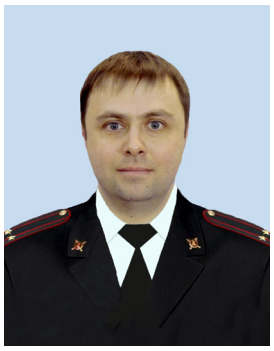
Научная статья
УДК 343.988
https://doi.org/10.36511/2078-5356-2024-3-208-215



Вопросы квалификации неправомерного доступа к объектам критической информационной инфраструктуры

Мельникова Екатерина Федоровна[1], Родионов Андрей Дмитриевич[2]
[1, 2]Нижегородская академия МВД России, Нижний Новгород, Россия,
[1]efmelnikowa@yandex.ru
[2]r-a-d@mail.ru

Аннотация. В статье проведен уголовно-правовой анализ преступления, предусмотренного частью 2 и частью 4 статьи 274[1] Уголовного кодекса Российской Федерации, — неправомерный доступ к объектам критической информационной инфраструктуры Российской Федерации. Авторами проведено сравнительное исследование объектов регулирования Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и частью 2 и частью 4 статьи 274[1] Уголовного кодекса Российской Федерации, дана юридическая оценка преступным действиям, выраженным в неправомерном доступе к сведениям с использованием чужой учетной записи при отсутствии таковых прав на нее. Рассмотрены вопросы квалификации преступлений в сфере компьютерной информации на примерах судебно-следственной практики.

Ключевые слова: компьютерная информация, неправомерный доступ, объекты критической информационной инфраструктуры, компьютерные экспертизы, вредоносные компьютерные программы

Для цитирования: Мельникова Е. Ф., Родионов А. Д. Вопросы квалификации неправомерного доступа к объектам критической информационной инфраструктуры // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 3 (67). С. 208–215. https://doi.org/10.36511/2078-5356-2024-3-208-215.

Original article

Issues of qualification of unauthorized access to critical information infrastructure facilities

Ekaterina F. Melnikova[1], Andrey D. Rodionov[2]
[1, 2]Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation
[1]efmelnikowa@yandex.ru
[2]r-a-d@mail.ru

Abstract. The article provides a criminal legal analysis of the crime provided for in part. 2.4 tbsp. 274[1] of the Criminal Code of the Russian Federation — unlawful access to objects of critical information infrastructure of the

Russian Federation. The authors conducted a comparative study of the objects regulated by the federal law no. 187-FZ of July 26, 2017 “On the security of critical information infrastructure of the Russian Federation” and part. 2.4 tbsp. 274[1] of the Criminal Code of the Russian Federation, a legal assessment is given to criminal actions expressed in unlawful access using someone else’s account in the absence of such rights to it. The issues of qualification of crimes in the field of computer information are considered using examples of forensic investigative practice.

Keywords: computer information, unauthorized access, critical information infrastructure objects, computer forensics, malicious computer programs

For citation: Melnikova E. F., Rodionov A. D. Issues of qualification of unauthorized access to critical information infrastructure facilities. *Legal Science and Practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2024, no. 3 (67), pp. 208–215. (In Russ.). https://doi.org/10.36511/2078-5356-2024-3-208-215.

Уровень цифровой модернизации России за последнее время существенно изменился и находится на лидирующем месте среди развитых стран мира. Цифровая логистика, государственные услуги, цифровые реестры сделали нашу жизнь удобной и быстрой. Россия уже не является аналоговой страной, поскольку в настоящее время мы полностью находимся в цифровой среде. Все платежи осуществляются дистанционно, в том числе налоговые и коммунальные, широко распространена телемедицина, в результате внедрения системы *FACE PAY* вход в московское метро стал возможен без платежных карт, путем распознавания лиц, что повысило уровень безопасности, а у правоохранительных органов появилась возможность отслеживать трекинг населения в общественном транспорте. Всеохватывающая цифровизация позволила добиться принципиального повышения уровня эффективности в той или иной отрасли. Это значительно повлияло на развитие экономики, на уровень ее доходности и рентабельность бизнеса. Государственные организации также не остались на периферии в плане цифровизации. Благодаря ежедневной обработке колоссальных объемов данных, в том числе персональных, информационный кластер внесен в специальные единые цифровые системы, к примеру, в российской медицине существует Единая государственная информационная система здравоохранения (далее — ЕГИСЗ). Удобство использования появившейся цифровой среды в России является неотъемлемым преимуществом перед устаревшим бумажным учетом, но при этом ее уязвимость от неправомерного воздействия со стороны третьих лиц является ее недостатком. Особенно это стало актуально в период противоборства со странами Запада. Ввиду этого в 2017 году был введен Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — ФЗ № 187-ФЗ) [1]. К объектам критической информационной инфраструктуры (далее — ОКИИ) относится совокупность информационных систем и телекоммуникационных сетей, критически важных для работы ключевых сфер жизнедеятельности государства и общества: здравоохранения, промышленности, связи, транспорта, энергетики, городского хозяйства. Защита данных объектов занимает приоритетное место в государственной политике, особенно в период военных действий, когда противоборствующие страны стремятся нанести не только силовой удар, но также и удар по более уязвимым сферам, таким как медицина, промышленность и др.

Реестр подобных объектов ведется Федеральной службой по техническому и экспортному контролю (далее — ФСТЭК). В свою очередь, субъекты критической информационной инфраструктуры должны обеспечивать достоверность и актуальность сведений, содержащихся в эксплуатируемых ими базах данных и программном обеспечении. В связи с введением вышеуказанного закона в 2017 году в Уголовный кодекс Российской Федерации (далее — УК РФ) [2] была добавлена статья 274[1] («Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»). Ответственность по данной статье наступает в случаях создания, распространения и (или) использования компьютерных программ, предназначенных для уничтожения, блокирования, модификации, копирования информации, содержащейся в критической информационной инфраструктуре Российской Федерации, а также внесение заведомо недостоверных сведений в ОКИИ, согласно части 2 и части 4 статьи 274[1], за неправомерный доступ к таковым, в том числе с использованием своего служебного положения. Предмет исследования

выбранной нами тематики включает части 2 и части 4 статьи 274[1] УК РФ ввиду наибольшего распространения данного состава преступления и сложности квалификации, вызываемой корреляцией со статьей 272 УК РФ.

С момента введения данная норма показала свою эффективность и востребованность. По данным Министерства внутренних дел Российской Федерации, в 2018 году было зарегистрировано лишь одно преступление (в Камчатском крае), в 2019 — 4, в 2020 — 22, в 2021 — 159, за 2022 год зарегистрировано уже 519 преступлений (рост на 226,41 %) однако в 2023 году имеется снижение роста, преступности: выявлено 52 преступления в Московской, Астраханской, Кировской областях [3]. Такая тенденция связана в основном с особенностями квалификации и применения данной статьи. Забегая немного вперед, нужно сказать, что по данной статье к уголовной ответственности привлекают в основном медицинских работников, которые, в свою очередь, осуществляя неправомерный доступ, модифицируют сведения ЕГИСЗ. Это особенно было актуально в период пандемии COVID-19. Но только ли для наказания за подобные случаи законодателем была создана статья 274[1] УК РФ в целом и рассматриваемые нами вторая, четвертая части статьи? Или законодатель возлагал на нее большие надежды в виде защиты цифровых государственных кластеров от хакерских атак и иного преднамеренного причинения вреда критической информационной инфраструктуре Российской Федерации? Для этого необходимо рассмотреть ретроспективу ее правоприменения.

Судебная практика по части 2 и части 4 статьи 274[1] УК РФ неоднозначна. Не совсем очевидным остается вопрос о толковании предмета рассматриваемого преступления. Первоначально на стадии правоприменения данной статьи суды и следственные органы исходили из того, что предметом преступления являются категорированные ОКИИ. Так, приговором Ленинского районного суда Владивостока гражданин Б. осужден к двум годам лишения свободы по части 2 статьи 274[1] УК РФ. Из материалов дела известно, что следствие направляло запрос в Управление ФСТЭК России по Дальневосточному федеральному округу, согласно которому включение системы самообслуживания абонентов «Сервис самообслуживания абонентов ПАО «Мегафон» в перечень, утверждаемый субъектом КИИ (ПАО «Мегафон»), является документальным подтверждением того, что данная система определена как объект ОКИИ, подлежащий категорированию филиала ПАО «Мегафон». В результате совершения преступления нанесен существенный вред критической информационной инфраструктуре Российской Федерации [4].

По мнению ряда правоприменителей, ситуация видится иначе: ОКИИ должны признаваться все без исключения информационные системы субъекта, независимо от их категорирования и участия в обеспечении критических процессов. Интересным представляется апелляционное определение Астраханского областного суда. Из материалов дела известно, что гражданин Б., работая в салоне сотовой связи МТС осуществил неправомерный доступ через систему «Единое окно», где имеются персональные данные клиентов, и за вознаграждение предоставлял указанные сведения иным лицам. Его действия были квалифицированы по части 4 статьи 274[1] УК РФ. В данной апелляционной жалобе стороной защиты указано, что в соответствии с постановлением Правительства Российской Федерации № 127 [5] в ПАО «МТС» имеется акт категорирования объектов, но при этом система «Единое окно», с помощью которой злоумышленник осуществил неправомерный доступ, не имеет ни одной из трех значимых категорий. Доводы стороны обвинения противоположны. Представитель ФСТЭК России отмечает, что ПАО «МТС» является субъектом критической информационной инфраструктуры Российской Федерации, а информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере связи, — ОКИИ, независимо от того, категорированы они или нет. Если даже объект ОКИИ не обеспечивает критические процессы, он не перестает быть ОКИИ, поэтому составление перечня ОКИИ не нужно путать с перечнем объектов критической информационной инфраструктуры, подлежащих категорированию [6]. Суд поддержал доводы стороны обвинения, и апелляционная жалоба была оставлена без удовлетворения.

Вышеуказанные примеры из судебной практики не могут образовывать состав преступления, предусмотренный статьей 274[1] УК РФ. С учетом вышесказанного, действия преступников по поводу внесения ложных сведений в ЕГИСЗ требуют квалификации по статье 272 УК РФ («Неправомерный доступ к компьютерной информации»).

Сложность определения предмета преступления, предусмотренного частью 2 и частью 4

статьи 274[1] УК РФ, возникла ввиду того, что в ФЗ № 187-ФЗ существуют два термина: «значимые объекты» и «объекты критической информационной инфраструктуры». Значимые объекты должны быть категорированы в обязательном порядке. К объектам относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры в различных областях, таких как здравоохранение, связь, энергетика, металлургическая и химическая промышленность. Кроме того, интересным представляется формулировка, что кроме крупных организаций к ОКИИ также относятся и индивидуальные предприниматели, которым на праве собственности или аренды принадлежат информационные сети, обеспечивающие взаимодействие указанных систем. Это весьма расширительное толкование приводит к отсутствию понимания, что же входит в ОКИИ, кроме того, таким кругом объектов трудно управлять и контролировать.

Ввиду этого у правоприменителя появляется сложность квалификации преступлений. Если объект не категорирован, то является ли он предметом преступления согласно части 2 и части 4 статьи 274[1] УК РФ, или данное деяние следует квалифицировать по статье 272 УК РФ? Практика отнесения сетей и объектов связи, которые являются обеспечивающими ОКИИ, не распространена. Чаще всего суды и следствие в таких случаях квалифицируют действия виновного по статье 272 УК РФ, не пользуясь расширительным толкованием ФЗ № 187-ФЗ. Представляется очевидным, что данный вопрос требует разъяснений Верховного Суда Российской Федерации.

Одно из первых уголовных дел, связанных с неправомерным доступом к ОКИИ, рассмотрено Первомайским районным судом Владивостока [7] по факту причинения имущественного вреда оборонному предприятию (ОКИИ). Группа лиц по предварительному сговору с помощью программного обеспечения проникла через протокол удаленного доступа в компьютеры оборонного предприятия, зашифровала данные на жестком диске и потребовала выкуп в виде криптовалюты в размере одного биткойна. Суд принял во внимание явку с повинной и добровольное возмещение ущерба и в особом порядке назначил наказание в виде лишения свободы сроком на два года с лишением права заниматься деятельностью, связанной с доступом к критической информационной инфраструктуре Российской Федерации сроком на два года.

Однако, начиная с 2019 года судебная практика меняется: по части 2 и части 4 статьи 274[1] УК РФ к уголовной ответственности стали привлекать в основном медицинских работников за изготовление поддельных сертификатов о прививках от COVID-19.

Так, в Кизилюрт Республики Дагестан в 2021 году программист городской больницы воспользовался логином и паролем коллеги к ЕГИСЗ, чтобы незаконно получить сертификат о вакцинации от коронавируса и *QR*-код для себя и своих родственников. Пароль и логин программист узнал, когда коллега, имевшая доступ к ЕГИСЗ, попросила его внести логин и пароль в настройки браузера: пароль был длинный, и его сложно было запомнить. Поскольку имелась в виду двухкомпонентная вакцина, то через 21 день были проделаны аналогичные действия. Данные преступные действия программиста стали известны, когда один из его родственников на очередном приеме у врача сознался, что не делал вакцинацию. Подсудимого приговорили к 3 годам и 6 месяцам условно с лишением права заниматься деятельностью в сфере компьютерных технологий на 2 года [8].

Похожее уголовное дело было рассмотрено Советским районным судом Нижнего Новгорода. В 2022 году был вынесен приговор в отношении гражданки Б., участковой медсестры поликлиники Советского района Нижнего Новгорода, которая внесла недостоверные сведения за вознаграждение в размере 2 000 рублей в ЕГИСЗ о вакцинированных от коронавирусной инфекции COVID-19 без фактического ее проведения. Подсудимая была признана виновной в совершении 100 тяжких преступлений, предусмотренных частью 2 статьи 274[1] УК РФ. За содеянное суд приговорил Б. к 5 годам лишения свободы [9].

Еще один аналогичный случай произошел на территории Советского района Нижнего Новгорода, где в отношении гражданки А., врача-терапевта городской поликлиники, было возбуждено уголовное дело по факту внесения посредством компьютера недостоверных сведений о профилактических прививках за вознаграждение в размере 6 000 рублей. Таким образом, гражданка А. совершила неправомерный доступ к ОКИИ и изменила составляющие ее данные. За совершение шести аналогичных эпизодов подсудимая осуждена к 3 годам

и 6 месяцам лишения свободы по части 2 статьи 274[1] УК РФ [10].

Рассматривая судебную практику, удивительным представляется полярность субъектов, которые привлекаются к уголовной ответственности: хакеры и медсестры поликлиник, что вызывает вопрос о соизмеримости общественной опасности вышеописанных действий и предусмотренной УК суровостью наказания по части 2 и части 4 статьи 274[1] УК РФ. Исходя из вышесказанного, если лицо внесло ложную запись о вакцинации, например, в журнал учета профилактических прививок по форме 064/у, то уголовная ответственность по статье 274[1] УК РФ ему не грозит, а будет вменяться статья 292 УК РФ (служебный подлог), наказание за которое не превышает 4 лет лишения свободы, что является преступлением средней тяжести. Но если внесение должностным лицом такой записи было осуществлено не с помощью шариковой ручки, а с помощью компьютера, то подобное действие квалифицируется как тяжкое преступление. Очевидно, что практика применения части 2 и части 4 статьи 274[1] УК РФ не может расцениваться как справедливая и адекватная. Вряд ли законодатель вкладывал в уголовный закон посыл столь жестокого уголовного преследования за модификацию электронной системы учреждений здравоохранения. Подобный перекос появился из-за неверного толкования норм уголовного закона в системе общего правового регулирования.

Согласно диспозиции статьи 274[1] УК РФ уголовная ответственность наступает в том случае, если деяние повлекло причинение вреда ОКИИ Российской Федерации. Позиция Конституционного Суда Российской Федерации по поводу толкования норм права такова: любое преступление должно быть четко определено в законе таким образом, чтобы каждый мог понимать, за какие действия или бездействия наступит уголовная ответственность. Таким образом, важны ясность нормы для любого толкователя (суда, следователя, потерпевшего, обвиняемого) и определение ее места в общей системе правового регулирования [11], а также соизмеримость наказания за преступления, повлекшие примерно одинаковые последствия. Кроме того, оценка нормы должна проводиться не только с учетом ее буквального смысла, но и смысла, придаваемого ей официальным и иным толкованием, в том числе с учетом иных нормативных актов, а также с учетом сложившейся правоприменительной практики [11].

Поскольку статья 274[1] УК РФ существует в неразрывной связи с ФЗ № 187-ФЗ, необходимо обратить внимание и на содержание данного закона.

Объективная сторона преступления, предусмотренного частью 2 и частью 4 статьи 274[1] УК РФ характеризуется действиями, состоящими в неправомерном доступе к ОКИИ.

Неправомерность доступа к компьютерной информации, согласно статье 272 УК РФ, можно разделить на два вида:

1) совершаемые условно неправомерно;

2) совершаемые безусловно неправомерно [12].

Для первого вида характерно совершение противоправных действий лицом, которое обладает определенными служебными полномочиями в той или иной организации, что закреплено трудовым договором, а также должностной инструкцией, на основании чего данным сотрудникам разрешен доступ к компьютерной информации в рамках осуществления своей профессиональной деятельности. Доступ к такой компьютерной информации в личных целях, включая корыстную заинтересованность, карается законом.

Второй вид представляет собой неправомерный доступ, который осуществляется лицами, не имеющими права доступа к подобным сведениям. Но в статье 1 ФЗ № 187-ФЗ сказано, что регулированию подлежат общественные отношения в области обеспечения безопасности критической инфраструктуры Российской Федерации при проведении в отношении нее *компьютерных атак.* Подобное воздействие на ОКИИ может быть осуществлено только с помощью специальных программно-аппаратных средств и вредоносных программ, например, внедрение вирусов, использование специальных вредоносных приложений (троянов), переполнение буфера, *DDoS*-атака (перегрузка системы, когда обслуживание пользователей делается невозможным), фишинг, использование слабых мест на сервере и др. Исходя из объекта, можно понять и цели ФЗ № 187-ФЗ: это охрана ОКИИ от компьютерных атак, при этом неправомерный доступ не является объектом правового регулирования данного федерального закона.

Что касается субъекта, то согласно статье 274[1] УК РФ им является лицо, достигшее возраста 16 лет. Кроме того, четвертая часть предусматривает специальный субъект — лицо, совершающее преступление с использованием своего служебного положения. Этот признак

субъекта имеет место в том случае, если действия лица находились в пределах его служебной компетенции, но совершались с явным нарушением порядка осуществления своих функциональных обязанностей, установленных законом или иным нормативным актом.

Субъективная сторона рассматриваемого преступления выражается в умышленных действиях, направленных именно на причинение вреда категорированным объектам. Но поскольку сведения о категорированности таковых являются ограниченными к ознакомлению, то возникает вопрос: если их нет в свободном доступе, то как доказать прямой умысел лица, если, совершая неправомерный доступ, злоумышленник не может знать категорирован объект или нет? Чаще всего органы следствия и суды для доказывания именно прямого умысла руководствуются наличием у лица должностной инструкции и прямо установленных в ней прав и обязанностей, а также наличием сведений из ФСТЭК о категорированности объекта. Также для глобализации явления категорированности цифровых данных в настоящее время активно привлекают организации к административной ответственности по статье 19.7.15 Кодекса об административных правонарушениях Российской Федерации в случае, если они вовремя не предоставили сведения для категорирования объектов, которые подпадают под соответствующие требования, таким образом исключая в дальнейшем спорные вопросы в суде о доказанности умысла на неправомерный доступ к ОКИИ.

Важным аспектом при квалификации является определение последствий, а именно вреда, который может быть причинен ОКИИ в результате совершения преступления, так как состав по рассматриваемой статье является материальным. В статье 7 ФЗ № 187-ФЗ сказано о прекращении или нарушении функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также об отсутствии доступа к государственной услуге. Таким образом, в ФЗ № 187-ФЗ и статьях 274^1 УК РФ сказано о нарушении или прекращении работы ОКИИ и создании угрозы безопасности ОКИИ. Очевидно, если произведена хакерская атака на систему электрической подстанции и во всех домах погас свет, то злоумышленника следует привлечь к уголовной ответственности по статье 274^1 УК РФ. В данном случае нарушена устойчивая работоспособность ОКИИ. Таким образом, можно сделать вывод, что фальсификация сведений, не нарушивших работу ОКИИ и не причинивших вред, предусмотренный ФЗ № 187-ФЗ, не может квалифицироваться по части 2 и части 4 статьи 274^1 УК РФ.

Исходя из вышесказанного, смысл, заложенный законодателем в ФЗ № 187-ФЗ и статье 274^1 УК РФ, не в полной мере соответствует практике правоприменения.

Проведенный уголовно-правовой анализ показал, что в законодательстве имеется еще достаточно много противоречий и неточностей применения статьи 274^1 УК РФ. Прежде всего, это касается объекта регулирования. В настоящее время Верховному Суду Российской Федерации необходимо внести разъяснения, что относится к ОКИИ, являются ли сети, коммуникации, вспомогательное программное обеспечение частью ОКИИ или нет. Спорным также остается вопрос реализации объективной стороны преступления. ФЗ № 187-ФЗ регулирует преступное поведение, совершенное с помощью хакерских атак на ОКИИ. Безусловно, расследование преступлений по данной категории дел связано не только с законодательными пробелами, а также и с отсутствием экспертов и специалистов, обладающих специальными познаниями, достаточными для проведения программно-технических исследований.

Список источников

1. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 года № 187-ФЗ // Собрание законодательства РФ. 2017. № 31, ст. 4736.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (ред. от 28 апреля 2023) // Собрание законодательства РФ. 1996. № 25, ст. 2954.

3. Состояние преступности. URL: https://мвд.рф/reports (дата обращения: 01.03.2024).

4. Приговор Ленинского районного суда г. Владивостока Приморского края от 7 октября 2020 года № 1-366/2020. URL: https://sudact.ru/regular/doc/2UTJssITJZHX/?page=6&regular-txt=&regularcase_doc=&regular-lawchunkinfo (дата обращения: 05.02.2023).

5. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: постановление Правительства Российской Федерации от 8 февраля 2018 года № 127

(ред. от 20 декабря 2022 года) (с изм. и доп., вступ. в силу с 21 марта 2023 года). URL: https://base.garant.ru (дата обращения: 02.04.2023).

6. Апелляционное определение Астраханского областного суда от 14 апреля 2022 года № 22-787/2022. URL: https://судебныерешения.рф/67736586/ (дата обращения: 05.02.2023).

7. Приговор Первомайского районного суд г. Владивостока по делу № 1-376/2019 части 4 статьи 274[1] УК РФ. URL: https://судебныерешения.рф/67736586/ (дата обращения: 05.02.2023).

8. Приговор Кизилюртовского районного суда г. Кизилюрт Республики Дагестан по делу № 1-148/2021, части 4 статьи 274[1]. URL: https://судебныерешения.рф/67736586/ (дата обращения: 05.02.2023).

9. Приговор Советского районного суда г. Нижнего Новгорода по делу № 1-300/2022. URL: https://sovetsky-nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=68535920&case_uid=1a61dbce-4bfa-4e69-89f5-205891e37253&delo_id=1540006 (дата обращения: 17.03.2024).

10. Приговор Советского районного суда г. Нижнего Новгорода по делу № 1-69/2023 (1-444/2022;). URL: https://sovetsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=6853 5920&case_uid=1a61dbce-4bfa-4e69-89f5-205891 e37253&delo_id=1540006 (дата обращения: 17.03.2024).

11. Конституционный Суд Российской Федерации: 30 лет на защите прав граждан на примерах практики. URL: https://www.ksrf.ru/ru/Decision/Documents/ (дата обращения: 05.12.2023).

12. Поздышев Р. С. Вопросы квалификации преступлений в сфере компьютерной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1 (61).

References

1. On the Security of the Critical Information Infrastructure of the Russian Federation: federal law no. 187-FZ dated July 26, 2017. *Collection of Legislation of the RF*, 2017, no. 31, art. 4736. (In Russ.)

2. The Criminal Code of the Russian Federation no. 63-FZ of dated June 13, 1996 (ed. dated April 28, 2023). *Collection of legislation of the RF*. 1996. № 25, art. 2954. (In Russ.)

3. The state of crime. URL: https://мвд.рф/reports (accessed 01.03.2024). (In Russ.)

4. Verdict of the Leninsky District Court of Vladivostok, Primorsky Territory no. 1-366/2020 dated October 7, 2020. URL: https://sudact.ru/regular/doc/2UTJsslTJZHX/?page=6&regular-txt=&regular-case_doc=&regular -lawchunkinfo (accessed 05.02.2023) (In Russ.)

5. On approval of the Rules for categorizing critical information infrastructure facilities of the Russian Federation, as well as the list of indicators of the criteria for the significance of critical information infrastructure facilities of the Russian Federation and their values: Resolution of the Government of the Russian Federation no. 127 of February 8, 2018 (as amended on December 20, 2022) (as amended and supplemented, entered into force on March 21, 2023). URL: https://base.garant.ru (accessed 02.04.2023) (In Russ.)

6. Appellate ruling of the Astrakhan Regional Court no. 22-787/2022 dated April 14, 2022. URL: https://судебныересения.рф/67736586/ (date of access: 05.02.2023) (In Russ.)

7. Verdict of the Pervomaisky District Court of Vladivostok in case no. 1-376/2019, part 4, art. 2741 of the Criminal Code of the Russian Federation. URL: https://судебныересения.рф/67736586/ (accessed 05.02.2023) (In Russ.)

8. Verdict of the Kizilyurt District Court of the city of Kizilyurt, Republic of Dagestan in case no. 1-148/2021, part 4 of art. 2741. URL: https://судебныересения.рф/67736586/ (accessed 05.02.2023) (In Russ.)

9. Verdict of the Sovetsky District Court of the city of Nizhny Novgorod in case no. 1-300/2022. URL: https://sovetsky-nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=68535920&case_uid=1a61dbce-4bfa-4e69-89f5-205891e37253&delo_id=1540006 (accessed 17.03.2024) (In Russ.)

10. Verdict of the Sovetsky District Court of Nizhny Novgorod in case no. 1-69/2023 (1-444/2022;). URL: https://sovetsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=68535920&case_uid=1a61dbce-4bfa-4e69-89f5-205891e37253&delo_id=1540006 (accessed 17.03.2024) (In Russ.)

11. The Constitutional Court of the Russian Federation: 30 years of protecting the rights of citizens based on practical examples. URL: https://www.ksrf.ru/ru/Decision/Documents/ (accessed 05.12.2023). (In Russ.)

12. Pozdyshev R. S. Issues of qualification of crimes in the field of computer information. *Legal science and practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2023, no. 1 (61). (In Russ.)

Информация об авторах

Е. Ф. Мельникова — кандидат юридических наук, старший преподаватель кафедры предварительного расследования Нижегородской академии МВД России;

А. Д. Родионов — старший преподаватель кафедры предварительного расследования Нижегородской академии МВД России.

Information about the authors

E. F. Melnikova — Candidate of Legal Sciences (Law), Senior Lecturer of the Department of Preliminary Investigation of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia;

A. D. Rodionov — Senior Lecturer, Department of Preliminary Investigation, Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia.

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2024, no. 3 (67)