Научная статья
УДК 343.2/.7

С. 102–108

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ВОЗМОЖНОСТИ УГОЛОВНО-ПРАВОВОГО ВОЗДЕЙСТВИЯ И ПРЕДУПРЕЖДЕНИЯ

Михаил Владимирович Ульянов
Научно-исследовательский институт Университета прокуратуры РФ, Москва, Россия
m.ulyanov2@yandex.ru, SPIN-код 3923-7825

Аннотация. В статье предпринимается попытка анализа особенностей превентивного воздействия норм, предусматривающих уголовную ответственность за совершение преступлений в сфере компьютерной информации (гл. 28 УК РФ). С этой целью рассматриваются примеры из судебной практики, анализируются приговоры по уголовным делам о преступлениях рассматриваемого вида.

Преступления в сфере компьютерной информации могут иметь вспомогательный характер, создавая условия для совершения иных преступлений или иных правонарушений. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) чаще всего квалифицируются по ст. 272, 273 и ст. 138, 146, 159.6, 183 УК РФ.

По мнению автора, привлечение к ответственности, предусмотренной ст. 272–274.2 УК РФ, связано с предупреждением хищений, нарушений тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, нарушений авторских и смежных прав, иных правонарушений, в том числе непреступного характера, а также преступлений против общественной безопасности. Что позволяет говорить о том, что нормы об ответственности за преступления в сфере компьютерной информации осуществляют двойную превенцию.

Ключевые слова: двойная превенция, преступность, информационно-телекоммуникационные сети, хищения, социальная инженерия, предупреждение преступности, компьютерная преступность

Для цитирования: Ульянов М. В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения // Правопорядок: история, теория, практика. 2022. № 4 (35). С. 102–108.

Research article

CRIMES IN THE SPHERE OF COMPUTER INFORMATION: POSSIBILITIES OF CRIMINAL LEGAL IMPACT AND PREVENTION

Mikhail V. Ulyanov
Research Institute of the University of the Prosecutor's office of the Russian Federation, Moscow, Russia
m.ulyanov2@yandex.ru, SPIN-code 3923-7825

Abstract. The article attempts to analyze the features of the preventive impact of the norms providing for criminal liability for committing crimes in the field of computer information (Chapter 28 of the Criminal Code of the Russian Federation). For this purpose, examples from judicial practice are considered, sentences in criminal cases on crimes of the type in question are analyzed.

Crimes in the field of computer information may have an auxiliary character, creating conditions for the commission of other crimes or other offenses. Illegal access to computer information (Article 272

of the Criminal Code of the Russian Federation) and the creation, use and distribution of malicious computer programs (Article 273 of the Criminal Code of the Russian Federation) are most often qualified under Articles 272, 273 and Articles 138, 146, 159.6, 183, 146 of the Criminal Code of the Russian Federation.

According to the author, the prosecution provided for in Articles 272-274.2 of the Criminal Code of the Russian Federation is connected with the prevention of theft, violations of the secrecy of correspondence, telephone conversations, postal, telegraphic or other messages, violations of copyright and related rights, other offenses, including non-criminal nature, as well as crimes against public safety. Which suggests that the norms on responsibility for crimes in the field of computer information carry out double prevention.

Keywords: prevention, crime, information and telecommunication networks, theft, social engineering, crime prevention, computer crime

For citation: Ulyanov MV. Crimes in the sphere of computer information: possibilities of criminal legal impact and prevention. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2022;(4):102-108. (In Russ.)

Введение

В июне 2022 г. представителем Сбербанка России было заявлено об обнаружении в г. Бердянске мошеннического колл-центра, располагавшего личными сведениями 20 млн граждан Российской Федерации[1]. Это не единственное сообщение подобного рода. Привычными стали сообщения об утечках данных клиентов провайдеров, пользователей сайтов интернет-магазинов, служб доставки, образовательных порталов, интернет-ресурсов федеральных органов исполнительной власти и т. д. Становясь достоянием общественности, такие факты не всегда получают надлежащую уголовно-правовую оценку. Все это ставит вопрос об эффективности уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные гл. 28 УК РФ.

Описание исследования

Исследователи обращают внимание на «инструментальный» характер компьютерных преступлений, выступающих способом достижения иных преступных целей, что обусловливает во многих случаях их квалификацию по совокупности с другими составами преступлений [1, с. 55]. Например, осуществляя неправомерный доступ к компьютерной информации, лицо посягает на такие самостоятельные объекты уголовно-правовой охраны, как право граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений или порядок обращения со сведениями, составляющими коммерческую, налоговую или банковскую тайну.

М. Д. Фролов относит преступления в сфере компьютерной информации к преступлениям с двойной превенцией, обращая внимание на то, что они создают условия для компьютерного мошенничества [2, с. 170].

Такая позиция согласуется с определением уголовно-правовых норм с двойной превенцией как норм, выступающих в качестве условия, способствующего совершению другого преступного деяния [3, с. 170–171]. Согласно еще одному определению, данные нормы трактуются в качестве «системы норм с двойным превентивным эффектом, устанавливающей уголовно-правовой запрет на совершение общественно опасных деяний, которые могут обусловливать последующее совершение других преступлений» [4, с. 13].

В то же время отнесение компьютерных преступлений к нормам с двойной превенцией представляется в достаточной мере дискуссионным. Тем более, что, как указывает Н. И. Пикуров, значимость и реальное действие общей превенции еще никому не удалось обосновать с более-менее конкретными показателями [5, с. 102].

Особенность превентивного воздействия норм, предусматривающих уголовную ответственность за совершение преступлений в сфере компьютерной информации, состоит в их направленности не только на предупреждение иных преступлений, но также правонарушений непреступного характера. Например, конфиденциальная информация, полученная незаконно, может использоваться в рекламных целях колл-центрами различных организаций.

Касаясь особенностей превентивного воздействия, в первую очередь, следует говорить

[1] Сбербанк рассказал о раскрытой сети мошеннических колл-центров в Бердянске // RG.RU. URL: https://rg.ru/2022/06/03/sberbank-rasskazal-o-raskrytoj-seti-moshennicheskih-koll-centrov-v-berdianske.html?Msn=& (дата обращения: 07.09.2022).

о наличии взаимосвязи компьютерных преступлений и хищений с использованием информационно-коммуникационных технологий. На это в определенной степени указывает возрастающая динамика количественных показателей большинства преступлений, совершаемых с использованием информационно-коммуникационных технологий, включая предусмотренные гл. 28 УК РФ, а также многие виды хищений, в период применения ограничительных мер в связи с коронавирусной инфекцией в 2020 г. и 2021 г.[1] В 2021 г. количество преступлений в сфере компьютерной преступности увеличилось более чем на 50 % (с 4498 до 6869), количество преступлений, предусмотренных ст. 159.6 УК РФ.

Между тем, в контексте взаимосвязи с хищениями речь следует вести не обо всех преступлениях, составляющих гл. 28 УК РФ. В данном случае следует учесть позицию криминологов, согласно которой информационная преступность слагается из двух подсистем: первая включает преступления, которые нарушают информационные правоотношения, вторая охватывает корыстные преступления, средством которых служат информационные системы [6, с. 98–99].

Анализ приговоров показывает, что на создание условий осуществления корыстных преступлений, прежде всего, направлены нормы, предусматривающие уголовную ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Количество преступлений, предусмотренных ст. 272 УК РФ, составляет основной сегмент в структуре преступлений в сфере компьютерной информации. В 2021 г. зарегистрировано 6392 таких преступлений (в 2019 г. –2420, в 2020 г. — 4105). Осуждено по ст. 272 УК РФ как основной статье квалификации в 2021 г. 133 лица (2019 г. — 85, 2020 г. — 84)[2].

Самой многочисленной группой осужденных являлись работники коммерческих организаций (в 2021 г. — 45 из 133). Речь идет о сотрудниках офисов продаж различных телефонных компаний, системных администраторах или сотрудниках магазинов, правомочных осуществлять подключение к операторам связи и др.

Во многих случаях полученная незаконным способом информация передается третьим лицам.

В качестве распространенной ситуации можно привести действия К., осужденного по ч. 3 ст. 272 УК РФ за совершение неправомерного доступа к компьютерной информации из корыстных побуждений. Работая в должности специалиста офиса продаж, А. осуществил около двухсот неправомерных копирований персональных данных клиентов ПАО «МТС» без регистрации сервисных запросов, которые передавал неустановленному лицу, используя мессенджер[3].

Персональные данные, полученные таким образом, могут быть использованы для совершения мошенничеств, в том числе путем распространенных сейчас методов социальной инженерии, а также иных противоправных деяний.

Во многих случаях деяния дополнительно квалифицируются судом по ст. 138 (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) УК РФ.

Так, в 2021 г. по ч. 1 ст. 138 и ч. 2 ст. 272 УК РФ осужден А., который являлся продавцом-консультантом на точке продаж оператора сотовой связи. А. откликнулся на объявление в телеграмм-канале, в котором предлагалось денежное вознаграждение в размере 1000 рублей за каждую отправленную детализацию и замененную сим-карту. Осуществляя замену номеров сим-карт, А. получил в качестве вознаграждения 40 000 рублей[4].

Наглядной демонстрацией вспомогательного характера этого посягательства служат факты, когда лицо, осуществившее неправомерный доступ к компьютерной информации, само совершает хищение.

По п. «б», «в» ч. 3 ст.159.6 (2 эпизода) и ч. 3 ст. 272 (2 эпизода) УК РФ была осуждена

---

[1] Форма государственного статистического наблюдения 4-ЕГС (494) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/law/podborki/forma_4-egs/ (дата обращения: 07.09.2022).

[2] О демографических признаках осужденных по всем составам преступлений Уголовного кодекса Российской Федерации : отчет Судебного департамента при Верховном Суде Российской Федерации по форме 11.1 за 12 мес. 2021 г. // Судебный департамент при Верховном Суде Российской Федерации : [сайт]. — URL: http://www.cdep.ru/index.php?id=79&item=6121 (дата обращения: 01.09.2022).

[3] Приговор Зеленоградского районного суда г. Москвы от 17.01.2022 по делу № 1-73/2022 // Архив Зеленоградского районного суда г. Москвы за 2022 г.

[4] Приговор Солнцевского районного суда г. Москвы от 16.06.2021 по делу № 1-339/2021 // Архив Солнцевского районного суда г. Москвы за 2021 г.

сотрудник ПАО «Вымпелком» Д., которая под своими учетными данными осуществила доступ в компьютерную программу, перевыпустила СИМ-карту, подделав заявление клиента, получив таким образом возможность пользоваться деньгами с лицевого счета[1].

Как указывают некоторые исследователи, раскрываемость преступлений, предусмотренных ст. 272 УК РФ, остается невысокой [7, с. 134–137]. Анализ приговоров показывает, что выявление сотрудников коммерческих организаций во многом связано с активностью служб безопасности самих компаний. Приведенное является дополнительным подтверждением высокой латентности данных преступлений.

Так, по ч. 3 ст. 272 и ч. 3 ст. 183 УК РФ осужден У., являвшийся системным администратором департамента IT-сервисов ООО «Яндекс. Технологии». Последний разместил в телеграмм-канале объявление о возможности оказания за денежное вознаграждение услуг по предоставлению неправомерного доступа к электронным ящикам клиентов. Под видом «клиента» к У. обратился сотрудник службы безопасности компании с просьбой осуществить доступ к конкретному адресу электронной почты и произвести копирование информации[2].

Еще одна категория осужденных, на которую следует обратить внимание, — сотрудники правоохранительных органов, имеющие доступ базам данным, разработанным в интересах, прежде всего, оперативных подразделений. Сторонним лицам могут быть переданы имеющиеся сведения о судимостях, нахождении в розыске, зарегистрированных автомобилях, а также иная исчерпывающая конкретизированная информация. Среди осужденных сотрудники правоохранительных органов составляют меньшинство (в 2021 г. был осужден лишь 1 сотрудник). В то же время очевидно то, что совершаемые ими преступления, обладают повышенной степенью общественной опасности. Действия таких лиц квалифицируются по совокупности преступлений, предусмотренных ч. 3 ст. 272 УК РФ и ст. 286 (Превышение должностных полномочий) УК РФ, либо в некоторых случаях ст. 290 (Получение взятки) УК РФ.

Например, по ч. 3 ст. 272 УК РФ и ст. 286 УК РФ осужден следователь следственного отдела ОМВД России С., который за денежное вознаграждение передавал информацию представителю детективного агентства из информационно-поисковой системы «Следопыт-М» и программно-технического комплекса «Розыск-Магистраль», предназначенного для выявления лиц, находящихся в розыске[3].

Еще одним преступлением, создающим условия для совершения хищений, является создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

В 2021 г. было зарегистрировано 317 данных преступлений (2019 г. — 455, 2020 г. — 371), осуждено лиц 77 (2019 г. — 76, 2020 г. — 45). По роду занятий (социальному положению) основная часть осужденных являлась трудоспособными лицами без постоянного источника дохода.

Как отмечают исследователи, использование вредоносных компьютерных программ нередко осуществляется для обеспечения неправомерного доступа к вычислительным ресурсам с целью извлечения материальной выгоды, например, для взлома программного обеспечения и его использования в личных целях или реализации, майнинга криптовалют [8, с. 106–125].

В качестве примера можно привести действия Б., осужденного в феврале 2022 г. по ч. 1 ст. 273 УК РФ. Б. скопировал с одного из сайтов компьютерную программу, с помощью которой создал вредоносные файлы, позволяющие получать несанкционированный доступ к логинам и паролям учетных записей, истории посещённых Интернет-страниц, файлам электронных криптокошельков чужого компьютера. Указанная информация передавалась на управляющий сервер по адресу «www.1237.zzz.com.ua». Данные файлы Б. разместил на канале «YouTube» во вкладке к описанию видео под видом читов для компьютерной игры[4].

Еще один пример наглядно показывает уровень раскрываемости организованных форм компьютерной преступности.

Так, в 2019 г. по ч. 3 ст. 272, ч. 2 ст. 273 и ч. 4 ст. 159.6 УК РФ осуждены Л. и Б., которые

[1] Приговор Октябрьского городского суда Республики Башкортостан от 29.07.2020 по делу № 03RS0014-01-2020-001990-69 // Архив Октябрьского городского суда Республики Башкортостан за 2020 г.

[2] Приговор Люблинского районного суда г. Москвы от 09.11.2021 по делу № 1-750-2021 // Архив Люблинского районного суда г. Москвы за 2021 г.

[3] Приговор Преображенского районного суда от 14.04.2022 по делу № 1-363/22 // Архив Преображенского районного суда г. Москвы за 2022 г.

[4] Приговор Прикубанского районного суда г. Краснодара от 21.02.2022 по делу № 1-494/2022 // Архив Прикубанского районного суда г. Краснодара от 2022 г.

в составе организованной группы получили неправомерный доступ к банкоматам одного из банков и возможность устанавливать на жесткие диски банкоматов файлы. После осуществления удаленного управление банкоматом участники организованной группы отправляли команды на выдачу денежных купюр в любом доступном объеме. В результате преступной деятельности с банкоматов было снято несколько миллионов рублей. Основная часть соучастников, в том числе организатор, не были установлены правоохранительными органами[1].

Проблемы невысокой раскрываемости подобных преступлений связана с целым рядом причин, в числе которых недостатки профессиональной подготовки сотрудников соответствующих ведомств, призванных бороться с киберпреступностью.

Трудоемкость расследования организованных форм преступлений в сфере компьютерной информации, в том числе необходимость проведения большого количества технических экспертиз, допросов экспертов в качестве свидетелей и др., обусловливает то, что за использование вредоносных программ в большинстве случаев к ответственности привлекаются лица за незаконное подключение к спутниковому телевидению, сети Интернет, «взлом» программного обеспечения.

Так, в июле 2020 г. был осужден Д. по ч. 2 ст. 272 УК РФ и ч. 2 ст. 273 УК РФ, который за 2000 руб. модифицировал ресивер, принадлежащий Я., что обеспечило декодирование защищенных спутниковых телеканалов «Триколор ТВ». Затем Д. продал лицу, действовавшему в рамках оперативно-розыскного мероприятия «проверочная закупка», за 4500 руб. модифицированный ресивер с пультом дистанционного управления и смарт-картой Триколор ТВ[2].

В случаях, когда вредоносные программы используются для обеспечения доступа к программному обеспечению деяния дополнительно квалифицируются по ст. 146 (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) УК РФ по совокупности преступлений.

Следует отметить, что длительное время предметом данных посягательств зачастую становились продукты Microsoft. В настоящее время предметами данных преступлений выступает отечественное программное обеспечение. С учетом нынешнего санкционного давления на российскую экономику, уход ряда иностранных ИТ-компаний с рынка, а также принятия мер, направленных на обеспечение технологической независимости, данная тенденция скорее всего сохранится.

Так, сотрудниками внутренних дел был выявлен Т., который за денежное вознаграждение установил контрафактное программное обеспечение «КОМПАС-3D». При ее установке на компьютер Т. использовал вредоносную программу для нейтрализации средств защиты. Помимо этого, Т. инкриминировалось незаконное использование в целях сбыта программного обеспечения Microsoft, что было исключено судом из объема обвинения, поскольку подтверждения о причинении компании крупного размера ущерба не было представлено[3].

Количественные показатели иных преступлений, составляющих главу 28 УК РФ, значительно ниже по сравнению с показателями ст. 272 и 273 УК РФ.

В 2021 г. было зарегистрировано лишь 1 преступление, предусмотренное ст. 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей) УК РФ, лица не выявлялись и не осуждались в период 2019–2021 гг.

Не случайно редакция данной статьи активно дискутируется. Проблемы правоприменительной практики зачастую связывают с тем, что диспозиция ст. 274 УК РФ является бланкетной [9, с. 393, 394].

Диспозиция ст. 274.1 (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации) УК РФ также подвергалась справедливой критики. Так, Л. Л. Кругликов, О. Г. Соловьев, С. Д. Бражник указывают на дискуссионные аспекты квалификации деяния, связанные, прежде всего, с недостатками законодательного формулирования объектов критической информационной инфраструктуры. Анализ показателей судебной статистики за период 2018 г. позволил авторам характеризовать данную норму в качестве «мертвой» [10, с. 49–52].

[1] Приговор Якутского городского суда Республики Саха (Якутия) от 26.08.2019 по делу № 1-681/2019 // Архив Якутского городского суда Республики Саха (Якутия) от 2019 г.

[2] Приговор Петушинского районного суда Владимирской области от 02.08.2020 по делу № 1-85/2020 // Архив Петушинского районного суда Владимирской области от 2020 г.

[3] Приговор Ленинского районного суда г. Кирова от 10.11.2021 по делу № 1-867/2021 // Архив Ленинского районного суда г. Кирова от 2021 г.

В настоящее время данные критерии во многом сохраняет свою актуальность. Правоприменительная практика по данной статье складывается при отсутствии четкого законодательного регулирования. В 2021 г. зарегистрировано 159 преступлений, предусмотренных ст. 274.1 УК РФ, осуждено 15 лиц (2019 г. — 4, 2020 г. — 8).

В качестве иллюстрации можно привести факт привлечения к уголовной ответственности по ст. 274.1 УК РФ А., который был оправдан. А. было предъявлено обвинение в совершении преступлений, предусмотренных ч. 1 ст. 273 УК РФ и ч. 4 ст. 274.1 УК РФ. А., являясь сотрудником государственного предприятия, созданного в целях обеспечения производства вооружения, активировал на служебном компьютере вредоносную программу для взлома операционной системы компании «Microsoft». После активации вредоносной программы с компьютера неконтролируемо были отправлены малые объемы данных в центр удаленного управления в иностранном сегменте сети Интернет. При этом ранее американские производители отказывались от сделок по продаже предприятию программного обеспечения, вынуждая данное предприятие использовать нелицензионное программное обеспечение[1]. По ч. 4 ст. 274.1 УК РФ А. был оправдан. Мотивируя свое решение, суд среди прочего указал на недоказанность факта передачи какой-либо информации из объектов критической информационной инфраструктуры иностранным спецслужбам.

Последняя на сегодняшний день ст. 274.2 УК РФ, включенная в гл. 28 УК РФ, была введена в июле 2022 г. Федеральным законом от 14.07.2022 № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации». Новая статья предусматривает ответственность за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования. Субъект преступления специальный — должностное лицо или индивидуальный предприниматель после его привлечения к административной ответственности по ч. 2 ст. 13.42 КоАП РФ или ч. 2 ст. 13.42.1 КоАП РФ.

Принятие подобных изменений говорит о том, что законодателем осознается, что в условиях нарастания угроз информационной безопасности нормы, закрепленные в гл. 28 УК РФ, нацелены на обеспечение уголовно-правовой охрану информационной среды, средств коммуникации и связи.

Заключение

Подытоживая изложенное следует отметить, что нормы об ответственности за преступления в сфере компьютерной информации, осуществляя двойную превенцию, направлены не только на защиту компьютерной информации, но также на защиту собственности, интеллектуальной собственности, личных прав граждан, а также общественной безопасности.

Причем превентивный потенциал уголовно-правовых норм об ответственности за совершение неправомерного доступа к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) в больше степени нацелен на предупреждение хищений, нарушений тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, нарушений авторских и смежных прав, иных правонарушений, в том числе непреступного характера. В свою очередь нормы об ответственности за иные преступления в сфере компьютерной информации (ст. 274, 274.1 и 274.2 УК РФ), прежде всего, связаны с предупреждением преступлений против общественной безопасности.

[1] Приговор Кировского районного суда г. Перми от 07.07.2021 по делу № 1-181/2021 // Архив Кировского районного суда г. Перми за 2021 г.

Список источников

1. Мелешко Д., Чернявский Д., Шарафетдинова Г. «Инструментальный» характер компьютерных преступлений и его влияние на квалификацию // Законность. 2020. № 3. С. 55–57.

2. Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации : дис. … канд. юрид. наук: 12.00.08. Москва, 2018. 211 с.

3. Ображиев К. В. Уголовно-правовые нормы с двойной превенцией // Проблемы укрепления законности и правопорядка: наука, практика, тенденции. 2010. № 3. С. 167–171.

4. Афанасьева О. Р. Нормы двойной превенции: понятие, сущность и значение // Двойная превенция в борьбе с преступностью: вопросы теории и практики : сб. материалов круглого стола (Москва, 25 апреля 2018 г.). Москва, 2018. С. 10–16.

5. Пикуров Н. И. Превентивная функция административной преюдиции в уголовном праве // Двойная превенция в борьбе с преступностью: вопросы теории и практики : сб. материалов круглого стола (Москва, 25 апреля 2018 г.). Москва, 2018. С. 97–104.

6. Криминология : учебник / под ред. проф. Н. Ф. Кузнецовой, проф. В. В. Лунеева. 2-е изд., перераб. и доп. Москва : Волтере Клувер, 2004. 640 с.

7. Поляков С. В., Зараева Ю. В. Неправомерный доступ к компьютерной информации как фактор использования киберпространства террористами и экстремистами // Ученые записки. 2019. №. 3. С. 134–137.

8. Русскевич Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. 2021. № 3. С. 106–125.

9. Степанов-Егиянц В. Г. Совершение кражи и мошенничества с использованием компьютера или информационно-телекоммуникационных сетей // Риск: ресурсы, информация, снабжение, конкуренция. 2012. № 4. С. 393–396.

10. Кругликов Л. Л., Соловьев О. Г., Бражник С. Д. Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в системе экономической и информационной безопасности государства // Вестник ЯрГУ. Серия: Гуманитарные науки. 2019. № 4. С. 49–52.

КОНФЛИКТ ИНТЕРЕСОВ
Конфликт интересов отсутствует.

CONFLICT OF INTEREST
There is no conflict of interest.

Дата поступления статьи / Received: 14.09.2022.
Дата рецензирования статьи / Revised: 19.09.2022.
Дата принятия статьи к публикации / Accepted: 30.09.2022.