системе судебных экспертиз. По такому сценарию в настоящее время происходит формирование частных теорий судебных в том числе экономических экспертиз.

Развитие частных теорий способствуют множество факторов:

1. Некоторые виды экспертиз, например экономическая экспертиза сталкиваются с нехваткой современных методик, что затрудняет проведение исследований.
2. Отсутствие стандартизации методов и процедур приводит к различиям в постановке вопросов и задач перед экспертом в результате проводит к применению разных методик и разным выводам, что вызывает сомнения в их объективности.
3. Для поддержание высокого уровня профессионализма экспертам экономической направленности необходимо постоянно повышать уровень знаний в области экономики и IT-технологий.
4. В связи со сложившейся мировой обстановкой и недостаточным материально-техническим обеспечением, могут увеличиваться сроки производства экспертиз.

Эти проблемы требуют комплексного подхода для их решения, включая совершенствование методик, стандартизацию процедур, повышения квалификации экспертов и улучшение материально-технической базы.

5. **Разработка единого подхода к методикам**[1] в работе как государственных, так и негосударственных экспертов. Так изучение ведомственных приказов, регламентирующих деятельность судебно-экспертных учреждений, позволяет делать вывод об отсутствии единообразия по ряду позиций: существуют различия как в делении судебных экспертиз на роды и виды, так и в наименованиях экспертиз, разрешающих одни и те же экспертные задачи, круга вопросов, решаемых экспертами одной специальности.

Федеральным законом от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (далее – ФЗ о ГСЭД) определяет правовую основу, принципы организации и основные направления государственной судебно-экспертной деятельности в нашей стране. В частности, в части шестой статьи 11 ФЗ о ГСЭД определено, что «государственные судебно-экспертные учреждения одного и того же профиля осуществляют деятельность по организации и производству судебной экспертизы на основе единого научно-методического подхода к экспертной практике, профессиональной подготовке и специализации экспертов»[2].

В научной литературе отмечается, что в судебно-экспертных учреждениях различных министерств и ведомств не редко используются несовпадающие методы и терминология проводимых исследований. В этой связи в направлении повышения качества судебных экспертиз актуальной становится задача систематизации, унификации и каталогизации стандартизированных методик по отдельным родам (видам) экспертных исследований в виде общероссийского электронного банка данных. Большое практическое значение имеет разработка национального Государственного стандарта, регулирующего научные методологические (понятийные), методические вопросы производства судебных экспертиз и оформления заключений судебных экспертов разных ведомств, а также обеспечение единства измерений, технической и информационной совместимости, сопоставимости результатов судебно-экспертных исследований; создания систем обеспечения качества экспертного производства.

Эти тенденции отражают стремление к повышению эффективности и точности судебно-экспертной деятельности, что, в свою очередь, способствует более справедливому и объективному правосудию.

Процесс развития и совершенствования методов исследования повышает точность и надёжность судебных экспертиз, сокращает сроки их проведения, повышает уровень работы и показателей не только отдельно взятого сотрудника СЭЦ СК России, но и всей организации в целом.

---

[1] См., например: Хаснутдинов Р.Р., Романова Е.А. Тенденции развития экспертной деятельности в РФ в условиях цифровизации // Международный журнал гуманитарных и естественных наук. 2020. №10-4. С. 121–125.

[2] Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».

Сотрудниками Судебно-экспертного центра Следственного комитета совместно с сотрудниками научно-исследовательского института (НИИ Криминалистики) Главного управления криминалистики Следственного комитета Российской Федерации по разработке научно-методических рекомендаций, написанию научных статей, разработку рабочих групп и участие в рабочих встречах.

- написаны и изданы методические рекомендации по производству налоговых экспертиз по ст. 199.1 УК РФ,
- разработаны и готовятся пройти научный совет методические рекомендации по производству оценочных экспертиз;
- в планах на 2025 год проведение аналитической работы по уголовным делам по ст. 199.1 УК РФ с целью выяснения раскрытия неуплаты налога на прибыль организаций и влияния наличия полноты документов на выводы эксперта, а также разработки методических рекомендаций.

Таким образом, можно с уверенностью утверждать, что актуальность развития и совершенствования методов исследования судебной экономической экспертизы в условиях информатизации и цифровизации современного общества очевидна, так как задача любого эксперта - гарантия достоверности и объективности заключения. В этом контексте применение и внедрение современных технологий в сферу экспертной деятельности значительно содействует достижению этих целей. Однако для повышения результативности и эффективности работы судебно-экспертных учреждений в расследовании преступлений важно не только обновить инструментарий и улучшить подготовку экспертов, но и оптимизировать нормативно-правовую базу России с учетом интеграции методик экспертной деятельности, принимая во внимание распространение электронных доказательств и средств их обработки.

С.Ю. Скобелин

Тактические особенности осмотра места совершения киберпреступлений

Аннотация. Анализируются тактические особенности подготовительного, рабочего и заключительного этапов осмотра места происшествия, связанного с использованием информационно-коммуникационных устройств. Даются общие рекомендации по определению границ такого места, последовательности действий следователя, специфики обнаружения, фиксации и изъятия цифровых следов преступлений.

Ключевые слова: Преступление, осмотр места происшествия, Интернет, гаджеты, информация, цифровые следы, фиксация.

Своевременное грамотное и правильно процессуально оформленное обнаружение, фиксация, изъятие и исследование цифровой информации на месте

происшествия по анализируемой категории уголовных дел в значительной мере способствует оперативному изобличению всех участников преступного события, розыску и задержанию последних, поиску других следов преступной деятельности и в целом обеспечению надежной и объективной доказательственной базы для органов следствия.

Местом происшествия по рассматриваемой категории преступлений выступают места использования цифровых устройств для совершения преступлений: выхода преступника в сеть «Интернет», совершения телефонных звонков, встреч преступника с жертвой (жилища, административные здания, служебные кабинеты, салоны транспортных средств, участки местности и др.)[1].

В целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для дела узловой точкой в осмотре места происшествия является рабочее место лица, совершающего преступные действия с использованием информационно-коммуникационных технологий. В зависимости от объекта преступных посягательств (конституционный строй, половая неприкосновенность личности, общественная безопасность или нравственность, собственность и т.д.) внимание следователя должно быть обращено не столько на само устройство (его сразу же необходимо перевести в авиарежим, исключив сетевую активность и возможность дистанционного блокирования), с помощью которого лицо устанавливал связь с жертвой или распространял запрещенный контент (его необходимо изъять и осмотреть отдельно), а на иные прямые или косвенные доказательства.

Это связано с трудностями идентификации конкретного лица, совершившего преступление с обнаруженного места и даже конкретного гаджета. Ведь обнаружение таких мест и устройств, даже если это место жительства (работы) или гаджет конкретного лица, далеко не всегда позволяет установить тот факт, что именно данное лицо совершало противоправные действия. В таких ситуациях на помощь следователю может прийти комплексный подход, использование всего арсенала криминалистичекого учения о следах преступной деятельности.

Внимательному изучению, фиксации и изъятию подлежат объекты, на которых преступник мог оставить свои биологические следы (ДНК, следы крови, спермы, волосы и др.), следы пальцев рук, обуви, транспортного средства, микроволокно, биллинговую информацию, данные видео камер и др.). Поэтому фиксации и изъятию могут подлежать не только компьютер, смартфон, роутер, иные цифровые устройства и внешние накопители, но и переферийное оборудование, такие как клавиатура, мышь, коврик, принтер, сканер, кресло, на котором сидел злоумышленник, данные видеокамер. Целесообразно делать смывы со стола за которым предположительно находился преступник, изъять объекты, вероятно находящиеся в непосредственном контакте с подозреваемым (посуда, остатки пищи, записные книжки, листы бумаги и пр.). Интерес представляет имеющаяся

[1]Цифровая криминалистика: учебник для вузов; под редакцией В.Б. Вехова, С.В. Зуева. – 2-е изд., перераб. и доп. – М.: Юрайт, 2024. 490 с.

на месте происшествия литература, визитные карточки, распечатанные тексты (в том числе черновики), одежда подозреваемого.

Безусловно, что подробной фото фиксации и описанию в протоколе подлежит сам компьютер, а также все подключенное периферийное оборудование, планшет, смартфон или иные гаджеты – средства коммуникации. В случае если компьютер выключен, включать его не рекомендуется, его марка, модель, возможно инвентаризационный номер указаны, как правило, на тыльной стороне моно или системного блока.

Если же компьютер включен, необходимо зафиксировать содержимое экрана, все прикрытые вкладки, историю браузера (программы просмотра содержимого сайтов) за последние сутки, а также открыть параметры (свойства) компьютера (системы) и отразить в протоколе конфигурацию операционной системы. Криминалистическое значение в последующем может иметь «Имя устройства», его MAC-адрес, характеристики фото-видео камер, данные процессора, код устройства и продукта, а также данные учетной записи и пароль для открытия самого компьютера. Последний (при наличии) целесообразно уточнить у пользователя, его работодателя, родственников, представителей охраны непосредственно в ходе следственного действия. Это, безусловно, относится и к смартфонам, простым кнопочным телефонам.

После этого фиксируются с помощью фото- видео-аппаратуры все сетевые подключения, описываются с помощью специалиста в протоколе. В случае большого количества кабелей, их рекомендуется нумеровать и маркировать цветными стикерами.

Следует обращать внимание на место нахождения и возможного сокрытия мобильных телефонов и, в особенности, извлекаемых из них накопителей (например, SIM-карт, micro SD), а также на поведение участников уголовного судопроизводства, пытающихся воспользоваться мобильным устройством для создания препятствий расследованию, либо удалить какую-либо информацию, блокировать устройство непосредственно или дистанционно.

Так, при осмотре места происшествия по данной категории уголовных дел (впрочем, как и в ходе обыска или выемки) следует изымать все компьютеры, планшеты, мобильные устройства, SIM-карты, micro SD находящиеся у подозреваемых для установления, в частности, последних их контактов, истории браузера, местонахождения в интересующее следователя время и других обстоятельств.

В виду специфики цифрового следообразования и возможности утраты цифровых следов осмотр в жилище проводят неотложно в соответствии с ч.5 ст. 165 УПК РФ без получения судебного решения на основании постановления следователя или дознавателя с последующим уведомлением судьи и прокурора о производстве следственного действия.

Сложности могут возникнуть в ходе осмотра в ситуациях, когда телефон (иной гаджет или внешний накопитель цифровой информации) находится при интересующем следствие лице, и он отказывается выдать его добровольно. В подобных случаях необходимо взаимодействовать с сотрудниками полиции,

которые вправе применить физическую силу для преодоления противодействия своим законным требованиям и наручники для пресечения сопротивления, оказываемого сотруднику полиции (п. 3 ч. 1 ст. 20, ст. 21 закона «О полиции»). Также стоит разъяснять таким лицам диспозицию и санкцию ст. 318 УК РФ – «Применение насилия в отношении представителя власти». Согласно ч. 4 ст. 166 УПК РФ факт применения, как физической силы, так и специальных средств должен быть отражен в протоколе следственного действия.

В соответствии с требованиями ст.164.1 УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий», электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации.

В данном случае следует учитывать два момента. Во-первых, в качестве специалиста в данном случае может приглашаться любое лицо обладающее познаниями в области электронных устройств (консультанты специализированных магазинов, программисты, сотрудники технических подразделений правоохранительных органов и др.), а, во-вторых, в ходе проведения данных следственных действий копировать информацию всё таки не желательно, так как это может повлечь ее утрату, либо спорные вопросы о консервации имеющейся информации на момент проведения следственного действия.

Следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия.

В протоколе должны быть указаны также технические средства, примененные при производстве следственного действия, условия и порядок их использования, объекты, к которым эти средства были применены, и полученные результаты, а также отмечено, что лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств.

При обнаружении мобильного телефона того или иного участника уголовного судопроизводства, алгоритм действий следователя должен быть следующим:

1. Зафиксировать в протоколе следственного действия и сфотографировать место расположения телефона.

2. Перевести телефон в авиарежим, исключив сетевую активность (возможное блокирование устройства) и выяснить не синхронизирован ли аппарат с компьютером и другими гаджетами пользователя.

При этом следует иметь в виду возможность и необходимость в последующем назначения по данному объекту молекулярно-генетической или одорологической экспертизы (при отказе собственника признавать принадлежность телефона, либо когда принадлежность установить невозможно), а соответственно перемещение его с использованием стерильных перчаток и упаковка в бумажный конверт;

3. Описать в протоколе и сфотографировать переднюю, заднюю панели телефона, его повреждения, информацию с экрана, все слоты, модель, IMEI и другие сведения о телефоне, а также все внешние источники (SIM-карты, карты памяти), батарею, чехол. Напомним, что модель и IMEI телефона (GSM) указаны у простых кнопочных телефонов под аккумулятором сверху, либо на задней крышке смартфона. Также IMEI на телефонах стандарта GSM можно определить путем набора следующей комбинации - *#06#. Информацию о модели, операционной системе телефона можно получить и зафиксировать с помощью фотоаппарата в памяти телефона (Меню – Настройки-Информация об устройстве).

4. Необходимо, прежде чем выключить телефон, просмотреть и зафиксировать в протоколе, а также с помощью фотоаппарата последние контакты.

5. Изъять телефон и комплектующие к нему (зарядное устройство, провода питания)

6. Выключить-включить телефон и убедиться отсутствует ли пароль на включение-активацию. В случае наличия пароля, ПИН-кода, постараться выяснить его у владельца и занести в протокол[1].

Изъятые в ходе следственного действия компьютеры, мобильные устройства, внешние накопители и другие объекты предъявляются понятым и другим лицам, присутствующим при следственном действии, фотографируются, упаковываются и опечатываются таким образом, чтобы исключить возможное внесение (удаление) в память какой-либо информации, любое подключение к устройству (в картонные коробки или полиэтиленовые мешки в выключенном состоянии).

[1]Цифровые следы преступлений: монография / Багмет А.М. и др. М.: Проспект, 2023. С. 43.

М.В. Соколова

Тактические особенности производства некоторых следственных действий при расследовании киберпреступлений

Аннотация. В статье рассматриваются особенности проведения таких следственных действий, как осмотр места происшествия, обыск и выемка, так как производство невербальных следственных действий по делам о киберпреступлениях основывается на грамотном изъятии электронных носителей информации, которые будут иметь доказательственное значение по уголовному делу. Особое внимание уделяется рекомендациям, необходимым для успешного проведения следственных действий как на стадии их подготовки, так и во время проведения.

Ключевые слова: осмотр места происшествия, обыск, выемка, информационно-телекоммуникационные технологии, киберпреступления, следственные действия.

Следственные действия, производимые по делам о киберпреступлениях, объединяет один главный признак – все они направлены на поиск и обнаружение информации, находящейся на электронном носителе. Несмотря на то, что идеальные следы преступления тоже имеют место быть по рассматриваемой категории преступления, они имеют скорее косвенное доказательственное значение по уголовному делу.

Изъятие электронных носителей информации может быть осуществлено в рамках осмотра места происшествия, обыска или выемки[1]. Для начала рассмотрим процессуальный аспект данного вопроса. Так, согласно ст. 164.1 УПК РФ изъятие электронных носителей информации не допускается, за исключением случаев, когда:

1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;

2) изъятие электронных носителей информации производится на основании судебного решения;

3) на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Несмотря на то, что УПК РФ дает четкий перечень оснований для изъятия электронных носителей информации само это понятие не раскрывается. Под материальными носителями информации понимается материальный носитель, используемый для записи, хранения и воспроизведения информации,

[1] Стурова Н.А. Некоторые особенности тактики производства следственных действий, направленных на получение доказательств в электронной форме // Криминалистика, оперативно-разыскная деятельность. 2019. № 2 (89). С. 226–231.

обрабатываемой с помощью средств вычислительной техники[1]. Как пишет В.Н. Григорьев и А.Н. Максимов, двойственность данного понятия порождает больше вопросов, нежели ответов, т.к., например, не ясно подходят ли под это описание электронно-вычислительные механизмы, непосредственно предназначенные для обработки этой информации[2]. В частности, современные сотовые телефоны типа смартфон являются как носителями информации, так и средством ее обработки, функция накапливания информации является неотъемлемой для данных гаджетов, а карта памяти представляет собой единое целое с системой телефона. Сегодня правоприменительная практика исходит из того, что электронным носителем информации может быть признан объект, у которого функция хранения электронной информации является основной и единственной. Т.е. это могут быть компакт-диски, дискеты, флэш-карты, дополнительные карты памяти сотового телефона и пр. Но при этом сразу стает закономерный вопрос, как быть с изъятием отдельных компонентов ЭВМ, функция которых исключительно хранить информацию. Например, если возникла необходимость в изъятии оперативной памяти персонального компьютера, ведь несмотря на то, что данное устройство является неотъемлемой части ПК, она может легко взаимозаменяться и использоваться отдельно как блок для хранения информации. Таким образом, для совершенствования методики расследования киберпреступлений, в первую очередь необходимо решить правовые пробелы, касающиеся порядка производства следственных действий по данной категории преступлений.

Производству любого следственного действия предшествуют подготовительные мероприятия, по делам о киберпреступлениях это определение круга участников следственного действия. Здесь опять следует обратиться к процессуальным требованиям, т.к. согласно ч. 2 ст. 164.1 УПК РФ электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. Так как в УПК РФ не конкретизируется профиль специалиста, привлекаемого к следственному действию, то с формальной стороны следователь может допустить участие и специалиста-криминалиста, но с точки зрения криминалистической значимости его содействие не будет иметь никакого смысла. Для того, чтобы носители были изъяты без ущерба для хранящейся в них информации к следственному действию необходимо привлекать специалиста в области компьютерно-технической экспертизы, к сожалению, сегодня на районных уровнях в территориальных подразделениях ОВД специалисты данного профиля отсутствуют, а штатная должность имеется только в экспертно-криминалистических центрах. Между тем его содействие может понадобиться в случае, если владелец изымаемого

[1] Марочкин Н.А., Асташкина Е.Н. Алгоритмизация -эффективный метод оптимизации расследования преступлений // Известия Алтайского государственного университета. № 2. 2001. С. 45–49.

[2] Григорьев В.Н., Максимов О.А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. №2 (84). С. 33–44.

носителя информации в ходе производства следственного действия сделал заявление о копировании имеющиеся на носителе информации для предоставления ему на время изъятия самого носителя. Также в ходе расследования может возникнуть ситуация, когда у следователя не представиться возможность изъять носитель информации, а саму информацию можно извлечь только путем копирования, к примеру с сервера (выделенного персонального компьютера или группы компьютеров) компании. Для того, чтобы изъять информацию с носителя без изъятия самого носителя у специалиста должно быть приготовлено соответствующее оборудование, а именно носитель информации, куда будет скопирована информация. Если речь идет о персональном компьютере или ноутбуке, то самый простой вариант это использовать компакт диск, между тем множество современных устройств не оборудовано дисководами для запуска диска, поэтому следователь может поручить специалисту скопировать информацию на флеш-карту. С копированием информации с сервера дело обстоит сложнее т.к. в своей конструкции выделенные компьютеры не предполагают копирование информации при помощи компакт-диска или флеш-карты, это возможно сделать только при подключении к серверу со стационарного устройства (ноутбука или ПК). Иными словами, сначала происходит копирование информации на ЭВМ, а с него на материальный носитель. При этом используемое ЭВМ не должно затем в себе содержать скопированной информации, в противном случае это будет считаться незаконным, а для того, чтобы удостоверить факт копирования информации только на материальный носитель привлекаются понятые[1].

Далее рассмотрим частные особенности производства невербальных следственных действий и начнем с тактики производства обыска. Обыск – это следственное действие, направленное на поиск материальных объектов преступления в зданиях, строениях, сооружениях. На подготовительном этапе обыска (выемки) следователю необходимо:

- осуществить анализ исходных сведений и определить вид и содержание компьютерной информации, которая предположительно находится в руках у преступника, а также выяснить на каких материальных носителях может находиться исходная информация;
- осуществить сбор информации о месте проведения обыска (выемки), включающий в себя точный адрес этого места, характеристику планировки помещений, наличие информации о наличии телефонной связи и работающего модема и т.д.
- изучить личность обыскиваемого. Здесь следователю необходимо получить всю информацию о навыках работы подозреваемого (обвиняемого) с компьютерной техникой. При изучении данной информации следователь сможет заранее предугадать возможное (в том числе и «интеллектуальное»)

[1]Соколова М.В., Подустова О.Л. Особенности осмотра места происшествия по уголовным делам о мошенничествах в сфере компьютерной информации // Российский следователь. 2023. № 1. С. 7–10.

противодействие со стороны лиц, находящихся в месте проведения обыска (выемки);

– подготовить материально-техническое обеспечение, использование которого следует изначально согласовать со специалистом, присутствующем при производстве обыска[1].

Применительно к расследованию киберпреступлений объектом поиска будут в первую очередь различного рода ЭВМ. Перед производством обыска следователь должен заранее подготовиться к тому, что злоумышленники могут предпринять попытку по уничтожению либо самих ЭВМ, либо хранящейся на них информации. Это достаточно легко сделать, т.к. сложное компьютерное оборудование является очень хрупким и любое механическое вмешательством может повлечь безвозвратную утерю данных. Поэтому следователь должен обеспечить контроль за участниками следственного действия, который целесообразнее всего поручить сотрудникам уголовного розыска. В частности, необходимо запретить всем участникам, кроме следователя, понятых и специалиста приближаться к устройствам ЭВМ, а также к блокам питания здания, т.к. резкое обесточивание техники может привести к потере информации.

Многие компьютерные устройства имеют функция удаленного доступа через другие гаджеты, например, с помощью таких программ как Microsoft Remote Desktop, Screen Sharing, Chrome Remote Desktop и многих других. Проще говоря, злоумышленник может с сотового телефона удаленно получить доступ к блоку памяти компьютера или ноутбука и удалить всю имеющуюся на нем информацию прямо во время обыска. Поэтому следователю нужно сразу забрать на время обыска у всех участников мобильные устройства и иные гаджеты, а в случае их использования участниками незамедлительно акцентировать на этом внимание понятых и делать соответствующую пометку в протоколе[2].

Осмотр места происшествия достаточно нетипичное следственное действие по делам о киберпреступлениях, т.к. зачастую место происшествия как таковое отсутствует, а место предварительно определяется с учетом места подачи заявления о преступлении, либо нахождения наибольшего числа участников уголовного судопроизводства. Между тем следственный осмотр по делам о киберпреступлениях проводиться может, но в юридической литературе о нем имеется крайне мало информации. В частности, в судебной и следственной практике набирает оборот такое следственное действие как осмотр интернет-

[1] Соколова М.В., Бондаренко И.А. Деятельность следователя по производству обыска при расследовании киберпреступлений // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства: сборник научных трудов Всероссийской научно-практической конференции. М., 2022. С. 266–268.

[2] Соколова М.В., Бондаренко И.А. Деятельность следователя по производству обыска при расследовании киберпреступлений // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства: сборник научных трудов Всероссийской научно-практической конференции. М., 2022. С. 266–268.

сайта[1]. Например, в 2022 году отмечается рост хакерских атак на официальные интернет-ресурсы государственных органов не с целью их отключить или заблокировать, а с целью разместить на них ложную информацию, призывающую к насилию, сепаратизму, дискредитирующую органы государственной власти и пр. В этой связи, целесообразным будет проведение следственного осмотра интернет-сайта. При осмотре сайта и составлении протокола, описательно-мотивировочную часть необходимо начинать заполнять с указания устройства, через которое будет осуществлен вход в сеть Интернет, после чего следователь должен указать какой использовался браузер (он должен быть обязательно легален на территории РФ). Далее следователь должен указать в строке поиска сайт, который он хочет посетить, он может это сделать, указав ключевые слова, например «Официальный сайт Конституционного Суда РФ» или «Официальный сайт Правительства РФ» или же указать электронный адрес сайта – URL. Далее следователь фиксирует информацию, находящуюся на сайте, в частности необходимо отобразить какой характер информации, предоставляемой на сайте (сайт государственного органа, частной организации, интернет-ресурс частного лица и пр.), после чего указывается информация, которая не соответствует характеру подаваемой на сайте информации, например поддельная новостная лента. Так, например, в марте 2022 года был взломан официальный сайт Верховного Суда РФ. Информация на главных страницах сайтов оказалась недоступна, а вместо данных злоумышленники разместили послание с нецензурными выражениями в адрес президента РФ Владимира Путина и россиян в связи с военной операцией на Украине. Для полноты фиксации информации, размещенной на сайте, рекомендуется копировать имеющуюся на нем информацию при помощи скриншотов, если это не представляется возможным (на некоторых интернет-ресурсах используются программы для защиты от снятия копии с экрана, такие как Lightshot), то нужно сфотографировать экран по правилам криминалистической фотофиксации[2].

Подводя итог вышеизложенному необходимо отметить, что производство невербальных следственных действий по делам о киберпреступлениях основывается на грамотном изъятии электронных носителей информации, а при невозможности этого – копировании информации на те носители, которыми располагает следователь. Производство невербальных следственных действий направлено на извлечение цифровой информации, что на практике затруднено из-за пробелов в законодательстве.

[1]Бегичев А.В. Использование протоколов осмотров интернет-сайтов в судебной практике // Вестник Московского университета МВД России. 2014. № 11. С. 208–212.

[2]Губарева Е.К., Калентьева Т.А. Особенности фиксации информации, содержащейся в сети Интернет // Вестник Волжского университета им. В.Н. Татищева. 2019. № 2. С. 161–168.

Э.Б. Хатов

О цифровых компетенциях следователя

Аннотация. Статья посвящена проблемным вопросам соответствия компетенций следователя перманентному росту киберпреступности и цифровизации уголовного процесса. На основе анализа содержания нормативно закрепленных индикаторов профессиональных компетенций, автор приходит к выводу, что для качественного исполнения следователями своих служебных обязанностей, соответствия современным вызовам и рискам новой цифровой реальности в органах Следственного комитета Российской Федерации требуется решение ряда организационно-структурных и кадровых вопросов.

Ключевые слова: цифровизация, индикатор, киберполигон, информационные технологии, компетенция, следователь.

Применение цифровых технологий на досудебной стадии, в том числе в рамках предварительного следствия, его криминалистического и экспертного сопровождения с учетом современных стандартов информационной безопасности является объективной реальностью сегодняшнего дня.

В правоохранительных органах развивается электронный документооборот, осваиваются информационно-аналитические платформы для идентификации участников криминальных сделок с криптовалютой. Широко обсуждается прогнозируемое внедрением программ – ассистентов, цифровых помощников следователей.[1]

Одновременно, данные статистики объективно подтверждают крайне тревожный рост преступлений, совершаемых с использованием ИКТ. Так, в 2024 году только учтенная правовой статистикой доля преступлений этой категории выросла до 38%. Таким образом, напрашивается вывод о том, что минимум каждый третий правонарушитель уже достаточно компетентен, чтобы применять свои знания информационных технологий в преступных целях.

При этом киберпреступления, под которыми нами понимаются деликты, совершенные с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), а также в сфере компьютерной информации (гл.28 УК РФ), характеризуются особым способом совершения, специфическими криминалистическими следами.

Поэтому и их расследование, предусматривающее собирание электронных следов, проверку и оценку не только самой электронной информации, но и ее носителей, невозможно без цифровизации следственной деятельности, в том числе с применением искусственного интеллекта (ИИ).

Цифровизация уголовного процесса наглядно продемонстрирована изменениями в УПК РФ, определяющая порядок электронного документооборота, в том числе посредством Единого портала госуслуг.

[1] См.: Хатов Э.Б. Цифровой помощник или цифровой прокурор? // Российский журнал правовых исследований. 2023. Т. 10, № 1. С. 87–92. DOI: 10.17816/RJLS109325.

В настоящее время следователи активно используют возможности различных ГИС, число которых уже более несколько сотен, а также массив открытых данных, работа с которыми также требует определенных компетенций. Так, по состоянию на 1 марта 2024 года в ФГИС УИС учтена 451 федеральная ГИС, введённая в эксплуатацию

Вместе с тем перечень и объем необходимых для следователя цифровых компетенций требует отдельного и углубленного обсуждения.

Например, в связи с требованиями УПК РФ по привлечению специалистов к отдельным процессуальным действиям с электронными носителями информации, будущих следователей в основной массе обучают лишь основам информационных технологий (с учетом специфики следственной деятельности).

По нашему мнению, следователь должен владеть достаточными знаниями, хотя бы чтобы удостовериться в компетенции привлекаемого лица, либо для производства безотлагательных следственных действий. Существование проблемы недостаточности владения следователями знаниями информационно-цифрового характера признают также Е.Р. Россинская, О.А. Малышева.[1]

Вместе с тем, с 1.09.2021 ФГОС специалитета по специальности «Правовое обеспечение национальной безопасности» дополнен общепрофессиональными компетенциями (п.3.3.) в части базовых информационно-коммуникационных технологий для профессиональной деятельности, а именно ОПК-9 (Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности).

Соответствующими углубленными компетенциями дополнены программы обучения будущих следователей СКР, в соответствии с ведомственным приказом СК России от 17.01.2017 № 15[2]

Поэтому следователь в настоящее время должен обладать необходимыми компетенциями, чтобы решать достаточно сложные задачи:

1) достоверно устанавливать механизм преступления, совершенного с применением IT-технологии;

2) своевременно устанавливать лиц, причастных к совершению преступлений, уверенно владеющих навыками обращения с информационными, телекоммуникационными технологиями;

3) формировать добротную доказательственную базу по уголовному делу, основу которой составляют электронные доказательства;

4) обеспечить соблюдение прав, законных интересов подозреваемого,

[1] Россинская Е.Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина. 2019. № 5 (57). С. 33; Малышева О.А. О новом векторе профессиональной подготовки следователя в условиях цифровой информации // Вестн. Том. гос. ун-та. 2022. № 480. С. 267.

[2] «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам специалитета и программам магистратуры в федеральных государственных организациях, осуществляющих образовательную деятельность и находящихся в ведении Следственного комитета Российской Федерации».

обвиняемого, потерпевшего, осложняющиеся спецификой производимых по уголовному делу следственных (осмотр устройства флеш-памяти и др.) и иных процессуальных действий (изъятие мобильного телефона, копирование электронной информации с ее носителя и др.)

5) принять меры к возмещению причиненного ущерба потерпевшим.

Представляется, что в сфере цифровых технологий следователям, помимо уверенного пользования программами - аналитическими таблицами (Exel, Googl-таблицы, их российскими аналогами), полезно было бы знать о возможности и основных вышеуказанных приемах и способах, а также:

установления, изучения профиля личности через открытые источники[1], навыки анализа социальных сетей, мессенджеров, истории браузера; поиска по фотографиям или видеозаписи, сетевым следам; мониторинга «Даркнета», деанонимизации;

использования программ шифрования;

получения и анализа биллинговых данных и т.п.; возможности извлечения сведений с использованием высокотехнологичной криминалистической техники;

получения информации о финансовых транзакциях, позволяющей идентифицировать цифровые финансовые активы, возможности и порядок применения информационно-аналитических платформ «Прозрачный блокчейн-2», Кристал (Crystal), Шард (Shard.ru), Криптотимб (Crypto.thibm.ru), гуглдоркинга, скоринга (деанонимизации); механизма наложения ареста на цифровые активы;

применения цифровых технологий, используемых при расследовании отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий;

элементарного программирования, принципов и сущности сетевых технологий, и т.д.

Следует отметить, что определенная работа по внедрению в практику таких цифровых инструментов в органах СКР организована.

Так программой дисциплины «Цифровые следы преступлений против личности» предусмотрены профессиональные компетенции (ПК-2): «Способен использовать современные (в том числе высокотехнологичные, цифровые) технико-криминалистические методы и средства, применяемые при расследовании отдельных видов и групп преступлений». Индикаторами наличия таких компетенций выступают (ИПК-2.2.) критерии: «Знает особенности и механизм цифрового следообразования в компьютерных сетях и системах, порядок формирования цифровых следов

В результате освоения дисциплины обучающийся должен знать:

понятие и значение цифровых следов преступлений против личности;

[1] Лебедева А.А. OSINT – законность использования для целей расследования преступлений // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции, Москва, 28 апреля 2023 года. М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2023. С. 87–93.

систему организации хранения данных в мобильных телефонах, средства защиты информации и методы её преодоления;

логическую взаимосвязь элементов сводки об извлечении из цифровых устройств с использованием высотехнологичной криминалистической техники;

способы извлечения криминалистически значимых данных из памяти цифровых устройств, внешних накопителей, социальных сетей и облачных хранилищ;

верно интерпретировать полученные данные исходя из следственной ситуации.

Или еще пример индикатора: ИПК-2.5: Умеет применять высокотехнологичную криминалистическую технику для поиска, фиксации, изъятия и анализа цифровых доказательств преступлений.

Продолжая знакомство с новыми компетенциями назову индикатор: ИПК-2.7. Владеет навыками сохранения, анализа и эффективного использования цифровых следов в раскрытии и расследовании преступлений; использования помощи специалистов в сфере высоких технологий В результате освоения дисциплины обучающийся должен владеть:

методикой и тактикой подготовки и проведения следственных действий, связанных с получением цифровых следов преступлений (следственные осмотры, эксперименты, получение информации о соединениях, экспертизы);

навыками обнаружения, фиксации, изъятия цифровых следов преступлений против личности;

навыками сохранения и эффективного использования цифровых следов в раскрытии и расследовании преступлений;

способностями подготовки к организации и назначению компьютерно-технических и иных экспертиз, использованию помощи специалистов в сфере высоких технологий

Конечно, указанные вопросы не могут полноценно решаться без соответствующего серьезного кадрового, материально-технического обеспечения, например, без киберполигонов, лабораторий, оперативной разработки информационных систем поддержки принятия решений, однако часть цифровых компетенций может быть получена на имеющейся в любом ВУЗе компьютерной базе, во взаимодействии с другими образовательными организациями, правоохранительными органами, ИТ компаниями (например, в рамках выездных ознакомительных занятий, в том числе совместных).

Так, в Московской и Санкт-Петербургской академиях Следственного комитета в 2021 годы образованы кафедры информационных технологий и организации расследования киберпреступлений, приобретен киберполигон на 15 рабочих мест с высокопроизводительными рабочими станциями, установлено прикладное программное обеспечение «Мобильный криминалист», «Конструктор места происшествия», «3D Свидетель» и др. для создания виртуальных мест происшествий с реалистичной следовой обстановкой и возможностью их моделирования (для ситуативного подхода, формирования криминалистического мышления следователя, фиксации (в том числе цифровой)

хода и результатов различных следственных действий), формирования трёхмерной модели лица человека.

Киберполигон позволил дополнительно включить в учебный процесс новые дисциплины, в том числе «Получение и анализ криминалистически значимой информации с использованием программных комплексов».

Организационно-распорядительными документами Следственного комитета ведомственным ВУЗам поручено принимать меры к подбору студентов и слушателей, проявляющих способности к научно-технической деятельности и активному использованию цифровых технологий, привлекать их к углубленному изучению современных возможностей расследования киберпреступлений, научно-исследовательской работе[1] и дальнейшему обучению в аспирантуре (например, в Московской академии создан научный студенческий кружок «Киберследователь»).

Академией тестировались программы -обозреватели криптовалют – информационно-аналитические платформы Шард и Криптотибм, с помощью которых можно не только проанализировать в истории браузера подозрительные транзакции условно-анонимных криптовалют и визуализировать их, но активизировать функцию мониторинга (отслеживания) для контроля вывода средств и деанонимизации. Результаты тестирования указанных информационно-аналитических платформ используются в процессе обучения.

В региональных следственных органах проходит апробацию разработанное ректором А.А. Бессоновым на базе искусственного интеллекта программное обеспечение «Портрет серийного убийцы» (PorSerO). Первые отзывы положительные.

Следует отметить, что указанные организационные процессы характерны не только для органов СКР, но и иных правоохранительных органов. Так, в Университете МВД помимо мощной полигонно-лабораторной базы учебно-научного комплекса информационных технологий с отделением технологий информационной безопасности, а также нескольких специализированных компьютерных классов, образованы три профильные кафедры: кафедра информационной безопасности, кафедра специальных информационных технологий, а также отдельная кафедра противодействия преступлениям в сфере информационно-телекоммуникационных технологий (последняя создана в 2022 г.).

Нельзя не отметить, что аналогичные мероприятия реализуются и в иных, в том числе «гражданских» отечественных ВУЗах, где в рамках федеральной программы «Приоритет 2030» образовано и действуют 115 специализированных цифровых кафедр, позволяя получить дополнительное образование обучающимся, чья будущая специальность не связана с IT-сферой.

---

[1] Бессонов А.А. Научное и учебно-методическое обеспечение расследования киберпреступлений в Московской академии Следственного комитета // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 3.

Таким образом, в условиях выраженного тренда цифровизации правоохранительной сферы, в том числе предварительного следствия, формируемом едином информационном пространстве правоохранительных и надзорных органов[1], заметно усиливается потребность в цифровых компетенциях следователей, необходимых для качественного исполнения своих служебных обязанностей и соответствия современным вызовам и рискам новой цифровой реальности, что требует оперативного решения обозначенных выше организационно-структурных, кадровых вопросов.

В частности, по примеру наших коллег из стран СНГ - это организация регулярного повышения квалификации в ведущих отечественных и зарубежных образовательных организациях, регулярных стажировок следователей, сотрудников образовательных ведомственных организаций в зарубежных правоохранительных органах, обладающих передовым опытом расследования преступлений в сфере высоких технологий, с целью его изучения и применения.

Представляется, что реализация указанных мер позволит удовлетворить насущную потребность наделения следователей необходимыми компетенциями, наличие которых определено состоянием преступности и научно-техническим прогрессом.

А.А. Чернопёров

Проблемы исследования артефактов баз данных 1С при расследовании экономических преступлений

Аннотация. Статья посвящена анализу использования сведений, обрабатываемых в системах разработчика российского программного обеспечения для бухгалтерского учёта и отчётности компании 1С. Указанное программное обеспечение используется на большинстве предприятий, что делает его исследование обязательной составной частью расследования уголовных дел о преступлениях в сфере экономики. Особенности цифровых следов, образующихся при работе с системами 1С требуют тщательного подхода к осмотру электронных устройств, соблюдения правил изъятия информации и следования определённым алгоритмам при их исследовании. Существенные сложности возникают при производстве следственных действий в случае использования на предприятии облачных версий продуктов 1С, что требует привлечения к участию в следственных действиях специалистов указанной компании.

Ключевые слова: 1С, базы данных, хэш-сумма, версионирование данных, облачные вычисления, следственные действия, компьютерно-техническая экспертиза, комплексная экспертиза.

[1] Хатов Э.Б. Состояние единого информационного пространства органов прокуратуры, иных правоохранительных, а также контрольно-надзорных органов и судов // Вестник Университета прокуратуры Российской Федерации. 2019. № 3(71). С. 38–41.

Расследование экономических преступлений является одной из приоритетных задач Следственного комитета Российской Федерации. Особенно это направление деятельности актуально сейчас, когда в условиях сложной экономической ситуации хозяйствующие субъекты злоупотребляют предоставленными мерами поддержки, цинично уклоняются от уплаты налогов, прикрываясь надуманными предлогами. Благодаря усилиям следственных подразделений Следственного комитета Российской Федерации в бюджет взысканы многомиллиардные недоимки по налогам, тысячи работников предприятий получили задержанную заработную плату.

Для лучшего понимания места информационных технологий в автоматизации бухгалтерского учёта следует уделить некоторое время освещению истории данного вопроса. Именно бухгалтерские задачи стали обрабатываться на производствах техническими средствами значительно раньше других экономических задач. Основными причинами, предопределяющими применение вычислительной техники в организации бухгалтерского учёта, были большие объёмы информации, многочисленные группировки, жёсткие сроки обработки первичной документации, высокие требования к точности и достоверности итоговых данных. Можно выделить механизированный и автоматизированный этапы обработки бухгалтерской информации.

Механизированный этап пришёлся на 1950-1960 годы. В этот период на крупных предприятиях организовывались машиносчётные станции, на которых главную роль играла комплексная механизированная обработка учётных записей таблично-перфокарточной системы счетоводства на базе типовых программ.

Первые попытки автоматизации задач бухгалтерского учёта на основе использования ЭВМ были предприняты в СССР примерно в середине 60-х гг. XX в. Использовавшиеся тогда ЭВМ второго поколения (типа «Минск-32») были малопроизводительными и обладали очень небольшим объёмом памяти. В соответствии с этим разрабатывались и программы.

В начале 1970-х годов появились ЭВМ, специализированные на решении задач в сфере экономики, что привело к переходу ко второму этапу – автоматизированному. Данный этап можно разделить на несколько этапов, различающихся друг от друга по формам взаимодействия машины и пользователя, а также по режимам работы ЭВМ.

Начальный период связан с централизованной обработкой бухгалтерских задач в вычислительном центре, где применялся однопрограммный режим работы ЭВМ. Бухгалтер мог влиять на процесс решения задачи. Оператор обрабатывал полученную учетную документацию по программе, после чего возвращал ведомости аналитического и синтетического учёта. С развитием ЭВМ и их операционных систем были созданы предпосылки для обеспечения взаимодействия между пользователем и программой. Основываясь на результатах полученных отчётов, пользователь оперативно принимал решения о дальнейшей работе с программой.

В начале 1980-х годов появились персональные ЭВМ, характеризующиеся высоким быстродействием, большой ёмкостью оперативной и внешней памяти,

а также широкий выбор внешних устройств ввода-вывода информации. Эти машины были ориентированы на выполнение функций формирования первичных документов и учётных регистров. Благодаря этому вопрос автоматизации решения бухгалтерских задач перешёл на новый уровень. Произошел переход от централизованной обработки бухгалтерской информации к децентрализованной. В результате вместо того, чтобы обрабатывать всю бухгалтерскую информацию в вычислительном центре предприятий, стало возможным установить персональную ЭВМ на рабочем месте бухгалтера, использовать компьютеры на малых и средних предприятиях. В условиях децентрализованной обработки появляется возможность решения отдельных учетных задач на АРМ и составления сводных регистров бухгалтерского учёта и отчетности на основе полученных результатов.

Не без гордости стоит отметить, что Российская Федерация перенесла последствия недружественной политики западных стран на фоне специальной военной операции без необходимости принятия каких-либо мер по импортозамещению программного обеспечения в сфере бухгалтерского учёта именно потому, что изначально такое программное обеспечение разрабатывается в нашей стране и даже экспортируется. Первое поколение российских систем (1988 – 1991) характеризуется небольшим числом автоматизированных операций и сложностью подстройки к быстро меняющимся правилам бухгалтерского учёта в Российской Федерации. Программы этого времени были предназначены для использования в виде АРМ бухгалтера на персональных компьютерах и производились с расчётом на большой тираж с учётом низкой стоимости копии программы. Самыми первыми бухгалтерскими программами являются: «Финансы без проблем» («Хакерс Дизайн»), «Турбо-бухгалтер» (ДИЦ), «Парус» («Парус»).

Второе поколение систем (1992–1994) имело такие особенности программ: увеличение числа автоматизированных операций, а также более высокая приспособленность к различным изменениям в правилах бухгалтерского учёта. Эти программы уже предполагали работу и в локальных сетях, и автономно. Среди них появились первые системы, сочетающие ряд функций учета, непосредственно не связанных с бухгалтерией. В это время доминировали универсальные бухгалтерские программы, однако уже тогда стали появляться программные продукты, которые ориентировались на определенный круг клиентов. Именно тогда были образованы сегодняшние фирмы-лидеры: 1С, «Диасофт», «Омега».

Третье поколение (1995 –1998). Программы этого поколения отличаются комплексным подходом и более узкой специализацией. Большая часть этих систем является интегрированными и предназначенными для полной автоматизации деятельности предприятий программами, которые имеют встроенные средства развития и полностью совместимы с другими программными продуктами фирмы-разработчика, обеспечивающими автоматизацию избранного объекта.

Четвёртое (современное) поколение – бухгалтерские системы, а по своей сути уже комплексные информационные системы, характеризующиеся интегрируемыми технологическими решениями. Они предполагают поставку методики организации производства и консалтинговых услуг. Таким образом, в сфере методологии разработки систем для автоматизации бухгалтерии практически завершен переход от программ, рассчитанных на широкий круг потребителей, к программам, максимально отвечающим потребностям конкретного заказчика[1].

Несмотря на разные сроки создания всех классов бухгалтерских систем на российских предприятиях до сих пор имеются бухгалтерские системы всех 4 поколений. Однако, с начала 2000-х, благодаря постоянному развитию и грамотному маркетингу самыми распространенными, известными и продаваемыми в России являются системы автоматизации бухгалтерского учета фирмы «1С».

По итогам прошлого, 2023 года компания 1С является лидером среди отечественных поставщиков соответствующего программного обеспечения. Количество пользователей в России сопоставимо с числом предприятий малого и среднего бизнеса. По статистике около 83% рабочих мест в нашей стране автоматизированы с помощью продуктов «1С». Следует отметить, что в это число не входят нелицензионные продукты и самостоятельные доработки.

Также развиваются международные разработки (1Ci), например, решения 1С: Drive, 1С: Enterprise и 1С: ERP. Постоянно увеличивается число стран, в которых используется указанное программное обеспечение (Чехия, Вьетнам, Объединённые Арабские Эмираты и другие).

Следуя потребностям развивающейся IT инфраструктуры, компанией 1С разработаны облачные версии систем бухгалтерского учёта, которые позволяют использовать мощные программы на персональных устройствах небольшой производительности, синхронно вводить данные с нескольких устройств, работать с данными из любой точки земного шара, параллельно вести бухгалтерский учёт нескольких предприятий.

Сложные процессы отражения бухгалтерских операций, особенности сохранения данных и их защиты требует использования в процессе расследования специальных знаний как в сфере информационно-телекоммуникационных технологий так и в сфере экономики. На это особо указал в своём докладе председатель Следственного комитета Российской Федерации А.И. Бастрыкин, который, в частности, указал, что: «Сложность расследования преступлений экономической направленности обусловлена также недостатками в законодательной регламентации различных экономических процессов и явлений. Преступники используют особенности экономической, финансовой, правовой системы, которые постоянно изменяются. В связи с этим от сотрудника следственных органов требуется наличие достаточных собственных знаний в указанных областях, а также активное использование

[1] От ненависти до любви: есть ли развитие в 1С для разработчика и какие там вообще тренды? https://habr.com/ru/companies/outlines_tech/articles/761272/

специалистов, обладающих углубленными знаниями в соответствующей сфере, для выяснения всех особенностей правовых, экономических, финансовых, технологических, производственных и иных механизмов, используемых участниками преступного деяния[1]». Экономическое направление экспертиз развивалось с учётом потребностей органов предварительного расследования, с появлением новых составов преступлений, примерно в одно время с принятием нового Уголовно-процессуального кодекса Российской Федерации появились новые виды направления экономических экспертиз. Вместе с тем, для успешного решения вопросов, которые ставятся на разрешение эксперта – экономиста, стало не хватать исследования только документарного (бумажного) учёта. Потребовались данные Федеральной налоговой службы Российской Федерации, банков, сведения из электронных баз данных самих организаций. В случае ведения так называемой «чёрной» бухгалтерии, учёт может вестись и исключительно в электронном виде, причём с использованием тех же средств вычислительной техники и того же программного обеспечения, что требует участия в производстве следственных действий специалистов в области компьютерной техники.

Функционирование систем 1С в организациях невозможно описать единым алгоритмом, что связано с наличием большого количества одновременно эксплуатируемых версий и модулей программы. Часто системы настраиваются под потребности конкретного бизнеса и имеют существенные отличия. Демократичная политика разработчика указанных программных продуктов позволяет создавать дополнительные модули, свою инфраструктуру, настраивать способы доступа и хранения рабочих баз данных и их резервных копий. Указанное обстоятельство требует от следователя и специалистов ответственного подхода к планированию следственных действий и их производству. Причём результативными проводимые следственные действия могут быть только при тесном взаимодействии участников предварительного расследования со стороны обвинения. Опираясь на сведения, полученные в ходе предшествующих следственных действий и оперативно-разыскных мероприятий следователь или руководитель следственной группы (уголовные дела о преступлениях в сфере экономической деятельности часто требуют создания таких групп) составляет максимально детальные планы расследования в целом и отдельных следственных действий, подбирает специалистов и экспертные организации, обеспечивает их необходимой информацией и координирует работу. От специалиста-экономиста требуется чёткое формирование перечня необходимых сведений (объекты учёта, интересующий период, конкретные операции). Специалист в области компьютерной информации должен тщательно исследовать интересующую следствие компьютерную систему, определить наличие возможности удалённого доступа,

[1] Тезисы выступления Председателя Следственного комитета Российской Федерации А.И. Бастрыкина на круглом столе на тему: «Криминалистическое и оперативно-разыскное обеспечение расследования экономических преступлений» URL: https://proza.ru/2018/04/02/1364?ysclid=lwxtzemzbn568357133

факт использование облачных систем, вероятное наличие резервных копий на съёмных носителях и так далее. Специфика баз данных программ 1С требует от специалиста знание алгоритмов работы. Простого копирования файлов программы для успешной работы эксперта-экономиста недостаточно. Завершение работы программы без корректного закрытия баз данных может привести к утрате сведений об операциях за значительный период времени. Ещё большие сложности вызывает анализ данных программ 1С при использовании «облачных» версий. На сегодняшний день единственным способом фиксации состояния баз данных на определённый момент остаётся выгрузка полного массива с расчётом hash-сумм и отражением их в протоколе следственного действия. Такой вариант, хотя и гарантирует сохранность цифровых следов, создаёт значительные сложности для эксперта – экономиста, так как требует подбора соответствующих версий программы для работы с изъятыми базами, хранения больших объёмов информации в период производства экспертизы. Отказ от работы с базами данных и использование только выгрузок в виде электронных таблиц существенно сужает диапазон поиска.

В то же время, детальный анализ протоколов действий пользователя, автоматически ведущихся всеми системами 1С позволяет специалистам выявить большое количество обстоятельств, которые позволяют установить факты фальсификации бухгалтерской отчётности, умышленного внесения ложных данных. Значимые сведения могут быть обнаружены в журнале регистрации событий, истории действий и в версиях данных.

Журнал регистрации событий представляет собой список всех событий, которые происходили в информационной базе. Доступ к этому файлу есть только у пользователя с полными правами (устанавливаются редко) или у администратора системы. Находится этот журнал обычно в разделе программы Администрирование – Обслуживание.

История действий пользователя – это интерфейсный механизм платформы, который может использовать любой человек, работающий в информационной системе. Этот механизм хранит все действия сотрудника компании с объектами прикладного решения. Удаление старых записей истории происходит автоматически, так как она может хранить не более 400 записей. Если человек несколько раз изменял какой-то объект базы данных, то этот механизм будет отображать только последнюю запись. Для регистров сохраняются записи про каждое изменение в разрезе его ключевых полей. Ограничением этого механизма является то, что он отображает действия того пользователя, под которым авторизовались в конфигурации[1].

Учёт всех изменений данных или версионирование, по умолчанию в программе отключен, но проверка наличия соответствующего журнала при осмотре системы должна проводиться в обязательном порядке, так как данный инструмент является самым подробным.

[1] Губернаторова Д. Действия пользователя в 1С. URL: www.koderline.ru/expert/instruktsii/article-deystviya-polzovatelya-v-1s/

Кроме того, помимо непосредственно систем бухгалтерского учёта большой объём цифровых следов может быть получен при осмотре личных устройств пользователей, персональных компьютеров, на которых производится обработка документации в организации (переписки в мессенджерах, сообщения электронной почты временные файлы программ для сканирования). Следует помнить, что в последних версиях систем 1-С реализован ввод данных из типовых форм бухгалтерского учёта, представленных в виде изображений (сканированные, сфотографированные), следовательно, в случае фальсификации, на устройстве, с которого пересылались указанные документы или среди временных файлов программы-сканера могут быть обнаружены изображения исходных документов.

При работе на данном направлении важно учитывать опыт работы органов ФНС Российской Федерации. Так, в статье А.А. Мошкина содержится ряд примеров конкретных ситуаций:

«Когда компания сдаёт бухотчетность, открывает банковский счёт или доступ к онлайн-банку, то оставляет цифровые следы в виде IP- и MAC-адресов. Одинаковые IP- и MAC-адреса у всех компаний в группе — признак подконтрольности при дроблении бизнеса (постановления АС Волго-Вятского от 19.10.2022 № А29-11957/2018, Уральского от 28.01.2021 № А60-69372/2019 округов). Общий IP-адрес у организации и её спорных контрагентов убедит судей, что компании действовали заодно, чтобы получить необоснованную налоговую выгоду (постановление АС Московского округа от 04.10.2022 № А41-6733/2022). Собственная программа налоговиков АСК НДС-2 выявляет налоговые разрывы по цепочке контрагентов. Система обнаруживает компании, у которых мало сотрудников или низкие средние зарплаты, нет внеоборотных активов, собственности, госконтрактов. А также компании, которые подали недостоверные сведения или имеют высокий процент вычетов по НДС при их несформированности. За каждый признак компаниям присваивают баллы. По ним ФНС автоматом делит всех на выгодоприобретателей, транзитеров и разрывщиков. Помимо собственных сервисов и баз данных проверяющие используют для проверки компаний внешние ресурсы. Так, из систем «Честный знак», ЕГАИС, «Меркурий» налоговая получает информацию о реальном движении прослеживаемых, чипированных и подакцизных товаров. Из системы «Платон» — о движении грузовиков»[1].

Таким образом, можно уверенно резюмировать, что на сегодняшний день экспертами Судебно-экспертного центра Следственного комитета, МВД, Министерства юстиции и других экспертных учреждений Российской Федерации, в том числе – коммерческими фирмами и частными экспертами наработан богатый опыт сбора цифровых следов по уголовным делам экономической направленности и их исследования. Работа экспертов позволяет следователям Следственного комитета формировать доказательственную базу

[1] Мошкин А.А. Цифровые следы как доказательства в налоговых спорах. URL: https://vk.com/wall499458708_741

по делам указанной категории, достоверно устанавливать суммы причинённого ущерба и принимать меры к его возмещению.

Вместе с тем, до настоящего времени отсутствует методика исследования облачных баз данных, изъятия цифровых следов из них и защита собираемой информации от применения контркриминалистических средств. Указанные вопросы могут быть успешно решены только в результате конструктивного взаимодействия заинтересованных ведомств.

К.С. Шубина

Искусственный интеллект как инструмент противодействия преступлениям в сфере информационно-телекоммуникационных технологий

Аннотация. В статье рассмотрены перспективы использования технологий искусственного интеллекта в деятельности правоохранительных органов; проанализированы проблемы, связанные с правовым регулированием искусственного интеллекта в России; на практических примерах продемонстрированы возможности искусственного интеллекта при раскрытии и расследовании преступлений.

Ключевые слова: искусственный интеллект, информационно-телекоммуникационные технологии, раскрытие и расследование преступлений, противодействие преступлениям, правоохранительные органы, нормативно-правовое регулирование, опыт зарубежных стран.

Появление и развитие информационно-коммуникационных технологий и информационно-телекоммуникационной сети Интернет связано с цифровой революцией, обозначившей переход от аналоговых технологий к цифровым. Внедрение инновационных технологий (искусственного интеллекта, блокчейна, интернета вещей и т.д.) в повседневную и профессиональную деятельность людей привело не только к повышению качества жизни, но и появлению новых видов преступлений. Согласно статистическим данным, представленным на официальном сайте МВД России, в январе-феврале 2024 г. зарегистрировано более 115 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 23,5% больше, чем за аналогичный период прошлого года[1].

На сегодняшний день для совершения имущественных преступлений в сфере информационно-телекоммуникационных технологий (краж, мошенничеств, вымогательств и др.) используются кибератаки. Так в мае 2017 г. произошла глобальная кибератака с использованием программы-вымогателя WannaCry. Она была направлена на компьютеры под управлением операционной системы

[1] Краткая характеристика состояния преступности в Российской Федерации за январь - февраль 2024 года [Электронный ресурс]. Официальный сайт МВД России. URL: https://мвд.рф/reports/item/48913905/ (дата обращения: 08.05.2024).

Microsoft Windows. В результате атаки пострадало около 230 тыс. компьютеров в 150 странах. Злоумышленники зашифровали данные на устройствах потерпевших и потребовали выкуп в криптовалюте Bitcoin за восстановление доступа. По оценкам экспертов, общий финансовый ущерб от этой кибератаки составил 4 млрд. долларов США, что делает её одним из самых масштабных киберпреступлений по размеру нанесённого ущерба[1].

Киберпреступники используют различные автоматизированные инструменты и интеллектуальные технологии автоматизации, чтобы избежать обнаружения. Например, они могут применять распределённые кибератаки, направленные одновременно на большое количество пользователей и ресурсов компаний. Также они используют целевые атаки (APT), заранее спланированные и нацеленные на конкретную компанию или инфраструктуру.

К интеллектуальным технологиям автоматизации можно отнести: искусственный интеллект (ИИ) и машинное обучение (для создания более сложных вирусов и программ-вымогателей, способных адаптироваться к защитным мерам); технологии глубокого обучения (для анализа больших объемов данных и выявления уязвимостей в системах безопасности); роботизированную автоматизацию процессов (для автоматизации рутинных задач, таких как отправка фишинговых писем или сбор данных, позволяющих действовать более масштабно и эффективно).

В соответствии с Указом Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», под искусственным интеллектом следует понимать – «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их».

Перспективным, по нашему мнению, является использование технологий искусственного интеллекта в деятельности правоохранительных органов. Однако на сегодняшний день существуют проблемы, связанные с правовым регулированием искусственного интеллекта в России. Технологии ИИ развиваются быстрее, чем законодательство успевает адаптироваться к ним. Сложность и многоаспектность технологий искусственного интеллекта требуют глубокого понимания и анализа, что приводит к замедлению процесса регулирования. Отсутствие единого подхода к ключевым понятиям в сфере ИИ затрудняет разработку и внедрение эффективных правовых норм.

Правительством Российской Федерации разработана Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г. Её целью является «определение основных

[1] Атака программы-вымогателя WannaCry [Электронный ресурс]. Fandom, Inc. URL: https://winencyclopedia.rus.fandom.com/ru/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B- %D0%B2%D1%8B%D0%BC%D0%BE%D0%B3%D0%B0%D1%82%D0%B5%D0%BB%D1%8F_WannaCry (дата обращения: 08.05.2024).

подходов к трансформации системы нормативного регулирования в Российской Федерации для обеспечения возможности создания и применения таких технологий в различных сферах экономики с соблюдением прав граждан и обеспечением безопасности личности, общества и государства», а также «создание предпосылок для формирования основ правового регулирования новых общественных отношений, складывающихся в связи с разработкой и применением технологий искусственного интеллекта и робототехники и систем на их основе, а также определение правовых барьеров, препятствующих разработке и применению указанных систем»[1].

К 2030 г. в России должна быть создана гибкая система нормативно-правового регулирования в области искусственного интеллекта, гарантирующая безопасность населения и стимулирующая развитие технологий ИИ[2].

Правоохранительные органы в целях противодействия высокотехнологичной преступности применяют технологии искусственного интеллекта в своей профессиональной деятельности несмотря на то, что правовое регулирование этой сферы ещё не до конца сформировано. Например, отечественная система «Криминалист» позволяет анализировать информацию из различных источников, таких как: базы данных министерств и ведомств (МВД, ФСБ, ФСИН, СК РФ, ФНС, Росфинмониторинг и др.), социальные сети (ВКонтакте, Одноклассники, Yappy и т.д.), ресурсы СМИ. Система способствует выявлению потенциальных преступников и установлению мест совершения преступлений. Система «Криминалист» позволила в 2020 г. выявить подозреваемого в хищении бюджетных средств, обнаружив его связь с другими участниками дела[3].

В 2023 г. было раскрыто более 9 тыс. преступлений, совершенных на территории г. Москвы, с помощью городских камер[4]. В этой связи развитие программ, прогнозирующих возможное время и место совершения преступления, следует рассматривать в контексте разработок по программе «Умный город», включая распознавание лиц (на улицах, вокзалах, аэропортах, транспорте и т.д.). При этом основным средством получения соответствующей информации являются камеры видеонаблюдения. В Москве установлено более 204 тыс. видеокамер, предоставляющих правоохранительным органам информацию, необходимую для раскрытия и расследования преступлений. Интеграция систем распознавания лиц, подобных FindFace, позволяет

---

[1] Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г.: Распоряжение Правительства РФ от 19.08.2020 № 2129-р.

[2] Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»).

[3] Нейронное дело: как ИИ помогает в борьбе с преступностью [Электронный ресурс] // Известия – URL: https://iz.ru/1569903/alena-svetunkova/neironnoe-delo-kak-ii-pomogaet-v-borbe-s-prestupnostiu (дата обращения: 08.05.2024).

[4] Информационный Центр Правительства Москвы [Электронный ресурс] // URL: https://icmos.ru/news/pocti-9-tys-prestuplenii-raskryli-v-gorode-s-pomoshhyu-gorodskix-kamer-za-11-mesyacev-2023-goda (дата обращения: 08.05.2024).

эффективно идентифицировать подозреваемых и существенно ускоряет процесс раскрытия преступлений.

На стратегической сессии по искусственному интеллекту 12.11.2020 министерством внутренних дел Российской Федерации был представлен проект по внедрению искусственного интеллекта для выявления серийных преступлений и определения внешности преступника. В настоящий момент связи между серийными преступлениями устанавливаются вручную, однако софт с использованием ИИ позволит автоматически анализировать описания преступлений (на основе протокола осмотра места происшествия), показания свидетелей и иные документы, выявляя в них совпадения (например, место преступления или найденные предметы). В целях установления внешности преступника, составляют фоторобот, а также анализируют биологический материал (кровь, слюну, ликвор и др.) и следы пальцев рук, обнаруженные на месте преступления. Однако это возможно только при наличии соответствующих сведений в банке данных. На сегодняшний день для полноценного анализа в России слишком маленькая база геномных данных[1].

В целях противодействия мошенничествам, совершенным с использованием технологии deepfake, АНО «Диалог регионы» была разработана программа «Зефир», предназначенная для мониторинга аудиовизуальных материалов на предмет наличия дипфейков. Система основана на технологии транскрибации в режиме реального времени, что позволяет незамедлительно обнаруживать аудио-видео- дипфейки благодаря алгоритмической оценке и анализу с использованием ИИ[2].

Технологии искусственного интеллекта также активно применяются зарубежными коллегами для раскрытия и расследования преступлений. Один из примеров – система PredPol (Predictive Policing). Это инновационная технология, использующая алгоритмы машинного обучения для прогнозирования совершения преступлений в определенных местах и в определенное время.

Принцип работы PredPol основан на анализе больших объемов данных о предыдущих преступлениях, совершенных в конкретном районе. Система учитывает вид преступления, место и дату его совершения, а затем использует эти сведения для создания модели, предсказывающей вероятность повторения подобных инцидентов в будущем. PredPol предоставляет полиции карту города, на которой отмечены зоны с высоким риском совершения преступлений. Это позволяет офицерам полиции сосредоточить свои усилия на наиболее уязвимых участках, предотвращая тем самым возможные правонарушения.

Эффективность системы PredPol была подтверждена результатами её внедрения в различных городах. Например, в Санта-Крузе (Калифорния) после

---

[1] МВД внедрит нейросети для поиска серийных убийц и создания «фотороботов» [Электронный ресурс] // РБК – URL: https://www.rbc.ru/rbcfreenews/663b30719a7947213ef9556d (дата обращения: 08.05.2024).

[2] ПО «Зефир» [Электронный ресурс] // Диалог. Цифровые коммуникации – URL: https://dialog.info/it- reshenie- dialoga- dlya- raspoznaniya- dipfejkov- zefir- vysoko- ocenili- v- administracii-prezidenta/ (дата обращения: 08.05.2024).

начала использования PredPol число ограблений снизилось на 44 %, а количество нападений с применением оружия – на 24 %.

Другим примером является система ShotSpotter, предназначенная для обнаружения выстрелов из огнестрельного оружия и установления места происшествия. Она состоит из сети датчиков, расположенных в стратегически важных точках города, способных фиксировать звуковые волны, возникающие при выстрелах. Эти датчики передают информацию на центральный сервер, где она обрабатывается посредством алгоритмов искусственного интеллекта.

Оператор, работающий на центральном сервере, прослушивает записи звуков, чтобы определить, действительно ли они являются выстрелами. Если это так, он передает информацию в полицию, указывая точное местоположение инцидента.

Система ShotSpotter доказала свою эффективность в снижении уровня преступности. Например, в городе Атланта (США) после её установки количество убийств сократилось на 30 %, а общее число преступлений с применением огнестрельного оружия – на 15 %.

Таким образом, использование искусственного интеллекта в деятельности правоохранительных органов позволяет автоматизировать процесс анализа больших объемов данных, способствует выявлению скрытых закономерностей, повышает эффективность раскрытия и расследования преступлений. Технологии ИИ дают возможность идентифицировать объекты, лица и звуки по видео- и аудиозаписям, обеспечивая сбор криминалистически значимой информации. Однако, несмотря на перечисленные преимущества, применение искусственного интеллекта поднимает этические вопросы, связанные с обеспечением конфиденциальности персональных данных и соблюдением прав и свобод человека и гражданина, что требует тщательного рассмотрения и правового регулирования.

В.А. Шурухнов

Внешние условия обстановки совершения преступлений с использованием информационно-коммуникационных технологий

Аннотация. В статье рассматриваются внешние условия, составляющие данные об обстановке совершения преступлений с использованием информационно-коммуникационных технологий, определен порядок их влияния на процесс совершения преступлений данного виду, а также влияние внешних условий обстановки на создание научных положений и разработку на их основе практических рекомендаций по выявлению, раскрытию и расследованию преступлений с использованием информационно-коммуникационных технологий.

***Ключевые слова*:** внешние условия, обстановка совершения преступления, выявление преступлений, расследование преступлений, следственные действия.

Большинство ученых и специалистов отмечают, что обстановка совершения преступлений – это объективные и субъективные условия в которых происходит преступный процесс. С данным положением следует согласиться, обозначив их взаимное воздействие на все элементы преступной деятельности. В частности, обстановка оказывает существенное влияние на выбор способа совершения преступления, подбор орудий и средств, используемых для его реализации, а также выбор места и времени его совершения. Важное значение для подготовки научных положений и разработку на их основе практических рекомендаций раскрытия и расследования преступлений с использованием информационно-коммуникационных технологий имеют данные об обстановке, как элемент криминалистической характеристики преступлений данного вида.

Анализ научной литературы, а также судебно-следственной практики, позволяет прийти к выводу, что условия, составляющие содержание обстановки совершения преступлений, следует дифференцировать на внутренние и внешние. При этом, внутренними условиями являются те, которые взаимозависимо связаны с конкретным лицами, осуществляющими подготовку, совершение и сокрытие преступлений, с использованием информационно-коммуникационных технологий и определенно зависят от их личностных качеств и свойств.

Внешние условия – это те условия, которые характеризуют обстановку внешней среды, независимо от свойств и качеств конкретного лица, оказывающих влияние на весь процесс совершения преступлений с использованием информационно-коммуникационных технологий.

Следует признать, что сегодня ситуация с преступлениями в сфере использования информационно-коммуникационных технологий в стране достаточно сложная. По данным правоохранительных органов, с каждым годом количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, увеличивается. В частности, если, например, в 2018 году таких преступлений было выявлено 174674, в 2019 году 294409, то уже в 2020 году указанных преступлений было выявлено 510396. В 2021 году было выявлено 517722 преступления, в 2022 году – 522065 преступлений, а в 2023 году – 676951 преступление[1].

Приходится констатировать, что данное положение негативно сказывается на всех отраслях народного хозяйства страны, особенно в экономической и банковской сферах.

Однако, следует признать, что сегодня государством предпринимаются значительные усилия, направленные на стабилизацию ситуации в сфере раскрытия, расследования и предупреждения преступлений с использованием информационно-коммуникационных технологий. В частности, Указом Президента утверждены «Основы государственной политики Российской

[1] Состояние преступности URL: https://xn--b1aew.xn--p1ai/folder/101762. (Дата обращения: 01.04.2024).

Федерации в области международной информационной безопасности», в которых определена государственная политика в области международной информационной безопасности, которая представляет собой совокупность скоординированных мер, направленных на формирование с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности [1].

В целях усиления борьбы с преступлениями, в рассматриваемой сфере в МВД России создано специальное подразделение, деятельность которого направлена на обеспечение и осуществление в пределах компетенции функции Министерства по выработке и реализации государственной политики и нормативно-правовому регулированию в области организации противодействия противоправным деяниям, совершаемым с использованием (в сфере) информационно-коммуникационных технологий[2].

Вообще нормативная деятельность является одним из внешних условий[3], которое оказывает существенное влияние на выбор конкретного вида и способа реализации преступлений с использованием информационно-коммуникационных технологий. Преступникам приходится разрабатывать и приспосабливать новые средства и технологии, для подготовки и реализации преступлений рассматриваемого вида. Обусловлено это тем, что государство, по итогам выявления новых видов преступлений с использованием информационно-коммуникационных технологий, разрабатывает и регламентирует ответственность за их совершение, а также соответствующие меры, направленные на нейтрализацию и выявление способов их совершения.

Одним из ключевых внешних условий, обстановки преступлений с использованием информационно-коммуникационных технологий, является то, что в орбиту преступной деятельности наиболее часто попадают лица, не имеющие представление о ее характере. То есть, граждане, которые считают обстановку, в которой они находятся, как законную деятельность сотрудников учреждений, в обязанности которых она входит. В зону повышенного риска попадают, как показывает анализ судебно-следственной практики, пенсионеры, а также молодежь и несовершеннолетние граждане.

---

[1] Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства РФ, 19.04.2021, № 16 (Часть I). Ст. 2746. Приказ МВД России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации». Федеральный закон от 24.07.2023 № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» //Собрание законодательства РФ. 31.07.2023. № 31 (Часть III). Ст. 5766.

[2] Приказ МВД России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации».

[3] См., например: Мецгер А.А. Профилактика правонарушений и защита прав человека в России // Закон и право. 2022. № 2. С. 60–63; *он же.* Понятие и содержание правоприменительной деятельности // Вопросы права. 2023. № 2. С. 32–37 и др.

В противовес такой деятельности, как существенное условие обстановки совершения преступлений с использованием информационно-коммуникационных технологий, входит активная просветительская деятельность. Сегодня она позволяет существенно противодействовать преступлениям с использованием информационно-коммуникационных технологий посредством использования средств массовой информации, которые позволяют охватить широкую аудиторию, в том числе указанных категорий граждан. Такое положение, в свою очередь, влияет на необходимость подыскания и разработки преступниками новых средств и способов совершения преступлений с использованием информационно-коммуникационных технологий.

Приходится констатировать, что существенным внешним условием обстановки преступлений рассматриваемого вида, является низкий уровень раскрываемости, расследования и предупреждения преступлений, что способствует их активному распространению. В частности, на данное обстоятельство указывает Председатель Следственного комитета А.И. Бастрыкин, который подчеркивая важность деятельности по раскрытию киберпреступлений, обозначил, что их число неуклонно возрастает. В частности, А.И. Бастрыкин отметил, что по итогам работы ведомства в первом полугодии (2023 год – *прим. автора*) стало расследование свыше 10 с половиной тысяч таких деяний, совершенных с применением современных цифровых технологий, в том числе криминальных атак на социально уязвимых граждан с использованием методов социальной инженерии[1].

Формированием соответствующей обстановки совершения преступлений с использованием информационно-коммуникационных технологий, стало повсеместное развитие цифровой экономики и внедрение ее возможностей и технологий во все отрасли и сферы страны. При этом, в отдельных случаях отсутствие альтернативы применения коммуникационных средств и технологий, значительно повышает количество вовлеченных в нее жителей страны и, как следствие, увеличивает шансы преступников, в выборе жертв своей преступной деятельности. Особенно активно в указанных целях используется социальная инженерия в отношении владельцев банковских карт и иных электронных продуктов банковской сферы.

Использование отдельных компьютерно-технических технологий, позволяющих эффективно скрывать преступную деятельность, обеспечивают возможность совершения преступлений с использованием информационно-коммуникационных технологий. В этой сфере активно используются технологии зашифровки данных абонентов, такие как анонимные прокси-серверы, VPN, временные учетные записи, виртуальные дебетовые карты и иные подобные технологии. Однако, наиболее до использования скрытых ресурсов и анонимных сетей (Darknet, TOR (The Onion Router) и т.п.).

[1] Председатель Следственного комитета России провел оперативное совещание. URL: https://sledcom.ru/news/item/1814874/ (дата обращения: 02.04.2024).

Следует отметить, что рассматривать каждое конкретное внешнее условие обстановки преступлений с использованием информационно-коммуникационных технологий в отрыве от других будет неправильно. Как правило, при совершении преступлений рассматриваемого вида на другие элементы криминалистической характеристики оказывает влияние весь комплекс или сочетание нескольких внешних условий обстановки, что и способствует выбору только конкретных и определенных особенностей совершения преступлений (конкретный способ совершения, орудия и средства, место, время, личностные характеристики и др.).

Разработка практических рекомендаций[1] по раскрытию, расследованию и предупреждению преступлений с использованием информационно-коммуникационных технологий, должна основываться на учете данных об обстановке преступлений рассматриваемого вида, которые корреляционно зависят от остальных элементов и также взаимозависимо влияют друг на друга. В целях создания эффективных средств противодействия преступлениям такого вида должен реализовываться комплексный подход[2], рассмотрения и описания, как внешних условий обстановки рассматриваемого вида преступлений, внутренних условий, а также характер и свойства других элементов криминалистической характеристики преступлений с использованием информационно-коммуникационных технологий.

[1] Технико-криминалистическое обеспечение расследования преступлений: учебное наглядное пособие / И.Н. Озеров, С.А. Пичугин, Э.С. Сарыгина [и др.]. Москва: Московская академия Следственного комитета Российской Федерации, 2023. 202 с.

[2] См., например: Белавин А.В., Савина Л.А. Проблемы использования цифровой информации в доказывании // Актуальные вопросы производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства: Всероссийская научно-практическая конференция. Сборник научных трудов, Москва, 07 апреля 2023 года / Сост. Д.А. Иванов. М.: Московский университет МВД России им. В.Я. Кикотя, 2023. С. 39–42; Савина Л.А., Евтюхова Е.В. Использование компьютерных следов в процессе доказывания // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы (к 20-летию образования Московского университета МВД России имени В.Я. Кикотя): сборник научных трудов Международного форума, Москва, 25 марта 2022 г. / Сост. В.В. Бушуев. М.: Московский университет МВД России им. В.Я. Кикотя, 2022. С. 274–277; и др.

А.Д. Яким

Нейронная сеть как инструмент совершения преступлений

Аннотация. В статье приведены примеры использования нейронной сети для совершения преступлений. Обозначены новые разработки в сфере использования искусственного интеллекта и нейросетей, функционал которых способен причинить ущерб обществу и отдельным лицам.

Ключевые слова: нейронные сети, преступления, искусственный интеллект, информационно-телекоммуникационные технологии.

В последние годы возможности, доступность и широкое внедрение технологий, основанных на искусственном интеллекте (далее – ИИ) и машинном обучении, резко возросли, и их рост не показывает признаков замедления. Особенно заметные технологии искусственного интеллекта, отраженные в «персональных помощниках», таких как Amazon Alexa, Apple Siri и Yandex Alisa, основанные на обучении, используются гражданами все чаще, так как дают возможности биометрической идентификации, определения маршрута, языкового перевода, управления производственными процессами и логистикой и многого другого. Так искусственный интеллект насыщает современный взаимосвязанный мир на многих уровнях и становится неотъемлемой частью жизни каждого человека. Современный ИИ, основанный на нейросетях, включает как системы предупреждения и раскрытия преступлений, так и технологии, которые могут быть использованы не по назначению для осуществления преступной деятельности.

По мере расширения возможностей и внедрения технологий искусственного интеллекта растут риски его преступной эксплуатации. Возможности для совершения преступлений с использованием ИИ существуют как в конкретной вычислительной области (пересекающейся с традиционными представлениями о кибербезопасности), так и в иных сферах человеческой деятельности. Некоторые из этих угроз возникают как продолжение существующей преступной деятельности, в то время как другие могут быть новыми. Современные угрозы применения нейросетей в преступных целях могут быть классифицированы по категориям в соответствии с взаимосвязью между преступностью и искусственным интеллектом: взлом устройств, защищенных функцией распознавания лиц; взлом криптографической защиты; мошеннические операции на финансовых рынках; совершения шантажа людей фальшивым видео (дипфейки); генерация поддельного контента для различных целей; состязательные помехи (для сокрытия запрещенных материалов от автоматического обнаружения).

В последнее время был предпринят ряд усилий по выявлению и классификации потенциальных угроз, связанных с преступлениями с помощью нейронной сети. Однако оказалось, что нельзя ожидать появления единого набора «правильных» ответов, и существование каждого из них следует рассматривать как дополнение к другим, а не как уменьшение их полезности.

Исследования показывают, что в современных условиях можно выделить три ключевых источника нейроугроз: взлом данных, дипфейки и персонализация фишинга. Количество нейросервисов для обработки и генерации фото и видео возросло. Нейросети для генеративного заполнения добавили в свои продукты многие крупные компании, такие как Adobe, Microsoft, Yandex.

За прошедший год нейропреступления с использованием технологии подмены лиц совершались и в России. Так, компания по производству цемента столкнулась с попыткой рейдерского захвата: мошенники нашли номинала-«инвестора» и от его имени общались с журналистами, используя дипфейк-технологию. Грамотными действиями компании удалось предотвратить атаку[1].

В связи со сложившейся ситуацией эксперты «Лаборатории Касперского» выпустили отчет: специалисты по безопасности проанализировали черный рынок дипфейков для атак на людей и организации. По их данным, стоимость минуты поддельного видео варьируется от 20 тыс. до 300 тыс. долларов. Основной рынок таких незаконных услуг – деструктивный контент, фейковые стримы от лица знаменитостей ради вымогательства денег[2].

Состязательные помехи (например, используемые для сокрытия запрещенных материалов от автоматического обнаружения) являются одним из возможных путей использования нейросетей в преступных целях. Однако эффективность борьбы с данной технологией в настоящее время достаточно низкая, поскольку сущность и природа данного вида преступления недостаточно определены.

Поддельные обзоры, созданные искусственным интеллектом, представляют собой автоматическую генерацию контента для таких сайтов, как Amazon или TripAdvisor, для создания ложного впечатления о продукте или услуге и привлечения клиентов либо к ним, либо от них в другую сторону. Такая подделка уже выполняется людьми, однако искусственный интеллект может повысить эффективность данной технологии, но прибыль и вред от отдельных инцидентов такого рода, скорее всего, останутся локализованными[3].

С помощью искусственного интеллекта создается навигационная сеть личности, состоящая в использовании обучающих систем для мониторинга местоположения и активности человека с помощью социальных сетей или данных личного устройства. Названное действие охватывает и другие преступления, связанные с отношениями по принуждению, домашним насилием, газлайтингом и т.д. Все это связано с текущими новостями о соучастии западных технологических компаний в предоставлении приложений для обеспечения соблюдения социальных норм в репрессивных обществах[4]. Ущерб для общества

от данного вида использования нейросетей представляется достаточно низким не потому, что эти преступления не наносят особого ущерба, а потому, что они по своей сути нацелены на отдельных людей и не имеют значимых последствий для масштабов общества в целом.

Таким образом, можно сделать вывод о существенном развитии технологий нейросетей и возможности их использования в преступных целях.

Список литературы

1. Нейросети превращаются в преступников. URL: https://rspectr.com/articles/nejroseti-prevrashhayutsya-v-prestupnikov?ysclid=lxhmn1h664538752176 (дата обращения: 17.06.2024).
2. Bonettini, N., Güera, D., Bondi, L., Bestagini, P., Delp, E.J. & Tubaro, S. (2019) Image anonymization detection with deep handcrafted features. Conference: *IEEE International Conference on Image Processing* (ICIP), Sept. 2019. DOI:10.1109/ICIP.2019.8804294.
3. Caldwell, M., Andrews, J. T. A., Tanay, T. & Griffin, L.D. (2020) AI‑enabled future crime. *Crime Science,* 9:14. DOI: 10.1186/s40163-020-00123-8.
4. Hubbard, B. (2019) Apple and Google urged to dump Saudi app that lets men track women. *New York Times.* Feb. 13, 2019. URL: www.nytimes.com/2019/02/13/world/middleeast/saudi-arabia-app-women.html (дата обращения 16.05.2024 г.).

Сведения об авторах

Алиев Алибек Ибрагимович – магистрант факультета подготовки криминалистов Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева.

Антропов Алексей Николаевич – магистрант факультета подготовки криминалистов Московской академии Следственного комитета Российской Федерации имени А.Я. Сухарева.

Бардачевский Руслан Игоревич – следователь по особо важным делам отделения по расследованию киберпреступлений и преступлений в сфере высоких технологий третьего следственного управления (с дислокацией в г. Нижний Новгород) Главного следственного управления Следственного комитета Российской Федерации, кандидат юридических наук, подполковник юстиции.

Гапанович Александр Михайлович – старший преподаватель кафедры управления органами предварительного следствия учреждения образования Института повышения квалификации и переподготовки Следственного комитета Республики Беларусь, подполковник юстиции.

Киселёв Максим Борисович – руководитель аналитического отдела организационно-статистического управления Главного следственного управления Следственного комитета Российской Федерации, аспирант Московской академии Следственного комитета имени А.Я. Сухарева, полковник юстиции.

Коимшиди Георгий Феофилактович – ведущий научный сотрудник ВНИИ МВД России, кандидат технических наук, доцент.

Коновалов Илья Борисович – прокурор Научно-методического центра цифровой криминалистики Правоохранительной академии Республики Узбекистан, советник юстиции, советник юстиции.

Коцюба Вероника Денисовна – специалист-эксперт управления международных связей Федеральной службы по финансовому мониторингу.

Кубасов Игорь Анатольевич – профессор кафедры информационных технологий Академии управления МВД России, доктор технических наук, доцент, почетный радист РФ, полковник внутренней службы в отставке.

Любавский Алексей Юрьевич – доцент кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева, кандидат технических наук, подполковник юстиции.

Меджевитдин Павел Валерьевич – руководитель отдела компьютерно-технических исследований Судебно-экспертного центра Следственного комитета Российской Федерации.

Озеров Игорь Николаевич – заведующий кафедрой судебно-экспертной и оперативно-разыскной деятельности факультета подготовки криминалистов Московской академии Следственного Комитета Российской

Федерации имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Озеров Кирилл Игоревич – доцент Межрегионального открытого социального института, кандидат юридических наук.

Побегайло Анастасия Эдуардовна – доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, кандидат юридических наук, советник юстиции.

Поляков Игорь Сергеевич – следователь по особо важным делам отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий управления по расследованию отдельных видов преступлений Главного следственного управления Следственного комитета Российской Федерации, майор юстиции.

Рыжиков Денис Александрович – старший преподаватель кафедры информационных технологий Академии управления МВД России, кандидат юридических наук, подполковник полиции.

Сааков Тигран Артемович – старший преподаватель кафедры судебно-экспертной и оперативно-розыскной деятельности Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, старший лейтенант юстиции.

Садыков Мухтар Бейбутович – докторант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, магистр юриспруденции, магистр государственного управления, младший советник юстиции.

Саркисян Армен Жораевич – декан факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент.

Сиделёва Елена Николаевна — инспектор научно-исследовательского Института Главного управления криминалистики (Криминалистического центра Следственного комитета Российской Федерации), полковник юстиции.

Скобелин Сергей Юрьевич – доцент кафедры информационных технологий и организации расследования киберпреступлений факультета подготовки криминалистов Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Соколова Марина Владимировна – доцент кафедры предварительного расследования Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, майор полиции.

Хатов Эдуард Борисович – заведующий кафедрой информационных технологий и организации расследования киберпреступлений факультета подготовки криминалистов Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Чернопёров Алексей Александрович – старший преподаватель кафедры информационных технологий и организации расследования

киберпреступлений Санкт-Петербургской академии Следственного комитета, полковник юстиции.

Шубина Ксения Сергеевна – преподаватель кафедры противодействия преступлениям в сфере информационно-телекоммуникационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, старший лейтенант полиции.

Шурухнов Владимир Александрович – заведующий кафедрой криминалистики факультета подготовки криминалистов Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции.

Яким Алина Дмитриевна – ассистент кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева, лейтенант юстиции.

СОДЕРЖАНИЕ

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

материалы II Международной научно-практической конференции

(Москва,26 апреля 2024 года)

Подписано в печать: 03.10.2024
Формат 60х90 1/16
Усл. печ. л. 9,27
Тираж 100 экз.
Печать офсетная
Компьютерная верстка,
техническое редактирование – И.Д. Нестерова
Печать – Р.В. Гришин

Заказ № 482

Отпечатано в типографии Московской академии
Следственного комитета имени А.Я Сухарева,
ул. Врубеля, д. 12