Научная статья
УДК: 343.3/.7
DOI: 10.17323/tis.2023.18200

Original article

УГОЛОВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УМНОГО ГОРОДА КАК ОБЪЕКТА КИИ

CRIMINAL LAW PROVISION OF INFORMATION SECURITY OF A SMART CITY AS AN OBJECT OF CII

Анна Константиновна ЖАРОВА
Институт государства и права РАН, Москва, Российская Федерация,
anna_jarova@mail.ru,
ORCID: 0000-0002-2981-3369

Информация об авторе
А.К. Жарова — старший научный сотрудник ИГП РАН, ассоциированный член Кафедры ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам НИУ ВШЭ, доктор юридических наук, доцент

Аннотация. Нарушение функционирования экосистемы умного города может привести к значительным негативным последствиям, например к остановке жизни города или всех промышленных предприятий. Информационные системы умного города являются весьма привлекательной целью для злоумышленников и все чаще подвергаются различным компьютерным атакам. Преступления против устойчивости функционирования умного города как объекта критической информационной инфраструктуры (КИИ) наносят существенный вред интересам государства, горожан и умного города как КИИ. В настоящее время этой проблеме не уделяется должного внимания, несмотря на формирование «института ответственности за преступления против информационной безопасности КИИ и информации, обрабатываемой в КИИ».

В статье проведен криминологический анализ преступности в сфере компьютерной информации за период с 2017-го по 2022 г. Представлена статистика компьютерных атак на умный город за 2021 г. и первую половину 2022-го и статистика привлеченных к ответственности лиц за совершение компьютерных атак. Проанализированы негативные социальные явления, связанные с преступлениями против безопасности и устойчивости функционирования умного города как объекта КИИ. Анализ статистики привлечения к ответственности лиц за совершенные преступления, предусмотренные ст. 274.1 УК РФ, позволяет заключить, что наибольшее число преступлений, связанных с причинением вреда КИИ РФ, совершаются группой лиц по предварительному сговору, или организованной группой, или лицом с использованием своего служебного положения (ч. 4 ст. 274.1 УК РФ). Привлечение к ответственности по ч. 5 ст. 274.1 УК РФ не осуществлялось в 2021 г. и в первой половине 2022 г., из чего можно сделать вывод, что, несмотря на сложную ситуацию в мире, атаки на КИИ РФ не приводили к тяжким последствиям.

Ключевые слова: умный город, информационная безопасность, КИИ, преступления, уязвимости, программное обеспечение

Для цитирования: *Жарова А.К.* Уголовно-правовое обеспечение информационной безопасности умного города как объекта КИИ // Труды по интеллектуальной собственности (Works on Intellectual Property). 2023. Т. 47, № 4. С. 8–19; DOI: 10.17323/tis.2023.18200

Anna K. ZHAROVA
Institute of State and Law RAS, Moscow, Russia,
anna_jarova@mail.ru,
ORCID: 0000-0002-2981-3369

Information about the author
A.K. Zharova — senior researcher of the ISL RAS, Associate Fellow of the UNESCO Chair on Copyright, Neighboring, Cultural and Information Rights at HSE University, Doctor of Legal Sciences, Associate Professor

Abstract. Disruption of the functioning of the smart city ecosystem can lead to significant negative consequences, for example, to the shutdown of the city or all industrial enterprises. Smart city information systems are a very attractive target for intruders and are increasingly exposed to various computer attacks. Crimes against the sustainability of a smart city as a critical information infrastructure (CII) cause significant harm to the interests of the state, the citizen, and the smart city as a CII. Currently, this problem is not given due attention, despite the formation of the "institute of responsibility for crimes against the information security of the CII and information processed in the CII".

The article provides a criminological analysis of crime in the field of computer information for the period from 2017 to 2022. The statistics of computer attacks on a smart city for the period of 2021 and the first half of 2022, and the persons brought to responsibility for committing computer attacks are presented. The negative social phenomena associated with crime against the security and sustainability of the functioning of the CII of a smart city are analyzed. Analysis of statistics on bringing persons to responsibility for crimes committed under art. 274.1 of the Criminal Code of the Russian Federation, allows us to conclude that the largest number of crimes related to causing harm to the CII of the Russian Federation are committed by a group of persons by prior agreement or by an organized group, or by a person using his official position (Part 4 of Article 274.1 of the Criminal Code of the Russian Federation). Prosecution under Part 5 of Article 274.1 of the Criminal Code of the Russian Federation was not carried out in 2021 and in the first half of 2022, from which it can be concluded that, despite the difficult situation in the world, attacks on the CII of the Russian Federation did not lead to serious consequences.

Keywords: Smart city, information security, CII, crimes, vulnerabilities, software

For citation: *Zharova A.K.* Criminal Law Provision of Information Security of a Smart City as an Object of CII // Works on Intellectual Property (Works on Intellectual Property). 2023. Vol. 47 (4). P. 8–19; DOI: 10.17323/tis.2023.18200

ВВЕДЕНИЕ

С каждым годом растет число компьютерных атак на различные автоматизированные системы управления (АСУ), информационные инфраструктуры, в том числе и на инфраструктуры города. В 2022 г. число компьютерных атак в России на АСУ увеличилось на 80%, также выросло количество целевых компьютерных атак на промышленные предприятия в России, в основном путем проникновения из интернета вредоносных программ (их доля составляет около 75%), увеличились риски эксплуатации уязвимостей нулевого дня[1] (за 2022 г. выявлено их рекордное количество) [1]. Новые технологии, с одной стороны, входят в число драйверов преступности, а с другой стороны, являются инструментом борьбы с ней и ее профилактики.

Риски осуществления компьютерных атак сопровождают информационные технологии с момента их создания. Однако в зависимости от важности отрасли, в которой функционирует информационная технология, последствия компьютерной атаки на нее могут привести к различным критическим ситуациям.

Необходимость обеспечения безопасности критической информационной инфраструктуры (КИИ) РФ, ее устойчивости к проводимым компьютерным атакам потребовала формирования института ответственности за совершенные преступления против информационной безопасности КИИ и информации, обрабатываемой в КИИ. Данный институт уголовной ответственности начал формироваться условно в 2017–2018 гг.

В 2017 г. в УК РФ Федеральным законом от 26 июля 2017 г. № 194-ФЗ [2] введена ст. 274.1 УК РФ — неправомерное воздействие на КИИ РФ. Криминализация деяний, ответственность за которые предусмотрена ст. 274.1 УК РФ, направлена на охрану отношений в сфере обеспечения устойчивости функционирования КИИ РФ, использования

[1] Уязвимость нулевого дня — это компьютерная атака, направленная на уязвимость программного обеспечения, которая неизвестна его поставщикам или антивирусным программам. Злоумышленник замечает уязвимость ПО до того, как производитель ее обнаружил, быстро создает эксплойт и использует его для проникновения. Такие атаки с большой вероятностью увенчаются успехом. Это делает уязвимости нулевого дня серьезной угрозой безопасности.

компьютерной информации, содержащейся в КИИ, противодействия компьютерным атакам на КИИ, т.е. обеспечения информационной безопасности КИИ уголовно-правовыми средствами.

В 2018 г. вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [3] (далее — ФЗ «О безопасности КИИ»), который формирует государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, а также определяет сферы функционирования КИИ.

Формирующаяся система уголовно-правовых норм в сфере КИИ Российской Федерации направлена на создание модели правомерного поведения участников общественных отношений в 14 областях (здравоохранение, наука, транспорт, связь, энергетика, государственная регистрация прав на недвижимое имущество и сделки с ним, банковская сфера и иные сферы финансового рынка, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность) и устанавливает виды наказаний и иные меры уголовно-правового характера за проведение компьютерных атак на КИИ.

Несмотря на формирующуюся систему уголовно-правовой охраны интересов государства, общества, граждан в сфере КИИ, пока остаются нерешенными проблема обеспечения защищенности КИИ, обрабатываемой в ней информации, а также проблема охраны интересов, прав и свобод горожанина, пользующегося инфраструктурой умного города как объекта КИИ.

Противодействие преступлениям в сфере информационной безопасности КИИ требует подготовки организационно-управленческой правовой основы противодействия этому виду преступности [4].

ЦЕЛИ КОМПЬЮТЕРНОЙ АТАКИ

В соответствии с ч. 4 ст. 2. ФЗ «О безопасности КИИ» под компьютерной атакой понимается «целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации».

Осуществление компьютерной атаки позволяет злоумышленнику, находясь далеко от информационной инфраструктуры, преодолевать государственные границы, совершать преступления, оставаясь при этом фактически анонимным. Для привлечения лица к ответственности необходимо выявить источник атаки, но проблема атрибуции компьютерной атаки сложна, что признано всеми государствами [5]. Кроме того, злоумышленник имеет преимущество перед лицами, осуществляющими защиту информационной инфраструктуры, поскольку ему достаточно найти только одну уязвимость информационной системы (в идеале — уязвимость нулевого дня) для организации компьютерной атаки.

Компьютерная атака может осуществляться посредством «закладок» в программной или аппаратной информационной технологии, вредоносного программного обеспечения и уязвимостей [6]. Злоумышленник, осуществляя компьютерную атаку на объект КИИ, может преследовать следующие цели:

1) изменение целостности и достоверности данных, обрабатываемых в КИИ;

2) нарушение устойчивости КИИ и конфиденциальности данных;

3) уничтожение КИИ.

Систематизация различных угроз и рисков информационных технологий, в том числе связанных с наличием уязвимостей, ведется Федеральной службой технического и экспортного контроля (ФСТЭК) России. Как отмечает ФСТЭК РФ, не всем рискам и угрозам может быть дана оценка, что не отменяет необходимости их предотвращения. Так, в случае отсутствия «у обладателя информации или оператора результатов оценки рисков (ущерба) возможные негативные последствия от реализации угроз безопасности информации могут определяться как на основе экспертной оценки специалистов, проводящих оценку угроз безопасности информации, так и на основе информации, представляемой профильными подразделениями или специалистами обладателя информации или оператора» [7].

Вопрос оценки рисков и угроз также важен для обеспечения информационной безопасности умного города, поскольку умный город — это крупная автоматизированная экосистема [8], объединяющая множество информационных систем из разных сфер, часть из которых относится к объектам КИИ в соответствии с ФЗ «О безопасности КИИ». Некоторые информационные системы умного города, например объекты жилищно-коммунального хозяйства (ЖКХ), не отнесены к объектам КИИ. Однако выведение из строя любой информационной системы, входящей в экосистему умного города, приведет к остановке ее работы [9].

Если информационная система не отнесена к объектам КИИ, то ей сложно присвоить категорию,

организовать защиту КИИ и информации, находящейся в информационной системе, и соответственно в дальнейшем обеспечить охрану интересов пользователей (горожан, государственных органов и др.) КИИ.

Нарушение функционирования экосистемы умного города может привести к значительным негативным последствиям [10], например к остановке общественного транспорта или всех промышленных предприятий. Информационные системы умного города являются весьма привлекательной целью для злоумышленников и все чаще подвергаются различным компьютерным атакам.

УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Компьютерная уязвимость — некая «слабость информационной технологии, которая может быть использована злоумышленником для нарушения функционирования системы или содержащейся в ней информации» [11]. Так, с «1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах КИИ» [12].

Уход с российского рынка крупных разработчиков аппаратного и программного обеспечения (ПО), таких как Microsoft, Oracle, Cisco, Coursera, Citrix, Docker, ESET, IBM, GoDaddy, Google Cloud, Grammarly, Adobe, Apple, Nokia, Atlassian (Jira), Autodesk, Avast, AWS, Canonical, Figma, Fiverr, Globalstar, VUE, Qt, Red Hat, SUSE, Acronis, Udemy, Unity, Upwork, Arbor (Netscout), Javarush, JetBrains, Juniper, Intel, MATLAB, Mikrotik, Miro, MongoDB, NortonLifeLock, NVIDIA, Pearson, TeamViewer, VMWare, Xsolla, Zabbix и других [13], и необходимость разработки аналогов российского программного обеспечения послужили сигналом к применению открытого ПО. Однако открытому ПО также нельзя доверять, поскольку, согласно исследованиям, более 29% популярных библиотек содержат уязвимости, а количество атак через них в 2022 г. увеличилось на 650% по сравнению с 2021 г. [14]. Некоторые разработчики открытого ПО преднамеренно включают в него вредоносный функционал, специально нацеленный на Россию и российские IP-адреса. Такие действия ставят под удар многие программные проекты, в которых используется открытое ПО.

Российские разработчики проанализировали 33 программных продукта с открытым кодом, предлагаемые на рынке. «Итоговая статистика оказалась следующей: найдено 2504 уязвимости в используемых компонентах, включая 598 уязвимостей критичного уровня, и 416 уязвимостей высокого уровня критичности; выявлено 197 компонентов с лицензиями, запрещающими коммерческое использование» [14]. Результаты аналитического исследования содержали некоторые уязвимости, однако остались и невыявленные. Количество компьютерных атак на различные информационные системы, совершаемых посредством эксплуатации уязвимостей, неуклонно растет [15]. Анализ социального портрета преступников в сфере компьютерной информации позволяет сделать вывод, что 20,89% из них имеют высшее техническое образование [16].

УМНЫЙ ГОРОД КАК ОБЪЕКТ КИИ

Умный город является сложным инфраструктурным комплексом, объединяющим две концепции — концепцию больших данных и концепцию интернета вещей. Умный город является КИИ, несмотря на то что в его инфраструктуре функционируют информационные системы, не отнесенные ФЗ «О безопасности КИИ» к объектам КИИ, но от устойчивости их работы зависят жизнь и здоровье горожан и функционирование города как социальной инфраструктуры.

Некоторые авторы видят структуру умного города как совокупность шести основных информационных инфраструктурных блоков (умное управление, умная экономика, интеллектуальная мобильность, интеллектуальная среда, умные люди и умное проживание) [17].

В соответствии с Приказом Минстроя России «Об утверждении концепции проекта цифровизации городского хозяйства “Умный город”» умный город может быть представлен тремя уровнями. Уровень 1: инфраструктура для функционирования умных городов (модель сервисов, возможных взаимодействий и используемых технологий между информационными системами умного города). Уровень 2: обеспечение функционирования умных городов (сервисы, направленные на сопровождение деятельности и контроль сроков и качества работы по предоставлению городских услуг). Уровень 3: сервисы и услуги (электронные сервисы: госуслуги, электронное образование, медицина, информационно-технологическое сопровождение, ЖКХ, безопасность, соцподдержка, экология) для физических и юридических лиц [18].

Несмотря на важность обеспечения охраны интересов города и горожан, исследований, посвященных проблемам правовой защиты умного города как объекта КИИ и информационной безопасности как объекта уголовно-правовой охраны, крайне мало. М.А. Ефремова доказала в своей докторской диссертации, что «информационная безопасность — это объект уголовно-правовой охраны и институт уголов-

ного права» [19]. Научные публикации, затрагивают отдельные проблемы обеспечения информационной безопасности в умном городе. Исследовались общие проблемы обеспечения безопасности в умном городе [20], применение умных технологий [21], место и роль умного города в цифровой экономике [22]. Ряд исследований посвящен обеспечению безопасности и приватности [23] кибербезопасности умного города [24], преступности в сфере жилищно-коммунального хозяйства [25], но работ по проблемам обеспечения безопасности умного города уголовно-правовыми методами мало.

Согласно ФЗ «О безопасности КИИ» и ст. 274.1 УК РФ, преступлением признаются действия, которые посягают на безопасность значимых в РФ объектов «в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности».

Н.А. Голованова и соавторы считают, что дополнительным объектом такого преступления может быть информационная безопасность в любой сфере деятельности государства и общества [26].

Статистика по преступлениям, связанным с неправомерным воздействием на КИИ РФ, показывает небольшое число лиц, привлеченных к ответственности. Так, за 2020 г. по ч. 1 и ч. 2 ст. 274.1 УК РФ осуждены три человека, по ч. 3 и ч. 4 ст. 274.1 УК РФ осужден один человек, по ч. 5 ст. 274.1 УК РФ вынесенные приговоры отсутствуют [27]. Диаграмма рассмотренных судом дел по ст. 274.1 УК РФ в 2017–2020 гг. приведена на рис. 1.

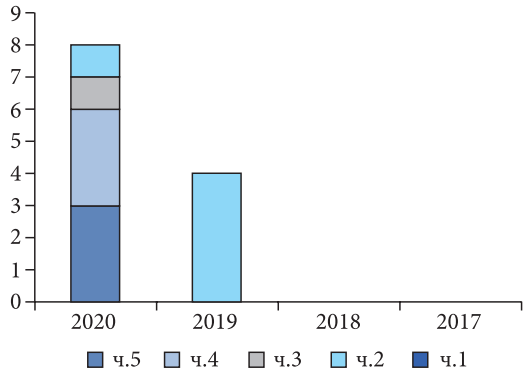

Рис. 1. Статистика рассмотренных судом дел по ст. 274.1 УК РФ в 2017– 2020 гг.

Ученые отмечают, что фактически отсутствует практика выявления преступлений, предусмотренных ст. 274.1 УК РФ [28, 29], хотя общая статистика преступлений, совершенных с использованием информационных технологий, демонстрирует иную ситуацию. Некоторые авторы считают, что несовершенство статистического учета позволяет проследить динамику лишь части преступлений в сфере компьютерных технологий, причем не самой значимой, и не дает объективной картины состояния преступности в этой сфере [30].

Несмотря на формирование института ответственности за совершение преступлений против информационной безопасности КИИ и обрабатываемой информации в КИИ и подчеркнутую государством важность охраны отношений в сфере устойчивости КИИ, не все отношения в этой сфере подлежат уголовно-правовой охране. В связи с такой ситуацией закономерны вопросы: могут ли общественные отношения в сфере умного города охраняться на основании ст. 274.1 УК РФ? Какова статистика компьютерных атак, совершенных на инфраструктуру умного города?

Проанализируем аналитику преступлений, связанных с компьютерными атаками на КИИ умного города.

АНАЛИЗ КОМПЬЮТЕРНЫХ АТАК НА КИИ УМНОГО ГОРОДА

Наиболее известные примеры компьютерных атак на КИИ умного города — это атаки на различные общественные платформы: экраны, билборды, банкоматы и другие устройства, подключенные к интернету. К менее распространенным, но более опасным относятся атаки на транспортные объекты, государственные информационные системы.

Для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них, выявления уязвимостей, рисков и систематизации угроз обеспечения безопасности КИИ в РФ функционирует киберполигон [31]. Так, на киберполигоне The Standoff в 2022 г. прошла самая масштабная в мире 123-часовая битва между нападающими на инфраструктуру умного города, имитирующими действия злоумышленников, и его киберзащитниками. На киберполигоне была создана цифровая копия инфраструктуры крупного умного города, содержащая все критически важные информационные системы: аэропорт, морской порт, железную дорогу, деловой центр, банк, парк развлечений, городские системы (светофоры и уличное освещение), систе-

му телерадиовещания, нефтедобывающую станцию, электроподстанцию, газораспределительную станцию, тепловую электростанцию, ветроэлектрическую установку, нефтехимический завод. Лица, имитирующие атаки на КИИ, старались устраивать аварии, взламывать системы заводов, останавливать работу метро, изменять работу светофоров, похищать деньги из банка. «Почти за шесть суток учений на киберполигоне The Standoff защитники выявили несколько сотен инцидентов на своих объектах. Хакеры реализовали 47% рисков всех заложенных в инфраструктуру умного города» [32].

Основными точками возможных атак на различных уровнях умного города являются оборудование, приложения, сети и облака (см. таблицу) [33].

Точки возможных атак на различных уровнях умного города

Элементы умного города	Уровень устройств/датчиков
Транспорт	Умные автомобили Дорожные знаки Светофоры Уличные фонари Парковочные датчики
Здравоохранение	Смарт-часы Фитнес-трекеры Кардиостимуляторы Автоматические инсулиновые помпы
Энергетика	Кондиционеры Датчики отопления Датчики утечки воды Датчики света Датчики температуры и влажности
Умные здания	Термостаты Камеры Умные колонки Умные дверные замки Радионяни

Статистика критических уязвимостей в ПО различных производителей представлена на рис. 2 [34].

Однако с точки зрения уголовно-правового регулирования возникает вопрос: может ли наступить уголовная ответственность за использование уязвимости информационной системы КИИ в целях создания угрозы безопасности обрабатываемой такими объектами информации?

В соответствии с ч. 1 ст. 274.1 УК РФ уголовной ответственности подлежит лицо, создавшее, распространившее и (или) использовавшее компьютерную программу либо иную компьютерную информацию, заведомо предназначенную для неправомерного воздействия на КИИ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в КИИ, или нейтрализации средств защиты указанной информации. В соответствии с ч. 2 ст. 274.1 УК РФ уголовной ответственности подлежит лицо, получившее неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ, в том числе с использованием компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ, если это повлекло причинение вреда.

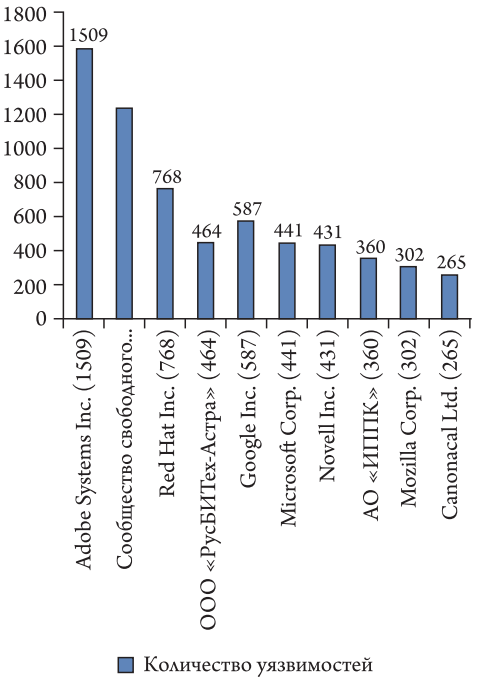

Рис. 2. Критические уязвимости в ПО различных производителей

Несмотря на то что уязвимости ПО используются для совершения компьютерных атак, они не являются программным обеспечением (компьютерной программой). Таким образом, уголовному наказанию подлежат действия, связанные с использованием знаний о слабых местах аппаратного или программного обеспечения и совершаемые с применением информационных технологий в целях осуществления атаки на КИИ.

СТАТИСТИКА КОМПЬЮТЕРНЫХ АТАК С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В первом квартале 2022 г. противостояние в киберпространстве возросло, количество компьютерных

атак на все интернет-ресурсы увеличилось на 14,8% по сравнению с четвертым кварталом 2021 г., общее число атак без привязки к отрасли экономики выросло с 18 до 23%.

Основными объектами компьютерной атаки были веб-ресурсы государственных органов и медицинских учреждений, промышленных предприятий. Во второй половине первого квартала 2022 г. их доля выросла до 22% по сравнению с 13%, наблюдаемыми в том же квартале предыдущего года (рис. 3). Увеличилась доля компьютерных атак, которые стали возможны из-за компрометации или подбора учетных данных. В основном атаки проводились на веб-ресурсы и аккаунты компаний в социальных сетях [35].

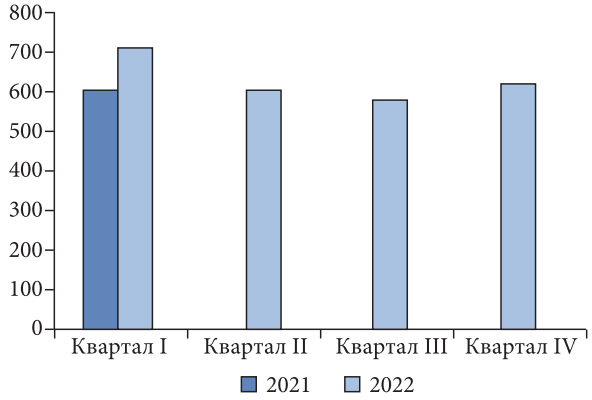

Рис. 3. Количество атак в 2021 и 2022 гг. (по кварталам) [35]

СТАТИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Согласно статистическим данным, в 2017 г. число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587. Их доля в общем числе всех зарегистрированных в России преступных деяний составляет 4,4% — это почти каждое двадцатое преступление.

В 2021 г. существенным фактором, оказывающим негативное влияние на криминогенную ситуацию в стране, продолжал оставаться рост IT-преступности. В январе — июне 2021 г. он составил 20,3%, удельный вес указанных противоправных деяний в общей структуре преступности достиг 26,5%. Зафиксирован рост преступлений, совершенных при помощи интернета (на 42,1%) и с использованием компьютерной техники (на 35,6%) [36]. По данным МВД России, за январь — август 2022 г. на 6,9% снизилось количество преступлений, совершенных с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. Возрос уровень безопасности на объектах транспорта, где преступлений зарегистрировано на 6,1% меньше [36].

По итогам шести месяцев 2022 г. МВД России зафиксировало 249 тыс. преступлений, совершенных с помощью информационных технологий, например мошенничества через телефонные звонки, кардинг, фишинг и др. Показатель 2022 г. на 8,2% ниже, чем за этот же период 2021-го. До этого МВД России регистрировало ежегодный рост таких преступлений [37], о чем свидетельствуют приведенные на рис. 4 и 5 диаграммы.

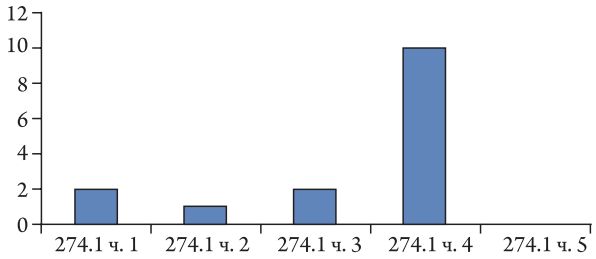

Рис. 4. Статистическая информация о числе осужденных по ст. 274.1 УК РФ за 2021 г.

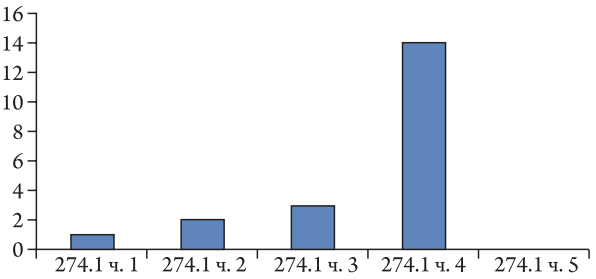

Рис. 5. Статистическая информация о числе осужденных по ст. 274.1 УК РФ за первое полугодие 2022 г.

Представленная статистическая информация о числе осужденных за совершенные преступления, предусмотренные ст. 274.1 УК РФ, показывает, что как в 2021 г., так и в первом полугодии 2022-го тенденцией преступных деяний было причинение вреда КИИ РФ, совершенное группой лиц по предварительному сговору, или организованной группой, или лицом с использованием своего служебного положения (ч. 4 ст. 274.1 УК РФ), путем:

- неправомерного доступа к охраняемой компьютерной информации, содержащейся в КИИ РФ;
- нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или информационных системах, информационно-телекоммуникационных сетях, АСУ, сетях электросвязи, относящихся

к КИИ РФ, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, АСУ, сетям электросвязи;

- создания, распространения и (или) использования компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, для нейтрализации средств защиты указанной информации либо для неправомерного воздействия на КИИ РФ, или создания иных вредоносных компьютерных программ, повлекшего за собой причинение вреда КИИ РФ.

Часть 5 ст. 274.1 УК РФ не применялась судами ни в 2021 г., ни в первой половине 2022-го. Таким образом, можно сделать вывод, что компьютерные атаки на КИИ РФ за прошедший период не приводили к тяжким последствиям, таким как «причинение смерти или тяжкого вреда здоровью человека, причинение средней тяжести вреда здоровью двух или более лиц, массовое причинение легкого вреда здоровью людей, наступление экологических катастроф, транспортных или производственных аварий, повлекших длительную остановку транспорта или производственного процесса, дезорганизацию работы конкретного предприятия, причинение особо крупного ущерба» [38].

Для целей проведенного исследования представляют большой интерес статистические данные, показывающие, какие именно информационные системы умного города — светофоры, государственные информационные системы, системы ЖКХ и др. — чаще других становятся объектами преступных посягательств. К сожалению, такая статистика не ведется.

ЗАКЛЮЧЕНИЕ

В настоящее время развивается система уголовно-правовой охраны информационной безопасности КИИ. Так, в 2022 г. в УК РФ введена [39] ст. 274.2, предусматривающая уголовную ответственность за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ информационно-телекоммуникационной сети Интернет и сети связи общего пользования. Этот факт позволяет утверждать, что в область уголовно-правовой охраны включены отношения, возникающие в связи с обеспечением централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ интернета и сети связи общего пользования и относящиеся к сфере деятельности операторов связи и интернет-провайдеров. Иными словами, государство заявляет о значимости отношений, возникающих в связи с обеспечением функционирования программно-аппаратного комплекса, позволяющего операторам связи и интернет-провайдерам ограничивать доступ к информации, распространение которой запрещено на территории России. В связи с этим обеспечение информационной безопасности умного города должно строиться на мониторинге уязвимостей аппаратного и программного обеспечения, их оперативного выявления и устранения.

Информационные системы умного города являются весьма привлекательной целью для злоумышленников, поскольку вывод из строя одной информационной инфраструктуры, входящей в систему умного города, может привести к сбоям в работе всей инфраструктуры умного города и коллапсу в самом городе. Преступления против устойчивости АСУ умного города как объекта КИИ или его информационной системы наносят существенный вред интересам государства, горожан и процессам жизнедеятельности города. В настоящее время этой проблеме не уделяется должного внимания, несмотря на формирование института ответственности за преступления против информационной безопасности КИИ и информации, обрабатываемой в КИИ.

Несмотря на увеличивающиеся число компьютерных атак на АСУ, на базе которых функционирует в том числе умный город, фактически отсутствует статистика выявления атак, совершенных на отдельные информационные системы умного города — светофоры, государственные информационные системы, системы ЖКХ и др.

Вопрос критичности инфраструктуры умных городов требует дальнейшего законодательного регулирования, распространения законодательства о безопасности КИИ на сферу ЖКХ, которая активно развивается с применением информационных технологий, а также законодательного закрепления понятия «умный город» и его соотношения с термином «объект КИИ».

СПИСОК ИСТОЧНИКОВ

1. Число кибератак в России и в мире. — https://www.tadviser.ru/index.php/Stat'ya:CHislo_kiberatak_v_Rossii_i_v_mire
2. Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Рос-

сийской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" // СЗ РФ. 2017. № 31 (Ч. I). Ст. 4743.
3. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (Ч. I). Ст. 4736.
4. *Ищук Я.Г., Пинкевич Т.В., Смольянинов Е.С.* Цифровая криминология: учебное пособие. М.: Академия управления МВД России, 2021. 244 с.
5. *Жарова А. К.* Обеспечение защиты государства от компьютерных атак в ИКТ-сфере // Труды Института государства и права Российской академии наук. 2022. Т. 17. № 4. С. 100–125. DOI 10.35427/2073-4522-2022-17-4-zharova. EDN ZDFJDA.
6. *Rosol Marit, Blue Gwendolyn.* From the smart city to urban justice in adigital age, City. 2022. Vol. 26:4. P. 684–705. DOI: 10.1080/13604813.2022.2079881
7. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.) Документ не опубликован // СПС «КонсультантПлюс».
8. Паспорт национального проекта «Национальная программа "Цифровая экономика Российской Федерации"», утв. Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам. Протокол от 4 июня 2019 г. № 7 // https://digital.gov.ru
9. *Zharova A., Elin V.* State regulation of the IoT in the Russian Federation: Fundamentals and challenges // International Journal of Electrical and Computer Engineering. 2021. Vol. 11. No 5. P. 4542–4549. DOI 10.11591/ijece.v11i5. P. 4542–4549. EDN TLEEFT.
10. *Саматов К.* Умный дом и умный город: КИИ или нет? (13.12.21). — URL: https://www.itsec.ru/articles/umnyj-dom-i-umnyj-gorod-kii-ili-net
11. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка, утв. ФСТЭК РФ 15 февраля 2008 г.) Документ не опубликован // СПС «Консультант Плюс».
12. Указ Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2022. № 14. Ст. 2242.
13. *Петрова Е.* Ушел и не вернулся: какие ИТ-компании покинули Россию и кто сможет занять их место. — URL: https://hightech.fm/2022/05/26/it-companies-went-away
14. *Шабалин Ю.* Опасность компонент с открытым исходным кодом в цифрах на реальном проекте. — URL: https://www.itsec.ru/articles/opasnost-komponent-s-otkrytym-iskhodnym-kodom-v-cifrah-na-realnom-proekte
15. Генпрокурор России Игорь Краснов провел совещание по теме борьбы с преступлениями, связанными с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий. — URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news/archive?item=56766040
16. Социальный портрет преступности. — URL: http://crimestat.ru/social_portrait
17. *Есаян А.К., Трунцевский Ю.В.* Общие подходы к нормативному правовому регулированию технологии в сфере «Умный город» // Международное публичное и частное право. 2020. № 1. С. 36–41. DOI: 10.18572/1812-3910-2020-1-36-41.
18. Приказ Минстроя России от 25 декабря 2020 г. № 866/пр «Об утверждении Концепции проекта цифровизации городского хозяйства "Умный город"» // Информационный бюллетень о нормативной, методической и типовой проектной документации. 2021. № 1-2.
19. *Ефремова М.А.* Уголовно-правовая охрана информационной безопасности: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: дисс. ... докт. юр. наук. М., 2017. 427 с. EDN GNIILS.
20. *Жарова А.К.* Правовое обеспечение информационной безопасности в «умных городах» // Юрист. 2019. № 12. С. 69–76. DOI: 10.18572/1812-3929-2019-12-69-76.
21. *Грищенко Л.Л., Ревин С.М., Коротаев Ю.В.* «Умные» технологии при обеспечении безопасности в «умном городе» // Муниципальная академия. 2020. № 2. С. 186–191.
22. Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие / М.О. Дьяконова, А.А. Ефремов, О.А. Зайцев и др.; под ред. И.И. Кучерова, С.А. Синицына. М.: ИЗиСП; НОРМА, 2022. 376 с. DOI: 10.12737/1839690.
23. *Елин В.М.* Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом / под общей ред. А.П. Баранова. М.: Московский институт государственного управления и права, 2016. 168 с. (Информационное право и кибербезопасность). ISBN 978-5-9909450-7-4. EDN XRCLFL.

24. *Головенчик Г., Краско М., Головенчик М.* Проблемы кибербезопасности умных городов // Наука и инновации. 2020. № 12(214). С. 51–57. EDN STLLAY.
25. *Кельм С.И.* Состояние, структура и динамика преступности в сфере жилищно-коммунального хозяйства // Вестник Санкт-Петербургского университета МВД России. 2021. № 2(90). С. 84–90. DOI: 10.35750/2071-8284-2021-2-84-90.
26. Уголовно-юрисдикционная деятельность в условиях цифровизации / Н.А. Голованова, А.А. Гравина, О.А. Зайцев и др. М.: ИЗиСП; КОНТРАКТ, 2019. 212 с.
27. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. — URL: https://beta.dostoevsky.io/ru/274.1/2020/parts/
28. *Крайнова Н.А.* Права и технологии в сфере противодействия киберугрозам // Право и цифровая экономика. 2021. № 2. С. 23–31. DOI: 10.17803/2618-8198.2021.12.2.023-031.
29. *Бегишев И.Р.* Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.
30. *Бугаев В.А., Чайка А.В.* Факторы преступности в сфере компьютерных технологий // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2019. № 4. С. 139–145. EDN EJELBM.
31. Постановление Правительства РФ от 12 октября 2019 г. № 1320 «Об утверждении Правил предоставления субсидий из федерального бюджета на введение в эксплуатацию и обеспечение функционирования киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности» // СЗ РФ 2019. № 42 (Ч. III). Ст. 5913.
32. Атака на «умный» город: как прошли киберучения по защите инфраструктуры. — URL: https://trends.rbc.ru/trends/industry/cmrm/5fd1dc729a7947a505d40c26
33. Открытые системы // СУБД. 2022. № 2. — URL: https://www.osp.ru/os/2022/02/13056210
34. Инфографика. — https://bdu.fstec.ru/charts
35. Актуальные киберугрозы: первый квартал 2022 г. — https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/#id2
36. Краткая характеристика состояния преступности в Российской Федерации за январь — июнь 2021 г. — https://мвд.рф/reports/item/25094008/
37. Быль и убыль: число преступлений с использованием ИТ упало впервые за пять лет. С чем связана позитивная динамика и сохранится ли этот тренд. — https://iz.ru/1371417/roza-almakunova/byl-i-ubyl-chislo-prestuplenii-s-ispolzovaniem-it-upalo-vpervye-za-5-let
38. *Решетников А.Ю., Русскевич Е.А.* Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Законы России: опыт, анализ, практика. 2018. № 2. С. 51–55.
39. Федеральный закон от 14 июля 2022 г. № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // СЗ РФ. 2022. № 29 (Ч. II). Ст. 5227.

REFERENCES

1. Chislo kiberatak v Rossii i v mire. — https://www.tadviser.ru/index.php/Stat'ya:CHislo_kiberatak_v_Rossii_i_v_mire
2. Federal'nyj zakon ot 26 iyulya 2017 g. No 194-FZ "O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i stat'yu 151 Ugolovno-processual'nogo kodeksa Rossijskoj Federacii v svyazi s prinyatiem Federal'nogo zakona "O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii" // SZ RF 2017. No 31 (Ch. I). St. 4743.
3. Federal'nyj zakon ot 26 iyulya 2017 g. No 187-FZ "O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii" // SZ RF. 2017. № 31 (Ch. I). St. 4736.
4. *Ishchuk Ya. G., Pinkevich T.V., Smol'yaninov E.S.* Cifrovaya kriminologiya: uchebnoe posobie. M.: Akademiya upravleniya MVD Rossii, 2021. 244 s.
5. *Zharova A.K.* Obespechenie zashchity gosudarstva ot komp'yuternyh atak v IKT-sfere // Trudy Instituta gosudarstva i prava Rossijskoj akademii nauk. 2022. T. 17. No 4. S. 100–125. DOI 10.35427/2073-4522-2022-17-4-zharova. EDN ZDFJDA.
6. *Rosol M., Blue G.* From the smart city to urban justice in adigital age, City. 2022. Vol. 26:4. P. 684–705. DOI: 10.1080/13604813.2022.2079881.
7. Metodicheskij dokument. Metodika ocenki ugroz bezopasnosti informacii (utv. FSTEK Rossii 5 fevralya 2021 g.) Dokument ne opublikovan // SPS "Konsul'tantPlyus".
8. Pasport nacional'nogo proekta "Nacional'naya programma "Cifrovaya ekonomika Rossijskoj Federacii". Utv. prezidiumom Soveta pri Prezidente RF po strategicheskomu razvitiyu i nacional'nym proektam, protokol ot 4 iyunya 2019 g. № 7. — URL: https://digital.gov.ru
9. *Zharova A., Elin V.* State regulation of the IoT in the Russian Federation: Fundamentals and challenges // Inter-

national Journal of Electrical and Computer Engineering. 2021. Vol. 11. No 5. P. 4542–4549. DOI 10.11591/ijece.v11i5.pp4542-4549. EDN TLEEFT.
10. *Samatov K.* Umnyj dom i umnyj gorod: KII ili net? 13/12/21. — URL: https://www.itsec.ru/articles/umnyj-dom-i-umnyj-gorod-kii-ili-net
11. Bazovaya model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh (Vypiska) (utv. FSTEK RF 15 fevralya 2008 g.) Dokument ne opublikovan // SPS "Konsul'tant Plyus".
12. Ukaz Prezidenta RF ot 30 marta 2022 g. No 166 "O merah po obespecheniyu tekhnologicheskoj nezavisimosti i bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii" // SZ RF. 2022. No 14. St. 2242.
13. *Petrova E.* Ushel i ne vernulsya: kakie IT-kompanii pokinuli Rossiyu i kto smozhet zanyat' ih mesto. — URL: https://hightech.fm/2022/05/26/it-companies-went-away
14. *Shabalin Yu.* Opasnost' komponent s otkrytym iskhodnym kodom v cifrah na real'nom proekte. — URL: https://www.itsec.ru/articles/opasnost-komponent-s-otkrytym-iskhodnym-kodom-v-cifrah-na-real-nom-proekte
15. Genprokuror Rossii Igor' Krasnov provel soveshchanie po teme bor'by s prestupleniyami, svyazannymi s posyagatel'stvami na bezopasnost' v sfere ispol'zovaniya informacionno-kommunikacionnyh tekhnologij. — URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news/archive?item=56766040
16. Social'nyj portret prestupnosti. — URL: http://crimestat.ru/social_portrait
17. *Esayan A.K., Truncevskij Yu.V.* Obshchie podhody k normativnomu pravovomu regulirovaniyu tekhnologii v sfere "Umnyj gorod" // Mezhdunarodnoe publichnoe i chastnoe pravo. 2020. No 1. S. 36–41. DOI: 10.18572/1812-3910-2020-1-36-41.
18. Prikaz Minstroya Rossii ot 25 dekabrya 2020 g. No 866/pr "Ob utverzhdenii Koncepcii proekta cifrovizacii gorodskogo hozyajstva "Umnyj gorod" // Informacionnyj byulleten' o normativnoj, metodicheskoj i tipovoj proektnoj dokumentacii. 2021. No 1-2.
19. *Efremova M.A.* Ugolovno-pravovaya ohrana informacionnoj bezopasnosti: special'nost' 12.00.08 "Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo": diss. ... dokt. yur. nauk. M., 2017. 427 s. EDN GNIILS.
20. *Zharova A.K.* Pravovoe obespechenie informacionnoj bezopasnosti v "umnyh gorodah" // Yurist. 2019. No 12. S. 69–76. DOI: 10.18572/1812-3929-2019-12-69-76.
21. *Grishchenko L.L., Revin S.M., Korotaev Yu.V.* "Umnye" tekhnologii pri obespechenii bezopasnosti v "umnom gorode"// Municipal'naya akademiya. 2020. No 2. S. 186–191.
22. Cifrovaya ekonomika: aktual'nye napravleniya pravovogo regulirovaniya: nauchno-prakticheskoe posobie / M.O. D'yakonova, A.A. Efremov, O.A. Zajcev i dr.; pod red. I.I. Kucherova, S.A. Sinicyna. M.: IZiSP; NORMA, 2022. 376 s. DOI: 10.12737/1839690.
23. *Elin V.M.* Sravnitel'nyj analiz pravovogo obespecheniya informacionnoj bezopasnosti v Rossii i za rubezhom / pod obshchej red. A.P. Baranova. M.: Moskovskij institut gosudarstvennogo upravleniya i prava, 2016. 168 s. (Informacionnoe pravo i kiberbezopasnost'). ISBN 978-5-9909450-7-4. EDN XRCLFL.
24. *Golovenchik G., Krasko G., Golovenchik M.* Problemy kiberbezopasnosti umnyh gorodov // Nauka i innovacii. 2020. No 12(214). S. 51–57. EDN STLLAY.
25. *Kel'm S.I.* Sostoyanie, struktura i dinamika prestupnosti v sfere zhilishchno-kommunal'nogo hozyajstva // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. 2021. No 2 (90). S. 84–90. DOI: 10.35750/2071-8284-2021-2-84-90.
26. Ugolovno-yurisdikcionnaya deyatel'nost' v usloviyah cifrovizacii: monografiya / N.A. Golovanova, A.A. Gravina, O.A. Zajcev i dr. M.: IZiSP; KONTRAKT, 2019. 212 s.
27. Nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii // https://beta.dostoevsky.io/ru/274.1/2020/parts/
28. *Krajnova N.A.* Prava i tekhnologii v sfere protivodejstviya kiberugrozam // Pravo i cifrovaya ekonomika. 2021. No 2. S. 23-31. DOI: 10.17803/2618-8198.2021.12.2.023-031.
29. *Begishev I.R.* Bezopasnost' kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii // Bezopasnost' biznesa. 2019. No 1. S. 27–32.
30. *Bugaev V.A., Chajka A.V.* Faktory prestupnosti v sfere komp'yuternyh tekhnologij // Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo // Yuridicheskie nauki. 2019. No 4. S. 139–145. EDN EJELBM.
31. Postanovlenie Pravitel'stva RF ot 12 oktyabrya 2019 g. No 1320 "Ob utverzhdenii Pravil predostavleniya subsidij iz federal'nogo byudzheta na vvedenie v ekspluataciyu i obespechenie funkcionirovaniya kiberpoligona dlya obucheniya i trenirovki specialistov i ekspertov raznogo profilya, rukovoditelej v oblasti informacionnoj bezopasnosti i informacionnyh tekhnologij sovremennym praktikam obespecheniya bezopasnosti" // SZ RF 2019. No 42 (Ch. III). St. 5913.

32. Ataka na "umnyj" gorod: kak proshli kiberucheniya po zashchite infrastruktury. — URL: https://trends.rbc.ru/trends/industry/cmrm/5fd1dc729a7947a505d40c26
33. Otkrytye sistemy // SUBD. 2022. No 2. — URL: https://www.osp.ru/os/2022/02/13056210
34. Infografika. — URL: https://bdu.fstec.ru/charts
35. Aktual'nye kiberugrozy: I kvartal 2022 goda. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/#id2
36. Kratkaya harakteristika sostoyaniya prestupnosti v Rossijskoj Federacii za yanvar'-iyun' 2021 g. — URL: https://mvd.rf/reports/item/25094008/
37. Byl' i ubyl': chislo prestuplenij s ispol'zovaniem IT upalo vpervye za 5 let. S chem svyazana pozitivnaya dinamika i sohranitsya li etot trend. — URL: https://iz.ru/1371417/roza-almakunova/byl-i-ubyl-chislo-prestuplenii-s-ispolzovaniem-it-upalo-vpervye-za-5-let
38. *Reshetnikov A.Yu., Russkevich E.A.* Ob ugolovnoj otvetstvennosti za nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii (st. 274.1 UK Rossii) // Zakony Rossii: opyt, analiz, praktika. 2018. No 2. S. 51–55.
39. Federal'nyj zakon ot 14 iyulya 2022 g. No 260-FZ "O vnesenii izmenenij v Ugolovnyj kodeks Rossijskoj Federacii i Ugolovno-processual'nyj kodeks Rossijskoj Federacii" // SZ RF 2022. No 29 (Ch. II). St. 5227.