Право. Журнал Высшей школы экономики. 2021. Т. 13. № 4.
Law. Journal of the Higher School of Economics. 2021. Vol. 13, no. 4.

Научная статья
УДК: 343.3/7
DOI: 10.17323/2072-8166.2021.4.152.176

Преступления в сфере компьютерной информации: критический взгляд

Юлия Викторовна Грачева[1],

Сергей Владимирович Маликов[2],

Александр Иванович Чучаев[3]

[1,2] Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), Москва, Россия

[3] Институт государства и права РАН, Москва, Россия

[1] uvgracheva@mail.ru, https://orcid.org/ 0000-0002-3341-7422

[2] s.v.malikov@yandex.ru, https://orcid.org/ 0000-0003-0892-2328

[3] moksha1@rambler.ru, https://orcid.org/ 0000-0002-5144-052X

Аннотация

Использование в правовых документах ссылок на частные технологические решения, реализующие тот или иной процесс, имеет риски оставить без оценки широкий спектр противоправных деяний в цифровой среде. Такой подход рискует описывать только существующие на определенный момент технологии и последствия их неправомерного применения, что, наблюдая динамику современного технологического развития, не выглядит предусмотрительным. Все это требует пересмотра терминологии Уголовного кодекса с целью адекватного парирования угроз в сфере компьютерной информации. В статье дается критический анализ необходимости специальных средств защиты и необходимости полномочий при квалификации действий, посягающих на компьютерную информацию. Факт наличия или отсутствия специальных средств защиты не всегда является существенным при определении преступности деяния. Возможно предоставление доступа к информации в результате технологических особенностей средств передачи информации или по ошибке. В статье анализируются также способы совершения компьютерных преступлений. Указывается, что вредоносное воздействие на информацию не всегда является следствием именно несанкционированного доступа. В частности, охарактеризованы случаи таких видов вредоносного воздействия

на информацию как отказ в обслуживании; передача ложной информации; атака посредника; веб-инжект; физическое воздействие. Наибольшая критика анализируемых преступлений связана с формулированием законодателем таких последствий, как уничтожение, блокирование, модификация либо копирование информации. В результате предложено авторское толкование ключевых понятий признаков составов преступлений, предусмотренных гл. 28 УК РФ. В качестве вывода констатируется, что преступления в отношении информации должны квалифицироваться как компьютерные вне зависимости от способа воздействия. Рассматривать последствия следует с точки зрения влияния на информационную систему в целом. При квалификации компьютерных преступлений не следует использовать в качестве конститутивных признаки, имеющие узко технологическую специфику. Перечень последствий может быть открытым, а их перечисление должно иметь лишь ориентирующий характер.

Ключевые слова

информационная безопасность, компьютерные преступления, компьютерная информация, неправомерный доступ, цифровизация, цифровые риски, последствия преступлений

Благодарности: публикация подготовлена при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16158.

Для цитирования: Грачева Ю.В., Маликов С.В., Чучаев А.И. Преступления в сфере компьютерной информации: критический взгляд // Право. Журнал Высшей школы экономики. 2021. № 4. С. 152-176. DOI: 10.17323/2072-8166.2021.4.152.176

Research article

Crimes in the Sphere of Computer Information: Critical Look

Yulia V. Gracheva[1],

Sergey V. Malikov[2],

Alexander I. Chuchaev[3]

[1,2] Kutafin Moscow State Law University, Moscow, Russia

[3] Institute of State and Law of the Russian Academy of Sciences, Moscow, Russia

[1] uvgracheva@mail.ru, https://orcid.org/ 0000-0002-3341-7422

[2] s.v.malikov@yandex.ru, https://orcid.org/ 0000-0003-0892-2328

[3] moksha1@rambler.ru, https://orcid.org/ 0000-0002-5144-052X

Abstract

The use of references in legal documents to private technological solutions that implement a particular process has the risks of leaving a wide range of illegal acts in the digital

environment unappreciated. Such an approach risks describing only the technologies that exist at a certain moment and the consequences of their illegal use, which, observing the dynamics of modern technological development, does not look prudent. All this requires a revision of terminology of the Criminal Code of the Russian Federation in order to adequately parry existing threats in the field of computer information. A critical analysis of the need to indicate special means of protection and the need for authority in the qualification of actions that infringe on computer information is given. The fact of the presence or absence of special means of protection is not always essential in determining the criminality of an act. It is possible to provide access to information as a result of technological features of the means of information transmission or by mistake. The article analyzes the following methods of committing computer crimes. The paper points out that the malicious impact on information is not always the result of unauthorized access. In particular, the cases of such types of malicious influence on information as: denial of service; transmission of false information; intermediary attack; web injection; physical impact. The greatest criticism of the analyzed crimes is related to the formulation by the legislator of such consequences as the destruction, blocking, modification or copying of information. As a result, the author's interpretation of the key concepts of signs of the elements of crimes provided for in Chapter 28 of the Criminal Code of the Russian Federation is proposed. As a conclusion, it is stated that information crimes should be classified as computer crimes, regardless of the method of influence. The consequences should be considered from the point of view of the impact on the information system as a whole. When qualifying computer crimes, you should not use as constitutive features that have a narrow technological specificity. The list of consequences can be open, and their enumeration should only be of an orienting nature.

Keywords

information security, computer crimes, computer information, illegal access, digitalization, digital risks, consequences of crimes

Acknowledgements: the publication was prepared with the financial support of the RFBR as part of the project No. 18-29-16158.

For citation: Gracheva Yu.V., Malikov S.V., Chuchaev A.I. Crimes in the sphere of computer information: critical look. *Law. Journal of the Higher School of Economics. 2021*, vol. 13, no. 4, pp. 152–176. (In Russ.). DOI: 10.17323/2072-8166.2021.4.152.176

Введение

Развитие цифровых технологий сформировало новую среду взаимодействия личности, общества и организаций. На заре технологического развития цифровые объекты и процессы использовались для учета, отражения и моделирования процессов жизни. Со временем развитие технологий привело к тому, что цифровые процессы стали использоваться для управления объектами реального мира, в том числе без непосредственного участия человека. Стало возможным изменять жизненные процессы, корректируя цифровые процессы.

Технологический скачок привел к появлению новых цифровых сущностей, понятий и процессов, не имеющих прямых аналогов в жизни человека,

общества и государства. Некоторые из этих сущностей имели ценность только для решения задач их владельца, но со временем все большее их количество стали приобретать объективную ценность и как следствие стали объектом аренды, купли-продажи с рыночной стоимостью в национальной валюте.

Другим фактором, изменившим взаимодействие личностей, стало изменение видов и способов коммуникаций. Цифровые технологии расширили возможности передачи информации, консолидации различных ее видов, а также влияние на человека. Увеличение количества цифровых активов, непосредственное влияние цифровых процессов на объекты реального мира, широкие возможности коммуникаций привели к миграции деловой, государственной и социальной активности в цифровую среду. К настоящему времени сформировалась среда, в которой ведется деловая, социальная активность; обмениваются и продают информационные активы, стоимость которых достигает миллиардов рублей; идут процессы, управляющие заводами и торговыми предприятиями; обеспечивается коммуникация и взаимное влияние, не имеющие исторических аналогов.

Рост стоимости активов и количества значимых для жизнедеятельности процессов также привел к появлению и непрерывному росту активности, направленной на присвоение чужой собственности, цифровому вандализму и иной деятельности криминального характера [Eun Y.-S., Aßmann J.S., 2016]; [Buchanan R., 2019]; [Stoddart K., 2016]. Естественным способом противодействия преступности в цифровой среде стало применение и непрерывное совершенствование мер информационной безопасности. Анализ рисков, совершенствование технических средств защиты информации, выявление и устранение уязвимостей программного обеспечения (далее — ПО) и информационных систем, оперативная реакция на изменение угроз безопасности легли в основу практики информационной безопасности.

Информационная безопасность как практика противодействия киберугрозам не снимает полностью проблемы компьютерных преступлений, в первую очередь потому, что ее задача — защита информационных активов их владельца, а решение социальных или государственных задач не является ее целью. Последние должны решаться путем правового регулирования. Юридическая защита информационных активов рассматривается как одна из важнейших мер обеспечения безопасности данных.

Нарастание криминальных рисков в цифровой среде предопределило появление отдельной группы норм в уголовном кодексе, направленных на охрану компьютерной информации — гл. 28 Уголовного кодекса Российской Федерации (далее — УК РФ). Скрупулезный анализ норм данной главы позволяет констатировать, что используемые понятия отстают от современных реалий, что вызывает сомнения в их применимости. Цель работы — дать оценку отдельным положениям норм гл. 28 УК РФ, выявить их недостатки и сформулировать предложения по изменению.

1. Постановка проблемы

На мировом уровне наиболее «унифицированным» преступным деянием в сфере компьютерной информации является неправомерный доступ к компьютерной информации. Согласно исследованию Управления ООН по наркотикам и преступности, неправомерный доступ (illegal access) является преступлением в 93% стран мира[1]. Характерно, что помимо частично унифицированного подхода к определению компьютерных преступлений, базирующегося на международных актах, страны по-разному подходят к криминализации отдельных компьютерных преступлений в зависимости от тех угроз, которые актуальны в каждом государстве. Так, в США первым актом об уголовной ответственности за совершение преступлений в сфере компьютерной информации был Закон о защите федеральных компьютерных систем (1977), позже вступил в силу закон об уголовной ответственности за компьютерные преступления — Закон о мошенничестве и злоупотреблении с использованием компьютеров (1984). В Великобритании составы новых компьютерных преступлений введены Законом о терроризме (2000). Германия закрепляет уголовную ответственность за преступления в сфере компьютерной информации впервые в рамках законодательства о борьбе с экономической преступностью (1987) [Громов Е.В., 2006: 30].

Это свидетельствует о единстве восприятия механизма компьютерного преступления, в котором вычислительная техника может быть орудием или средством совершения преступления, либо предметом посягательства. Однако даже в отечественном праве нет консенсуса в описании потенциальных рисков цифровизации общества, что прежде всего проявляется в терминологическом хаосе.

Значительное количество проблем возникает при трактовке деяния, предусмотренного ст. 272 Уголовного кодекса Российской Федерации (далее — УК РФ) «неправомерный доступ к информации». Более общее понятие (доступ к информации) введено Федеральным законом от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2] и определяется как возможность получения информации и ее использование. В отличие от понятия «доступ к информации», определения «неправомерный доступ к информации» в нормативном акте не дается.

Под данным деянием понимается тот или иной способ проникновения в информацию с использованием интеллектуальных средств или технических ресурсов компьютера, что позволяет совершать действия с компьютерной

[1] См.: Comprehensive Study on Cybercrime. Available at: http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_ 210213.pdf (дата обращения: 23.04.2021)

[2] С изм. и доп., вступ. в силу с 20.03.2021 // СЗ РФ.2006. № 31 (1 ч.). Ст. 3448.

информацией [Рарог А.И., 2018: 426]. Если у лица отсутствует право на доступ к компьютерной информации или лицо, обладающее таким правом, нарушает правила защиты информации и порядок воздействия на информацию, то такое воздействие на компьютерную информацию будет считаться неправомерным. Неправомерный доступ к компьютерной информации — незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации[3]. Иногда выделяется дополнительный признак неправомерного доступа — защищенность информации, т.е. доступ к незащищенной и открытой информации не будет являться уголовно наказуемым [Тропина Т.Л., 2005: 186].

По мнению Генеральной прокуратуры России, неправомерный доступ — это «доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты». Исходя из этого следует, что для квалификации деяния как преступного необходимо установление факта наличия специальных средств ее защиты и получение доступа без «необходимых полномочий».

В данном определении используется понятие «специальное средство защиты». В профессиональной среде к ним относят программные, аппаратные и физические средства защиты информации: интегрированный в прикладное приложение функционал авторизации; сервисы авторизации и аутентификации операционной системы; накладные специализированные средство разграничений прав доступа; внешние относительно информационной системы сервисы (например, сервисы google или apple); вспомогательные сервисы, позволяющие в одной информационной системе использовать одну службу авторизации; усиленные средства аппаратной аутентификации и др.

Таким образом, основные проблемы связаны с пониманием неправомерности доступа в части необходимости установления специальных средств защиты и наличия специальных прав.

2. Наличие специальных средств защиты информации как условие неправомерности доступа

Буквальное понимание неправомерного доступа приводит к тому, что для квалификации деяния как преступного требуется установление факта нали-

[3] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. Available at: URL: https://genproc.gov.ru/documents/nauka/execution /document-104550 (дата обращения: 23.04.2021)

чия специальных средств ее защиты и получение доступа без необходимых полномочий. Если обладатель информации самостоятельно предоставляет к ней доступ (в терминологии Генеральной прокуратуры — «наделяет полномочиями на доступ»), действия по ее компрометации осуществляются без преодоления технических средств защиты, поскольку нарушителю не приходится их преодолевать.

Факт наличия или отсутствия специальных средств защиты не всегда является существенным при определении преступности деяния. Возможно предоставление доступа к информации в результате технологических особенностей средств передачи информации или по ошибке.

2.1. Предоставление доступа к информации владельцем с целью ее обработки

В настоящее время многие задачи с применением информационных технологий решаются посредством передачи информации провайдерам IT-сервисов в силу того, что они требуют большой производительной мощности аппаратных ресурсов, например, обработка потоков данных, анализ больших объемов данных, обработка данных с помощью систем искусственного интеллекта и др. В связи с этим получили распространение системы, проводящие обработку потоков информации с использованием не только оборудования пользователя системы, но и так называемых облачных вычислительных и программных ресурсов.

К таким системам относятся, в частности, системы распознавания речи и перевода. Одна компонента программного обеспечения для таких решений устанавливается непосредственно на мобильный телефон, персональный компьютер или интегрируется в бытовую технику и т.п. и является фактически интерфейсной частью, взаимодействующей непосредственно с пользователем. Сами вычисления проводятся на серверных мощностях поставщика услуги.

Такая архитектура системы обусловлена намерением поставщиков сервисов обойти ограничения в вычислительных мощностях каждого конкретного пользователя сервиса. Такими ограничениям конечных устройствам являются, в частности: малая вычислительная мощность; малый объем оперативной памяти; отсутствие возможности хранить огромные объемы «моделей данных», с помощью которых осуществляется целевое действие. Применение сервисного подхода позволяет получать результат сложных вычислений для каждого отдельного пользователя, недостижимый с помощью его собственного оборудования. Для получения результата пользователь сервиса должен сначала отправить информацию на обработку.

Таким образом, вводя информацию в приложение стороннего поставщика, пользователь фактически передает эту информацию в приложение тре-

тьей стороны, откуда она в преобразованном или исходном виде по каналам сетей общего доступа передается на центры обработки данных поставщика сервиса, обрабатывается и результат обработки возвращается на оконечное устройство.

Другим примером таких сервисов является голосовой помощник — специальное программное обеспечение, устанавливаемое на мобильные телефоны, персональные компьютеры и другие устройства. Для распознавания команд голосового помощника необходимо анализировать весь поток аудиоинформации, преобразованный с помощью микрофона в электронные сигналы, а затем — в цифровую информацию. Если пользователь, например, диктует конфиденциальную информацию, она может попасть на сервер поставщика сервиса, где к ней могут получить доступ и использовать владельцы сервиса, не преодолевая технических ограничений доступа со стороны владельца информации.

Скрытое использование сервиса, выходящее за рамки декларированного основного функционала (определения голосовых команд), — весьма распространенное явление. Например, владельцы сервисов используют функции голосового ввода для распознавания предполагаемых потребностей покупателя и формирования рекламных кампаний. Формально лицензионное соглашение на использование сервиса позволяет это делать, но таким образом может происходить и сбор конфиденциальной информации, на что не может быть получено разрешения в условиях лицензионного соглашения как нарушающее законодательство.

Третий пример сервиса — программное обеспечение, предоставляющее возможность автоматического переключения шрифта между различными языками. Программа считывает все нажатия клавиш пользователя, фактически собирая всю информацию, вводимую пользователем, включая пароли. Эта информация может обрабатываться в локальном приложении (установленном непосредственно на оконечном устройстве) или пересылается на сервера владельца сервиса. Состав информации на наличие информации ограниченного доступа не может быть установлен автоматически, вследствие чего происходит распространение конфиденциальной информации.

Четвертый пример — программа, которая ведет сбор информации о нажатии клавиш клавиатуры с целью составления журнала. Принцип действия состоит в том, что пользователь вводит информацию, используя различные программы, а она аккумулируется в одном файле. Эти журналы могут быть переданы разработчику программного обеспечения, т.е. разработчики получают доступ, также не преодолевая средств защиты информации.

Таким образом, весь класс программного обеспечения и сервисов, использующих поступающие для обработки потоки информации в необработанном виде, содержит возможности несанкционированного использова-

ния информации охраняемой законом. Нарушения посредством такого рода получения доступа к информации, содержащую какого-либо вида тайну, по УК РФ не могут быть квалифицированы в качестве преступных.

2.2. Получение информации за счет изменения маршрута передачи информации (man-in-the-middle)

Следующая группа ситуаций касается действий криминального характера, в которых несанкционированный доступ может быть получен без преодолений средств защиты, поскольку используются технологические особенности передачи данных.

Первый пример — перехват данных, передаваемых по беспроводным сетям. Для получения доступа к информации преступник с помощью технических средств создает точку доступа Wi-Fi, в том числе она может быть представлена как бесплатная общественная точка доступа. В этой ситуации, подключаясь к Интернету, пользователь фактически сам настраивает передачу информации через оборудование преступника, исходя из предположения о добросовестности владельцев бесплатного сервиса. Такой информацией могут являться пароли и иные данные, не защищенные посредством шифрования.

В случае посягательств на данные, составляющие коммерческую тайну, злоумышленник не только делает возможным подключение к Интернету и передачу информации через свою точку доступа, но также имитирует корпоративное оборудование атакуемой стороны. В процессе посягательства используется принудительный сброс всех штатно работающих подключений и создается ситуация, в которой пользователя побуждают подключиться через оборудование нарушителя. В первом и втором случаях невозможна квалификация действий как получение доступа с преодолением ограничений средств защиты, поскольку формально пользователи самостоятельно пересылают данные злоумышленнику, предоставляя доступ к информации без получения каких-либо обязательств принимающей стороны.

Такого рода атаки могут проводиться не только в отношении информации, передаваемой по беспроводным сетям Wi-Fi, но также при передаче данных по локальной сети (для этого преступник должен иметь физический доступ к сетевому оборудованию или кабельной системе) и сетям общего доступа.

Противоправные действия с применением беспроводных устройств совершить проще, поскольку: не требуется физического доступа к какому-либо оборудованию жертвы; преступник может находиться в десятках метров от компрометируемого устройства жертвы; частные лица зачастую не могут проанализировать отклонение своей работы от штатной; для обеспечения безопасности в корпоративных локальных сетях и глобальных сетях общего

пользования выделяются эксперты и специальные средства защиты информации, что затрудняет атаки типа man-in-the-middle.

Это позволяет утверждать, что частные лица (по сравнению с корпоративными пользователями информационных систем) не только обрабатывают информацию в более уязвимых для атак системах, но и юридически не защищены.

2.3. Ошибочная пересылка данных

Ситуация неосознанной передачи доступа к информации возникает также при ошибочной пересылке конфиденциальной информации по электронной почте. В этом случае информация передается без формального преодоления мер защиты. Ошибочная пересылка может быть инициирована злоумышленником, который присылает запрос на предоставление данных, вызывающий у потерпевшего доверие. Эффект доверия достигается путем подделки информации в заголовке, об отправителе запроса и др.

2.4. Предоставление доступа с целью передачи данных

Трудно квалифицировать деяния, связанные с технологическими особенностями Интернета, в котором любая информация передается по условно бесплатным каналам связи. В процесс передачи вовлечено неопределенное количество государственных и коммерческих организаций, используется заведомо неопределенное количество сетевого оборудования. Каждое сообщение разбивается на так называемые пакеты, и каждая часть сообщения может иметь свой маршрут доставки. Таким образом, передавая данные в незашифрованном виде по Интернету, владелец de facto делает их доступными неопределенному кругу лиц. Иными словами, любая информация, когда-либо переданная в Интернет в незащищенном виде, не может быть признана охраняемой законом как информация, доступ к которой не ограничен.

Такие технологические особенности не позволяют однозначно квалифицировать деяния по перехвату электронной почты как преступные, равно как и доступ к архиву электронной переписки, если она осуществлялась в незащищенном виде, вне зависимости от содержания и наличия информации, имеющей вид охраняемой законом тайны.

2.5. Сканирование

В организациях используемые средства защиты информации, их настройки, режим работы, матрицы и временные рамки доступа относят к коммерческой тайне, наделяя эту информацию статусом охраняемой зако-

ном. Разнообразные методы сканирования состояния средств защиты информации, интерфейс которых доступен в сетях общего доступа, позволяет получать информацию о характеристиках используемых средств защиты и прикладных решений (например, веб-сайты и другие веб-сервисы). Такого рода сканирование является фактически получением конфиденциальной информации, а в случае выявления уязвимостей — первой фазой атаки с целью получения несанкционированного доступа или блокирования доступа к информационным ресурсам владельца. Квалификация сканирования как преступного деяния, несмотря на его опасный характер, является весьма трудной задачей.

2.6. Методы социальной инженерии

Методы социальной инженерии направлены на получение преступником доступа с целью последующего обхода технических средств защиты информации, либо непосредственно к интересующей их информации.

Таким образом, наличие средств защиты — неоднозначный критерий для определения правомерности доступа. Получение доступа к информации без преодоления средств защиты нельзя однозначно квалифицировать как неправомерное.

3. Отсутствие необходимых полномочий как условие неправомерности доступа

Как отмечалось, по определению Генпрокуратуры России неправомерный доступ — получение доступа без «необходимых полномочий». В области информационной безопасности терминологическая база, предназначенная для описания мер защиты информации от несанкционированного доступа, существенно шире. Основные термины, используемые в этой области информационной безопасности: а) права доступа — совокупность возможностей и ограничений на использование информации; б) управление доступом — предотвращение несанкционированного использования ресурса, включая предотвращение пользования ресурса неполномочным образом.

Права доступа определяют порядок и условия доступа субъекта к объектам информационной системы (информации, ее носителям, процессам и другим ресурсам), установленные нормативными документами или собственником, владельцем информации. Права доступа определяют набор действий (чтение, запись, выполнение и др.), разрешенных для выполнения субъектам (например, пользователям системы) над объектами данных.

Так, для использования информации, составляющей коммерческую тайну, некоторые сотрудники компании имеют возможность чтения инфор-

мации, другие могут информацию редактировать и изменять, третья группа обладает полномочиями информацию удалять. Полномочия могут быть ограничены по видам доступа, по времени доступа, по территориальным зонам, в которых должен находиться субъект, получающий доступ и другими существенными для владельца информации факторами.

Виды доступа. Виды доступа определяют действия, которые получивший доступ может осуществлять с информацией:

чтение (права доступа такого вида ограничивают пользователя возможностью читать информацию, без прав на копирование, изменение и прочие действия);

изменение (корректировки информации, зачастую изменения вносятся в журнал с целью возможного восстановления действий пользователя при анализе их корректности);

удаление (в некоторых системах это право дается отдельно от прав на изменение; например, удаление журналов изменений не позволит отследить несанкционированные коррекции);

дополнение (права, позволяющие создавать новые документы в учетных системах; например, только сотрудники склада могут создавать документы на списание товаров со склада или вносить новую информацию в базу данных другим способом);

выполнение (информация в системах может представлять собой исполняемый код или исполняемые файлы. Исполняемый код и файлы, с одной стороны, являются информацией, хранимой и обрабатываемой в системе, как и другие виды информации; с другой стороны, после запуска их выполнения они определяют вычислительный процесс, который управляется и обусловлен исполняемым кодом и переменными окружения. Факт выполнения того или иного файла является влиянием на информационную систему, поскольку автономные программные процессы чаще всего наследуют полномочия запустившего их пользователя).

Временны́е зоны. Во избежание несанкционированных действий в системе в политике безопасности могут задаваться временны́е зоны, в которых права на доступ имеют силу. Например, чтение и изменение информации в рабочее время являются санкционированными, а в нерабочее время и выходные рассматриваются как нарушение прав доступа.

Геозоны. Аналогичный подход к понятию санкционированного доступа применяется с ограничением по месту физического доступа к информационной системе. Доступ с полными правами может быть разрешен только с территории предприятия из определенных помещений.

Способ доступа. Ограничения могут применяться для операционных систем, которые предоставляют доступ, только когда пользователь с полными правами находится в физической близости к серверу. Для линейных сотруд-

ников или руководителей может быть разрешен или запрещен доступ к Интернету в зависимости от их должностных обязанностей, режима работы и чувствительности информации.

Таким образом, с точки зрения специалиста информационной безопасности нарушением будет являться не факт доступа к информации, а ее использование, выходящее за рамки полномочий — прав доступа. Данный подход продиктован одним из базовых положений в организации защиты данных — не предоставлять избыточных прав для исполнения функций пользователя. Следует также отметить, что вредоносное воздействие на информацию не всегда является следствием несанкционированного доступа. Приведем примеры.

Отказ в обслуживании, т.е. предотвращение или прерывание авторизованного доступа к ресурсу системы или задержка в действиях или функциях системы. В системах промышленной автоматики и контроля отказ в обслуживании может относиться к прекращению функционирования процесса, а не только к прекращению передачи данных[4].

Атаки на отказ в обслуживании заключаются в следующем: сетевые ресурсы, такие как веб-серверы, имеют ограничения по количеству запросов, которые они могут обслуживать одновременно. Помимо допустимой нагрузки на сервер существуют также ограничения пропускной способности канала, соединяющего сервер с Интернетом. Когда количество запросов со стороны злоумышленника превышает производительность любого компонента инфраструктуры, может произойти: существенное замедление время ответа на запросы; отказ в обслуживании всех запросов пользователей или части из них. Для этой атаки получение неправомерного доступа не является необходимым. Ущерб, наносимый атакой, зависит от атакуемого ресурса и функций, исполняемых ресурсом.

Передача ложной информации: злоумышленник, передавая ложную информацию от имени доверенного контрагента, может ввести в заблуждение и вынудить перечислить денежные средства на свой счет, получить конфиденциальную информацию в ответ (в данном случае доступ является целью, а не условием преступных действий).

Атака посредника, или атака «человек посередине» (man in the middle, MITM) — кибератака, при которой злоумышленник тайно ретранслирует и в некоторых случаях изменяет данные обмена между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Один из примеров — подслушивание, при котором злоумышленник устанавли-

[4] См.: ГОСТ Р 56205-2014. IEC/TS 62443-1-1:2009. Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели. Available at: URL: https://docs.cntd.ru/document/1200114169 (дата обращения: 17.04.2021)

вает независимые связи с жертвами и передает сообщения между ними, чтобы заставить их поверить, что они разговаривают непосредственно друг с другом по приватному каналу связи, хотя весь разговор контролируется злоумышленником. Злоумышленник должен уметь перехватывать все соответствующие сообщения, передаваемые между двумя жертвами, и вводить новые (в данном случае получение доступа к передаваемой информации является целью преступных действий, а не признаком).

Веб-инжект — технология, позволяющая изменить содержимое веб-страницы на стороне клиента (в браузере) и добавить в него контент через внедрение вредоносного кода в адресное пространство браузеров и перехват всех HTTP-запросов и ответов от сервера. Таким способом злоумышленник, не получая доступа, добивается выполнения нужных ему действий на стороне атакуемого ресурса.

Физическое воздействие на информацию. Вредоносное влияние на информацию посредством физического воздействия на каналы и носители информации не требует доступа к данным в установленном нами смысле. Например, гарантированное уничтожение данных с использованием программного обеспечения — это управляемый физический процесс изменения электромагнитными волнами состояния физического носителя информации.

К вредоносным действиям в отношении информации посредством физического воздействия на информационную систему или ее элементы, имеющие целью уничтожить, блокировать, модифицировать информацию относятся: физическая порча носителей информации, т.е. приведение в негодность флеш-карт, накопителей на жестких магнитных дисках, систем хранения данных и пр.; физическая порча средств и каналов обмена с целью блокировать доступ к данным, например, разрыв кабеля, оптики; радиочастотное навязывание, т.е. искажение электромагнитного поля с целью заблокировать обмен данных по беспроводным каналам (Wi-Fi, Bluetooth); силовое электромагнитное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение функционирования их технических и программных средств.

Отдельно следует рассмотреть вредоносные воздействия на датчики, интегрированные в вычислительные системы:

датчики *температуры,* передающие информацию о температуре помещений, на основании чего системы управления «умным домом» дают команды на включение или отключение элементов отопления; вывод из строя датчика приведет к сбоям системы в целом. Датчик в данном контексте является элементом информационной системы и источником данных. Доступ к генерируемым им данным не представляет ценности, но блокировка, унич-

тожение или искажение предоставляемой им информации, посредством физического воздействия является компьютерным преступлением; выведение из строя датчиков в автономных системах хранения лекарств может привести как к финансовому ущербу в результате списания испорченных экземпляров, так и вреду здоровья человека;

датчики движения, передающие информацию об перемещениях по охраняемой территории. Блокирование информации, передаваемой датчиком, выведет из строя часть функционала программно-аппаратной системы безопасности; манипулирование датчиком создаст условия для других криминальных действий;

считыватели карт доступа, обеспечивающие контроль доступа в помещение, выведение их из строя может привести к снятию защиты с охраняемых зон и создание угроз хищения или незаконного проникновения;

датчики *GPS,* лидары, радары, участвующие в управлении автономными транспортных средств. На эти датчики можно осуществить влияние посредством навязывания радио или оптического сигнала, что может привести к авариям.

Вредоносное влияние на датчики, интегрированные в информационно-вычислительные системы, следует рассматривать как влияние на вычислительную систему посредством блокирования и искажения информации, предоставляемой датчиком и квалифицировать как компьютерное преступление.

В информационной безопасности меры физической защиты рассматриваются как необходимая часть защиты информации. Под ней понимается защита информации путем применения организационных мер и совокупности средств, создающих препятствия проникновению или доступу неуполномоченных физических лиц к объекту защиты. Она включает организационные мероприятия, т.е. установление режимных, временны*ы*х, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты; ее объектами могут быть признаны охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Таким образом, приемлемой является трактовка неправомерного доступа, закрепленная Национальным стандартом Российской Федерации (ГОСТ Р 53114-2008)[5], где под ним понимается получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации. Данное определение полностью охватывает спектр возможных деяний, со-

[5] ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Available at: URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 17.04.2021)

стоящих в доступе к информации, оно позволяет не сужать круг деяний до тех, которые были произведены над информацией в системах с использованием средств защиты.

4. Проблемы понимания последствий компьютерных преступлений

Наибольшая критика анализируемых преступлений связана с формулированием законодателем таких последствий, как уничтожение, блокирование, модификация либо копирование информации. В силу отсутствия легального определения в науке уголовного права каждое из указанных последствий наполняется собственным содержанием.

Одни авторы считают, что модификация имеет обобщающее значение и может включать в себя удаление, блокирование, ввод информации и другие способы воздействия на информацию [Хилюта В.В., 2014: 112]. Другие рассматривают модификацию как один из способов воздействия на компьютерную информацию, например, частичную замену первоначальной информации, в том числе путем ее удаления или ввода новой информации [Третьяк М.И., 2016: 99]. Третьи под модификацией предлагают понимать лишь изменение компьютерных программ (которое требует согласия правообладателя) и баз данных, но не иных компьютерных данных [Рарог А.И., 2017: 295]. Методические рекомендации Генеральной прокуратуры определяют модификацию информации как внесение изменений в компьютерную информацию (или ее параметры). ГОСТ Р 53114-2008 данного термина не использует.

Блокирование компьютерной информации некоторыми рассматривается как невозможность реализации доступа к компьютерной информации обладателем такой информации в течение долгого времени при неизменности самой информации в компьютерной системе [Омаров М.Д., 2011: 56]. В.М. Мешков определяет блокирование как создание условий, при которых отсутствует возможность или существенно затрудняется возможность использования компьютерной информации, при этом сохраняя такую информацию в неизменном состоянии [Мешков В.М., 2003: 59]. ГОСТ Р 53114-2008 под блокированием доступа к информации понимает прекращение или затруднение доступа к ней законных пользователей. Методические рекомендации Генеральной прокуратуры предлагают трактовать блокирование информации как результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, т.е. совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целена-

правленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением.

Уничтожение ученые рассматривают как невозможность восстановления содержимого компьютерной информации [Южин А.А., 2012: 17]. В.И. Гладких указывает, что совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации и (или) в результате которых уничтожаются носители компьютерной информации [Гладких В.И., 2014: 27]. Специалисты в сфере компьютерной безопасности отмечают, что при удалении компьютерной информации программными средствами всегда остается возможность восстановления, гарантировать безвозвратное уничтожение компьютерной информации можно лишь путем физического уничтожения носителя информации [Быков В.М., Черкасов В.Н., 2021: 18]. В связи с этим исследователи считают информацию уничтоженной с момента выполнения компьютерной команды «удалить», несмотря на возможность ее восстановления [Ефремова М.А., 2021: 56].

Генеральная прокуратура указывает, что уничтожением информации считается ее приведение (или ее части) в непригодное для использования состояние независимо от возможности ее восстановления, а также отмечает, что переименование файлов и их автоматическое обновление уничтожением считать нельзя. ГОСТ Р 53114-2008 данного термина не использует.

Сущность копирования многими рассматривается как дублирование компьютерной информации или создание копии этой информации, дискутируя лишь по вопросу о способах копирования:

только с основного носителя компьютерной информации на любой иной носитель, исключая из способов копирования фотографирование монитора, на котором выведена информация, распечатку и иные способы [Борчева Н.А., 2001: 9];

не ограничивается лишь программной командой «копировать» и может включать в себя вывод компьютерной информации на дисплей или другое устройство, что сопровождается копированием (в широком смысле слова) информации с носителей в оперативную память, память видеокарты, принтера или другого устройства [Рарог А.И., 2017: 295];

воспроизведение информации в любой материальной форме [Панфилова Е.И., 2003: 563–564];

действия лица, направленные на открытие доступа к информации, ранее ограниченной обладателем информации, в целях использования такой информации неограниченным числом лиц или самим злоумышленником [Халиулин А.И., 2015: 23–26].

Генеральная прокуратура под копированием информации предлагает понимать создание копии имеющейся информации на другом носителе, т.е. перенос информации на обособленный носитель при сохранении неизменной

первоначальной информации, воспроизведение информации в любой материальной форме — от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п. ГОСТ Р 53114-2008 не использует данный термин.

Иначе оценивают приводимые термины специалисты в области информационной безопасности.

Уничтожение информации. Первый вопрос: следует ли считать операцию удалением, если компьютерную информацию впоследствии можно восстановить или же удаление — это операция, подразумевающая невозможность восстановления. В зависимости от выбранного подхода одно и то же деяние с одинаковым ущербом может иметь различную правовую оценку. Если потерпевшая сторона относится добросовестно к защите охраняемой законом информации, то наказание преступника может оказаться мягче, чем преступление в отношении менее добросовестных потерпевших вне зависимости от умысла преступника. Так, безвозвратное удаление данных и причинение экономического ущерба приводит к длительной остановке деятельности организации, а ущерб может быть значительным. Если же в организации есть резервные копии компьютерной информации, аналогичные действия приведут к минимальному простою и ущерб будет минимальным.

Технологически безвозвратному уничтожению данных препятствует несколько существенных факторов; далеко не всегда попытка удаления завершается успехом. Это обусловлено представлением компьютерной информации в информационных системах и распространенными практиками принятия мер противодействия угрозам информационной безопасности.

На успешность удаления влияют следующие факторы: штатная операция удаления в операционных системах фактически не удаляет информацию, а указывает системным службам, что некая область памяти свободна, туда может быть занесена другая информация и только в случае такой записи исходная информация уничтожается; процедура гарантированного удаления без возможности восстановления требует существенного времени и может быть не завершена; большинство информационных систем имеют системы резервного копирования и с их помощью информация может быть восстановлена.

Понимая многообразие возможных трактовок, Генеральная прокуратура предлагает следующее определение уничтожения информации — это приведение ее в такое состояние, при котором информация не может быть восстановлена, либо такое ее стирание (удаление), при котором остается возможность ее восстановления. Поскольку потеря информации в большинстве случаев является наиболее опасным последствием, уголовно наказуемым следует считать, как собственно уничтожение информации, так и ее стирание (удаление).

Вопрос частичного или полного удаления остался не раскрытым. В частности, Генеральная прокуратура приравнивает попытку лица удаления

данных, не завершившуюся успехом по не зависящим от него причинам, к успешной попытке. Такой подход логически оправдан и во избежание спорных трактовок должен быть отражен в законе или постановлении Пленума Верховного Суда Российской Федерации.

В то же время приведенная формулировка содержит смысловую неточность. Понятия «информация» и «компьютерная информация» определяют разные сущности. Компьютерная информация или данные — это физическое представление информации, для нее может быть однозначно определен физический носитель. Компьютерную информацию физически уничтожить и стереть можно; информацию как таковую стереть нельзя, поскольку существование информации не подразумевает определенного физического носителя. Говорить об уничтожении информации можно только в случае уничтожения всех ее возможных копий, включая бумажные и прочие виды копии, очистив память всех лиц, знающих эту информацию. Понятие уничтожения информации тождественно стиранию компьютерной информации только когда информация представлена на носителе. Полагаем, что следует избегать подобных неточностей.

Другой спорный вопрос при определении термина «уничтожение компьютерной информации» — понимание удаления в качестве исключительно полного удаления или также частичного. В некоторых случаях компьютерная информация имеет ценность только в ситуации ее сохранения в полностью неизменном виде, а удаление ее части сделает непригодной к использованию информацию, представленную в виде данных. В других случаях прикладную ценность имеют условно независимые блоки данных, из которых состоит компьютерная информация, поэтому уничтожение нескольких блоков на возможность использования критично не повлияет. Например, таблица данных может содержать несколько миллионов строк, удаление одной строки можно трактовать как оконченное преступление и квалифицироваться по ст. 272 УК РФ вне зависимости от размера ущерба. Отсутствие точного определения позволят трактовать удаление информации произвольно как в случае полного удаления базы данных или только при удалении ее существенной части и при удалении несущественной части. Этот вопрос методические рекомендации Генеральной прокуратуры не проясняют.

Полагаем, что под уничтожением следует понимать невозможность использования информации в определенных владельцем целях.

Блокировка информации. В рекомендациях Генеральной прокуратуры блокировка определяется как создание условий, при которых возникает постоянная или временная невозможность осуществления блокируемой информацией своих функций. Данное определение спорно. В частности, требуется уточнение понятия временной блокировки. Задержка выполнения запроса на формирование отчета на несколько миллисекунд, вызванная фак-

том несанкционированного доступа, является временной блокировкой. Поскольку доступ — операция, использующая ресурсы вычислительной системы и действительно приводящая к задержке выполнения прочих операций, с технологической точки зрения утверждение верно. В указанном контексте любой несанкционированный доступ может быть квалифицирован как преступление и делает избыточными прочие квалификационные признаки.

Модификация информации. В рекомендациях Генеральной прокуратуры модификация информации — несанкционированное изменение первоначального состояния охраняемой законом компьютерной информации, которое трансформирует содержание этой информации либо нарушает выполняемые ею функции.

Данная трактовка трудно применима по следующим причинам:

модификация информации определяется через модификацию компьютерной информации, что логически не оправдано, поскольку компьютерная информация является частным представлением информации на носителе. Как уже упоминалось ранее, изменить информацию посредством изменения данных можно только в случае уникальности этой копии данных;

ряд определений используются как заведомо известные, что не всегда соответствует действительности. Например, вызывают сомнения в возможности однозначного понимания следующие формулировки:

первоначальное состояние информации: к большинству информационных систем такое понятие не применимо, поскольку компьютерная информация в них непрерывно дополняются и уточняются. Говоря о представлении, речь может идти только о корректности состояния компьютерной информации в определенный момент времени, применительно к содержанию — об актуальности информации на определенный момент времени. Иными словами, понятие «первоначальное состояние» в таких ситуациях не имеет определенного смысла;

трансформация содержания информации: содержание информации — это интерпретация данных человеком — понятие, не имеющее общепринятого определения и не раскрываемое законодательно. В силу этих причин вводить через термин трансформация термин модификация не обосновано.

Копирование информации. В рекомендациях Генпрокуратуры копирование информации — это создание копии информации на другом носителе, т.е. перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме — от руки, фотографированием текста с экрана дисплея, а также считывание информации путем любого перехвата информации и т.п.

В данном определении заложены следующие ограничения:

использование в определении указания на создание копии информации на другом носителе не позволяет отнести к противоправным действиям чте-

ние и запоминание человеком сведений, составляющих коммерческую тайну, а такого рода чтение позволит их распространять, в частности устно, не используя какие-либо физические носители;

считывание путем перехвата предложено вне контекста статьи, такой способ характерен только для ст. 272 УК РФ, предусматривающей неправомерный доступ, иными словами, нет необходимости что-либо перехватывать при наличии доступа;

перенос информации на обособленный носитель не является определяющим признаком действия — виновный может скопировать данные на тот же самый носитель. Получив несанкционированный доступ к файловому хранилищу, данные можно скопировать на тот же самый носитель, но уже в раздел, к которому злоумышленник имеет права доступа. Одной из серьезных проблем в применения ст. 272 и 273 УК РФ является закрытый перечень последствий. Видов вредоносных последствий существенно больше, а с развитием технологий они будут изменяться и дополняться. Приведем несколько известных примеров опасных последствий, появляющихся при воздействии на компьютерную информацию [Арямов А.А., 2019].

Снижение скорости доступа к данным. Злоумышленники создают большое количество задач для вычислительной системы имитирующие формально корректные обращения, что приводит к снижению скорости корректных запросов на предоставление доступа к информации и повлечет, например: в коммерческих организациях замедление доступа к каталогу товаров интернет-магазина, приводящее к оттоку покупателей и причинению финансового ущерба; в лечебных учреждениях, оказывающих помощь посредством систем телемедицины при проведении операций, связанных с хирургическим вмешательством в режиме удаленного подключения к труднодоступным местам (судна дальнего плавания, лес и пр.), а также при проведении удаленного оперативного консилиума в режиме реального времени, снижение скорости доступа к информации может привести к причинению вреда здоровью и жизни человека.

Снижение скорости обработки данных — создание условий, ограничивающих скорость доступа к данным, которые могут приводить к потере актуальности получаемой информации. Такого рода воздействие может заключаться в запуске конкурирующих за ресурс процессов или, например, намеренном применении неэффективных алгоритмов, связанных с обработкой больших объемов данных. Так, в коммерческих организациях выводы, сделанные на основании неактуальной информации, могут приводить к финансовому ущербу; в логистических компания в случае применения вычислительных систем для управления транспортными средствами снижение скорости обработки данных может приводить к авариям, нанесению вреда здоровью и жизни человека.

Дополнение (внесение) информации. Посредством дополнения базы данных ложными сведениями можно исказить смысл всей базы данных. Например, дополняя информацию о росте продаж ложной информацией об эффективности определенного канала продаж, злоумышленник может получить личную выгоду и нанести ущерб организации за счет нерационального использования маркетингового бюджета, сформированного на основании искаженной аналитики.

Нейтрализация средств защиты — косвенный способ воздействия на информацию. Такое воздействие создает повышение рисков информационной безопасности, что с точки зрения специалистов информационной безопасности, имеет криминальный характер. На практике это воздействие практически всегда является сопутствующим для большинства компьютерных преступлений. Нейтрализация средств защиты является распространенной целью несанкционированного доступа.

Близким к этому последствием является нейтрализация средств контроля эффективности защиты информации. Влияние на режим обработки информации которое также создает риски информационной безопасности, является по характеру криминальным и на текущий момент не может быть квалифицировано по статьям гл. 28 УК РФ.

Перехват информации — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов (ГОСТ Р 53114-2008). Не является копированием, поскольку злоумышленник информацию не копирует, но ее получает. Один из самых распространенных видов компьютерных преступлений.

Нарушение достоверности информации. Достоверность — это строгая принадлежность информации субъекту, который является ее источником, либо тому субъекту, от которого она принята. В случае, если получатель начнет принимать информацию из недостоверного источника, он может быть введен в заблуждение и выполнить действия, к которым его побуждает злоумышленник, например, перевести денежные средства по полученным недостоверным реквизитам.

Снижение доверия к информации — изменение, снижение ожиданий получателей результата обработки информации к достоверности получаемого результата. К получателям результата относятся как стороны информационного обмена, так и пользователи информационных систем, имеющих непосредственный доступ к данным. Снижение доверия может быть осуществлено: за счет предоставления ошибочной информации (этот способ реализуют посредством подмены доверенного источника информации на источник информации, контролируемый злоумышленником и дальнейшей выдачи измененных данных); путем появления регулярных и (или) трудно определяемых ошибок, вызванных технологическими сбоями, также снижают до-

верие к информации и вычислительной системе вне зависимости от причин сбоев; посредством внесения данных, изменяющих смысл информации, что приводит к ошибочным выводам и обесцениванию результата.

Несмотря на отсутствие формального понимания снижения доверия к информации, отсутствие ожиданий достоверного результата может привести к отказу от ее использования. Снижение доверия к таким службам, как удостоверяющий центр сертификатов электронной подписи, может привести к полному закрытию организации и крупному финансовому ущербу.

Заключение

Отсутствие однозначных и практически применимых определений указанных видов воздействий на информацию в нормативной базе снижает эффективность правоприменительной практики, делает законодательство неадекватным угрозам, не позволяют квалифицировать как преступные целый ряд вредоносных воздействий на информацию, имеющих место в цифровой среде.

С учетом изложенного считаем, что преступления в отношении информации должны квалифицироваться как компьютерные вне зависимости от способа воздействия: механического, магнитного или программного. Рассматривать же последствия следует с точки зрения влияния на информационную систему в целом. При квалификации компьютерных преступлений не следует использовать в качестве конститутивных признаки, имеющие узко технологическую специфику. Технологические понятия не всегда имеют однозначное соответствие общепринятым терминам. Кроме того, они меняются со временем, что требует постоянной актуализации законодательной базы. Перечень последствий может быть открытым, а их перечисление должно иметь лишь ориентирующий характер.

Список источников

1. Арямов А.А. и др. Девиации в цифровом мире: уголовно-правовое измерение. Часть I. М.: Контракт, 2019. 160 с.

2. Борчева Н.А. Компьютерные преступления в России: Комментарий к Уголовному кодексу Российской Федерации. М.: Прима-Пресс, 2001. 22 с.

3. Быков В.М., Черкасов В.Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. № 5. С. 14–19.

4. Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. № 22. С. 25–31.

5. Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. 2006. № 11. С. 30–35.

6. Ефремова М.А. Ответственность за неправомерный доступ к компьютерной информации по действующему законодательству // Вестник Казанского юридического института. 2012. № 8. С. 54–56.

7. Мешков В.М. Компьютерные преступления и защита компьютерной информации. Калининград: МВД России, 2003. 119 с.

8. Омаров М.Д. Проблемы определения состава преступления за неправомерный доступ к информационным ресурсам информационных систем // Юридический вестник ДГУ. 2011. № 4. С. 56–58.

9. Панфилова Е.И. Компьютерные преступления. СПб.: С.-Петерб. юрид. ин-т Генеральной прокуратуры, 2003. 47 с.

10. Рарог А.И. (отв. ред.) Качество уголовного закона: проблемы особенной части. М.: Проспект, 2017. 381 с.

11. Рарог А.И. (ред.) Уголовное право России. Части общая и особенная. М.: Проспект, 2018. 624 с.

12. Третьяк М.И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества // Уголовное право. 2016. № 2. С. 95–101.

13. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … к. ю. н. Владивосток, 2005. 235 с.

14. Халиуллин А.И. Неправомерное копирование как последствие преступления в сфере компьютерной информации // Российский следователь. 2015. № 8. С. 23–26.

15. Хилюта В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. № 3. С. 111–118.

16. Южин А. А. Дискуссионные вопросы мошенничества в сфере компьютерной информации // Право и кибербезопасность. 2014. № 2. С. 15–18.

17. Buchanan R. Cyber espionage and international law. Oxford: Hart, 2019. 219 p.

18. Eun Y.-S., Aßmann J.S. Cyberwar: taking stock of security and warfare in the digital age. International Studies Perspectives, 2016, vol. 17, no. 3, pp. 343–360.

19. Stoddart K. UK cyber security and critical national infrastructure protection. International Affairs, 2016, vol. 92, no. 5, pp. 1079–1105.

References

1. Aryamov A.A. et al. (2019) *Deviations in the digital world: criminal and legal dimension.* Part I. Moscow: Kontrakt, 160 p. (In Russ.).

2. Borcheva N.A. (2004) Computer crimes in Russia: Commentary to the Russian Criminal Code. Moscow: Prima Press, 22 p. (In Russ.).

3. Buchanan R. (2019) *Cyberspionage and international law.* Oxford: Hart, 219 p.

4. Bykov V.M., Cherkasov V.N. (2012) New law on computer crimes: Art. 272 of the Criminal Code. *Rossijskij sud'ya = Russian Judge,* no. 5, pp. 14–19. (In Russ.).

5. Criminal law of Russia (2018) A.I. Rarog (ed.). Moscow: Prospekt, 624 p. (In Russ.).

6. Efremova M.A. (2012) Liabiibility for illegal access to computer information. *Vestnik Kazanskogo yuridicheskogo instituta* = Herald of Kazan Jaw Institute, no. 8, pp. 54–56. (In Russ.).

7. Eun Y.-S., Aßmann J. S. (2016) Cyberwar: Summing up security and war in the digital age. *Prospects for International Studies,* vol. 17, no. 3, pp. 343–360.

8. Gladkikh V.I. (2014) Computer fraud: and were there any grounds for criminalizing it? *Rossijski sledovatel'*=Russian Investigator, no. 22, pp. 25–31. (In Russ.).

9. Gromov E.V. (2006) Development of criminal legislation on crimes in the field of computer information in foreign countries (USA, Great Britain, Germany, the Netherlands, Poland). *Vestnik TGPU*=Herald of Tyumen Politechnical University, no. 11, pp. 30–35. (In Russ.).

10. Khaliullin A. I. (2015) Illegal copying as a consequence of a crime in the field of computer information. *Rossijskij sledovatel'*=Russian Investigator, no. 8, pp. 23–26. (In Russ.).

11. Khilyuta V.V. (2014) The liability for theft with using computer technology.*Zhurnal rossijskogo prava*=Journal of Russian Law, no. 3, pp. 111–118. (In Russ.).

12. Meshkov V.M. (2003) *Computer crimes and protection of computer information.* Kaliningrad: MVD Institute, 119 p. (In Russ.).

13. Omarov M.D. (2011) Composition of illegal access for information systems resources. *Yuridicheskiy vestnik DGU* = Law Herald of Far East University, no. 4, pp. 56–58. (In Russ.).

14. Panfilova E.I. (2003) *The computer crimes.* Saint Petersburg: Prosecutor General research institute, 47 p. (In Russ.).

15. The quality of the criminal law: special part (2017) A.I. Rarog (ed.). Moscow: Prospekt, 381 p. (In Russ.).

16. Stoddart K. (2016) Cybersecurity of Great Britain and protection of critical national infrastructure. *International Affairs*, vol. 92, no. 5, pp. 1079–1105.

17. Tretyak M. I. (2016) Modification of computer information and its correlation with other methods of computer fraud. *Ugolovnoe pravo*=Criminal Law, no. 2, pp. 95–101. (In Russ.).

18. Tropina T.L. (2005) Cybercrime: concept, state, legal struggle. Candidate of Juridical Sciences Thesis. Vladivostok, 235 p. (In Russ.).

19. Yuzhin A.A. (2014) Debatable issues of fraud in the field of computer information. *Pravo i kiberbezopasnost'*=Law and Cybersecurity, no. 2, pp. 15–18. (In Russ.).

Информация об авторах:

Ю.В. Грачева — доктор юридических наук, профессор;

С.В. Маликов — доктор юридических наук, профессор;

А.И. Чучаев — доктор юридических наук, профессор.

Information about the authors

Yu.V. Gracheva — Doctor of Sciences (Law), Professor;

S.V. Malikov — Doctor of Sciences (Law), Professor;

A.I. Chuchaev- Doctor of Sciences (Law), Professor.

Статья поступила в редакцию 07.03.2021; одобрена после рецензирования 19.05.2021; принята к публикации 26.05.2021.

The article was submitted 07.03.2021; approved after reviewing 19.08.2021; accepted for publication 26.08.2021.