DOI 10.22394/2686-7834-2022-1-83-88

КИБЕРПРЕСТУПНОСТЬ В РОССИИ: АКТУАЛЬНЫЕ ВЫЗОВЫ И УСПЕШНЫЕ ПРАКТИКИ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Мордвинов Константин Владимирович
директор Центра исследований проблем общественной безопасности и правопорядка Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте РФ (РАНХиГС), Санкт-Петербург, Российская Федерация; mordvinov-kv@ranepa.ru
Удавихина Ульяна Андреевна
директор проекта Центра исследований проблем общественной безопасности и правопорядка Северо-Западного института управления Российской академии народного хозяйства и государственной службы при Президенте РФ (РАНХиГС), Санкт-Петербург, Российская Федерация;
udavikhina-ua@ranepa.ru

АННОТАЦИЯ
Глобализация и стремительное развитие компьютерных и IT-технологий привели к возникновению нового вида правонарушений — киберпреступления. Данное понятие еще законодательно не закреплено, и существует проблема классификации преступлений, совершенных в киберпространстве. Авторами предлагается анализ актуального состояния киберпреступности в России за последние 10 лет. Представлен обзор современных мер противодействия киберпреступности в России и за рубежом. Обозначены некоторые рекомендации по обеспечению корпоративной кибербезопасности и перспективные направления исследований.
Ключевые слова: киберпреступность, мошенничество, кибербезопасность, общественная безопасность, технологии, способы предотвращения.

CYBERCRIME IN RUSSIA: CURRENT CHALLENGES AND GOOD PRACTICES IN COMBATING CYBERCRIME

Konstantin V. Mordvinov
Director of the Centre for Public Security and Law Enforcement Studies of North-West Institute of Management of Russian Presidential Academy of National Economy and Public Administration (RANEPA), Saint Petersburg, Russian Federation; mordvinov-kv@ranepa.ru
Uliana A. Udavikhina
Project Director of the Centre for Public Security and Law Enforcement Studies of North-West Institute of Management of Russian Presidential Academy of National Economy and Public Administration (RANEPA), Saint Petersburg, Russian Federation; udavikhina-ua@ranepa.ru

ABSTRACT
Globalization and the rapid development of computer and IT technologies have led to the emergence of a new type of offence — cybercrime. This concept has not yet been legislated, and there is a problem of classification of crimes committed in cyberspace. The authors offer an analysis of current state of cybercrime in Russia for the last 10 years. An overview of modern countermeasures of cybercrime in Russia and abroad is presented. Some recommendations for ensuring corporate cyber security and promising areas of research are outlined.
Keywords: cybercrime, fraud, cyber security, public safety, technology, prevention.

В эпоху глобализации, цифровой трансформации и стремительного развития компьютерных и IT-технологий современное общество, с одной стороны, пользуется преимуществами новых технологий (например, доступом к информации из любой точки мира, мгновенными электронными переводами денежных средств и другими[1]), с другой — столкнулось с новым направлением преступности — киберпреступностью. На сегодняшний день понятие «киберпреступность» законодательно не закреплено, однако в правовой практике под киберпреступностью

[1] См.: *Мальцева А. П.*, *Лошкарев А. В.* Влияние цифровой экономики на киберпреступность. Международный журнал гуманитарных и естественных наук, 2019. № 10-2 (37). С. 117–120. DOI: 10.24411/2500-1000-2019-11664.

чаще всего понимается «ограниченный круг деяний, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных»[2, 3]. Российская Федерация предложила резолюцию «Противодействие использованию информационно-коммуникационных технологий в преступных целях», на основе которой Генеральная Ассамблея ООН в 2021 г. приступила к работе над конвенцией по борьбе с киберпреступностью[4]. Согласно данной резолюции, государства будут иметь возможность закреплять цифровой суверенитет над своим информационным пространством. В целом можно отметить, что общественные отношения в сфере компьютерных и IT-технологий образовали новый объект для совершения преступлений, средств и способов правонарушений, что делает борьбу с киберпреступлениями одной из самых актуальных проблем современности[5].

Характеристики киберпреступности и ее актуальное состояние

Киберпреступления имеют специфические характеристики, которые осложняют процесс их обнаружения и предотвращения. К таким можно отнести[6]:

- высокую латентность[7] — киберпреступники успешно скрывают следы преступлений и долгое время остаются неустановленными;
- преимущественную неосведомленность потерпевших о факте преступного воздействия;
- трансграничность — преступник, потерпевший и объект преступления (например, база данных, банковский счет) могут быть расположены на территориях как разных субъектов страны, так и разных государств;
- автоматизированность преступлений — совершение преступлений возможно в автоматизированном режиме;
- особую подготовленность преступников, интеллектуальный характер преступной деятельности (правонарушители являются экспертами в IT-технологиях и пользуются слабыми местами в информационных системах, в программном обеспечении);
- невозможность предотвращения и пресечения киберпреступлений традиционными средствами.

Обращаясь к статистическим данным по киберпреступности, можно отметить следующее: 1) киберпреступность составляет от ⅓ до ½ от всех преступлений в развитых государствах в период с 2010 по 2020 гг.[8]; 2) 20-кратный рост киберпреступности в России в период с 2013 по 2020 гг.[9]; 3) значительный рост объемов убытков от киберпреступности (например, в банковском секторе[10]). Так, в 2019 г., по данным Центрального банка, мошенники похитили 6,4 млрд руб. у клиентов российских банков[11], а в 2020 г. объем похищенного вырос на 52% и составил 9,77 млрд руб., из которых 11,3% было возвращено[12].

Также в 2020 г. число зарегистрированных дел по ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» по сравнению с 2018 г. выросло почти в 12 раз (2018 г. — 239 дел; 2020 г. — 3083 дела)[13]. С одной стороны, можно отметить значительный рост активности мошенников, с другой — увеличение количества осужденных преступников по ст. 159.3 УК РФ. При этом около 50% судебных дел по ст. 159.3 УК РФ завершаются приговором к условному лишению свободы, выплате штрафа на незначительную сумму и назначению общественных работ. Это может быть связано со сложностью практики правоприменения при разграничении преступлений по ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа», п. 3 ст. 158 УК РФ «Кража с банковского счета равно в отношении электронных денежных средств» и ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации, совершенное с банковского счета равно в отношении электронных денежных средств». На данный момент наиболее актуальным для классификации дел, связанных с киберпреступлениями, может

---

2 См.: *Кувшинова В. С.* Криминологическая характеристика киберпреступности. Международный журнал гуманитарных и естественных наук, 2020. № 5–4. С. 53–57. DOI: 10.24411/2500-1000-2020-10598.

3 См.: *Агаркова А. А.*, *Синицына В. А.* Киберпреступность в современной России. Международный журнал гуманитарных и естественных наук, 2021. № 5–3. С. 13–16. DOI: 10.24412/2500-1000-2021-5-3-13-16.

4 Резолюции 73-й сессии (2018–2019 гг.) Третьего комитета по социальным, гуманитарным вопросам и вопросам культуры Генеральной Ассамблеи ООН [Электронный ресурс]. URL: https://undocs.org/ru/A/73/590 (дата обращения 11.08.2021).

5 См.: *Дерюгин Р. А.* Киберпреступность в России: современное состояние и актуальные проблемы. Вестник Уральского юридического института МВД России, 2019. № 2. С. 46–49.

6 См.: *Бондарь Е. О.* Киберпреступность как новая криминальная угроза. Вестник Московского университета МВД России, 2020. № 1. С. 155–158. DOI: 10.24411/2073-0454-2020-10033.

7 См.: *Лакомов А. С.* Киберпреступность: современные тенденции. Академическая мысль, 2019. № 2 (7). С. 53–56.

8 См.: *Кириленко В. П.*, *Алексеев Г. В.* Киберпреступность и цифровая трансформация. Теоретическая и прикладная юриспруденция, 2021. №1 (7). С. 39–53. DOI: 10.22394/2686-7834-2021-1-39-53.

9 См.: *Приходько А. А.*, *Керопян Г. Б.* Потери банков от киберпреступности. StudNet, 2020. Т. 3. № 12. С. 212–217.

10 См.: *Ковтун К. А.* Банковская киберпреступность как одна из основных проблем современного общества. Теоретическая и прикладная юриспруденция, 2021. № 1 (7). С. 94–97. DOI: 10.22394/2686-7834-2021-1-94-97.

11 Указ соч. Сноска 9.

12 Потери россиян от действий кибермошенников достигли почти 10 млрд руб. Информационное агентство ТАСС. 12.04.2021 [Электронный ресурс]. URL: https://tass.ru/ekonomika/11124421 (дата обращения 02.08.2021).

13 Судебная статистика РФ. Уголовное судопроизводство. Данные о назначенном наказании по статьям УК. 2021 [Электронный ресурс]. URL: http://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения 21.07.2021).

считаться Постановление Пленума Верховного суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[14].

Согласно исследованию 2019 г. Д. В. Лобача и Е. А. Смирновой, кибератакам наиболее часто подвергаются «государственные учреждения (19%), промышленные компании (10%), медицинские учреждения (8%), финансовая отрасль (6%), а также наука и образование (6%) <...> в оставшихся 27% случаев кибератаки обращены к IT-компаниям, сфере услуг, коммерческим структурам, блокчейн-проектам, транспортной инфраструктуре и другим объектам без отраслевой привязки»[15]. Важно отметить, что уровень развития компетенций по информационной безопасности у сотрудников как государственных учреждений[16], так и коммерческих компаний недостаточно высок для обеспечения кибербезопасности компании[17].

Современные меры противодействия киберпреступности

Несмотря на существующие сложности в обнаружении киберпреступлений и противодействии им, в мире разрабатываются успешные практики по обеспечению кибербезопасности. Одной из таких практик является привлечение «этичных» хакеров к борьбе с кибермошенничеством в банковской сфере, осуществляемое полицией Японии с 2013 г.[18] Правительство США успешно применяет данный способ борьбы с киберпреступностью, финансируя привлечение порядка 9 тыс. хакеров для сотрудничества с государством[19]. Кроме того, существуют образовательные курсы по «этичному хакерству», пользующиеся популярностью среди людей, заинтересованных в кибербезопасности[20, 21].

В Российской Федерации обнаружение лиц, совершающих противоправные действия с использованием информационно-телекоммуникационных технологий, обусловлено, во-первых, совершенствованием центров ГосСОПКА[22, 23], AntiFraud-систем банков, которые опознают подозрительные операции с банковским счетом и обеспечивают его временную блокировку[24]; во-вторых, просветительской деятельностью среди населения об алгоритмах работы мошенников и порядке действий в случае столкновения с ними, которую проводят правоохранительные органы, банки и IT-компании; в-третьих, совершенствованием российского законодательства в квалификации данного типа правонарушений[25].

От кибератак наиболее часто страдают не только физические лица, но и юридические, особенно компании, специализирующиеся на продуктах интеллектуального труда (IT-компании, научные центры и лаборатории). К актуальным средствам предотвращения хищения данных в корпоративной среде можно отнести следующие:

- внедрение руководящих документов для четкого распределения обязанностей и зон ответственности сотрудников компании;

---

[14] Постановление Пленума Верховного суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021) «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_283918 (дата обращения 11.08.2021).

[15] См.: *Лобач Д. В.*, *Смирнова Е. А.* Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам. Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса, 2019. № 4 (11). С. 23–32. DOI: 10.24866/VVSU/2073-3984/2019-4/023-032.

[16] См.: *Сладкова Н. М.*, *Ильченко О. А.*, *Степаненко А. А.*, *Шапошников В. А.* Особенности оценки компетенций по информационной безопасности государственных и муниципальных служащих. Вопросы государственного и муниципального управления, 2021. № 1. С. 122–149.

[17] См.: *Купирова Ч. Ш.*, *Кузьмин Ю. А.* Информационная безопасность как объект киберпреступности. Oeconomia et Jus. 2019. № 4. С. 41–46.

[18] См.: *Hayashi H.*, *Yukawa M.*, *Tsuta D.* Japan: Cybersecurity Laws and Regulations. In Cybersecurity: A practical cross-border insight into cybersecurity law. The International Comparative Legal Guides. UK: Global Legal Group, 2021. P. 120–128.

[19] *Коломыченко М.* В интернет ввели кибервойска. Газета «Коммерсантъ», № 2 от 10.01.2017, стр. 1 [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3187320 (дата обращения 11.08.2021).

[20] Become an Ethical Hacker. LinkedIn Learning [Электронный ресурс]. URL: https://www.linkedin.com/learning/paths/become-an-ethical-hacker (дата обращения 11.08.2021).

[21] Ethical Hacking Training. The Knowledge Academy Ltd [Электронный ресурс]. URL: https://www.theknowledgeacademy.com/jp/courses/ethical-hacking-training (дата обращения 11.08.2021).

[22] См.: *Лобач Д. В.*, *Смирнова Е. А.* Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам. Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса, 2019. № 4 (11). С. 23–32. DOI: 10.24866/VVSU/2073-3984/2019-4/023-032.

[23] См.: *Смирнов Г. Е.*, *Макаренко С. И.* Использование тестовых информационно-технических воздействий для превентивного аудита защищенности информационно-телекоммуникационных сетей. Экономика и качество систем связи, 2020. № 3 (17). С. 43–59.

[24] См.: *Чепрасова Ю. В.*, *Шмарион П. В.* Основные направления противодействия киберпреступности. Вестник Воронежского института МВД России. 2020. № 3. С. 256–262.

[25] См.: *Кириленко В. П.*, *Алексеев Г. В.* Киберпреступность и цифровая трансформация. Теоретическая и прикладная юриспруденция, 2021. № 1. С. 39–53. DOI: 10.22394/2686-7834-2021-1-39-53.

- введение пропускного режима;
- внедрение видеонаблюдения;
- отсутствие персональной информации на мобильных устройствах;
- внедрение программно-аппаратных решений по комплексному обеспечению безопасности информации, в частности сегментации компьютерной корпоративной сети;
- внедрение этики использования программного обеспечения (использование только лицензионного программного обеспечения, его регулярное обновление);
- наделение сотрудников минимальным достаточным доступом для выполнения своих задач;
- проведение внешнего аудита информационной безопасности, внешних и внутренних информационных систем;
- внедрение системы Honeypot для прогнозирования взломов системы.

Представителями университета МВД России также были обозначены актуальные направления повышения кибербезопасности, такие как: изменение алгоритма блокировки электронных ресурсов; повышение квалификации каждого сотрудника любой организации по информационной безопасности; анализ организаций, вовлеченных в разработку средств вычислительной техники; организация хакатонов для решения кейсов по кибербезопасности, создание киберполигонов, а также создание кибердружин из добровольцев, которые могут способствовать обеспечению кибербезопасности совместно с полицией[26].

Развитие и внедрение успешных практик противодействия киберпреступлениям с использованием информационно-телекоммуникационных технологий требуют консолидации усилий по организации комплексных исследований, объединяющих ведущих ученых и практиков для решения актуальных проблем в сфере информационной безопасности[27]. Для объединения усилий по решению данных задач в 2021 г. при Северо-Западном институте управления Российской академии народного хозяйства и государственной службы при Президенте РФ был создан Центр исследований проблем общественной безопасности и правопорядка. Его миссия — это повышение общественной безопасности и доверия общества к органам правопорядка в РФ через сотрудничество с ключевыми специалистами государственных структур, такими как МВД, Интерпол, Росгвардия, Федеральная служба исполнения наказаний, Прокуратура, Следственный комитет, правозащитные организации, молодежные общественно-политические объединения. В основные задачи Центра входит организация исследований в различных направлениях, создание практических руководств по результатам исследований, создание и поддержание системы мониторинга эффективности и контроля качества в сфере общественной безопасности, а также реализация программ дополнительного образования и повышения квалификации в данной сфере. В своей работе Центр отталкивается от интересов заказчика, привлекает высококвалифицированных, независимых экспертов, организует прозрачный процесс исследования и помогает внедрять его результаты на практике.

Таким образом, в условиях цифровой трансформации в отношении киберпреступлений, в частности компьютерного мошенничества, наблюдается две тенденции: с одной стороны, это рост активности злоумышленников благодаря технологическому прогрессу, модернизации способов совершения и сокрытия преступлений при помощи информационно-телекоммуникационных технологий; с другой — это развитие способов контроля финансовых операций и имущественных сделок, прозрачности взаимодействия граждан с государством и многое другое. Усиление второй тенденции возможно только при качественном взаимодействии государственных, правоохранительных органов, общественных и коммерческих организаций.

Данная статья подготовлена по материалам доклада авторов на секции «Киберпреступность: вопросы противодействия на современном этапе» в рамках Международной научно-практической конференции «Третьи Баскинские чтения» на тему «Право и государство информационной эпохи: новые вызовы и перспективы».

Литература

1. *Агаркова А. А., Синицына В. А.* Киберпреступность в современной России. Международный журнал гуманитарных и естественных наук, 2021. № 5–3. С. 13–16. DOI: 10.24412/2500-1000-2021-5-3-13-16.
2. *Бондарь Е. О.* Киберпреступность как новая криминальная угроза. Вестник Московского университета МВД России, 2020. № 1. С. 155–158. DOI: 10.24411/2073-0454-2020-10033.
3. *Дерюгин Р. А.* Киберпреступность в России: современное состояние и актуальные проблемы. Вестник Уральского юридического института МВД России, 2019. № 2. С. 46–49.
4. *Кириленко В. П., Алексеев Г. В.* Киберпреступность и цифровая трансформация. Теоретическая и прикладная юриспруденция, 2021. № 1 (7). С. 39–53. DOI: 10.22394/2686-7834-2021-1-39-53.

[26] Заседание секции «Киберпреступность: вопросы противодействия на современном этапе» 28 апреля 2021 г. в рамках Международной научно-практической конференции «Третьи Баскинские чтения» на тему «Право и государство информационной эпохи: новые вызовы и перспективы» [Электронный ресурс]. URL: https://spb.ranepa.ru/news-science/zasedanie-sekczii-kiberprestupnost-voprosy-protivodejstviya-na-sovremennom-etape (дата обращения 11.08.2021).

[27] См.: *Филимонов С. А.* Некоторые особенности борьбы с транснациональным компьютерным мошенничеством. Вопросы управления, 2014. № 5 (11). С. 236–243.

5. *Ковтун К. А.* Банковская киберпреступность как одна из основных проблем современного общества. Теоретическая и прикладная юриспруденция, 2021. № 1 (7). С. 94–97. DOI: 10.22394/2686-7834-2021-1-94-97.
6. *Кувшинова В. С.* Криминологическая характеристика киберпреступности. Международный журнал гуманитарных и естественных наук, 2020. № 5–4. С. 53–57. DOI: 10.24411/2500-1000-2020-10598.
7. *Купирова Ч. Ш., Кузьмин Ю. А.* Информационная безопасность как объект киберпреступности. Oeconomia et Jus, 2019. № 4. С. 41–46.
8. *Лакомов А. С.* Киберпреступность: современные тенденции. Академическая мысль, 2019. № 2 (7). С. 53–56.
9. *Лобач Д. В., Смирнова Е. А.* Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам. Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса, 2019. № 4 (11). С. 23–32. DOI: 10.24866/VVSU/2073-3984/2019-4/023-032.
10. *Мальцева А. П., Лошкарев А. В.* Влияние цифровой экономики на киберпреступность. Международный журнал гуманитарных и естественных наук, 2019. № 10-2 (37). С. 117–120. DOI: 10.24411/2500-1000-2019-11664.
11. *Приходько А. А., Керопян Г. Б.* Потери банков от киберпреступности. StudNet, 2020. Т. 3. № 12. С. 212–217.
12. *Сладкова Н. М., Ильченко О. А., Степаненко А. А., Шапошников В. А.* Особенности оценки компетенций по информационной безопасности государственных и муниципальных служащих. Вопросы государственного и муниципального управления, 2021. № 1. С. 122–149.
13. *Смирнов Г. Е., Макаренко С. И.* Использование тестовых информационно-технических воздействий для превентивного аудита защищенности информационно-телекоммуникационных сетей. Экономика и качество систем связи, 2020. № 3 (17). С. 43–59.
14. *Филимонов С. А.* Некоторые особенности борьбы с транснациональным компьютерным мошенничеством. Вопросы управления, 2014. № 5 (11). С. 236–243.
15. *Чепрасова Ю. В., Шмарион П. В.* Основные направления противодействия киберпреступности. Вестник Воронежского института МВД России, 2020. № 3. С. 256–262.
16. *Hayashi H., Yukawa M., Tsuta D.* Japan: Cybersecurity Laws and Regulations. In Cybersecurity: A practical cross-border insight into cybersecurity law. The International Comparative Legal Guides. UK: Global Legal Group. 2021. P. 120–128.

References

1. Agarkova, A. A., Sinitsyna, V. A. Cybercrime in modern Russia [Kiberprestupnost' v sovremennoj Rossii]. International Journal of Humanities and Natural Sciences [Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk], 2021. № 5–3. P. 13–16. DOI: 10.24412/2500-1000-2021-5-3-13-16. (In rus.)
2. Bondar, E. O. Cybercrime as a new criminal threat [Kiberprestupnost' kak novaya kriminal'naya ugroza]. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia [Vestnik Moskovskogo universiteta MVD Rossii], 2020. № 1. P. 155–158. DOI: 10.24411/2073-0454-2020-10033. (In rus.)
3. Deryugin, R. A. Cybercrime in Russia: Current State and Current Problems [Kiberprestupnost' v Rossii: sovremennoe sostoyanie i aktual'nye problemy]. Bulletin of the Ural Law Institute of the Russian Ministry of Internal Affairs [Vestnik Ural'skogo yuridicheskogo instituta MVD Rossii], 2019. № 2. P. 46–49. (In rus.)
4. Kirilenko, V. P., Alekseev, G. V. Cybercrime and Digital Transformation [Kiberprestupnost' i cifrovaya transformaciya]. Theoretical and Applied Law [Teoreticheskaya i prikladnaya yurisprudentsiya], 2021. № 1 (7). P. 39–53. DOI: 10.22394/2686-7834-2021-1-39-53. (In rus.)
5. Kovtun, K. A. Banking Cybercrime as One of the Main Problems of Modern Society [Bankovskaya kiberprestupnost' kak odna iz osnovnyh problem sovremennogo obshchestva]. Theoretical and Applied Law [Teoreticheskaya i prikladnaya yurisprudentsiya], 2021. № 1 (7). P. 94–97. DOI: 10.22394/2686-7834-2021-1-94-97. (In rus.)
6. Kuvshinova, V. S. Criminological characteristic of cybercrime [Kriminologicheskaya harakteristika kiberprestupnosti]. International Journal of Humanities and Natural Sciences [Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk], 2020. № 5–4. P. 53–57. DOI: 10.24411/2500-1000-2020-10598. (In rus.)
7. Kupirova, Ch. Sh., Kuzmin, Yu. A. Information security as an object of cybercrime [Informacionnaya bezopasnost' kak ob'ekt kiberprestupnosti]. Oeconomia et Jus, 2019. № 4. P. 41–46. (In rus.)
8. Lakomov, A. S. Cybercrime: Current Trends [Kiberprestupnost': sovremennye tendencii]. Academic Thought [Akademicheskaya mysl'], 2019. № 2 (7). P. 53–56. (In rus.)
9. Lobach, D. V., Smirnova, E. A. State of cybersecurity in Russia at the present stage of digital transformation of society and the formation of a national system to counter cyberthreats [Sostoyanie kiberbezopasnosti v Rossii na sovremennom etape cifrovoj transformacii obshchestva i stanovlenie nacional'noj sistemy protivodejstviya kiberugrozam]. Territory of new opportunities. Bulletin of Vladivostok State University of Economics and Service [Territoriya novyh vozmozhnostej. Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa], 2019. № 4 (11). P. 23–32. DOI: 10.24866/VVSU/2073-3984/2019-4/023-032. (In rus.)

10. *Maltseva, A. P., Loshkarev, A. V.* The impact of digital economy on cybercrime [Vliyanie cifrovoj ekonomiki na kiberprestupnost']. International Journal of Humanities and Natural Sciences [Mezhdunarodnyj zhurnal gumanitarnyh i estestvennyh nauk], 2019. № 10-2 (37). P. 117–120. DOI: 10.24411/2500-1000-2019-11664. (In rus.)
11. *Prikhodko, A. A., Keropyan, G. B.* Bank losses from cybercrime [Poteri bankov ot kiberprestupnosti]. StudNet, 2020. V. 3. № 12. P. 212–217. (In rus.)
12. *Sladkova, N. M., Ilchenko, O. A., Stepanenko, A. A., Shaposhnikov, V. A.* Peculiarities of assessing the information security competence of state and municipal employees [Osobennosti ocenki kompetencij po informacionnoj bezopasnosti gosudarstvennyh i municipal'nyh sluzhashchih]. State and municipal government issues [Voprosy gosudarstvennogo i municipal'nogo upravleniya], 2021. № 1. P. 122–149. (In rus.)
13. *Smirnov, G. E., Makarenko, S. I.* Application of test information-technical impacts for preventive security audit of information-telecommunication networks [Ispol'zovanie testovyh informacionno-tekhnicheskih vozdejstvij dlya preventivnogo audita zashchishchennosti informacionno-telekommunikacionnyh setej]. Economics and quality of communication systems [Ekonomika i kachestvo sistem svyazi], 2020. № 3 (17). P. 43–59. (In rus.)
14. *Filimonov, S. A.* Some peculiarities of combating transnational computer fraud [Nekotorye osobennosti bor'by s transnacional'nym komp'yuternym moshennichestvom]. Management issues [Voprosy upravleniya], 2014. № 5 (11). P. 236–243. (In rus.)
15. *Cheprasova, Y. V., Shmarion, P. V.* Main directions of counteraction to cybercrime [Osnovnye napravleniya protivodejstviya kiberprestupnosti]. Bulletin of Voronezh Institute of MIA of Russia [Vestnik Voronezhskogo instituta MVD Rossii], 2020. № 3. P. 256–262. (In rus.)
16. *Hayashi H., Yukawa M., Tsuta D.* Japan: Cybersecurity Laws and Regulations. In Cybersecurity: A practical cross-border insight into cybersecurity law. The International Comparative Legal Guides. UK: Global Legal Group, 2021. P. 120–128.