Научная статья
УДК 343.1, 343.98

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Волченко Анастасия Владимировна[1], Лакеева Екатерина Витальевна[2], Когтева Анна Николаевна[3]

[1,2]Белгородский юридический институт МВД России имени И. Д. Путилина, Белгород, Россия

[3]Финансовый Университет при правительстве РФ, Москва, Россия

[1]espy207@yandex.ru
[2]ms.volnyagina@mail.ru
[3]annelya1@yandex.ru

Аннотация. В статье анализируются статистические данные, которые указывают на высокий рост преступлений, предусмотренных статьёй 272 Уголовного кодекса Российской Федерации; также авторы рассматривают некоторые существующие способы неправомерного доступа к компьютерной информации. Предлагается алгоритм процессуальных и следственных действий, которые должны проводить органы предварительного расследования для выявления и раскрытия преступлений, связанных с неправомерным доступом к компьютерной информации в том числе на примере взлома портала федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)». Авторы приходят к выводам, которые будут способствовать увеличению раскрываемости преступлений, предусмотренных статьёй 272 УК РФ.

Ключевые слова: неправомерный доступ, компьютерная информация, Госуслуги, фишинг, вредоносная программа, брутфорс-атаки, инсайдерские угрозы, SIM-свопинг, IP-адрес, MAC-адрес, логи-авторизации.

Для цитирования: Волченко А. В., Лакеева Е. В., Когтева А. Н. Расследование преступлений, связанных с неправомерным доступом к компьютерной информации // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2025. № 2(103). С. 182–190.

ON THE QUESTION OF INVESTIGATION OF CRIMINAL CRIMES RELATED TO ILLEGAL ACCESS TO COMPUTER INFORMATION USING

Anastasiya V. Volchenko[1], Ekaterina V. Lakeeva[2], Anna N. Kogteva[3]

[1,2]Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin, Belgorod, Russia

[3]Financial University under the Government of the Russian Federation, Moscow, Russia

[1]espy207@yandex.ru
[2]ms.volnyagina@mail.ru
[3]annelya1@yandex.ru

Annotation. The article analyses statistical data, which indicate a high growth of crimes under Art. 272 of the Criminal Code of the Russian Federation. 272 of the criminal code of the russian federation. Among other things, the authors consider some existing methods of unlawful access to computer information. The authors propose an algorithm

of procedural and investigative actions to be carried out by preliminary investigation bodies to identify and solve crimes related to unlawful access to computer information, including the example of hacking the portal of the federal state information system 'Unified Portal of State and Municipal Services (Functions)'. The authors come to conclusions that will contribute to an increase in the disclosure of offences under Art. 272 of the criminal code of the russian federation.

Keywords: unlawful access, computer information, Public Services, phishing, malware, bruteforce attacks, insider threats, SIM-swapping, IP address, MAC address, logging authorisations.

For citation: Volchenko A. V., Lakeeva E. V., Kogteva A. N. On the issue of investigating crimes related to unauthorized access to computer information using // Scientific Bulletin of the Orel Law Institute of the Ministry of the Interior of the Russian Federation named after V.V. Lukyanov. 2025. № 2(103). P. 182–190.

Ежедневно мы видим, как растёт цифровизация общества, новые технологии внедряются во все сферы жизнедеятельности. Данные изменения указывают как на положительные стороны, так и на отрицательные, которые связаны с новыми видами и способами совершения преступлений. Одним из видов таких преступлений является неправомерный доступ к компьютерной информации, наказание за которое предусмотрено ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ)[1]. Статистические данные за последние три года говорят о значительном росте рассматриваемого вида преступлений, а также о низком проценте раскрываемости. Так, за период времени с января по декабрь 2024 года зарегистрировано 105 311 преступлений, из которых раскрыто 2 959, что составляет лишь 3 % раскрываемости[2]; с января по декабрь 2023 года зарегистрировано 36 788, из которых раскрыто 1 552, что составило 20 % раскрываемости[3]; а с января по декабрь 2022 года зарегистрировано 9 308, из которых раскрыто 1 293, что составило 0,5 % раскрываемости[4]. Анализ статистических данных говорит о том, что требуются новые меры и способы предупреждения, выявления и расследования данного вида преступлений.

Неправомерный доступ к компьютерной информации может осуществляться несколькими способами, которые мы проанализировали ниже.

1. Фишинг. Самый распространённый способ, который направлен на создание злоумышленниками поддельных сайтов или писем для кражи логинов, паролей и платёжных данных[5]. Примером может служить создание фейковой страницы входа на Госуслуги, с помощью которой злоумышленники собирали данные граждан, затем оформляли на них микрозаймы[6].

[1] Уголовный кодекс Рос. Федерации [Электронный ресурс]: Федер. закон Рос. Федерации от 13 июня 1996 № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
[2] Состояния преступности в России за январь - декабрь 2024 года [Электронный ресурс]. URL: http: //xn--b1aew.xn--p1ai/reports/item/60248328/ (дата обращения: 30.03.2025).
[3] Состояния преступности в России за январь - декабрь 2023 года [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/47055751/ (дата обращения: 30.03.2025).
[4] Состояния преступности в России за январь - декабрь 2022 года [Электронный ресурс]. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 30.03.2025).
[5] Что такое фишинг: как не стать жертвой хакеров // РБКТренды [Электронный ресурс]. URL:https://trends.rbc.ru/trends/industry/602e9fe79a7947a4bd611504 (дата обращения: 01.04.2025).
[6] Мошенники придумали новую схему для кражи аккаунтов с «Госуслуг» [Электронный ресурс]. URL: https://rg.ru/2024/12/23/moshenniki-pridumali-novuiu-shemu-dlia-krazhi-akkauntov-s gosuslug.html?utm_referrer=https%3A%2F%2Fwww.google.com%2F (дата обращения: 01.04.2025).

2. Вредоносная программа. Направлена на распространение вирусов, троянов, шифровальщиков, которые крадут или блокируют данные[1]. В 2023 году троян заразил более 500 устройств в РФ, похитив доступ к мобильным банкам[2].

3. Брутфорс-атаки. Осуществляются путём автоматического подбора паролей к аккаунтам почты, социальных сетей, Госуслуг[3].

4. Инсайдерские угрозы. Совершаются путём кражи данных сотрудниками компаний и госорганов[4]. Так, к примеру, в 2024 году менеджер продаж салона сотовой связи осуществил несанкционированный доступ к карточкам абонентов в информационно-биллинговой системе компании, что причинило вред компании как субъекту критической информационной инфраструктуры РФ в виде нарушения безопасности информации и разглашения конфиденциальных сведений об абонентах[5].

5. SIM-свопинг (перехват СМС). Правонарушители переоформляют сим-карту потерпевшего на себя, чтобы получать коды подтверждения[6].

Официальная статистика, связанная с конкретным способом совершения неправомерного доступа к компьютерной информации, отсутствует, однако, изучив различные интернет-ресурсы, а также ссылаясь на решение коллегии МВД РФ, согласимся о необходимости противодействия неправомерному доступу к личным кабинетам граждан портала Госуслуг[7]. Преступления данной направленности несут широкий общественный резонанс и наносят значительный ущерб пострадавшим.

В связи с вышесказанным считаем необходимым рассмотреть проблемные аспекты выявления и расследования преступлений, связанных с неправомерным доступом к компьютерной информации путём взлома портала Госуслуг.

Единый портал государственных и муниципальных услуг (далее – ЕПГУ) – это федеральная информационная система, где граждане, организации и индивидуальные предприниматели могут оформить документы, получить выписки и справки в электронном виде, найти юридически значимую информацию и т. д. Рассмотрим более детально, к какой информации может быть получен неправомерный доступ на Госуслугах. Согласно информации портала основными целями злоумышленников при неправомерном доступе к учётным записям граждан являются: оформление кредита или микрозайма; подача заявки на кредит; вход в онлайн-банк через Госуслуги; запрос справки 2-НДФЛ для одобрения кредита; оформление электронной сим-карты на имя пострадавшего и использование её для других мошеннических схем; продажа информации о пострадавшем: адрес, СНИЛС, данные паспорта и других документов,

---

[1] Вредоносная программа // Tadvicer Государство. Бизнес. Технологии [Электронный ресурс].URL: https://www.tadviser.ru/index.php/Статья:Вредоносная_программа_(зловред) (дата обращения: 01.04.2025).

[2] Трояны // Tadvicer Государство. Бизнес. Технологии [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Трояны (дата обращения: 01.04.2025).

[3] Брутфорс-атака: определение, примеры, защита [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/definitions/brute-force-attack (дата обращения: 01.04.2025).

[4] Как обнаружить и предотвратить внутренние угрозы [Электронный ресурс]. URL: http://www.sberbank.ru/ru/person/kibrary/articles/kak-obnaruzhit-i-predotvratit-vnutrennie-ugrozy (дата обращения: 01.04.2025).

[5] Менеджер салона сотовой связи незаконно торговал личными данными абонентов в Белгородской области [Электронный ресурс]. URL: https://openbelgorod.ru/news/kriminal/2024-02-09/menedzher-salona-sotovoy-svyazi-nezakonno-torgoval-lichnymi-dannymi-abonentov-v-belgorodskoy-oblasti-371589 (дата обращения: 01.04.2025).

[6] О новых способах мошенничества и стоимости клиентских данных на черном рынке [Электронный ресурс]. URL: https://www.cbr.ru/press/event/?id=8115# highlight=карту (дата обращения: 01.04.2025).

[7] О мерах, принимаемых органами внутренних дел Российской Федерации по борьбе с преступлениями, совершенными с использованием информационно-коммуникационных технологий [Электронный ресурс]: решение коллегии МВД России от 4 июня 2024 г. № 2 км. Документ опубликован не был. Доступ из справ.- правовой системы «ГАРАНТ».

номера счетов; получение информации о конкретном лице с целью обмана его близких; получение налогового вычета за лицо, чей аккаунт был взломан[1].

Прежде всего отметим, что расследование неправомерного доступа к компьютерной информации сопряжено с рядом сложностей, обусловленных спецификой киберпреступлений, в том числе с разграничением смежного состава преступления, предусмотренного ст. 159.6 УК РФ [1, с. 61]. В том числе мы согласимся с мнением, что основной задачей по расследованию преступлений информационно-телекоммуникационной направленности является идентификация конкретного пользователя, совершившего преступное деяние, и криминалистически значимая информация, представленная в виде электронных данных, не вписывается в классическую криминалистическую теорию механизма следообразования [2, с. 194].

Для возбуждения уголовного дела, предусмотренного ст. 272 УК РФ, требуется установление наличия признаков преступления, а именно: факт несанкционированного доступа, способ доступа (взлом пароля, использование вредноносного ПО и др.), последствий (уничтожение, блокирование, модификацию либо копирование компьютерной информации), в том числе для квалификации важно определить размер ущерба.

Остановимся на последовательности процессуальных и следственных действий, которые должны провести органы предварительного расследования для выявления и раскрытия преступлений, связанных с неправомерным доступом к компьютерной информации на примере взлома портала Госуслуг.

1. Необходимо доказать, был ли осуществлен доступ к информации (вход в систему, который привёл к уничтожению, блокированию, модификации либо копированию компьютерной информации), был ли доступ неправомерным (без разрешения владельца). Данная информация может быть получена следователем в процессе получения объяснения (допроса) потерпевшего в том числе с приобщением соответствующих документов (например, выписка из банка об оформлении кредита онлайн).

2. Определить способ совершения преступления (фишинг, вредоносная программа, брутфорс-атаки, инсайдерские угрозы или др.), каналы связи (через интернет, локальную сеть, физический носитель). Для определения способа необходимо в процессе получения объяснения (допроса) потерпевшего выяснить, приходили ли письма, сообщения с просьбой ввести пароль, был ли осуществлён переход по ссылке, вводил ли потерпевший какие-либо данные; посещал ли потерпевший портал Госуслуг с указанием *URL* адреса сайта и т. п. При этом если будет выявлено, что потерпевший получал какие-либо письма или сообщения, переходил на какие-либо сайты самостоятельно, необходимо провести выемку электронного устройства с последующим его осмотром, а также получение снимков экрана (скриншотов), на которых отображены сообщения, истории запросов в браузере и т. п., и приобщением данной информации к материалам уголовного дела в качестве вещественных доказательств.

Если самостоятельно установить способ не удаётся, назначается компьютерно-техническая судебная экспертиза, которая определяет, был ли установлен вредоносный код, каким образом произошла утечка данных, какие именно данные были получены.

3. Идентификация подозреваемого лица. Для этого необходимо органам предварительного расследования незамедлительно и безошибочно собрать цифровые следы:

[1] Зачем мошенники взламывают учётные записи на Госуслугах [Электронный ресурс]. URL:https://www.gosuslugi.ru/help/faq/personal_data/230820245(дата обращения: 01.04.2025).

– *IP*-адрес (время, дата, провайдер), но учитывать, что он может быть подменён (*VPN, прокси, TOR*). Для установления сведений об *IP*-адресе, подтверждающих неправомерный вход, органы предварительного расследования проводят осмотр места происшествия – личный кабинет портала Госуслуг потерпевшего. Для этого необходимо зайти на сайт «ЕПГУ», перейти во вкладки «профиль», далее – «безопасность», «действия в системе» и произвести выгрузку информации за интересующий период времени с отражением IP-адресов, с которых осуществлялся вход на Госуслуги. Независимо от полученных в личном кабинете сведений об истории посещения необходимо направить запрос в МинЦифры РФ (курирует Госуслуги) или оператору единой системы идентификации и аутентификации (далее – ЕСИА) (ПАО «Ростелеком»), где запросить сведения, подтверждающие неправомерный доступ к личному кабинету, а также об *IP*-адресах, использовавшихся для входа, номерах телефонов и электронных ящиках, указанных для направления уведомлений о посещении ресурса, обо всех сайтах организаций, посещение которых происходило через авторизацию в личном кабинете Госуслуг;

– *MAC*-адрес, если взлом был внутри локальной сети. Для установления *MAC*-адреса корпоративной сети органы предварительного расследования направляют запрос администратору компании для установления *MAC*-адреса публичного *Wi-Fi* (например, кафе, ТЦ) – запрос владельцу точки доступа, для домашнего интернета – провайдеру, но в данном случае обычно *MAC*-адреса нет. Все направляемые запросы должны быть официальными в рамках ч. 4 ст. 21 УПК РФ;

– логи-авторизации Госуслуг – журнал событий входа в систему. Логи-авторизации содержат записи обо всех попытках входа в систему (успешных и неудачных). Важный аспект – это своевременное изъятие, иначе логи-авторизации могут быть перезаписаны или удалены. Для установления логов-авторизации следователь направляет запрос в МинЦифры РФ, оператору ЕСИА или в организацию, ответственную за безопасность портала. После установления логов-авторизации органы предварительного расследования должны провести анализ полученных данных с целью обнаружения подозрительных *IP*-адресов, несанкционированных входов (например, с одного *IP*-адреса было множество попыток входа). Если логи-авторизации были удалены, то их необходимо попытаться восстановить через компьютерно-техническую судебную экспертизу;

– данные устройств (*IMEI* телефона). Если неправомерный доступ был осуществлён при помощи мобильного интернета, органам предварительного расследования необходимо в соответствии со ст. 186.1 УПК РФ обратиться в суд с ходатайством о разрешении предоставления операторами связи информации об *IMEI*-устройстве и других данных, позволяющих идентифицировать абонентов;

– связь с другими преступлениями (например, продажа данных в даркнете).

Кроме того, все получаемые органами предварительного расследования ответы подлежат тщательному анализу, осмотру (при необходимости со специалистом) и приобщению в качестве вещественных доказательств. Также необходимо предпринять иные действия к идентификации подозреваемого лица. Например, если ко взломанному личному кабинету пользователя портала Госуслуг был привязан новый номер телефона, необходимо в рамках ст. 186.1 УПК РФ получить сведения о лице, на чьё имя зарегистрирован номер телефона, о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приёмопередающих базовых станций. Г. Ф. Шипулин верно отметил, что «...для привлечения лица к ответственности по рассматриваемой статье необходимо наличие причинно-

следственной связи между действиями лица и наступившими последствиями» [3, с. 124]. Данную связь возможно установить лишь при сборе всех частей в большом «пазле».

4. Фиксация последствий взлома: какая информация была похищена, изменена, удалена; размер и вид причинённого ущерба (материальный, репутационный и т. д.).

5. Доказательственная база. В качестве доказательств по уголовному делу о неправомерном доступе к компьютерной информации будут выступать:

– показания потерпевшего, в отношении которого был осуществлён неправомерный доступ к компьютерной информации; показания свидетелей (администраторы портала Госуслуг, сотрудники МинЦифры РФ и подведомственных организаций (например, «Ростелеком»), специалисты в области кибербезопасности и др.;

– показания подозреваемого (обвиняемого) в случае его установления.

В том числе согласимся с мнением Бердниковой О. П., которая считает, что вне зависимости от процессуального положения допрашиваемого лица следователю необходимо тщательно подготовиться к его допросу, в том числе при необходимости обратиться за консультацией к оперативным сотрудникам отдела «К» [4, с. 68];

– заключение и показания эксперта и специалиста. Однако стоит учитывать, что квалифицированного специалиста в области кибербезопасности в определённое время и в определённом месте может попросту не оказаться, особенно если речь идёт о небольших и отдалённых населённых пунктах. Полагаем, что данный вопрос необходимо проработать на уровне субъекта (например, областного управления МВД РФ), чтобы каждый следователь из любого муниципального образования при необходимости мог оперативно обратиться к соответствующему специалисту, в том числе допросить его в рамках уголовного дела по интересующим вопросам, например путём использования систем видео-конференц-связи (в порядке ст. 189.1 УПК РФ), т. е. следователь должен знать конкретных специалистов и иметь возможность быстро и продуктивно с ними связаться в интересах предварительно расследования;

– вещественные доказательства, которые можно разделить на физические носители (компьютеры, ноутбуки, серверы, мобильные устройства, внешние носители, роутеры, модемы, сетевые устройства и т. п.) и цифровые следы (IP-адреса, логи-авторизации, снимки и записи экранов, электронные переписки, базы данных и т. п.);

– протоколы следственных и судебных действий;

– иные документы (приказы, должностные инструкции и т. п.).

Вся доказательственная база по рассматриваемой категории уголовных дел должна собираться своевременно, а также в соответствии с требованиями УПК РФ.

Как можно заметить, рассмотренный порядок процессуальных и следственных действий, направленный на расследование уголовного дела, предусмотренного ст. 272 УК РФ, включает сложный алгоритм действий по обнаружению и фиксации цифровых следов. Существует много исследований по вопросам борьбы с киберпреступлениями, в том числе связанных с неправомерным доступом к компьютерной информации.

Нам близки мнения Вехова В. Б. и Пастухова П. С., которые отметили о необходимости создания специализированных групп «...органов предварительного расследования, специализированных органов дознания, специалистов-криминалистов со специалистами из области информационных технологий и смежных отраслей знаний, провайдерами связи, интернет-провайдерами, а также с зарубежными аналогичными и правоохранительными органами» [5, с. 140]. Кроме того, ткакже интересным видится мнение о необходимости использования «...специализированного оборудования для обнаружения и сбора цифровых доказательств» [6, с. 76]. В свете современных реалий интересна точка зрения Володина А. А. и Глинской Е. В., которые

видят решение проблемы информационной безопасности через призму внедрения новейших технологий искусственного интеллекта в информационную безопасность крупных компаний и организаций, что поспособствует оптимизации процессов обеспечения информационной безопасности [7, с. 1].

По нашему мнению, следователь является должностным лицом, уполномоченным осуществлять предварительное следствие, и от его знаний и опыта зависит ход и результат расследования, поэтому базовых навыков для работы с цифровыми следами будет недостаточно.

Действительно, создание специализированных групп может поспособствовать увеличению раскрываемости преступлений данной направленности, однако для этого необходимо увеличение штата должностей и рассмотрения вопроса о сотрудничестве органов предварительного расследования с *IT*-специалистами.

Считаем необходимым систематически повышать профессиональный уровень сотрудников предварительного расследования по направлениям в области кибербезопасности, в том числе обучать выявлению и фиксации цифровых следов. Современный сотрудник, который расследует информационные преступления, в данном случае связанные с неправомерным доступом к компьютерной информации, не должен выполнять лишь цикл определённых действий, он должен уметь установить и идентифицировать цифрового преступника. Мы согласимся с Тимофеевым С. В., который считает, что «работа с цифровыми следами – это составная часть всей борьбы с киберпреступностью» [8, с. 266].

1. Филаненко А. Ю. Отграничения мошенничества в компьютерной информации от неправомерного доступа к компьютерной информации // Право и государство: теория и практика. 2013. № 1(97). С. 59–62.
2. Сретенцев Д. Н. Современные возможности криминалистической идентификации в расследовании преступлений // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4(93). С. 192–197.
3. Шипулин Г. Ф. Объективные признаки преступления, предусмотренного статьей 272 УК РФ // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3(96). С. 119–127.
4. Бердникова О. П. Тактические особенности допросов на первоначальном этапе расследования уголовных дел по мошенничествам в сфере компьютерной информации // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2021. № 1(86). С. 67–72.
5. Вехов В. Б., Пастухов П. С. Преступления в информационном сообществе: совершенствование расследования на основе положений электронной криминалистики // Ex jure. 2018. № 3. С. 134–148.
6. Ростовцев А. В., Берестенко Е.Д. Использование специальных знаний при расследовании преступлений в сфере информационно-телекоммуникационных технологий // Известия ТулГУ. Экономические и юридические науки. 2023. № 4. С. 72–80.
7. Володин А. А., Глинская Е. В. Развитие и проблемы использования искусственного интеллекта в области информационной безопасности // Политехнический молодежный журнал. 2024. № 2. С. 1–13.
8. Тимофеев С. В. Перспективы совершенствования Российского законодательства в области использования цифровых следов преступления // Вестник Восточно-Сибирского института МВД России. 2024. № 4(111). С. 262–277.

1. Filanenko A. Yu. Otgranicheniya moshennichestva v komp`yuternoj informacii ot nepravomernogo dostupa k komp`yuternoj informacii // Pravo i gosudarstvo: teoriya i praktika. 2013. № 1(97). S. 59–62.
2. Sretencev D. N. Sovremenny`e vozmozhnosti kriminalisticheskoj identifikacii v rassledovanii prestuplenij // Nauchny`j vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk`yanova. 2022. № 4(93). S. 192–197.
3. Shipulin G. F. Ob``ektivny`e priznaki prestupleniya, predusmotrennogo stat`ej 272 UK RF // Nauchny`j vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk`yanova. 2023. № 3(96). S. 119–127.
4. Berdnikova O. P. Takticheskie osobennosti doprosov na pervonachal`nom e`tape rassledovaniya ugolovny`x del po moshennichestvam v sfere komp`yuternoj informacii // Nauchny`j vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V.V. Luk`yanova. 2021. № 1(86). S. 67–72.
5. Vexov V. B., Pastuxov P. S. Prestupleniya v informacionnom soobshhestve: sovershenstvovanie rassledovaniya na osnove polozhenij e`lektronnoj kriminalistiki // Ex jure. 2018. № 3. C. 134–148.
6. Rostovcev A. V., Berestenko E.D. Ispol`zovanie special`ny`x znanij pri rassledovanii prestuplenij v sfere informacionno-telekommunikacionny`x texnologij // Izvestiya TulGU. E`konomicheskie i yuridicheskie nauki. 2023. № 4. S. 72–80.
7. Volodin A. A., Glinskaya E. V. Razvitie i problemy` ispol`zovaniya iskusstvennogo intellekta v oblasti informacionnoj bezopasnosti // Politexnicheskij molodezhny`j zhurnal. 2024. № 2. S. 1–13.
8. Timofeev S. V. Perspektivy` sovershenstvovaniya Rossijskogo zakonodatel`stva v oblasti ispol`zovaniya cifrovy`x sledov prestupleniya // Vestnik Vostochno-Sibirskogo instituta MVD Rossii. 2024. № 4(111). S. 262–277.

Информация об авторах

Анастасия Владимировна Волченко. Старший преподаватель кафедры уголовного процесса, кандидат юридических наук.
Белгородский юридический институт МВД России имени И.Д. Путилина.
308024, Россия, г. Белгород, ул. Горького, 71.

Екатерина Витальевна Лакеева. Преподаватель кафедры уголовного процесса.
Белгородский юридический институт МВД России имени И.Д. Путилина.
308024, Россия, г. Белгород, ул. Горького, 71.

Анна Николаевна Когтева. Доцент кафедры информационной безопасности, кандидат экономических наук.
Финансовый Университет при Правительстве РФ.
125167, Россия, г. Москва, Ленинградский пр-т., 49.

Information about the authors

Anastasiya V. Volchenko. Senior Lecturer at the Department of Criminal Procedure. Candidate of Law Sciences.
Putilin Belgorod Law Institute of the Ministry of Internal of Russia.
308024, Russia., Belgorod, Gorkogo Str., 71.

Ekaterina V. Lakeeva. Lecturer at the Department of Criminal Procedure.
Putilin Belgorod Law Institute of the Ministry of Internal of Russia.
308024, Russia., Belgorod, Gorkogo Str., 71.

Anna N. Kogteva. Associate Professor of the Department of Information Security. Candidate of Economic Sciences.
Financial University under the Government of the Russian Federation.
125167, Russia, Moscow, Leningradsky Pr., 49.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Авторами внесён равный вклад в написание статьи.
The authors have made an equal contribution.

Статья поступила в редакцию 10.04.2025; одобрена после рецензирования 22.05.2025; принята к публикации 17.06.2025.
The article was received in the editorial office on 10.04.2025; approved after review on 22.05.2025; accepted for publication on 17.06.2025.