ISSN 2500-1442

Научная статья
УДК 343.34
EDN BJELYH
DOI 10.17150/2500-4255.2024.18(5).482-493

О КРИМИНАЛИЗАЦИИ ДЕЯНИЙ, НАПРАВЛЕННЫХ НА УНИЧТОЖЕНИЕ, БЛОКИРОВАНИЕ ИЛИ МОДИФИКАЦИЮ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

И.Н. Мосечкин
Вятский государственный университет, г. Киров, Российская Федерация

Информация о статье

Дата поступления
13 августа 2023 г.

Дата принятия в печать
26 ноября 2024 г.

Дата онлайн-размещения
6 декабря 2024 г.

Ключевые слова

Компьютерная информация; вредоносная программа; неправомерный доступ; уничтожение информации; блокирование информации; модификация информации

Аннотация. Статья посвящена исследованию проблем противодействия уничтожению, блокированию или модификации компьютерной информации уголовно-правовыми средствами. Актуальность темы связана с продолжающейся цифровизацией сфер деятельности человека и внесением изменений в уголовный закон. Автор приходит к выводу о том, что действующее законодательство не свободно от пробелов, несмотря на предпринятые в последнее время меры по его совершенствованию. Судебная практика и теоретические труды свидетельствуют о наличии различного рода посягательств, направленных на уничтожение, блокирование или модификацию цифровых данных. Среди них повреждение машинных носителей, завладение ими и удаление информации с помощью электромагнитного воздействия. Отсутствие неправомерного доступа к компьютерной информации, вредоносных программ и обязанности соблюдать правила обращения с информации не позволяют квалифицировать совершенные деяния по какой-либо из статей УК РФ. Повреждение машинных носителей или завладение ими не в полной мере охватываются уголовным законом, поскольку игнорируется цель уничтожения, блокирования или модификации цифровых данных. При этом ценность информации для потерпевшего в отдельных случаях существенно превышает стоимость носителя. В зарубежных странах применяются различные подходы, при которых лицо подлежит уголовной ответственности за нарушение целостности компьютерной информации или ее блокирование независимо от способа. В ходе анализа автор пришел к выводу о целесообразности заимствования положений о криминализация умышленных уничтожения, блокирования и модификации компьютерной информации не только посредством неправомерного доступа, но и иными способами. Обращается внимание на необходимость учета направленности умысла виновного на уничтожение значимых цифровых данных. Авторская позиция дополнительно аргументируется посредством обращения к результатам исследования авторитетных деятелей науки. В выводах статьи формулируется предложение по дополнению УК РФ новой статьей с рекомендованной конструкцией диспозиции, предусмотренной частью первой. В работе содержится также перечень квалифицирующих признаков, какими могла бы быть дополнена новая статья.

Original article

ON THE CRIMINALIZATION OF ACTS AIMED AT DESTROYING, BLOCKING OR MODIFYING COMPUTER INFORMATION

Ilya N. Mosechkin
Vyatka State University, Kirov, the Russian Federation

Article info

Received
2023 August 13

Accepted
2024 November 26

Available online
2024 December 6

Abstract. The author discusses the problems of counteracting the destruction, blocking or modification of information through criminal law means. The topic is highly relevant due to the ongoing digitization of human activities and the introduction of amendments to the criminal law. The author concludes that, in spite of the recent measures aimed at improving the current legislation, it is still not free from gaps. Both court practice and theoretical works describe various infringements aimed at the destruction, blocking or modification of digital data. These include damaging machine-readable media, appropriating them or destroying their information through an electromagnetic impact. The absence of unauthorized access to computer information, malware or the obligation to observe the rules of information processing make

Keywords
Computer information; malware; unauthorized access; destruction of information; information blocking; modification of information

it impossible to qualify the committed actions under some Article of the Criminal Code of the Russian Federation. The destruction of machine-readable media or their appropriation are not fully covered by the criminal law since the goal of destroying, blocking or modifying digital data is ignored. Besides, in some cases the value of information for the victim could be considerably higher than the price of the information carrier. International experience shows different approaches under which a person is held criminally liable for violating the integrity of computer information or for blocking it regardless of the used means. The analysis allowed the author to conclude that it is expedient to borrow certain clauses on criminalizing the intentional destruction, blocking and modification of computer information not only in cases of unauthorized access, but also through other means. The author draws attention to the necessity of taking into account the intention of the guilty person to destroy relevant digital data. Additional arguments are presented in support of this position by citing the research findings of authoritative scholars. In conclusion, the author suggests that the Criminal Code of the Russian Federation should be amended by adding a new article with the recommended disposition provided in its first part. A list of qualifying features that could be used to amend the new article is also presented.

Введение

В ходе цифровизации многих сфер деятельности человека необходимо надлежащее правовое регулирование и правовая защита данного процесса. Не возникает сомнений в том, что появление новых технологий или их внедрение в какую-либо область создает угрозу их применения в противоправных целях. Сказанное достаточно проиллюстрировать современными примерами дистанционных мошенничеств и использования беспилотных летательных аппаратов при совершении диверсий и террористических актов. В данном контексте убедительным видится высказывание И.Р. Бегишева: «…предупреждение, прогнозирование и устранение рисков компьютерных преступлений и правонарушений в современных условиях становится приоритетным направлением деятельности, концентрирующим усилия специалистов различных областей знаний» [1].

Правовые меры играют далеко не последнюю роль в противодействии киберпреступности. Большое значение имеет степень соответствия уголовно-правовых норм новым или явлениям, измененным в связи с использованием технологических устройств. Стоит отметить усилия законодателя по оптимизации законодательства — периодически осуществляется его подстраивание под соответствие запросам преображающейся общественной жизни. В 2022 г. в Уголовный кодекс Российской Федерации (далее — УК РФ) введена ст. 274.2, призванная обеспечить стабильность так называемому «суверенному интернету». Правоприменителям еще лишь предстоит проверить ее эффективность.

Появились также новые составы преступлений, включающие признак использования информационно-телекоммуникационных сетей (например, предусмотренный п. «в» ч. 2 ст. 280.4 УК РФ). Давно известные отечественному праву преступления тоже дополняются данным признаком. В частности, следует обратить внимание на норму, запрещающую понуждение к действиям сексуального характера. Квалифицированный состав, закрепленный в ч. 3, обогатился цифровыми признаками.

В основном совершенствуется именно Особенная часть УК РФ. При этом не сложилось однозначного подхода к ее «цифровизации». В отдельных случаях законодатель закрепляет соответствующие признаки в качестве обязательных, в других — в качестве квалифицированных, в третьих — нормативно игнорирует их фактическое наличие в большой части совершаемых деяний. Например, клевета, совершенная с использованием информационно-телекоммуникационных сетей, образует квалифицированный состав преступления (ч. 2 ст. 128.1 УК РФ). То есть, по мнению законодателя, дистанционное распространение негативных ложных сведений обладает повышенной общественной опасностью. Совершенно непонятно, почему же тогда клевета в отношении судьи, совершенная с использованием информационно-телекоммуникационных сетей, образует основной состав (ч. 1 ст. 298.1 УК РФ), причем наказывается менее строго? Наиболее очевидной причиной видится отсутствие системного подхода при внесении изменений в закон. В свете сказанного следует согласиться с мнением Е.А. Русскевич, согласно которому доктрина уголовного права также пока не решила вопрос разработки модели системного обновления уголовного законодательства в условиях информационного общества [2].

До сих пор не выработан и общепринятый подход к наименованию компьютерных преступлений (например, встречаются такие понятия, как «преступления, совершаемые с использованием информационно-телекоммуникационных сетей», «киберпреступления» и иные). Достаточно бурные дискуссии происходят по поводу расширения или сужения перечня правонарушений в сфере компьютерной информации [3]. Количество трудов, посвященных отдельным цифровым признакам составов преступлений, пополняется с каждым годом. Часть из них нашла отражение в законотворческом процессе.

Считаем необходимым отметить, что несмотря на предпринимаемые усилия, отечественный уголовный закон не остается свободным от правовых пробелов в области защиты компьютерной информации. Речь идет не только о высокотехнологичных деяниях, но и тех, где использование электронных устройств вовсе не требуется, а вред компьютерной информации все же наносится. Едва ли можно назвать адекватной правовую защиту цифровых данных от посягательств, связанных с уничтожением физического носителя (флеш-карты или, например, жесткого диска). Отдельного состава преступления для таких случаев не предусмотрено, а аналогию права или закона проводить недопустимо. Не в полной мере охватываются нормативными положениями использование электромагнитных комплексов для повреждения информации или банальное хищение накопителя. Внешне подобные деяния едва ли напоминают компьютерные преступления, однако они могут быть направлены исключительно на причинения вреда отношениям, обеспечивающим безопасность компьютерной информации. Неслучайно группа отечественных ученых в результате глубокого исследования пришла к выводу о том, что преступления в отношении информации следует квалифицировать как компьютерные без учета способа воздействия: механического, магнитного либо иного [4]. Нам близка данная позиция, но ради справедливости и объективности все же необходимо добавить, что в литературе встречается категорический отказ от отнесения физических воздействий на машинный носитель к компьютерным преступлениям [5, с. 18–19].

Уголовным законом строго определены критерии отнесения деяний к категории преступлений в сфере компьютерной информации. Принципиальное значение имеет наличие неправомерного доступа или вредоносных программ либо нарушение установленных правил. В то же время зарубежные исследователи говорят о достаточно широком распространении различного рода деяний, направленных именно на уничтожение или блокировку информации любым образом [6]. В связи с этим необходимо установить, встречаются ли в действительности иные способы посягательств на цифровые данные, а также определить, насколько адекватным является уголовно-правовой ответ им.

Основное исследование

Высокий уровень абстракции отечественных уголовно-правовых норм позволяет охватить большинство деяний, направленных против общественных отношений, складывающихся по поводу обеспечения безопасности компьютерной информации. Об уничтожении или блокировке цифровых данных прямо говорится в ряде правовых положений. В частности, именно такие последствия закреплены в качестве обязательных признаков составов преступлений, предусмотренных ст. 272 и 274 УК РФ. На уничтожение информации (уже не в качестве общественно опасного последствия) также указывается в ст. 273 УК РФ и в ст. 274.1 УК РФ, защищающей критическую информационную инфраструктуру Российской Федерации.

Важно отметить: при конструировании норм гл. 28 УК РФ законодатель изначально явно стремился разграничить традиционные преступления, совершение которых возможно при помощи компьютера, и непосредственно компьютерные преступления. Это во многом объясняет особенности правовой защиты цифровой информации от уничтожения. Недостатки такого подхода привели к существующим правоприменительным проблемам.

Например, анализ юридических конструкций, закрепленных в ст. 272 УК РФ, позволяет говорить о том, что защита информации обеспечивается исключительно от неправомерного доступа, который имеет строго очерченные рамки. Под неправомерным доступом, как следует из Постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»[1] (далее — Постановление), понимается получение

[1] ИПП «ГАРАНТ.РУ». URL: https://www.garant.ru/products/ipo/prime/doc/405863329 (дата обращения: 10.07.2024).

данных без согласия их обладателя лицом, не наделенным необходимыми полномочиями, либо в нарушение установленного порядка. Сама форма доступа значения не имеет. Она может быть высокотехнологичной и связанной с использованием вредоносных программ, а может осуществляться при помощи подбора или хищения пароля. Если неправомерный доступ отсутствовал, но компьютерная информация все же была уничтожена, содеянное не может квалифицироваться по ст. 272 УК РФ. Кроме того, по мнению И.Р. Бегишева, конструкция данной статьи не включает перехват как способ завладения цифровыми данными. Главное отличие перехвата кроется в направленности на информацию, циркулирующую в пространстве. При этом не требуется обязательного нарушения системы защиты информации, в отличие от неправомерного доступа [7, с. 56].

Статья 273 УК РФ защищает от потенциального уничтожения или блокирования информации посредством установления запрета на создание, распространение или использование программ, для этой задачи предназначенных. Статья 274 УК РФ охватывает лишь преступное нарушение определенных правил, а ее применение можно охарактеризовать как очень редкое. Весьма похожими (но не идентичными) элементами обладают конструкции составов, защищающих критическую информационную инфраструктуру РФ, закрепленных в ст. 274.1 УК РФ. Во всех вышеуказанных статьях определены жесткие рамки объективной стороны, что позволило охватить наиболее распространенные виды посягательств. Тем не менее остаются способы уничтожения или блокирования информации, не подпадающие под признаки данных преступлений.

Пункт 4 Постановления раскрывает понятие «уничтожение информации». Под данным явлением понимается приведение информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена. Судебное толкование положило конец спорам о том, признается ли уничтоженной информация, подлежащая восстановлению силами специалистов. Кроме того, совершенно верно сделан акцент на полной или частичной непригодности для дальнейшего использования.

Практика показывает, что уничтожение информации обычно осуществляется с помощью ввода соответствующих команд в электронной системе. Реже встречаются (но все же имеют место) варианты добиться желаемого результата посредством воздействия на носитель. Такой способ не противоречит понятию, сформулированному в акте судебного толкования, однако законом охватывается лишь частично. Повреждение электронного устройства, его комплектующих и носителей обычно квалифицируется по ст. 167 УК РФ, если установлен достаточный размер ущерба. В научной литературе правильно отмечается, что носитель не всегда представляет значительную материальную ценность. Квалификация по ст. 167 УК РФ в таких случаях недопустима [8], что не исключает возможности применения ст. 7.17 КоАП РФ.

Однако утрата информации так или иначе остается за пределами состава преступления или правонарушения. Иначе говоря, при высокой материальной ценности электронного устройства квалификация по ст. 167 УК РФ будет юридически верной, но не в полной мере отвечающей фактическим обстоятельствам. Умысел преступника может иметь разную направленность:

1. Причинить исключительно материальный вред посредством уничтожения носителя.

2. Причинить материальный вред и уничтожить значимую информацию одновременно.

3. Уничтожить значимую информацию посредством посягательства на носитель. Стоимость поврежденного имущества для преступника имеет меньшее значение.

В частности, как следует из приговора суда, Б. Л. Р. совершила преступление, предусмотренное ч. 1 ст. 167 УК РФ, при следующих обстоятельствах. Возле дома Б. Л. Р. осуществляли журналистскую деятельность сотрудники АО «Телекомпания НТВ», имея при себе дорогостоящие видеокамеру и объективы. Б. Л. Р. возражала против видеосъемки и дальнейшей публикации материалов, в связи с чем случился конфликт со съемочной группой. Желая остановить съемку, Б. Л. Р. выхватила у корреспондента мобильный телефон и оторвала элементы видеокамеры, причинив тем самым ущерб на сумму, превышающую 500 тыс. р. Как в ходе судопроизводства пояснила сама Б. Л. Р., у нее отсутствовал умысел на повреждение чужого имущества, а действия были направлены исключительно на прекращение незаконной видеосъемки[2].

[2] Приговор мирового судьи судебного участка № 367 Тверского района города Москвы от 29 сентября 2014 г. по делу № 1-30/14. URL: https://sudact.ru/magistrate/court/reshenya-sudebnyi-uchastok-no-367-tverskogo-sudebnogo-raiona-gorod-moskva (дата обращения: 10.07.2024).

Даже если не учитывать судебную практику, достаточно просто смоделировать ситуацию, при которой виновное лицо уничтожает телефон потерпевшего, чтобы прервать нежелательную для себе видеосъемку или избавиться от компрометирующих его цифровых материалов. При подобной направленности умысла квалификацию исключительно по ст. 167 УК РФ в действующей редакции нельзя назвать справедливой. По нашему мнению, это означало бы игнорирование отдельных компонентов вины. К тому же при уничтожении носителя информации санкция предусмотрена более мягкая, чем в квалифицированных составах, закрепленных в ст. 272 УК РФ, в то время как потерпевший утрачивает доступ к цифровым данным в любом случае [9].

Иногда в научных трудах в качестве решения названной проблемы предлагается квалифицировать содеянное как совокупность преступлений, предусмотренных ст. 167 и 272 УК РФ [10]. Однако нам такая юридическая оценка представляется несоответствующей законодательству, поскольку отсутствует обязательный признак — неправомерный доступ. Подобное толкование, по существу, выходит за пределы смысла закона и является аналогией.

Если бы уничтожение или повреждение носителя оставались единственными неучтенными законодателем способами посягательства на компьютерную информацию, то достаточно было бы включить соответствующий признак в ст. 167 УК РФ. К сожалению, это не так. Известно и доказано, что электромагнитные импульсы способны стирать информацию на определенных носителях, но сами носители не всегда теряют возможность функционирования [11]. Как квалифицировать содеянное в таком случае? Применение ст. 167 УК РФ или ст. 7.17 КоАП РФ исключается, поскольку нет уничтоженного или поврежденного оборудования. К тому же под вопросом остается стоимость носителя. Отсутствие факта неправомерного доступа и вредоносных программ не дает квалифицировать содеянное по какой-либо из статей гл. 28 УК РФ.

Практические материалы свидетельствуют о хищениях, совершаемых виновными лицами для дальнейшего уничтожения информации или воспрепятствования ее использованию потерпевшим. Например, приговором Ленинского районного суда г. Ульяновска Т. А. Р. был признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 112 и ч. 1 ст. 161 УК РФ. Подсудимый в состоянии опьянения вместе с друзьями распивал спиртные напитки возле подъезда. Проходящий мимо потерпевший сделал Т. А. Р. замечание по поводу его поведения и стал фиксировать правонарушение на камеру телефона. Т. А. Р. в грубой форме потребовал передать ему телефон с целью удаления видеозаписи, что привело к конфликту и нападению на потерпевшего. Причинив здоровью потерпевшего вред средней тяжести, Т. А. Р. завладел его телефоном стоимостью около 5 тыс. р. Сам подсудимый пояснил, что намеревался взять телефон с целью удаления записи, а изначально умысла на хищение у него не было[3].

После совершения хищения виновное лицо способно уничтожить информацию путем неправомерного доступа, повреждения носителя или иным образом. Кроме того, сам факт отсутствия электронного устройства у потерпевшего лишает его возможности пользоваться хранящимися на нем цифровыми данными. Указанное совпадает с определением блокирования, отраженном в п. 4 Постановления по ряду признаков: воздействие на источник хранения информации; невозможность временно или постоянно надлежаще ее использовать; искусственно затрудняется или ограничивается доступ законного пользователя.

В теории уголовного права существует и аргументирована позиция относительно отсутствия общественной опасности у блокировки компьютерной информации, если это не приводит к какому-либо иному вреду. Соответственно, возникает вопрос об обоснованности криминализации подобного явления [12].

На наш взгляд, ограничение или лишение возможности использовать цифровую информацию, безусловно, нарушает права и свободы граждан, а также потенциально способно повлечь вред, не поддающийся точному исчислению. Представим, например, коммерческую организацию, деятельность которой была парализована в результате блокировки доступа к базе данных. Весьма затруднительно будет посчитать упущенную выгоду, если сотрудники организации не смогли принять какое-либо число заказов от клиентов. Тем не менее сами предприниматели в ходе опросов убедительно говорят о больших суммах ущерба от киберпреступлений [13].

[3] Приговор Ленинского районного суда г. Ульяновска от 26 ноября 2018 г. по делу № 1-196/2018. URL: https://actofact.ru/case-73RS0001-1-196-2018-2018-09-28-2-0 (дата обращения: 10.07.2024).

Само по себе хищение носителя в целом достаточно просто квалифицируется в соответствии с одной из статей гл. 21 УК РФ, если при этом нет признаков иных преступлений. При сумме ущерба, не превышающей 2 500 р., необходимо обращаться к КоАП РФ. Однако умысел преступника, направленный на блокировку доступа к значимой для потерпевшего информации, вновь остается за пределами составов преступления или правонарушения. Квалифицирующих признаков, связанных с уничтожением, блокировкой информации, в составах хищений не имеется. Целесообразность их закрепления сомнительна, поскольку приведет, как правильно отмечает Е.А. Русскевич, к «цифровым двойникам» традиционных уголовно-правовых запретов и избыточному дублированию положений закона [2]. Кроме того, применение норм, направленных на противодействие хищениям, как правило, зависит от суммы ущерба. Материальную ценность информации оценить затруднительно или невозможно, как ценность памятной фотографии, любительского рисунка или записей в личном дневнике.

Между тем игнорирование возрастающей с каждым годом ценности информации является, на наш взгляд, ошибкой. В современных электронных устройствах пользователи хранят большие объемы фотографий и видеороликов, ведут деловые календари и записи, фиксируют логины и пароли от аккаунтов. На телефоны приходят специальные ключи для доступа в государственные информационные системы. Современные устройства также считывают и хранят биометрические данные (например, отпечатки пальцев). Ценность вышеуказанной информации для потерпевшего зачастую превышает материальную стоимость самого носителя.

В частности, как следует из приговора мирового судьи Троицко-Печорского судебного участка Республики Коми, С. Е. Н. распивала с потерпевшим спиртные напитки. В процессе употребления алкогольной продукции она пользовалась телефоном потерпевшего с его разрешения для прослушивания музыки. В дальнейшем у С. Е. Н. внезапно возник преступный умысел на хищение, что она и совершила, воспользовавшись состоянием опьянения потерпевшего. Сам потерпевший пояснил, что телефон не представляет для него значительной материальной ценности, в отличие от информации, хранящейся на сим-карте и флеш-карте[4].

Казалось бы, в отсутствие надлежащей уголовно-правовой и административно-правовой защиты компьютерной информации лицо, утратившее ее, не лишено возможности обратиться в суд с исковыми требованиями для возмещения вреда. Однако исследование судебных актов показывает, что в этом случае благоприятный исход для истца не гарантирован, а ответчик не привлекается к гражданско-имущественной ответственности.

Об этом свидетельствует решение мирового судьи по гражданскому делу № 2-7/2016. Т. Н. К. посредством обращения в суд потребовала от К. М. И. возмещение материального ущерба и компенсацию морального вреда. Было установлено, что ответчик систематически в хулиганских целях отключал электрообеспечение ее квартиры, за что привлекался к административной ответственности. В результате его действий произошел скачок напряжения, повредивший блок питания, цепь питания, контроллер питания, видеокарту компьютера, принадлежащего Т. Н. К. Сумма ущерба превысила 18 тыс. р. Кроме того, Т. Н. К. пояснила, что из-за повреждения компьютера были утеряны ценные для нее файлы. Судом были удовлетворены исковые требования о возмещении материального ущерба (в размере стоимости ремонта компьютера), однако требования о взыскании компенсации морального вреда оставлены без удовлетворения[5].

Необходимо обратить внимание, что для потерпевшего в целом не имеет большого значения способ уничтожения информации или создания препятствий к ее использованию. Если цифровые данные играют огромную роль сами по себе, то их обладателю практически все равно, уничтожены они путем неправомерного доступа, с помощью использования вредонос-

[4] Приговор мирового судьи Троицко-Печорского судебного участка Республики Коми от 20 марта 2014 г. по делу № 1-4/2014. URL: http://troitsko-pechosky.komi.msudrf.ru/modules.php?name=sud_delo&op=cs&case_id=19183317&delo_id=1540006 (дата обращения: 10.07.2024).

[5] Решение мирового судьи судебного участка № 48 Железнодорожного судебного района Московской области от 13 января 2016 г. по делу 2-7/2016. URL: http://48.mo.msudrf.ru/modules.php?name=sud_delo&op=sd&number=97389837&case_number=96886593&delo_id=1540005 (дата обращения: 10.07.2024).

ных программ или в результате повреждения жесткого диска. В соответствии с требованиями закона преступник, подобравший пароль к электронному устройству и удаливший файл, понесет уголовную ответственность. В то же время лицо, повредившее карту памяти телефона с целью уничтожения информации, не подвергнется уголовному наказанию (возможно, и административному тоже). Для потерпевшего, не обладающего специальными юридическими познаниями, столь отличающийся исход по одинаковым для него вредным последствиям будет выглядеть крайне несправедливым. Все это лишь способствует росту социальной напряженности и недоверию к правовой системе. Кроме того, в рассматриваемом контексте верным представляется суждение А.А. Гребенькова о том, что уничтожение информации в ходе неправомерного доступа обычно происходит выборочно. Если же поврежден носитель, то уничтожается вся информация [8].

Таким образом, материалы судебной практики и исследования ученых доказывают, что в действительности имеют место различного рода посягательства на носители, совершаемые с целью уничтожения цифровых данных. Общественная опасность таких деяний не уступает преступлениям, предусмотренным ст. 272 и 274 УК РФ. Изложенное подталкивает к выводу о целесообразности криминализации более широкого спектра способов, ведущих к уничтожению, модификации или блокировке информации. Более того, если обратить внимание на законодательство отдельных зарубежных стран, можно заметить далеко не единичное применение данного подхода.

Статья 4 Конвенции о компьютерных преступлениях (Будапешт, 23 ноября 2001 г.) призывает каждую сторону принять законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных неправомерно.

Уголовный кодекс Республики Казахстан запрещает неправомерные уничтожение или модификацию информации, которая хранится на электронном носителе, содержится в информационной системе или передается по сетям телекоммуникаций. Состав материальный, т.е. для признания деяния оконченным необходимо наступление указанных в законе последствий. Способ не является обязательным признаком, поэтому буквальное толкование позволяет говорить о том, что деяние может быть совершено и с помощью физического воздействия [14].

Не так давно была изменена ст. 350 Уголовного кодекса Республики Беларусь, ранее предусматривавшая ответственность лишь за модификацию компьютерной информации. В настоящее время запрещены также уничтожение, блокирование и приведение в негодное состояние компьютерной информации [15]. Способ не конкретизируется, однако уточняется, что должны отсутствовать признаки преступления против собственности. Отметим, что подход законодателя Республики Беларусь представляется нам весьма интересным и заслуживающим внимания не только в рамках рассматриваемой темы, но и по отношению к регулированию всех компьютерных преступлений.

Уголовный закон Италии содержит ряд составов, охватывающих противоправные посягательства на компьютерную информацию и компьютерные системы. В частности, запрещаются: повреждение компьютерных данных и программ (ст. 635-bis); повреждение компьютерных данных и программ, используемых государством или общественной организацией (ст. 635-ter); повреждение компьютерных систем (ст. 635-quater) и повреждение компьютерных систем общественных организаций (ст. 635-quinquies). Перечень преступлений расширялся с учетом появления новых посягательства и изменения подхода к ценности информации [16].

В соответствии с законодательством Индонезии наказываются штрафом или лишением свободы на срок от восьми до десяти лет незаконные изменение, добавление, передача, удаление, подделка, перемещение или сокрытие электронной информации независимо от способа совершения деяния. Отдельный состав преступления образуют создание, изменение, уничтожение или повреждение электронной информации с целью изготовления поддельных документов [17].

Согласно турецкому уголовному закону (ст. 244), наказуемым признается искажение, уничтожение, изменение или приведение в недоступное состояние данных в информационной системе. Способ такого деяния не оказывает влияния на квалификацию. Более строго наказывается посягательство на информационную систему государственного или кредитного учреждения [18].

Статья 286 Уголовного кодекса КНР запрещает ряд действий, приводящих к невозмож-

ности нормального функционирования компьютерной системы. Среди них указывается не только взаимодействие с информацией (удаление, исправление), но и создание помех, имеющее широкое значение [19]. Непосредственно получение неправомерного доступа к системе не включается в качестве обязательного признака данного состава преступления.

В Индии с 2000 г. действует Закон об информационных технологиях, в разд. 43 которого предусмотрены штрафы и компенсация за повреждение компьютера или компьютерной системы без соответствующего на то разрешения [20].

Нормативные акты отдельных штатов США также запрещают разнообразные посягательства на цифровую информацию и ее носители. В рамках исследования нецелесообразно проводить подробный анализ их всех, достаточно лишь упомянуть о встречающейся повышенной защите (по сравнению с иным имуществом) компьютерной техники и цифровых данных. Например, ст. 815.06 Уголовного закона штата Флорида признает преступным уничтожение, хищение, повреждение оборудования, используемого в компьютере, компьютерной системе, компьютерной сети или электронном устройстве, а также разрушение или повреждение любого компьютера, компьютерной системы, компьютерной сети или электронного устройства [21, с. 224]. Статья NRS 205.4765 Уголовного закона штата Невада запрещает повреждение или уничтожение любым образом данных, существующих внутри компьютера (ч. 1), а также уничтожение компьютерного оборудования (ч. 2) и самого компьютера (ч. 3) [22].

Краткое ознакомление с зарубежными нормативными актами позволяет говорить о наличии подхода, при котором наказуемым признается посягательство на компьютер, компьютерную систему или электронное устройство. Российским законодателем последствия в виде уничтожения или блокировки информации, ее ценность часто игнорируются. В контексте настоящего исследования мы находим подобный подход избыточным. Само по себе техническое устройство представляет материальную ценность и мало отличается в этом смысле от других предметов. Его уничтожение или повреждение в достаточной мере защищаются уголовным, административным и гражданским законом. Однако состояние цифровой информации, как говорилось ранее, остается за пределами надлежащего правового регулирования. Изложенное подталкивает к мысли о возможности заимствования положений зарубежного законодательства в области уголовно-правовой защиты цифровых данных.

Предложения такого рода в целом высказывались в отечественной научной литературе. В частности, К.Н. Евдокимов предлагает сконструировать новый состав преступления, охватывающий незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации [23]. Рекомендация автора нашла поддержку среди других ученых [24]. Выше нами упоминалось (и приводились примеры из практики), что такие действия имеют место, а их общественная опасность ничуть не меньше, чем деяния, предусмотренные ст. 272 УК РФ. Однако предлагаемая авторами конструкция видится слишком ограниченной и казуистичной, поскольку предусматривает весьма узкий спектр посягательств.

Е.А. Русскевич настаивает на необходимости введения ст. 272.1 УК РФ, предусматривающей ответственность за умышленные уничтожение, блокирование или модификацию компьютерной информации при отсутствии признаков состава преступления, предусмотренного ст. 272 УК РФ [25]. Позиция автора представляется весьма логичной и аргументированной. В то же время следует обратить внимание на формальный вид состава преступления по конструкции объективной стороны. Буквальное толкование позволяет говорить о том, что уголовную ответственность влекут любые умышленные действия по блокированию или модификации информации независимо от последствий.

Ввод словосочетаний в текстовый документ также является модификацией, но не всегда причиняет какой-либо вред обладателю информации. Создание препятствий в использовании электронного устройства является блокировкой, но, опять же, не обязательно имеющей вредные последствия. Разумеется, в таких случаях можно обращаться к положениям о малозначительности деяния, закрепленным в ч. 2 ст. 14 УК РФ, однако их границы достаточно размыты. В то же время недобросовестный потерпевший может использовать малейшее нарушение своих прав (в виде модификации или блокирования) в попытке наказать какого-либо человека из личной неприязни или желании извлечь доход посредством дальнейшего предъявления гражданского иска в уголовном судопроизводстве.

Думается, сама концепция введения в уголовный закон отдельного состава, охватывающего уничтожение, блокирование или модификацию компьютерной информации, является верной. Однако для исключения вышеуказанных проблем толкования и правоприменения необходимо указание на обязательные общественно опасные последствия. Иначе говоря, состав следует сконструировать как материальный. В качестве последствий предлагается определить причинение существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства. Такая конструкция позволит избежать оценки утраченной информации в денежном выражении и при этом исключит излишнюю репрессивность статьи.

Уничтожение, повреждение носителя или завладение им следует квалифицировать по статьям, размещенным в гл. 21 УК РФ «Преступления против собственности». В этом смысле дублирование запретов не образуется. Например, повреждение жесткого диска охватывается ст. 167 УК РФ. Если эти действия привели к уничтожению информации, причинили правам и интересам потерпевшего существенный вред и охватывались умыслом виновного, то содеянное должно квалифицироваться дополнительно по ст. 272.1 УК РФ. Подобным образом квалификация может производиться в случае блокирования информации, вызванной завладением носителя. Описанное составляет идеальную совокупность преступлений, совершаемую одним действием, но влекущую принципиально разные последствия. Неосторожное причинение вреда состоянию компьютерной информации, по нашему мнению, введения дополнительных уголовно-правовых запретов не требует.

Выводы

Действующий уголовный закон в целом обеспечивает защиту от посягательств, направленных на уничтожение или блокировку цифровой информации. Вносимые изменения свидетельствуют о пристальном внимании к данной области регулирования. Однако отдельные правовые пробелы преодолеть к настоящему времени не удалось.

Уничтожение или повреждение носителя информации охватываются ст. 167 УК РФ или ст. 7.17 КоАП РФ, — это зависит от размера ущерба. Данные действия иногда совершаются с целью уничтожения или блокирования компьютерной информации, что не уступает по степени общественной опасности деянию, предусмотренному ст. 272 УК РФ, но остается за рамками состава и юридической ответственности.

Завладение носителем информации охватывается рядом статей, преимущественно размещенных в гл. 21 УК РФ «Преступления против собственности». Однако завладение также может осуществляться с целью блокирования доступа потерпевшего к собственной компьютерной информации, что вновь остается за рамками состава и юридической ответственности.

В зарубежных странах применяются различные подходы, при которых лицо подлежит уголовной ответственности за совершение посягательств, направленных на целостность информации или ее блокирование независимо от способа. Хотя уголовная наказуемость любых посягательств на компьютерную систему видится избыточной, некоторые положения иностранных нормативных актов заслуживают рассмотрения на предмет заимствования в отечественное законодательство. В частности, оправданной кажется (и поддерживается учеными-правоведами) криминализация умышленных действий по уничтожению, блокированию и модификации компьютерной информации не только посредством неправомерного доступа, но и иными способами.

Развивая и дополняя идеи, высказанные деятелями науки, считаем целесообразным введение в УК РФ новой статьи 272.1, предусматривающей ответственность за уничтожение, блокирование и модификацию компьютерной информации. Диспозиция ч. 1 могла бы выглядеть следующим образом: «1. Умышленные уничтожение, блокирование или модификация компьютерной информации при отсутствии признаков состава преступления, предусмотренного статьей 272 настоящего Кодекса, если эти деяния повлекли причинение существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства, — …»

Квалифицированные составы, на наш взгляд, могут содержать такие признаки, как: тяжкие последствия; совершение деяния группой лиц по предварительному сговору; совершение деяния организованной группой; цель скрыть другое преступление или облегчить его совершение; совершение деяния лицом с использованием своего служебного положения.

Данные выводы носят во многом дискуссионный характер и, возможно, не получат единодушной поддержки. Однако дальнейшие исследования проблемы, безусловно, помогут выработать наиболее правильное и эффективное решение, поддерживаемое большинством ученых.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Бегишев И.Р. Цифровые преступления, совершаемые в отношении роботов / И.Р. Бегишев. — DOI 10.33693/2223-0092-2021-11-3-67-73. — EDN ZYLJHI // Социально-политические науки. — 2021. — Т. 11, № 3. — С. 67–73.

2. Русскевич Е.А. О цифровизации особенной части УК РФ / Е.А. Русскевич. — DOI 10.24411/2073-0454-2019-10038. — EDN CXCGHD // Вестник Московского университета МВД России. — 2019. — № 1. — С. 146–151.

3. Иванова Л.В. Виды киберпреступлений по российскому уголовному законодательству / Л.В. Иванова. — DOI 10.25136/2409-7136.2019.1.28600. — EDN OPWTXO // Юридические исследования. — 2019. — № 1. — С. 25–33.

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

5. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук : 12.00.08 / А.А. Жмыхов. — Москва, 2003. — 178 с. — EDN NOEEOZ.

6. Abd ALNomani M.M. Informational destruction crime; a comparative Study / M.M. Abd ALNomani, A.H.T. Birmani // PalArch's Journal of Archaeology of Egypt/Egyptology. — 2020. — Vol. 17, no. 3. — P. 2266–2281.

7. Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации : дис. … канд. юрид. наук / И.Р. Бегишев. — Казань, 2017. — 204 с. — EDN YRUCWK.

8. Гребеньков А.А. Уничтожение компьютерной информации как информационное преступление / А.А. Гребеньков. — EDN WMJTCF // Апробация. — 2016. — № 7. — С. 26–27.

9. Ходусов А.А. К вопросу о совершенствовании законодательства об уголовной ответственности за совершение преступлений в сфере обращения цифровой информации / А.А. Ходусов. — EDN MTSQOI // Цифровые технологии и право : сб. науч. тр. I Междунар. науч.-практ. конф., Казань, 23 сент. 2022 г. — Казань, 2022. — С. 221–228.

10. Озерова А.С. О необходимости изменения подхода к понятию «информация» в законодательстве и судебной практике / А.С. Озерова. — DOI 10.21638/spbu25.2019.107. — EDN QYRWXZ // Правоведение. — 2019. — Т. 63, no. 1. — С. 137–156.

11. Threats to information security in computer systems, sources of threats, information risks, methods of their assessment / N. Kushnir, E. Yatskevich, A. Vlasova, V. Arustamyan. — DOI 10.24412/9215-0365-2022-83-1-62-65 // The Scientific Heritage. — 2022. — Vol. 83, no. 1. — P. 62–65.

12. Антонов А.Г. К вопросу об общественной опасности неправомерного доступа к компьютерной информации / А.Г. Антонов, Д.В. Крюков. — DOI 10.17223/22253513/44/1. — EDN MLMAPM // Вестник Томского государственного университета. Право. — 2022. — № 44. — С. 5–16.

13. Вестов Ф.А. Уголовная политика по использованию возможностей цифровых технологий в противодействии мошенничеству / Ф.А. Вестов, Н.Р. Шамьенов. — DOI 10.24411/2305-8641-2020-10019. — EDN PMAFHW // Основы экономики, управления и права. — 2020. — № 6 (25). — С. 53–57.

14. Topical Issues in the Fight Against Criminal Offences in the Field of Informatisation and Communications / A. Kambarov, M. Karazhanov, A. Smagulov, S. Kumisbekov. — DOI https://doi.org/10.26512/lstr.v15i1.44728 // Law, State and Telecommunications Review. — 2023. — Vol. 15, no. 1. — P. 177–190.

15. Цепелев К.В. Совершенствование законодательства Российской Федерации и республики Беларусь в части установления уголовной ответственности за преступления, связанные с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий (информационно-аналитический обзор) / К.В. Цепелев, Е.Н. Карабанова, Н.А. Швец. — EDN WOIHLT // Вестник Университета прокуратуры Российской Федерации. — 2022. — № 3 (89). — С. 124–135.

16. Filipkowski W. Criminalizing Cybercrimes: Italian and Polish Experiences / W. Filipkowski, L. Picarella. — DOI 10.15290/bsp.2021.26.03.09 // Białostockie Studia Prawnicze. — 2021. — Vol. 26, no. 3. — P. 171–183.

17. Suhendi D. Cyber laws related to prevention of theft of information related to acquisition of land and infrastructure resources in Indonesia / D. Suhendi, E. Asmadi. — DOI 10.5281/zenodo.4766552 // International Journal of Cyber Criminology. — 2022. — Vol. 15, no. 2. — P. 135–143.

18. Crime control in the sphere of information technologies in the Republic of Turkey / A. Shukan, A. Abdizhami, G. Ospanova, D. Abdakimova. — DOI 10.1016/j.diin.2019.07.005 // Digital Investigation. — 2019. — Vol. 30. — P. 94–100.

19. Li X. Regulation of cyber space: An analysis of Chinese law on cyber crime / X. Li. — DOI 10.5281/zenodo.56225 // International Journal of Cyber Criminology. — 2015. — Vol. 9, no. 2. — P. 185.

20. Patil J. Cyber Laws in India: An Overview / J. Patil // Indian Journal of Law and Legal Research. — 2022. — Vol. 4, no. 1. — P. 1391–1411.

21. Hill J.B. Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century / J.B. Hill, N.E. Marion. — Santa Barbara : ABC-CLIO, 2016. — 290 p.

22. Brenner S.W. US cybercrime law: Defining offenses / S.W. Brenner. — DOI 10.1023/B:ISFI.0000025780.94350.79 // Information Systems Frontiers. — 2004. — Vol. 6. — P. 115–132.

23. Евдокимов К.Н. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации / К.Н. Евдокимов. — EDN TGHXAT // Вектор науки Тольяттинского государственного университета. Сер.: Юридические науки. — 2014. — № 4. — С. 33–36.

24. Сердюкова Е.В. Особенности уголовной ответственности за преступления в сфере компьютерной информации / Е.В. Сердюкова, А.А. Чуниха, Е.О. Зиновьева. — DOI 10.31618/ESSA.2782-1994.2021.1.72.104. — EDN TRKLBJ // Восточно-европейский научный журнал. — 2021. — № 8-1 (72). — С. 57–59.

25. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. ... д-ра юрид. наук : 12.00.08 / Е.А. Русскевич. — Москва, 2020. — 499 с. — EDN IXNSFI.

REFERENCES

1. Begishev I.R. Digital Crimes, Committed Against Robots. *Sotsial'no-politicheskie nauki = Sociopolitical Sciences*, 2021, vol. 11, no. 3, pp. 67–73. (In Russian). EDN: ZYLJHI. DOI: 10.33693/2223-0092-2021-11-3-67-73.

2. Russkevich E.A. On Digitalization of a Special Part of the Criminal Code. *Vestnik Moskovskogo universiteta MVD Rossii = Bulletin of Moscow University of the Ministry of Internal Affairs of Russia*, 2019, no. 1, pp. 146–151. (In Russian). EDN: CXCGHD. DOI: 10.24411/2073-0454-2019-10038.

3. Ivanova L.V. Kinds of Cybercrime According to the Russian Law. *Yuridicheskie issledovaniya = Legal Studies*, 2019, no. 1, pp. 25–33. (In Russian). EDN: OPWTXO. DOI: 10.25136/2409-7136.2019.1.28600.

4. Gracheva Yu.V., Malikov S.V., Chuchaev A.I. Crimes in the Sphere of Computer Information: Critical Look. *Pravo. Zhurnal Vysshey shkoly ekonomiki = Law Journal of the Higher School of Economics*, 2021, no. 4, pp. 152–176. (In Russian). EDN: UYXHEB. DOI: 10.17323/2072-8166.2021.4.152.176.

5. Zhmyhov A.A. *Computer Crimes in other Countries and their Prevention. Cand. Diss*. Moscow, 2003. 178 p. EDN: NOEEOZ.

6. Abd ALNomani M.M., Birmani A.H.T. Informational Destruction Crime; a Comparative Study. *PalArch's Journal of Archaeology of Egypt/Egyptology,* 2020, vol. 17, no. 3, pp. 2266–2281.

7. Begishev I.R. *Concept and Types of Crimes in the Sphere of Application of Digital Information. Cand. Diss.* Kazan, 2017. 204 p. EDN: YRUCWK.

8. Grebenkov A.A. Destruction of Computer Information as an Information Crime. *Aprobatsiya = Approbation*, 2016, no. 7, pp. 26–27. (In Russian). EDN: WMJTCF.

9. Hodusov A.A. On the Issue of Improving the Legislation on Criminal Liability for Crimes in the Field of Digital Information Circulation. *Digital Technologies and Law. Collection of Scientific papers of the I International Scientific and Practical Conference*, Kazan, 23 September, 2022. Kazan, 2022, pp. 221–228. (In Russian). EDN: MTSQOI.

10. Ozerova A.S. On the Need to Change the Approach to the Concept of "Information" in Legislation and Judicial Practice. *Pravovedenie = Jurisprudence*, 2019, vol. 63, no. 1, pp. 137–156. (In Russian). EDN: QYRWXZ. DOI: 10.21638/spbu25.2019.107.

11. Kushnir N., Yatskevich E., Vlasova A., Arustamyan V. Threats to Information Security in Computer Systems, Sources of Threats, Information Risks, Methods of their Assessment. The Scientific Heritage, 2022, vol. 83, no. 1, pp. 62–65. DOI: 10.24412/9215-0365-2022-83-1-62-65.

12. Antonov A.G., Zorina E.A., Kryukov D.V. On the Public Danger of Illegal Access to Computer Information. *Vestnik Tomskogo gosudarstvennogo universiteta. Pravo = Tomsk State University Journal of Law*, 2022, no. 44, pp. 5–16. (In Russian). EDN: MLMAPM. DOI: 10.17223/22253513/44/1.

13. Vestov F.A., Shamienov N.R. Criminal Policy on Using the Opportunities of Digital Technologies in Countering Fraud. *Osnovy ekonomiki, upravleniya i prava = Basics of Economy, Management and Law*, 2020, no. 6, pp. 53–57. (In Russian). EDN: PMAFHW. DOI: 10.24411/2305-8641-2020-10019.

14. Kambarov A., Karazhanov M., Smagulov A., Kumisbekov S. Topical Issues in the Fight Against Criminal Offences in the Field of Informatization and Communications. *Law, State and Telecommunications Review*, 2023, vol. 15, no. 1, pp. 177–190. DOI: https://doi.org/10.26512/lstr.v15i1.44728.

15. Tsepelev K.V., Karabanova E.N., Shvets N.A. Improving the Legislations of the Russian Federation and the Republic of Belarus Regulating Criminal Liability for Crimes Infringing on Security in the Sphere of Information-Communication Technologies (an Information-analytical Overview). *Vestnik Universiteta prokuratury Rossiiskoi Federatsii = Bulletin of the University of the Prosecutors Office of the Russian Federation*, 2022, no. 3, pp. 124–135. (In Russian). EDN: WOIHLT.

16. Filipkowski W., Picarella L. Criminalizing Cybercrimes: Italian and Polish Experiences. *Białostockie Studia Prawnicze*, 2021, vol. 26, no. 3, pp. 171–183. DOI: 10.15290/bsp.2021.26.03.09.

17. Suhendi D., Asmadi E. Cyber Laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia. *International Journal of Cyber Criminology,* 2022, vol. 15, no. 2, pp. 135–143. DOI: 10.5281/zenodo.4766552.

18. Shukan A., Abdizhami A., Ospanova G., Abdakimova D. Crime Control in the Sphere of Information Technologies in the Republic of Turkey. *Digital Investigation*, 2019, vol. 30, pp. 94–100. DOI: 10.1016/j.diin.2019.07.005.

19. Li X. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology*, 2015, vol. 9, no. 2, pp. 185. DOI: 10.5281/zenodo.56225.

20. Patil J. Cyber Laws in India: An Overview. *Indian Journal of Law and Legal Research*, 2022, vol. 4, no. 1, pp. 1391–1411.

21. Hill J.B., Marion N.E. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. Santa Barbara, ABC-CLIO, 2016. 290 p.

22. Brenner S.W. US Cybercrime Law: Defining Offenses. *Information Systems Frontiers*, 2004, vol. 6, pp. 115–132. DOI: 10.1023/B:ISFI.0000025780.94350.79.

23. Evdokimov K.N. Problems of Criminal-Legal Qualification of Crimes in the Sphere of Computer Information. *Vektor nauki Tolyattinskogo gosudarstvennogo universiteta Seriya: Yuridicheskie nauki. = Science Vector of Togliatti State University. Series: Legal Sciences*, 2014, no. 4, pp. 33–36. (In Russian). EDN: TGHXAT.

24. Serdyukova E.V., Chunikha A.A., Zinovieva E.O. Features of Criminal Liability for Crimes in the Field of Computer Information. *Vostochno-evropeiskii nauchnyi zhurnal = Eastern European Scientific Journal*, 2021, no. 8-1, pp. 57–59. (In Russian). EDN: TRKLBJ. DOI: 10.31618/ESSA.2782-1994.2021.1.72.104.

25. Russkevich E.A. *Differentiation of Liability for Crimes Committed with the Use of Information-communication Technologies and the Issues of their Qualification. Doct. Diss*. Moscow, 2020. 499 p. EDN: IXNSFI.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Мосечкин Илья Николаевич — доцент кафедры уголовного права, процесса и национальной безопасности Юридического института Вятского государственного университета, кандидат юридических наук, г. Киров, Российская Федерация; e-mail: Weretowelie@gmail.com.

ДЛЯ ЦИТИРОВАНИЯ

Мосечкин И.Н. О криминализации деяний, направленных на уничтожение, блокирование или модификацию компьютерной информации / И.Н. Мосечкин. — DOI 10.17150/2500-4255.2024.18(5).482-493. — EDN BJELYH // Всероссийский криминологический журнал. — 2024. — Т. 18, № 5. — С. 482–493.

INFORMATION ABOUT THE AUTHOR

Mosechkin, Ilya N. — Ass. Professor, Department of Criminal Law, Process and National Security, Law Institute, Vyatka State University, Ph.D. in Law, Kirov, the Russian Federation; e-mail: Weretowelie@gmail.com.

FOR CITATION

Mosechkin I.N. On the Criminalization of Acts Aimed at Destroying, Blocking or Modifying Computer Information. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2024, vol. 18, no. 5, pp. 482–493. (In Russian). EDN: BJELYH. DOI: 10.17150/2500-4255.2024.18(5).482-493.