АКТУАЛЬНЫЕ ПРОБЛЕМЫ ГОСУДАРСТВА И ПРАВА
2023. Т. 7. № 3
http://journals.tsutmb.ru/current-issues-of-the-state-and-law/

AKTUAL'NYE PROBLEMY GOSUDARSTVA I PRAVA =
= CURRENT ISSUES OF THE STATE AND LAW
2023, vol. 7, no. 3
http://journals.tsutmb.ru/current-issues-of-the-state-and-law-eng/
ISSN 2587-9340 (Print) ISSN 2782-3334 (Online)

НАУЧНАЯ СТАТЬЯ
УДК 343.9
https://doi.org/10.20310/2587-9340-2023-7-3-370-378
Шифр научной специальности 5.1.4

Особенности криминалистической характеристики преступлений в сфере компьютерной информации

© КИСЕЛЕВ Александр Сергеевич,
кандидат юридических наук, доцент кафедры гражданского права, ФГБОУ ВО «Государственный университет просвещения», Российская Федерация, 105005, г. Москва, ул. Радио, 10А; старший научный сотрудник Центра исследований и экспертиз, ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Российская Федерация, 125993, г. Москва, Ленинградский просп., 49, https://orcid.org/0000-0002-5044-4721, alskiselev@fa.ru
© ГОРБУНОВА Ксения Анатольевна,
делопроизводитель кафедры предпринимательского права, ФГБОУ ВО «Государственный университет просвещения», Российская Федерация, 105005, г. Москва, ул. Радио, 10А, https://orcid.org/0009-0007-7475-6096, gorbynya.rambler.ru@yandex.ru

Аннотация

Цель работы состоит в выявлении основных особенностей криминалистической характеристики преступлений в сфере компьютерной информации, поскольку это имеет огромное значение в современном мире, так как компьютерные преступления становятся все более распространенными и угрожают безопасности информации, объектам критической инфраструктуры, личной жизни и финансов граждан, организаций и всего государства. Проанализирован терминологический аппарат, изучены классификации современных киберпреступников, определены основные подходы к совершению преступлений в сфере компьютерной информации. В исследовании были использованы следующие методы: анализ и синтез, индукция и дедукция, системный метод, диалектический и материалистический методы, формально-юридический метод. Изучение и анализ криминалистической характеристики позволяет определить наиболее распространенные способы совершения подобных преступлений, разработать эффективные меры противодействия. Установлено, что основной сложностью при расследовании данных преступлений является сложный технологический характер и порядок их совершения. Многие преступники постоянно совершенствуют свои навыки, наиболее квалифицированные из них стараются быть осторожными, разрабатывают собственные контрмеры против правоохранительных органов, используя шифры, специальные программы удаленного доступа, чтобы максимально затруднить как сбор доказательств, так и розыскные мероприятия. Помимо прочего, сложность привлечения киберпреступников осложняется в том случае, если злоумышленники находятся в другом государстве, а на международное сотрудничество в сфере правопорядка и общественной безопасности со многими западными странами на сегодняшний день, к сожалению, рассчитывать не приходится.

Ключевые слова

киберпреступления, киберпреступность, компьютерная информация, преступления в сфере компьютерной информации, криминалистика, криминалистическая характеристика

Для цитирования
Киселев А.С., Горбунова К.А. Особенности криминалистической характеристики преступлений в сфере компьютерной информации // Актуальные проблемы государства и права. 2023. Т. 7. № 3. С. 370-378. https://doi.org/10.20310/2587-9340-2023-7-3-370-378

ORIGINAL ARTICLE
https://doi.org/10.20310/2587-9340-2023-7-3-370-378

Crimes' forensic characteristics features in the computer information field

© Alexander S. KISELEV,
PhD (Law), Associate Professor of Civil Law Department, State University of Education, 10A Radio St., Moscow, 105005, Russian Federation; Senior Research Scholar of Research and Expertise Center, Financial University under the Government of the Russian Federation, 49 Leningradsky Ave., Moscow, 125993, Russian Federation, https://orcid.org/0000-0002-5044-4721, alskiselev@fa.ru
© Ksenia A. GORBUNOVA,
Filing Clerk of Entrepreneurial Law Department, Management and Law, State University of Education, 10A Radio St., Moscow, 105005, Russian Federation, https://orcid.org/0009-0007-7475-6096, gorbynya.rambler.ru@yandex.ru

Abstract
The purpose of the research is to identify the main crimes' forensic characteristics features in the computer information field, inasmuch it makes a great importance in the modern world, as computer crimes are becoming more widespread and threaten the information security, critical infrastructure, personal life and citizens' finances, organizations and the entire state. The terminological apparatus is analyzed, the classifications of modern cybercriminals are studied, the main approaches to the commission of crimes in the field of computer information are determined. The following methods are used in the research: analysis and synthesis, induction and deduction, system method, dialectical and materialistic methods, formal legal method. The study and analysis of the forensic characteristics allows us to determine the most common ways of committing such crimes, to develop effective counteraction measures. It is established that the main difficulty in the investigation of these crimes is the complex technological nature and the order of their commission. Many criminals are constantly improving their skills, the most qualified of them try to be careful, develop their own countermeasures against law enforcement agencies, using ciphers, special remote access programs to make it as difficult as possible to collect evidence and search activities. Among other things, the difficulty of cybercriminals holding liable is complicated if intruders are located in another state, and unfortunately, one cannot count on international cooperation in the field of law and order and public security with many Western countries today.

Keywords
cybercrime, cybercriminality, computer information, crimes in the computer information field, forensic, forensic characteristics

For citation
Kiselev, A.S., & Gorbunova, K.A. (2023). Crimes' forensic characteristics features in the computer information field. *Aktual'nye problemy gosudarstva i prava = Current Issues of the State and Law*, vol. 7, no. 3, pp. 370-378 (In Russ., abstract in Eng.) https://doi.org/10.20310/2587-9340-2023-7-3-370-378

Введение. Постановка проблемы

Сегодня наше общество живет в период, когда человечество находится на границе новой научно-технической революции, где основными движущими силами являются достижения микроэлектроники, информатики, биотехнологии, генной инженерии, новых видов энергии, материалов, освоения космического пространства, спутниковой связи и т. п. Очевидно, главенствующим фактором всех этих изменений стало развитие информационных технологий, создание на их основе компьютерной техники, сетей и их активное проникновение во все сферы

человеческой жизни. К сожалению, технологический прогресс позволяет правонарушителям использовать новые информационно-коммуникационные технологии с целью совершения противоправных деяний, совершенствовать методы организации преступной деятельности. Именно поэтому при проведении криминалистической характеристика преступлений в сфере компьютерной информации следует учитывать тип личности современных киберпреступников, понимать всю цепочку преступных действий в сети Интернет, что позволит установить причинно-следственные связи, добыть электронные (цифровые) доказательства, разыскать подозреваемого и привлечь к ответственности.

В российской и зарубежной литературе сегодня появляется немало научных работ, посвященных искомой тематике, выделим некоторые из них: А.А. Файзуллина в своих трудах в целом исследует криминалистическую характеристику преступлений в условиях вызовов современного мира; работы С.А. Григорян, Ю.В. Белевитиной и Н.В. Мартыновой акцентируются вокруг личности киберпреступника, его основных психологических характеристик. Отдельно стоит отметить монографическое исследование М.В. Жижиной и Д.В. Завьяловой, посвященное особенностям расследования киберпреступлений в России и за рубежом. Иностранные исследователи Ж.Л. Рише, Ю. С. Чанг и П. Грабоски обращают особое внимание на совершенствование процессов расследования киберпреступлений, создание безопасного киберпространства [1–2]. В целом, бесспорно, что внимание отечественных и зарубежных юристов-теоретиков, криминалистов-практиков приковано к проблемным вопросам характеристики и расследования преступлений в сфере компьютерной информации.

Результаты исследования

1. О подходах к толкованию термина «киберпространство». Е.П. Ищенко высказывает тезис о том, что «отличительная черта нашего времени – это окончательное стирание границ и различий между реальностью и виртуальностью, между миром вещей и миром информации, между деятельностью онлайн и офлайн, между социальной средой и киберсредой» [3, с. 377]. Вне всякого сомнения, с активным развитием информационных технологий жизнь человека претерпела колоссальные изменения.

Примечательно, что появление словосочетания «кибернетическое пространство» связано далеко не с наукой, впервые этот термин употребил в 1982 г. Уильям Гибсон в своем научно-фантастическом произведении [4, p. 30]. Под киберпространством У. Гибсоном понималась виртуальная среда, существующая внутри компьютерных сетей, с которой может взаимодействовать человек. Писатель поднимал многие социальные, психологические и философские вопросы существования человека в условиях высоких технологий, многие из которых актуальны до сих пор и изучаются научным сообществом. Несмотря на то, что в наши дни общепринятое определение киберпространства отсутствует, его, тем не менее, активно используют в юридической и криминалистической литературе как интуитивно понятное. Это произошло во многом благодаря фантастическим романам, образам в поп-культуре, и самое главное – идеям, которые активно распространялись учеными различных областей.

Например, в теории оперативно-розыскной деятельности принято рассматривать киберпространство как виртуальную среду реализации общественных отношений, которая связывает информационное и физическое пространство и образуется в результате сложных взаимодействий пользователей сети Интернет посредством информационных ресурсов.

Киберпространство – это термин, который обозначает совокупность информационных технологий, сетей и Интернета. Это виртуальное пространство, которое создается и развивается посредством инструментария информационных технологий путем взаимодействия участников этого пространства. В киберпространстве существуют различные виды информации, обмен которой между пользователями происходит в реальном времени. В киберпространстве возможно как сотрудничество, так и конкуренция между участниками, оно затрагивает все аспекты нашей жизни от экономики и политики до культуры и развлечений.

2. Об элементах криминалистической характеристики преступлений в сфере компьютерной информации. По мнению А.А. Файзуллиной, «криминалистическую характеристику следует рассматривать в качестве информационной модели, представляющей описание существенных признаков противоправного деяния, важных с точки зрения его раскрытия и расследования» [5, с. 141].

Криминалистическая характеристика преступлений в сфере компьютерной информации включает в себя следующие элементы: личность и мотивацию преступника, место, время и способ совершения преступления. Стоит обратить внимание, что одной из главных особенностей является техническая составляющая данного вида преступления.

Вполне очевидно, что личность преступника является основным элементом в криминалистической характеристике преступлений в сфере компьютерной информации. Существует некое общепринятое представление, отождествляющее киберпреступника с хакером – молодой гений в области компьютерных технологий, способный проникнуть в информационную сеть преступным путем.

Такие авторы, как С.А. Григорян, Ю.В. Белевитина, Н.В. Мартынова и многие другие представляют свои собственные классификации личности киберпреступников, в качестве критериев выделяя их опыт и навыки, технические устройства, которыми они оперируют, степень общественно опасных последствий, цели и мотивы [6–8]. Это наталкивает на мысль, что единую классификацию киберпреступников создать в принципе не представляется возможным, вполне вероятно в большей степени из-за того, что ежедневно возникают новые технологии, которые открывают возможности как обычным пользователям, так и лицам, которые могут использовать эти технологии в противоправных целях.

Изучение личности киберпреступника является актуальным ввиду значительной компьютеризации общественных отношений [9, с. 115]. По уровню навыков и умений киберпреступников разделяют на следующие группы: «с разным уровнем развития навыков в сфере информационных технологий, которые не ведут систематическую преступную деятельность; без развитых навыков в сфере информационных технологий или со средним их уровнем, которые ведут систематическую преступную деятельность, часто состоят в преступных группировках; с высоким уровнем навыков в сфере информационных технологий, которые ведут систематическую преступную деятельность» [10, с. 28].

Ученые исследуют и выделяют отдельные группы киберпреступников в зависимости от их целей и мотивов:

1) фрикеры – лица, которые нацелены на незаконное получение доступа к различным информационным системам, сайтам, аккаунтам, могут выполнять чей-то заказ или заниматься взломом ради развлечения и совершенствования своих навыков;

2) кибертеррористы – одни из наиболее опасных киберпреступников, используют кибератаки для дестабилизации и повреждения объектов национальной безопасности, например, государственных организаций и критической инфраструктуры [11, с. 57];

3) крэкеры – проникают в компьютерные системы несанкционированно, используя программное обеспечение, которое позволяет им осуществлять такое вторжение [10, с. 30-31];

4) вирусмэйкеры или вредоносщики – создают вредоносные компьютерные программы, такие как вирусы, троянские программы и т. д. Они используют эти программы для получения доступа к информации или для порчи информационной системы, помимо этого могут продавать свои «продукты» другим людям в даркнете;

5) фишеры или фишингеры – занимаются мошенническими действиями с использованием электронной почты, социальных сетей и других средств коммуникации [12, с. 139]. Их цель – получить доступ к личной информации и деньгам жертв, убеждая их предоставить свои данные;

6) кардеры – осуществляют кражи финансовых данных с помощью взлома банковских систем и интернет-магазинов. Они могут получать доступ к банковским счетам, номерам кредитных карт и другим платежным данным;

7) бот-мастера – используют ботнеты (группы зараженных компьютеров) для проведения кибератак. Они могут получить дос-

туп к компьютерам других людей и использовать эти сети для распространения вредоносного ПО, атак на сайты и т. д.

Далее рассмотрим способ совершения преступления в сфере компьютерной информации. В.Б. Вехов указывает, что «под способом совершения преступления в криминалистике обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, который оставляет различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления» [13, с. 12-13].

В свое время, когда компьютеры только начинали появляться и существовали обособленно, они, как правило, располагались в крупных научных, государственных и коммерческих организациях. Хакерам было непросто воздействовать на объекты, которые не имеют доступа в Интернет. Но в настоящее время преступления в сфере компьютерной информации уже вышли за пределы виртуального мира. Некоторые вирусы могут не просто воздействовать на информационные системы, а непосредственно влиять на наш материальный мир.

По мнению некоторых ученых, «компьютерный вирус Stuxnet (The Stuxnet Warm) был разработан в первом десятилетие XXI века для атаки на ядерную промышленность Ирана и представляет собой вредоносное программное обеспечение, изначально созданное для промышленных систем управления или группы аналогичных систем, используемых, например, в электростанциях или в газопроводах» [14, с. 721]. Он был обнаружен в июне 2010 г. и вызвал широкий интерес у общественности и СМИ в связи с тем, что его разработка и использование были связаны с государственными структурами США и Израиля.

Вирус Stuxnet был специально создан для внедрения в контроллеры Siemens, которые используются на ядерных заводах Ирана. Его целью было изменение режимов работы оборудования и осуществление направленных операций, что должно было привести к серьезным повреждениям или поломкам оборудования. Предполагается, что целью атаки было замедлить или остановить программу ядерной энергетики Ирана. Вирус Stuxnet был чрезвычайно сложен, требовал значительной экспертизы целей воздействия для его создания. Он использовал несколько уязвимых мест в операционной системе Windows, которые были неизвестны тогда еще разработчикам антивирусного и защитного ПО (далее – ПО). Stuxnet сыграл важную роль в истории компьютерной безопасности, так как показал, насколько сильно может быть опасен компьютерный вирус, особенно если он используется для реализации политических целей.

В целом, сложно привести исчерпывающий список способов совершения компьютерных преступления, поскольку их содержимое может включать самые разнообразные действия, в зависимости от изобретательности, технического обеспечения, мотива, интеллектуальных способностей преступника и преступной «квалификации». Некоторые из них включают:

1) создание вирусов и вредоносного ПО: злоумышленники могут разработать и распространять вредоносные программы, такие как вирусы, черви, трояны и шпионское ПО, которые могут захватывать контроль над компьютерами пользователей;
2) фишинг и социальную инженерию;
3) взлом сетей;
4) кражу личных данных;
5) кибершпионаж;
6) кибертерроризм (атаку на критическую информационную инфраструктуру или захват компьютерных систем).

С развитием технологий и Интернета появляются новые угрозы, и злоумышленники постоянно совершенствуют свои методы. Как отмечают специалисты, «к современным способам несанкционированного доступа к компьютерной информации, хранящейся на смартфоне, можно отнести, например, изготовление «искусственных» отпечатков пальцев для аутентификации в системе смартфона. Программные способы совершения преступлений в сфере компьютерной информации включают в себя как

создание, распространение и эксплуатацию вредоносного программного обеспечения, так и модификацию узаконенного ПО и даже прямое использование такого ПО в случае, если оно удовлетворяет требованиям злоумышленника и способствует реализации его замысла» [10, с. 33].

Согласно статье 273 УК РФ, вредоносные программы представляют собой компьютерную информацию или компьютерную программу, способную нелегально удалить, заблокировать, изменить или украсть цифровую информацию или нейтрализовать средства защиты компьютерной информации.

Приведем пример из судебной практики. Так, приговором Павловского районного суда (Воронежская область) установлено, что у г-н К. возник умысел, направленный на использование вредоносной компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации.

В соответствии со статьей 73 УПК РФ в процессе расследования преступлений в сфере компьютерной информации следователи были обязаны устанавливать место совершения преступления, которое, с точки зрения криминалистики, является элементом обстановки. В ходе следствия данные были получены.

На неустановленном следствием интернет-ресурсе, находясь по месту своего проживания, а далее у родителей, г-н К. скопировал из неустановленного следствием источника на свою персональную электронно-вычислительную машину файлы вредоносной компьютерной программы, предназначенной для нейтрализации средств защиты компьютерной информации[1]. Данный пример наглядно отражает тот факт, что при необходимости вычислить злоумышленника, особенно неопытного, для правоохранительных органов не составляет труда. Для квалификации преступления не требуется выяснение, где и каким образом злоумышленник «скачал» вредоносное ПО.

Выяснение обстановки совершения преступления является важным звеном при расследовании любого уголовного преступления, в том числе преступлений в сфере компьютерной информации, которые имеют свою специфику. Стоит отметить, что следствию бывает достаточно сложно установить место и время совершения преступления [10, с. 43]. Эти сведения крайне важны для установления причинно-следственных связей и причастности обвиняемого к совершению противоправных деяний. Это обусловлено тем, что рассматриваемый вид противоправных деяний совершается в виртуальном пространстве, в котором жертвами преступников могут стать не только обычные люди, но и целые государства. В этой связи подход определения места совершения преступления в сфере компьютерной информации является специфическим.

Если обратиться к Постановлению Пленума Верховного суда РФ от 15 декабря 2022 г. № 37, то в нем имеются разъяснения, что местом совершения киберпреступления является то, откуда преступник действовал[2]. Так, если преступник использует сервисы VPN, то процесс установления места совершения преступления сильно осложняется. Более того, ввиду текущей международной политической обстановки, возможность передачи лиц, подозреваемых в совершении преступлений в отношении граждан нашей страны, зарубежными правоохранителями ставится под сомнение.

Процесс установления времени совершения преступления в сфере компьютерной информации также имеет свои особенности. Как отмечает В.В. Поляков, «…работа некоторых программ связана со временем, установленным на компьютере, и при желании преступник может его изменить на любое удобное ему время. Установление точного времени совершения преступления является непростой задачей, разрешение которой не всегда возможно, в том числе в связи с отсутствием его синхронизации с эталоном»

[1] Приговор Павловского районного суда от 25.11.2020 № 1-40/2020. URL: http://sudact.ru/regular/doc/KL22CmxCcxU/ (дата обращения: 20.03.2023).

[2] 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»: постановление Пленума Верховного суда РФ от 15.12.2022 № 37 // Российская газета. 2022. № 294.

[15, с. 114]. Соответственно, киберпреступления могут быть совершены в любое время суток. Киберпреступники могут оперировать как днем, так и ночью, в зависимости от своих потребностей и целей, а также технических возможностей.

3. Особенности преступлений в сфере компьютерной информации. Таким образом, на основе изученной информации мы можем выделить следующие особенности преступлений в сфере компьютерной информации.

1. Виртуальный характер. Преступления в сфере компьютерной информации совершаются в виртуальном пространстве, в котором изначально отсутствуют физические объекты.

2. В большинстве случаев требуется компьютерная экспертиза. Она включает изучение жестких дисков, сетевых протоколов, программного обеспечения и других аспектов компьютерных систем.

3. Сложность квалификации и разнообразие преступлений. Преступления в сфере компьютерной информации могут включать в себя хакерство, распространение вредоносного ПО, кибермошенничество, нарушение авторских прав и другие виды преступлений, которые предусмотрены главой 28 Уголовного кодекса РФ. Более того, киберпреступники зачастую совершают ряд противоправных деяний с помощью информационно-телекоммуникационных технологий (к примеру, с целью мошеннических действий происходит взлом баз данных), в результате чего возникают проблемы при определении состава преступления и при поиске доказательств по каждому конкретному случаю.

4. Глобальность. В отличие от традиционных преступлений, преступления в сфере компьютерной информации могут быть совершены из любой точки мира и направлены против людей, организаций и целых государств (как в случае с атакой на объекты критической инфраструктуры Ирана). Это существенным образом затрудняет розыскные действия органов следствия.

5. Специализация. Расследование преступлений в сфере компьютерной информации требует наличия специализированных компетенций сотрудников правоохранительных органов. Это связано с быстрым развитием информационных технологий и постоянно меняющимися методами совершения данного вида преступлений.

6. Электронные доказательства. В качестве доказательств в расследовании преступлений в сфере компьютерной информации часто используются электронные следы (или электронно-цифровые следы), такие как записи логов, электронная почта, сетевые данные и т. д. Это требует специального подхода к их сбору, анализу и представлению в суде.

7. Профилактика. Во многом противодействие киберпреступникам сводится к превентивным действиям, к которым относятся такие меры профилактики, как обучение компьютерной грамотности, проведение информационных компаний с населением о рисках в цифровом пространстве и способах защиты от мошенников и других преступников, совершающих преступления в киберпространстве, и т. д.

Заключение

Установлено, что криминалистическая характеристика преступлений в сфере компьютерной информации представляет собой сбор информации о личности преступника, способе, месте и времени, мотивах и целях, технологиях и программах, которые использовались для совершения преступления. Особую роль играют знания и навыки следователей в сфере информационно-коммуникационных технологий, поскольку от их корректных и своевременных действий зависит весь процесс расследования.

Изучение и анализ криминалистической характеристики позволяет определить наиболее распространенные способы совершения подобных преступлений, разработать эффективные меры противодействия. Многие преступники постоянно совершенствуют свои навыки, наиболее квалифицированные из них стараются быть осторожными, разрабатывают собственные контрмеры против правоохранительных органов, используя шифры, специальные программы удаленного доступа, чтобы максимально затруднить как сбор доказательств, так и розыскные мероприятия.

В целом криминалистическая характеристика помогает оптимизировать процесс расследования и использовать практические

методы и современные средства криминалистики для раскрытия преступлений в сфере компьютерной информации. Основная сложность при расследовании данных преступлений – это сложный технологический характер и порядок их совершения. Именно выявление всех этапов и методов совершения преступлений в сфере компьютерной информации являются значимыми для проведения дальнейших научных исследований в этой сфере.

Список источников

1. *Richet J.L.* How Cybercriminal Communities Grow and Change: A study of communities Engaged in advertising fraud // Technological Forecasting and Social Change. 2022. Vol. 174. https://doi.org/10.1016/j.techfore.2021.121282
2. *Chang L.Y.C., Grabosky P.* Cybercrime and Establishing a Secure Cyberworld // The Handbook of Security. L.: Palgrave Macmillan, 2014. P. 321-339. https://doi.org/10.1007/978-1-349-67284-4_15
3. *Ищенко Е.П.* О технологии искусственного интеллекта в криминалистике // 30 лет юридической науки КубГАУ: сб. науч. трудов по материалам Всерос. науч.-практ. конф. с междунар. участием / под ред. В.Д. Зеленского. Краснодар: Кубан. гос. аграрный ун-т им. И.Т. Трубилина, 2021. С. 375-380. https://elibrary.ru/xgjggm
4. *Henthorne T.* William Gibson: A Literary Companion. Jefferson: McFarland & Company, 2011. 176 p.
5. *Файзуллина А.А.* К вопросу о соотношении понятий «криминалистическая характеристика преступлений» и «следственная ситуация» // Инновационная наука. 2017. № 2-2. С. 140-142. https://elibrary.ru/xvsiqn
6. *Григорян С.А.* Особенности личности современного «киберпреступника» // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 8 (147). С. 103-106. https://elibrary.ru/seyfyc
7. *Белевитина Ю.В.* Криминологический портрет личности киберпреступника в современной России // Инновационная наука. 2022. № 12-2. С. 61-64. https://elibrary.ru/xcfqlv
8. *Мартынова Н.В.* Некоторые аспекты криминологической характеристики личности киберпреступника // Студенческий вестник. 2022. № 17-5 (209). С. 7-10. https://elibrary.ru/jgqysk
9. *Сулейманов Р.Т., Атик Х.Б.* Общая характеристика личности киберпреступника // Научный электронный журнал Меридиан. 2021. № 4 (57). С. 114-116. https://elibrary.ru/dbwcer
10. *Жижина М.В., Завьялова Д.В.* Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах. М.: Проспект, 2023. 136 с. https://elibrary.ru/oimenm
11. *Попова С.В., Агафонова М.С., Машин А.А.* Угрозы экономической безопасности в концепции войн шестого поколения // Цифровая и отраслевая экономика. 2020. № 4 (21). С. 55-63. https://elibrary.ru/seuuiy
12. *Могунова М.М.* Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2020. № 4 (135). С. 135-141. https://doi.org/10.24411/2227-7315-2020-10110, https://elibrary.ru/hfbjrg
13. *Вехов В.Б.* Компьютерные преступления. Способы совершения, методики расследования. М.: Право и Закон, 1996. 182 с. https://elibrary.ru/yqclwu
14. *Клебанов Л.Р., Полубинская С.В.* Компьютерные технологии в совершении преступлений диверсионной и террористической направленности // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2020. Т. 24. № 3. С. 717-734. https://doi.org/10.22363/2313-2337-2020-24-3-717-734, https://elibrary.ru/isbbpl
15. *Поляков В.В.* Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. № 2-1 (78). С. 114-116. https://elibrary.ru/rapmrx

References

1. Richet J.L. (2022). How Cybercriminal Communities Grow and Change: A study of communities Engaged in advertising fraud. *Technological Forecasting and Social Change*, vol. 174. https://doi.org/10.1016/j.techfore.2021.121282
2. Chang L.Y.C., Grabosky P. (2014). Cybercrime and Establishing a Secure Cyberworld. *The Handbook of Security*. London, Palgrave Macmillan Publ., pp. 321-339. https://doi.org/10.1007/978-1-349-67284-4_15
3. Ishchenko E.P. (2021). About artificial intelligence technology in criminology. In: Zelenskii V.D. (ed.). *Sbornik nauchnykh trudov po materialam Vserossiiskoi nauchno-prakticheskoi konferentsii s mezhdunarod-*

nym uchastiem «30 let yuridicheskoi nauki KubGAU» [Collection of Scientific Papers based on Proceedings of the All-Russian Scientific and Practical Conference with International Participation "30 Years of Kuban State Agrarian University Legal Science"]. Krasnodar, Kuban State Agrarian University Publ., pp. 375-380. (In Russ.) https://elibrary.ru/xgjggm
4. Henthorne T. (2011). *William Gibson: A Literary Companion*. Jefferson, McFarland & Company Publ., 176 p.
5. Faizullina A.A. (2017). K voprosu o sootnoshenii ponyatii «kriminalisticheskaya kharakteristika prestuplenii» i «sledstvennaya situatsiya» [On the question of the relationship between the concepts of "criminalistic characteristics of crimes" and "investigative situation"]. *Innovatsionnaya nauka = Innovation Science*, no. 2-2, pp. 140-142. (In Russ.) https://elibrary.ru/xvsiqn
6. Grigoryan S.A. (2022). Osobennosti lichnosti sovremennogo «kiberprestupnika» [Personality features of a modern "cybercriminal"]. *Nauka i obrazovanie: khozyaistvo i ekonomika; predprinimatel'stvo; pravo i upravlenie* [Science and Education: Economy and Economics; Entrepreneurship; Law and Management], no. 8 (147), pp. 103-106. (In Russ.) https://elibrary.ru/seyfyc
7. Belevitina Yu.V. (2022). Criminological portrait of the personality of a cybercriminal in modern Russia. *Innovatsionnaya nauka = Innovation Science*, no. 12-2, pp. 61-64. (In Russ.) https://elibrary.ru/xcfqlv
8. Martynova N.V. (2022). Nekotorye aspekty kriminologicheskoi kharakteristiki lichnosti kiberprestupnika [Some aspects of criminological characteristics of a cybercriminal's personality]. *Studencheskii vestnik* [Student Bulletin], no. 17-5 (209), pp. 7-10. (In Russ.) https://elibrary.ru/jgqysk
9. Suleimanov R.T., Atik Kh.B. (2021). Obshchaya kharakteristika lichnosti kiberprestupnika [General characteristics of the cybercriminal's personality]. *Nauchnyi elektronnyi zhurnal Meridian* [Scientific Electronic Journal Meridian], no. 4 (57), pp. 114-116. (In Russ.) https://elibrary.ru/dbwcer
10. Zhizhina M.V., Zav'yalova D.V. (2023). *Rassledovanie prestuplenii v sfere komp'yuternoi informatsii v Rossiiskoi Federatsii i zarubezhnykh stranakh* [Investigation of Crimes in the Field of Computer Information in the Russian Federation and Foreign Countries]. Moscow, Prospekt Publ., 136 p. (In Russ.) https://elibrary.ru/oimenm
11. Popova S.V., Agafonova M.S., Mashin A.A. (2020). Threats to economic security in the sixth generation wars concept. *Tsifrovaya i otraslevaya ekonomika = Digital and Industry Economy*, no. 4 (21), pp. 55-63. (In Russ.) https://elibrary.ru/seuuiy
12. Mogunova M.M. (2020). Technology of implementation and legal regulation of illegal possession of personal banking data (phishing). *Vestnik Saratovskoi gosudarstvennoi yuridicheskoi akademii = Bulletin of Saratov State Law Academy*, no. 4 (135), pp. 135-141. (In Russ.) https://doi.org/10.24411/2227-7315-2020-10110, https://elibrary.ru/hfbjrg
13. Vekhov V.B. (1996). *Komp'yuternye prestupleniya. Sposoby sovershеniya, metodiki rassledovaniya* [Computer Crimes. Ways of Commission, Methods of Investigation]. Moscow, Law and Legislation Publ., 182 p. (In Russ.) https://elibrary.ru/yqclwu
14. Klebanov L.R., Polubinskaya S.V. (2020). Computer technologies for committing sabotage and terrorism. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Yuridicheskie nauki = RUDN Journal of Law*, vol. 24, no. 3, pp. 717-734. (In Russ.) https://doi.org/10.22363/2313-2337-2020-24-3-717-734, https://elibrary.ru/isbbpl
15. Polyakov V.V. (2013). The situation of crime in the computer information sphere as a part of criminalistic characteristic. *Izvestiya Altaiskogo gosudarstvennogo universiteta = Izvestiya of Altai State University*, no. 2-1 (78), pp. 114-116. (In Russ.) https://elibrary.ru/rapmrx

Авторы заявляют об отсутствии конфликта интересов. / Authors declare no conflict of interests.

Поступила в редакцию / Received 23.08.2023
Поступила после рецензирования / Revised 18.09.2023
Принята к публикации / Accepted 22.09.2023