Научная статья
УДК 343.98
DOI: 10.47475/2411-0590-2024-11-4-528-537

Киберугрозы в новой реальности России: состояние и способы противодействия

Наиля Рашидовна Шевко

Казанский государственный энергетический университет, Казань, Россия
mos_shev@mail.ru
https://orcid.org/0000-0003-1092-3389

Аннотация. В современном мире вопросы защиты информации становятся неотъемлемой частью жизни. В связи с повсеместным внедрением современных информационных технологий в деятельность человека, его быт, информационные ресурсы являются наиболее уязвимой частью системы, подвергающиеся все большим атакам со стороны злоумышленников и представляющими интерес. Причем с каждым годом киберпреступники применяют новые способы и методы совершения злодеяний, находя уязвимости как в компьютерных сетях, системах защиты информации, так и используя доверчивость и компьютерную безграмотность пользователей, применяя в том числе приемы социальной инженерии. Это и обуславливает необходимость акцентирования внимания на безопасности данных в киберпространстве, обеспечении должного уровня защиты информации, комплексного подхода к решению данной проблемы. В современном мире пользователи применяют множество приемов и методов защиты данных — криптографию, аппаратные средства защиты компьютерной техники, аутентификацию и многие другие. В данной статье на основе материалов научных исследований, специальной литературы по предмету исследования представлены возможности одной из наиболее надежных технологий — технологии блокчейна, позволяющую за счет ряда отличительных свойств и характеристик обеспечить более надежную защиту информации. Дальнейшая цифровизация общества обуславливает развитие и новых приемов и методов защиты информации. Основными тенденциями развития киберзащиты являются дальнейшее изучение и использование искусственного интеллекта, квантовой криптографии, облачные технологии. Немаловажную роль в области защиты данных играет и повышение уровня обеспечения информационной безопасности общества, ликвидация компьютерной безграмотности пользователей, соблюдение правил использования компьютерных сетей.

Ключевые слова: киберпреступность, кибербезопасность, киберугроза, киберзащита, виртуальное пространство, информационная безопасность, защита данных, блокчейн, преступления с использованием информационных технологий

Для цитирования: Шевко Н. Р. Киберугрозы в новой реальности России: состояние и способы противодействия // Виктимология. 2024. Т. 11, № 4. С. 528–537. DOI: 10.47475/2411-0590-2024-11-4-528-537

Research article

Cyber Threats in the New Reality of Russia: Status and Methods of Countering

Nailya R. Shevko

Kazan State Energy University, Kazan, Russian Federation
mos_shev@mail.ru
https://orcid.org/0000-0003-1092-3389

Abstract. In the modern world, information security issues are becoming an integral part of life. In connection with the widespread introduction of modern information technologies into human activity, his life, information resources are the most vulnerable part of the system, subject to increasing attacks from intruders and of interest. Moreover, every year, cybercriminals use new ways and methods of committing atrocities, finding vulnerabilities both in computer networks, information security systems, and taking advantage of the gullibility and computer illiteracy of users, including using social engineering techniques. This necessitates the need to focus on data security in cyberspace, ensuring the proper level of information protection, and an integrated approach to solving this problem. In the modern world, users use many techniques and methods for protecting data — cryptography, hardware protection for computer equipment, authentication and many others. This article, based on scientific research materials and special literature on the subject of research, presents the capabilities of one of the most reliable technologies — blockchain technology, which, due to a number of distinctive properties and characteristics, allows for more reliable information protection. Further digitalization of society determines the development of new techniques and methods for protecting information. The main trends in the development of cyber defense are the further study and use of artificial intelligence, quantum cryptography, and cloud technologies. An important role in the field of data protection is also played by increasing the level of information security of society, eliminating computer illiteracy of users, and complying with the rules for using computer networks.

Keywords: cybercrime, cybersecurity, cyberthreat, cyberdefense, virtual space, information security, data protection, blockchain, crimes using information technology

For citation: Shevko NR. Cyber threats in the new reality of Russia: status and methods of countering. *Viktimologiya* [Victimology]. 2024;11(4):528-537. (In Russ.) DOI: 10.47475/2411-0590-2024-11-4-528-537

Введение

В современном мире использование интернет-технологий стало особенностью развития во всех сферах деятельности, от переписки в социальных сетях и электронной почте до функционирования систем, которые обеспечивают доступ к различным государственным порталам, с помощью которых мы можем автоматизировать свою жизнь и не только. Столь быстрое развитие интернет-технологий привело к возникновению и развитию криминальной деятельности в киберсфере. Обеспечение информационной безопасности на современном этапе невозможно без мониторинга потенциальных и реальных угроз. Причем фактор криминальной деятельности в современном информационном обществе представляет собой угрозу экономической и национальной безопасности государства. Поэтому одной из основных задач государства на современном этапе становится обеспечение информационной безопасности, защиты человека и гражданина в киберпространстве, создание надежного щита не только на физических границах, но и безопасности в информационном пространстве, противостояние информационной войне.

Киберпреступления (в силу их относительно недавнего появления) являются одними из новейших направлений исследований ученых. Об основных положениях, проблемах квалификации, способах расследования подобного рода преступных деяний в виртуальном пространстве было освещено в трудах таких известных ученых как В. Б. Вехов [7], Т. А. Абрамян [4], М. А. Простосердов [18], Е. А. Лысак [14], М. А. Ефремова [8], Н. С. Зорина [10], Е. А. Кошечкина и С. В. Новиков [13], Д. В. Завьялова [9]. Однако, ввиду ограничения целей исследования, а также стремительного развития научно-технического прогресса, когда ежедневно появляются новые технические и технологические возможности, аппаратные средства, разрабатываются и внедряются новые технологии, учеными эта проблема до конца не изучена.

В современной науке формируются отдельные направления изучения киберпреступности [23; 19]:

— кибермошенничество [21];

— вымогательство в сети [16];

— легализация денежных средств в киберпространстве [17];

— мошенничество с использованием электронных средств платежа [6];

— кибербуллинг [1; 2; 3; 25];

— преступления против собственности с применением информационных технологий [27] и др. [11; 24].

В целях установления состояния и основных направлений развития сферы информационной безопасности в Российской Федерации использованы материалы научных исследований по вопросам регулирования киберпространства, ответственности за преступления с использованием информационных технологий, в сфере компьютерной информации, специальная литература по предмету исследования.

Основными задачами проведенного исследования являются:

— обобщить статистические сведения по киберпреступлениям, выделить наиболее распространенные виды;

— выявить причины стремительного роста и распространения киберпреступности;

— вычленить современные методы и способы защиты информации.

Методологической основой исследования являются общенаучные методы, анализ статистических данных, методы научного познания.

Теоретической базой проведенного исследования выступают труды ведущих специалистов в области противодействия преступлениям, совершенным с использованием информационных технологий.

Эмпирической базой исследования выступают официальные статистические данные по теме исследования.

Практическая значимость проведенного исследования заключается в том, что на основе полученных результатов можно производить среднесрочное криминологические прогнозирование развития киберпреступлений, а также планирование профилактических мер по защите данных в киберпространстве и противодействию преступным посягательствам в информационной сфере.

Процесс и результаты проведенного исследования

В течение последних трех лет, по данным статистики МВД РФ, каждое четвертое преступление совершается с использованием IT-технологий. По официальным данным, количество киберпреступлений, зарегистрированных в Российской Федерации, за последние 15 лет возросло почти в 60 раз (с 12 тыс. в 2007 г. до 700 тыс. в 2023 г.). Необходимо отметить, что первая большая волна киберпреступности произошла в конце 1990-х и начале 2000-х годов, задолго до того, как киберпреступность появилась, как термин (понятие) [12, с. 60]. По данным Национального отделения ФБР США по компьютерным преступлениям, от 85 до 97 % киберпреступлений остаются невыявленными[1].

Проведенное исследование «Лаборатории Касперского»[2] показало полную зависимость молодежи от гаджетов. Так, 73 % подростков не представляют жизни без

[1] ФБР расследует инцидент кибербезопасности в своей внутренней сети. URL: https://habr.com/ru/news/t/717704/ (дата обращения 01.09.2024).

[2] Лаборатория Касперского. Воспитание юного жителя Сети. URL: https://www.kaspersky.ru/blog/connected-kids/7079/ (дата обращения: 05.09.2024).

смартфонов, 40% детей раскрывают в интернете конфиденциальную информацию, включая домашний адрес. Особенно часто посещают сеть Интернет дети. Не каждый родитель может отследить то, чем занимается его ребенок на своем телефоне или компьютере. Пользоваться современными технологиями с ранних лет — это шанс, ведь с такого возраста можно получить и развить навыки, необходимые для безопасного пользования интернет-ресурсами.

Киберпреступления, ввиду их относительной ненаказуемости, являются достаточно привлекательным видом деятельности. Так, одно из самых громких преступлений, совершенным в киберпространстве, было совершено россиянином под ником «lucky12345» — Евгением Богачевым[1]. Ему с единомышленниками с помощью вируса «Zeus», заражающего тысячи компьютеров, удалось похитить у американских граждан и компаний порядка 100 миллионов долларов.

Число преступлений в киберпространстве с каждым годом растет. Если в 2022 году в Казани было зарегистрировано 6500 киберпреступлений, из них 1400 краж с банковских карт и около 3000 интернет-мошенничеств, то в 2023 — уже более 9500. Среди жертв мошенников люди разного возраста, социального положения и материального достатка. Киберпреступники используют в качестве арсенала информационного оружия совокупность средств, предназначенных для нарушения (копирования, искажения или уничтожения) целостности информационной системы. Обзор специальных отчетов, изучающих текущее состояние кибербезопасности в мире, подтверждает, что неправомерное использование информации и получение финансовой выгоды остаются приоритетом для большинства кибератак.

В 2020 году зарубежные компании оказались уязвимы для кибератак хакеров. Злоумышленники продемонстрировали, что могут использовать и хитроумные схемы. Так, злоумышленники не проникали в правительственные системы, а взломали компанию Netsential, занимающуюся веб-разработкой, которая предоставляла федеральным и местным властям технические возможности для обмена информацией. В результате хакерам Anonymous удалось похитить более миллиона файлов правоохранительных и разведывательных органов США: в общей сложности 269 гигабайт информации. Хакеры опубликовали эти данные на сайте DDoSecrets. Несмотря на предварительную проверку DDoSecrets, среди просочившихся файлов были обнаружены конфиденциальные данные.

Взлом является одним из видов киберпреступлений. Говоря простыми словами, взлом является актом, посредством которого злоумышленник получает доступ к компьютерной системе или сети без разрешения владельца. Взломщик называется хакером. У них, как правило, есть профессиональные знания в компьютерной сфере, а также понимание компьютера и компьютерной программы. Они злоупотребляют своими знаниями и совершают преступления посредством взлома.

Интернет-кражи являются основным типом киберпреступности. В настоящее время люди используют Интернет, где часто используют свои конфиденциальные данные, такие как банковские реквизиты, данные кредитной карты и т. д. Действия киберпреступников направлены на эти данные и совершение их кражи. Кроме того, киберпреступники имеют также целевые, защищенные авторским правом контенты в интернете. Это одна часть онлайновой кражи. С другой стороны имеется расширенный этап онлайн-кражи, который называется Identity Theft. Обычный пользователь интернета использует множество онлайн-сайтов и мессенджеров, для входа на каждый из них требуется авторизоваться и ввести логин и пароль. В глобальной компьютерной сети активно распространяется новый способ киберпреступлений — киберкража информации из почтовых ящиков. Большинство пользователей сети Интернет сохраняют почтовые пароли в сети, что делает их практически легкодоступными. В стремлении облегчить себе жизнь пользователи сохраняют коды

[1] 10 громких преступлений, за которыми стояли русские хакеры. URL: https://vc.ru/flood/92374-10-gromkih-prestupleniy-za-kotorymi-stoyali-russkie-hakery (дата обращения 01.09.2024).

доступа в проводнике по сети, чем заодно помогают хакерам. Программы для взлома страниц можно найти в свободном доступе и, как правило, абсолютно бесплатно. Низкий уровень информационной грамотности населения способствует возникновению новых способов и росту кибепреступности. Жертвами киберворов становятся, как правило, не обычные пользователи, а сотрудники крупных корпораций, работающих на дистанте. После одного из таких взломов из электронного почтового ящика сотрудника исчезло очень важное рабочее письмо, стоимость которого — 4,5 миллиона рублей упущенной прибыли. За подобными ресурсами компьютерные вирусологи следят давно и знают, как с ними бороться. Однако, если пароли практически выставлены в открытом доступе, антивирусные программы тут бессильны. Ведь доступ осуществляется от имени идентифицированного пользователя, то есть взлома ключа доступа к почтовому ящику не фиксируется.

Следующим видом является взлом с целью отказа в обслуживании клиента. Под «отказом в сервисе» понимается акт, посредством которого пользователю любого веб-сайта или услуги отказано воспользоваться услугой или веб-сайтом. При этом целевым является веб-сервер из веб-сайтов, к которому осуществляется большое количество запросов. Это вызывает использование максимальной пропускной способности веб-сайта, за счет которого замедляется доступ или он вовсе становится недоступным в течение некоторого времени.

Фишинг — акт, с помощью которого киберпреступники попытаются узнать конфиденциальные данные любого интернет-пользователя. Такими данными могут быть номер кредитной карты, а также имя пользователя и пароль любой учетной записи. Основная цель фишинга является кража денег или приобретение других важных данных пользователя, которые, как правило, могут вызвать финансовые потери. Как правило, фишинг реализуется посредством писем по электронной почте или с веб-сайтов, в которых киберпреступники спрашивают вашу личную информацию или представляют ссылку на сайт, схожий с официальным, и просят перейти по ней. После нажатия на эту ссылку, человек может стать жертвой фишинга.

Следующей разновидностью киберпреступности является спам-сообщение, также осуществляемое как письмо с нежелательной почты, отправленное с помощью веб-ссылки или бизнес-предложения. При нажатии на эту ссылку или отвечая на бизнес-предложение, вы перенаправляетесь на сайт фишинга или устанавливаете вредоносное программное обеспечение на вашем гаджете. Отправитель этих электронных писем всегда неизвестен. Как правило, в имени адресата используются наиболее распространенные имена, например, Иван Петров. Пользователь должен понимать все последствия таких спам-сообщений, могущих повлечь не только заражение гаджета компьютерным вирусом, но и финансовый ущерб, а также потери данных. Еще одним видом современных киберпреступлений является «мир веб-домкрата». В этом случае злоумышленники осуществляют захват за контролем веб-сайта. Они могут изменить содержание этого веб-сайта, используют этот сайт также как владелец, а реальный владелец веб-сайта не имеет больше контроля над действиями на нем. Впоследствии, как правило, злоумышленники требуют выкуп от владельца сайта.

Предоставление в пользование контрафактного программного обеспечения также является киберпреступлением и, к сожалению, большинство компьютерных пользователей являются частью этого преступления. В эту эпоху Интернета, можно легко скачать фильм или программное обеспечение через многие веб-сайты или торрентов. Люди часто используют программное обеспечение без надлежащего разрешения от владельца авторских прав на программное обеспечение. Как правило, они загружают программное обеспечение, взломанный код и используют программное обеспечение без покупки, что является частью компьютерного пиратства. Вообще к компьютерному пиратству относят:

1) крекинг — взлом лицензионного ключа программного обеспечения;

2) использование нелицензионного программного обеспечения на персональном компьютере;

3) использование единого лицензионного программного обеспечения к нескольким компьютерам;

4) распространение такого типа программного обеспечения для других лиц.

В современном обществе, в условиях глобализации, имеем дело со многими формами и видами киберпреступлений. Как правило, киберпреступность носит транснациональный характер [20, с. 55], то есть лица, которые совершают подобного рода преступления, находятся в разных странах и зачастую даже не знакомы друг с другом лично, а общаются исключительно во всемирной сети. К примеру, если говорить о преступлениях, совершаемых в сфере функционирования международных платежных систем, то банковская карточка может быть скомпрометирована преступниками в Грузии, а дубликат делается в Мексике, где и снимают с нее денежные средства. Это помогает злоумышленникам скрывать следы своих преступлений.

Сейчас правоохранители столкнулись с большим количеством преступлений, связанных с использованием сервисов, предоставляемых банковскими учреждениями. Функционирование систем интернет-банкинга основано на привязке сервисов к мобильному телефону клиента. Злоумышленники легко находят номера телефонов пользователей (при объявлениях в интернете люди оставляют номера), звонят на эти номера, и таким образом знают о последних звонках и могут «восстановить» карту телефона. Эта карта дает возможность в некоторых банках получить доступ к данным пользователя бесконтактно. Также некоторые банки предоставляют клиентам возможность снятия денежных средств без присутствия карты, инициируя выдачу денег в банкомате, используя мобильный телефон, чем преступники и пользуются.

Часто пользователи сталкиваются с мошенничеством, связанным с уязвимостью на серверах. Особенно это актуально для компаний, в которых внимание безопасности особо не уделяется. Например, на сервере установлена программа «1С», с помощью которой осуществляется основная бухгалтерская деятельность компании. Путем специфического шифрования злоумышленники полностью блокируют программу. Затем в виде письма в компанию поступает предложение восстановить данные за определенную сумму. Деньги предлагают вывести на какие-то виртуальные платежные системы (как правило, иностранные). В половине случаев информация восстанавливается после оплаты, но в другой половине — отправленные деньги уходят в никуда.

Самым распространенным мошенничеством на сегодняшний день остается продажа несуществующих товаров. Создание фиктивных интернет-магазинов, форумов, торговых площадок, где размещается объявление о товарах, которые не существуют. Люди переводят какие-то деньги либо в качестве предоплаты, либо полной платы — переводят деньги, а товар, естественно, не получают. Это один из самых массовых видов мошенничества сегодня.

Учитывая растущие угрозы в сфере защиты информации, кибербезопасность становится неотъемлемой частью государственной политики [22, с. 375]. Они представляют угрозу не только для отдельных людей, но и для всего государства и национальной безопасности, поскольку утечка конфиденциальной информации дает возможность мошенникам из другой сферы присоединиться к атаке и нанести окончательный удар по неприкосновенности государства, по его гражданам.

Сегодня применяется множество методов защиты информации для обеспечения конфиденциальности, целостности и доступности данных [15, с. 213]. К наиболее распространенным относятся:

— *криптография*. Симметричное и ассиметричное шифрование используется для защиты данных как в статичном, так и в динамическом состоянии. Электронная подпись гарантирует целостность и подлинность электронных документов;

— *защиты сети*. Файерволы используются для блокировки нежелательного доступа посредством фильтрации входящего и исходящего трафика;

— *политика безопасности*. Регулярное обновление программного обеспечения, обновление защиты информации, обучение пользователей и др.

В современных условиях организациям необходимо внедрять комплексные стратегии кибербезопасности, включая обучение сотрудников, регулярные аудиты безопасности и использование современных технологий защиты информации, чтобы минимизировать риски и обеспечить безопасность данных.

Пользователи эффективно применяют современные технологии и в сфере обеспечения безопасности. Особый интерес представляет технология блокчейн, которая имеет ряд преимуществ [26, с. 68], такие как децентрализация (осуществляется за счет хранения данных на множестве узлов сети, что делает систему более устойчивой к кибератакам), прозрачность (все транзакции в блокчейне видны всем участникам сети, обеспечивая быстрое реагирование на подозрительные или противоправные действия), умные контракты (автоматически выполняются при соблюдении определенных условий) и др. [5, с. 10].

Общие выводы по результатам проведенного исследования

Преступления сегодня перешли на новый уровень. Использование современных информационных технологий позволило применять новые способы и методы совершения традиционных преступлений в виртуальном пространстве.

На основе официальных статистических данных выявлен стремительный рост числа киберпреступлений. К наиболее распространенным видам относятся кибермошенничество, кибер-кража, создание киберугроз (посредством DDoS-атак, распространения компьютерных вирусов, создание фальшивых контентов и т. д.).

Причинами стремительного роста преступлений с использованием информационных технологий являются научно-технический прогресс, доступность гаджетов и телекоммуникационных сетей. Зачастую жертвами злоумышленников становятся пользователи ввиду своей информационной безграмотности, а также высокого профессионализма преступников в сфере компьютерной техники и программного обеспечения. Кроме того, большинство киберпреступлений носят трансграничный характер. Успешная борьба с ними возможна лишь при комплексном подходе к расследованию и профилактике, а также сотрудничестве на международном уровне.

Среди современных способов защиты информации можно выделить криптографию, аппаратно-программную защиту компьютерной техники, сетевые фильтры и экраны, а также новую технологию блокчейн.

Создание единого пространства, в котором можно хранить, управлять, создавать любые системы и информацию с помощью компьютеров или других устройств, информационных технологий, приводит к глобальной компьютеризации, глобализации компьютерной сферы. Это упрощает решение государственных задач, но в то же время подвергает их опасности, поскольку единое киберпространство позволяет злоумышленникам на международном уровне завладеть любой информацией или системой другого государства и тем самым нанести вред людям, гражданам, что противоречит сути национальной безопасности.

Таким образом, в ближайшие годы ожидается значительное обновление действующих информационных технологий, внедрение новых. Это потребует и переоценки подходов к защите информации, чтобы эффективно отражать вызовы, связанные с киберугрозами, обеспечивая сохранность данных.

Список источников

1. Aricak T., Siyahhan S., Uzunhasanoglu A., Saribeyoglu S., Ciplak S., Yilmaz N., Memmedov C. Cyberbullying among Turkish adolescents // Cyberpsychology & behavior. 2008. Vol. 11, No. 3. P. 253–261. DOI: https://doi.org/10.1089/cpb.2007.0016

2. Topçu Ç., Erdur-Baker Ö., Çapa-Aydin Y. Examination of cyberbullying experiences among Turkish students from different school types // Cyber Psychology & Behavior. 2008. Vol. 11, No. 6. P. 643–648. DOI: https://doi.org/10.1089/cpb.2007.0161

3. Zhou Z., Tang H., Tian Y., Wei H., Zhang F., Morrison C.M. Cyberbullying and its risk factors among Chinese high school students // School Psychology International. 2013. Vol. 34, No. 6. P. 630–647. DOI: https://doi.org/10.1177/0143034313479692

4. Абрамян Т.А. Актуальные проблемы привлечения к ответственности лиц за преступления в сфере информационных технологий // Юрист. 2018. № 5. С. 68–72. DOI: https://doi.org/10.18572/1812-3929-2018-5-68-72

5. Антипко А.В. Блокчейн: влияние на будущее технологий // Молодой ученый. 2023. № 6 (453). С. 10–11.

6. Бриллиантов А.В., Простосердов М.А. Актуальные вопросы квалификации мошенничества с использованием платежных карт и средств компьютерной техники // Библиотека уголовного права и криминологии. 2017. № 5 (23). С. 163–171.

7. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия. Москва : Право и Закон, 1996. 182 с.

8. Ефремова М.А. Уголовно-правовая охрана информационной безопасности : монография. Москва, 2018. 306 с.

9. Завьялова Д.В. Транснациональная кибербезопасность как объект криминалистического обеспечения // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 3. С. 160–165. DOI: https://doi.org/10.17803/2311-5998.2019.55.3.160-165

10. Зорина Н.С. Информационная безопасность подростков в Интернете как средство предупреждения преступности среди несовершеннолетних // Закон и право. 2022. № 2. С. 152–155. DOI: https://doi.org/10.24412/2073-3313-2022-2-152-155

11. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25–33. DOI: https://doi.org/10.25136/2409-7136.2019.1.28600

12. Иванова Ю.А., Сарбаев Г.М. К вопросу о киберпреступности // Цифровые трансформации экономики и права : сборник научных тезисов Национальной научно-практической конференции. Волгоград, 2022. С. 58–64.

13. Кошечкина Е.А., Новиков С.В. К вопросу о проблемах законодательства в сфере кибертерроризма // Омский научный вестник. Серия «Общество. История. Современность». 2017. № 4. С. 101–105.

14. Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ. 2013. № 90. С. 997–1006.

15. Поспелов Н.В. Особенности использования информационных технологий в борьбе с киберпреступностью // Уголовно-процессуальное и технико-криминалистическое обеспечение для борьбы с киберпреступлениями в современном обществе : материалы II Всероссийской научно-практической конференции. Тамбов, 2023. С. 211–215.

16. Простосердов М.А. Вымогательство, совершенное в сети Интернет // Библиотека криминалиста. Научный журнал. 2013. № 6 (11). С. 150–152.

17. Простосердов М.А. Легализация денежных средств в киберпространстве // Российское правосудие. 2014. № 9 (101). С. 75–80.

18. Простосердов М.А. Проблемы квалификации компьютерных преступлений // Российское правосудие. 2012. № 6 (74). С. 106–108.

19. Русскевич Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. 2018. № 3. С. 10–13.

20. Чекунов И.Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53–56.

21. Шевко Н.Р. Кибермошенничество в России: способы совершения и пути решения проблемы // Вестник НЦБЖД. 2021. № 1 (47). С. 125–130.

22. Шевко Н.Р. К вопросу об обеспечении информационной безопасности россиян в условиях глобализации общества // Правовые механизмы защиты прав человека и гражданина в современных условиях : материалы научно-практической конференции (к 25-летию Университета управления «ТИСБИ»). 2016. С. 371–378.

23. Шевко Н. Р. Кибербезопасность: состояние и перспективы // Державинские чтения : сборник статей XVI международной научно-практической конференции. Москва, 2021. С. 168–170.

24. Шевко Н. Р. Киберпреступность: состояние и перспективы // Актуальные проблемы правоохранительной деятельности органов внутренних дел на современном этапе : материалы Всероссийской научно-практической конференции. Казань, 2019. С. 221–227.

25. Шевко Н. Р., Исхаков И. И. Особенности проявления кибербуллинга в социальных сетях // Ученые записки Казанского юридического института МВД России. 2017. Т. 2. № 3. С. 19–22.

26. Шольц Ю., Шелер Т., Соколов Ю. И. и др. Технология блокчейн. Принципы работы и перспективы применения // ЭТАП. 2017. № 6. С. 66–76.

27. Юхименко Д. М.-К. Преступления против собственности с применением информационных технологий // Социальное управление. 2023. Т. 5, № 5. С. 218–229. URL: https://smgmt.ru/index. php/smgmt/article/view/62

References

1. Aricak T, Siyahhan S, Uzunhasanoglu A, Saribeyoglu S, Ciplak S, Yilmaz N, Memmedov C. Cyberbullying among Turkish adolescents. *Cyberpsychology & behavior*. 2008;11(3):253-261. DOI: https://doi.org/10.1089/cpb.2007.0016

2. Topçu Ç, Erdur-Baker Ö, Çapa-Aydin Y. Examination of cyberbullying experiences among Turkish students from different school types. *Cyber Psychology & Behavior*. 2008;11(6):643-648. DOI: https://doi.org/10.1089/cpb.2007.0161

3. Zhou Z, Tang H, Tian Y, Wei H, Zhang F, Morrison CM. Cyberbullying and its risk factors among Chinese high school students. *School Psychology International*. 2013;34(6):630-647. DOI: https://doi.org/10.1177/0143034313479692

4. Abrahamyan TA. Actual problems of bringing persons to responsibility for crimes in the field of information technology. *Jurist*. 2018;(5):68-72. (In Russ.) DOI: https://doi.org/10.18572/1812-3929-2018-5-68-72

5. Antipko AV. Blockchain: impact on the future of technology. *Young Scientist*. 2023;(6):10-11. (In Russ.)

6. Brilliantov AV, Prostoserdov MA. Actual issues of qualification of fraud with the use of payment cards and means of computer technology. *Library of criminal law and criminology*. 2017;(5):163-171. (In Russ.)

7. Vekhov VB. *Computer Crimes: Ways of Committing and Disclosing.* Moscow: Pravo i Zakon, 1996. 182 p. (In Russ.)

8. Efremova MA. *Criminal-legal protection of information security*: [monograph]. Moscow, 2018. 306 p. (In Russ.)

9. Zavyalova DV. Transnational cybersecurity as an object of criminalistic support. *Bulletin of O. E. Kutafin University (MGJA)*. 2019;(3):160-165. (In Russ.) DOI: https://doi.org/10.17803/2311-5998.2019.55.3.160-165

10. Zorina NS. Information security of teenagers on the Internet as a means of preventing juvenile delinquency. *Law and Legal*. 2022;(2):152-155. (In Russ.) DOI: https://doi.org/10.24412/2073-3313-2022-2-152-155

11. Ivanova LV. Types of cybercrimes under Russian criminal legislation. *Legal Studies*. 2019;(1):25-33. (In Russ.) DOI: https://doi.org/10.25136/2409-7136.2019.1.28600

12. Ivanova YA, Sarbaev GM. To the question of cybercrime. *Digital transformations of economy and law* : a collection of scientific theses of the National Scientific and Practical Conference. Volgograd, 2022:58-64. (In Russ.)

13. Koshechkina EA, Novikov SV. To the issue of the problems of legislation in the field of cyberterrorism. *Omsk Scientific Bulletin. Series "Society. History. Modernity"*. 2017;(4):101-105. (In Russ.)

14. Lysak EA. Problems of qualification of crimes in the sphere of computer information. *Scientific Journal of KubGAU*. 2013;(90):997-1006. (In Russ.)

15. Pospelov NV. Features of the use of information technology in the fight against cybercrime. *Criminal-procedural and technical-criminalistic support for the fight against cybercrime in modern society* : proceedings of the II All-Russian scientific-practical conference. Tambov, 2023:211-215. (In Russ.)

16. Prostoserdov MA. Extortion committed on the Internet. *Library of criminalist. Scientific journal*. 2013;(6):150-152. (In Russ.)

17. Prostoserdov MA. Money laundering in cyberspace. *Russian justice*. 2014;(9):75-80. (In Russ.)

18. Prostoserdov MA. Problems of qualification of computer crimes. *Russian justice*. 2012;(6):106-108. (In Russ.)

19. Russkevich EA. International legal approaches to counteracting crimes committed with the use of information and communication technologies. *International criminal law and international justice*. 2018;(3):10-13. (In Russ.)

20. Chekunov IG. The concept and distinctive features of cybercrime. *Russian investigator*. 2014;(18):53-56. (In Russ.)

21. Shevko NR, Iskhakov II. Features of the manifestation of cyberbullying in social networks. *Scientific notes of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*. 2017;2(3):19-22. (In Russ.)

22. Shevko NR. Cyber fraud in Russia: ways of committing and ways to solve the problem. *Bulletin of the NCBJD*. 2021;(1):125-130. (In Russ.)

23. Shevko NR. Cyber security: state and prospects. *Derzhavinskie readings* : collection of articles of the XVI International Scientific and Practical Conference. Moscow, 2021:168-170. (In Russ.)

24. Shevko NR. Cybercrime: state and prospects. *Actual problems of law enforcement activity of internal affairs bodies at the present stage* : proceedings of the All-Russian scientific-practical conference. Kazan, 2019:221-227. (In Russ.)

25. Shevko NR. To the issue of ensuring information security of Russians in the globalization of society. *Legal mechanisms for the protection of human and civil rights in modern conditions* : proceedings of the scientific and practical conference (to the 25th anniversary of the University of Management "TISBI"). 2016:371-378. (In Russ.)

26. Scholz Y, Scheler T, Sokolov YI. et al. Blockchain technology. Principles of work and prospects of application. *ETAP*. 2017;(6):66-76. (In Russ.)

27. Yukhimenko DM-K. Crimes against property with the use of information technology. *Social Management*. 2023;5(5):218-229. (In Russ.) URL: https://smgmt.ru/index. php/smgmt/article/view/62

ИНФОРМАЦИЯ ОБ АВТОРЕ

Шевко Наиля Рашидовна

Кандидат экономических наук, доцент, доцент кафедры «Информационные технологии и интеллектуальные системы», Казанский государственный энергетический университет.

420066, Казань, ул. Красносельская, д. 51.

mos_shev@mail.ru

https://orcid.org/0000-0003-1092-3389

INFORMATION ABOUT THE AUTHOR

Nailya R. Shevko

Candidate of Economic Sciences, Associate Professor, Associate Professor, Department of Information Technologies and Intelligent Systems, Kazan State Energy University.

51 Krasnoselskaya str., Kazan 420066, Russia.

mos_shev@mail.ru

https://orcid.org/0000-0003-1092-3389

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 16.10.2024.

Дата рецензирования статьи / Revised: 27.11.2024.

Дата принятия статьи к публикации / Accepted: 05.12.2024.