ISSN 2500-4255

УДК 343.34
DOI 10.17150/2500-4255.2021.15(2).229-237

ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ УГОЛОВНО-ПРАВОВЫХ МЕР ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В.И. Гладких[1], И.Н. Мосечкин[2]
[1] Всероссийский научно-исследовательский институт МВД России, г. Москва, Российская Федерация
[2] Вятский государственный университет, г. Киров, Российская Федерация

Информация о статье

Дата поступления
7 декабря 2019 г.

Дата принятия в печать
5 апреля 2021 г.

Дата онлайн-размещения
30 апреля 2021 г.

Ключевые слова
Компьютерная информация; вирус; вредоносная программа; неправомерный доступ; приобретение; создание; распространение; цель

Аннотация. Статья посвящена проблемам совершенствования уголовно-правовых норм, регулирующих ответственность за совершение преступлений в сфере компьютерной информации. В качестве цели исследования выступала разработка рекомендаций по совершенствованию положений УК РФ, устанавливающих ответственность за неправомерный доступ к компьютерной информации, а также за создание, использование и распространение вредоносных компьютерных программ. Методологической основой исследования послужил диалектический метод, а получение и обработка научно значимых результатов осуществлялись с помощью формально-юридического, сравнительно-правового методов, а также методов количественного и качественного анализа. Материалом для исследования выступили нормативно-правовые акты, регулирующие ответственность за совершение преступлений в сфере компьютерной информации, а также данные судебной практики. Изучение судебных приговоров позволило установить, что достаточно часто преступления в сфере компьютерной информации являются лишь начальным звеном цепи противоправной деятельности. В дальнейшем результаты таких преступлений используются в целях совершения иных деликтов. При этом составы преступлений, предусмотренных ст. 272–274.1 УК РФ, не включают в качестве конструктивного или квалифицирующего признака цель скрыть другое преступление или облегчить его совершение. Авторами предлагается закрепить такую цель в качестве признака, усиливающего ответственность, в ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ. Кроме того, было обнаружено, что вредоносная программа зачастую не только создается, но и приобретается для дальнейшего использования. В связи с тем что приобретение таких программ характеризуется общественной опасностью, предлагается криминализировать данное действие посредством внесения изменений в ст. 273 УК РФ. Наконец, авторами доказывается необходимость конкретизации диспозиции ч. 1 ст. 273 УК РФ для разграничения преступной и непреступной деятельности. Буквальное толкование ст. 273 УК РФ не позволяет исключить привлечение к уголовной ответственности в случае создания и использования вредоносных программ в научных, учебных и экспертных целях. Авторы пришли к выводу о необходимости включения в диспозицию ст. 273 УК РФ указания на противоправность действий.

PROBLEMS OF IMPROVING CRIMINAL LAW MEASURES OF COUNTERACTING CRIMES IN THE SPHERE OF COMPUTER INFORMATION

Viktor I. Gladkikh[1], Ilya N. Mosechkin[2]
[1] All-Russian Research Institute of the Ministry of Internal Affairs of Russia, Moscow, the Russian Federation
[2] Vyatka State University, Kirov, the Russian Federation

Article info

Received
2019 December 7

Accepted
2021 April 5

Available online
2021 April 30

Abstract. The paper discusses the improvement of criminal law norms regulating liability for cybercrimes. The goal of the conducted research was to develop recommendations for improving clauses of the Criminal Code of the Russian Federation that determine liability for unauthorized access to digital information as well as for developing, using and distributing computer malware. The methodological basis of this research was the dialectic method, while the results were obtained and processed using the formal-legal and the comparative-legal methods as well as the methods of quantitative and qualitative analysis. The examined materials included normative

© Гладких В.И., Мосечкин И.Н., 2021

ISSN 2500-4255

Keywords
Computer information; virus; malware; unauthorized access; acquiring; creation; distribution; aim

legal acts regulating liability for cybercrimes, and data from court practice. The examination of court sentences allowed the authors to state that cybercrimes are often just a first link in a chain of illegal activities. The results of such crimes are used to commit further delicts. The formal components of crimes under Art. 272–274.1 of the Criminal Code of the Russian Federation do not include, either as a constructive or a qualifying feature, the goal of hiding another crime or facilitating it. The authors suggest including this goal, as a feature that aggravates liability, into Part 2, Art. 272 and Part 2, Art. 273 of the Criminal Code of the Russian Federation. Besides, the authors found out that malware is often not only developed, but also purchased for further use. As the purchase of such software is connected with public danger, it is suggested that this action should be criminalized through amendments in Art. 273 of the Criminal Code of the Russian Federation. Finally, the authors prove that it is necessary to specify the wording of Part 1, Art. 273 of the Criminal Code of the Russian Federation to delineate criminal and non-criminal activities. Literal interpretation of Art. 273 of the Criminal Code of the Russian Federation does not preclude criminal prosecution in cases when malware is developed for research, educational and expert purposes. The authors conclude that it is necessary to add an indication of the illegal character of actions to the wording of Art. 273 of the Criminal Code of the Russian Federation.

Жизнь современного человека тесно связана с компьютерными технологиями. Их использование существенно повышает эффективность деятельности в самых разных сферах: здравоохранении, образовании, экономике и иных. Однако согласимся с мнением зарубежных исследователей о том, что возрастающее удобство создания, размещения и обработки информации хотя и имеет множество преимуществ, в то же время несет риски и угрозы, которые ранее обществу известны не были [1, p. 185].

Как отмечается в литературе, из-за действий киберпреступников крупные организации терпят убытки в среднем на сумму 20 млн р., а предприятия среднего и малого бизнеса — 780 тыс. р. [2, с. 62]. В расчет суммы ущерба входят вынужденный простой, упущенная прибыль и расходы на дополнительные услуги специалистов. Дополнительные траты влечет ликвидация последствий и профилактика будущих атак. В банковской сфере ежегодный объем хищений с использованием компьютерных технологий достигает 2 млрд р., хотя ученые такие показатели называют весьма заниженными [3, с. 36].

Значительные убытки от компьютерных преступлений наблюдаются по всему миру. В США киберпреступность ежегодно наносит ущерб гражданам и организациям на сумму, превышающую 100 млрд долл. При этом число успешных атак растет, несмотря на противодействие им [4, p. 2]. В Великобритании с 2012 по 2018 г. размер ущерба от компьютерной преступности увеличился более чем в 2 раза. Отдельные преступления (преимущественно разновидности мошенничеств и использование вредоносных программ) причинили убытки на суммы, превышающие 1 млрд фунтов стерлингов [5]. Здесь все же необходимо отметить, что зарубежное законодательство предусматривает составы преступлений, отличающиеся от отечественных (включая множество видов мошенничества, фишинга, вымогательства и др. [6]), поэтому простое соотнесение ущерба, наносимого компьютерными преступлениями в разных странах, было бы неправильным.

Таким образом, вред, причиняемый компьютерной преступностью, является крайне существенным, даже если не брать в расчет политический, культурный, научный и иные аспекты. Экономический ущерб в совокупности с растущим числом преступлений, предусмотренных гл. 28 УК РФ, лишь подчеркивает актуальность проблемы. Кроме того, появляются и новые разновидности преступлений, связанные, например, с использованием криптовалюты или систем искусственного интеллекта.

Противодействие компьютерной преступности всегда носит комплексный характер, включая организационные, технические, политические и иные меры. Однако такие меры не могут быть эффективными без должного правового регулирования, в том числе со стороны уголовного права. В связи с этим в настоящем исследовании хотелось бы обратить внимание на несколько проблем уголовной ответственности за совершение компьютерных преступлений.

В действующем уголовном законе непосредственно таким деяниям посвящена гл. 28 УК РФ, которая включает четыре статьи. Предусматривается ответственность за неправомерный доступ к компьютерной информации; создание, использование и распространение вредонос-

ных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Согласно статистическим сведениям ФКУ «ГИАЦ МВД России», число зарегистрированных преступлений, предусмотренных ст. 272 УК РФ, в 2018 г. составило 1 761, в 2019 г. — 2 420, а в 2020 г. — 4 105. Как видно из показателей, пандемия COVID-19 и связанные с ней ограничительные мероприятия существенным образом повлияли на компьютерную преступность.

Количество зарегистрированных случаев создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ) в 2018 г. составило 733, в 2019 г. — 455, в 2020 г. — 371. В значительно меньшем объеме фиксируется число преступлений, предусмотренных ст. 274 УК РФ. В 2018 г. их было зарегистрировано 5, а в 2019 г. — 8.

Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) была установлена лишь в середине 2017 г. Но с этого момента норма уже нашла отражение в практической деятельности. В 2018 г. было зарегистрировано одно преступление, в дальнейшем сформировалась тенденция к росту числа таких деяний.

Статистические сведения в целом демонстрируют востребованность норм, предусмотренных гл. 28 УК РФ, хотя необходимо понимать влияние высокой латентности компьютерной преступности на эти показатели. В то же время, на наш взгляд, существуют некоторые недостатки уголовно-правового регулирования рассматриваемых преступлений. Их устранение позволит сделать привлечение к ответственности более эффективным, а также охватить деяния, не подпадающие под признаки преступлений, предусмотренных ст. 272–274.1, но являющиеся общественно опасными.

Необходимо отметить, что уголовный закон предусматривает деяния, которые связаны с компьютерными технологиями, но посягают на другие охраняемые объекты. К ним можно отнести, например, мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ) и иные. Хотя в зарубежной литературе подобные деяния включаются в понятие киберпреступности [7, p. 15], настоящее исследование сосредоточено на преступлениях в сфере компьютерной информации, включенных в гл. 28 УК РФ.

Авторами был проведен количественный и качественный анализ 90 судебных приговоров по уголовным делам, связанным со ст. 272–274.1 УК РФ[1]. Анализ показал, что во многих случаях имеет место совокупность преступлений. По итогам анализа из исследовательской базы была исключена такая совокупность, при которой деяния совершались в разное время и не были связаны между собой.

Изучению в первую очередь подлежали случаи, когда киберпреступление совершалось с целью облегчения совершения другого преступления или его сокрытия. Число приговоров по таким случаям составило 27 из 90 проанализированных приговоров. То есть почти треть киберпреступлений (30 %) направлена на совершение иных противоправных деяний.

Как правило, «первоначальными» выступали преступления, предусмотренные ст. 272 или 273 УК РФ. Они создавали условия для дальнейших нарушений авторских и смежных прав (ст. 146 УК РФ), незаконных получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), совершения краж в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), мошенничеств в сфере компьютерной информации (ст. 159.6 УК РФ) и иных противоправных деяний.

Так, Р. А. Г., обладая знаниями и навыками в области программирования и использования программного обеспечения, обнаружил в ресурсах сети Интернет поэтапную инструкцию, позволяющую осуществить создание вредоносного программного обеспечения, имитирующего сайт одного из платежных сервисов, после чего у него возник корыстный умысел, направленный на хищение денежных средств граждан. Р. А. Г. совершил разработку вредоносного про-

[1] Материалом для исследования явились 90 судебных приговоров, которыми отдельные лица были признаны виновными в совершении преступления, предусмотренного хотя бы одной из статей: 272, 273, 274 или 274.1 УК РФ. Для объективного исследования в эмпирическую базу были включены приговоры из различных субъектов Российской Федерации: гг. Москвы и Санкт-Петербурга, Кировской, Ульяновской, Свердловской, Нижегородской, Иркутской областей и других субъектов Российской Федерации.

граммного обеспечения, имитирующего сайт платежного сервиса, а затем разместил его в сети Интернет. В дальнейшем Р. А. Г., являясь администратором данной программы, осуществлял несанкционированное копирование компьютерной информации в виде персональных данных пользователей, позволяющих получать доступ к денежным средствам, находящимся на счетах интернет-кошельков пользователей, и возможность распоряжения ими, а также применял их в последующем в корыстных целях при совершении преступления — хищения денежных средств граждан из числа пользователей платежного сервиса[2].

В ходе изучения материалов судебной практики был выявлен наглядный пример, когда совершенное в сфере компьютерной информации преступление являлось предикатным по отношению к целой серии иных противоправных деяний. В частности, М. Я. В., обладая навыками работы со специальной банковской компьютерной программой, в целях обогащения и извлечения материальной выгоды осуществил с мобильного телефона звонок кредитному специалисту банка и представился руководителем регионального управления. Кредитный специалист сообщила М. Я. В. логин и пароль для доступа к банковской компьютерной программе, являющейся системой управления взаимоотношениями с клиентами, в которой содержалась информация о личных данных клиентов (физических лиц), их вкладах и счетах, операциях, ранее выданных потребительских кредитах, данные о банковских картах. Собрав необходимые для совершения преступления сведения, М. Я. В. осуществлял звонки клиентам банка, представлялся оператором службы поддержки, с помощью обмана выяснял защитный код безопасности для платежной системы, расположенный на оборотной стороне карты. Получив данную информацию, М. Я. В. оформлял покупки и пополнял электронные кошельки денежными средствами, которые принадлежали потерпевшим, чем причинял им материальный ущерб. М. Я. В. был признан виновным в совершении более чем 20 дистанционных краж (ст. 158 УК РФ), 7 фактов незаконных получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УКРФ), и 6 фактов осуществления неправомерного доступа к компьютерной информации (ст. 272 УК РФ)[3].

Анализ приговоров показал, что наиболее часто преступления в сфере компьютерной информации являются предикатными по отношению к нарушению авторских и смежных прав (ст. 146 УК РФ). Доля таких деяний среди всех исследованных материалов составила 8,9 % (8 случаев из 90). Кроме того, полученная информация используется в дальнейшем для совершения краж электронных денежных средств — 6,7 % (6 случаев из 90), а также мошенничеств в сфере компьютерной информации (4,4 %) и мошенничеств с использованием электронных средств платежа (4,4 %). Несмотря на то что преступление, предусмотренное ст. 183 УК РФ, не является широко распространенным, в контексте настоящего исследования оно встречается так же часто, как и мошенничество (4,4 %). Как показало содержание проанализированных приговоров, наиболее редко преступления в сфере компьютерной информации используются для дальнейшего нарушения неприкосновенности частной жизни (ст. 137 УК РФ). Нами был выявлен всего один подобный случай.

Изложенное показывает, что преступления в сфере компьютерной информации довольно часто выступают способом совершения иных преступлений, перечень которых достаточно разнообразен. Следовательно, необходимо адекватное отражение данной особенности в уголовном законе.

В настоящее время составы преступления, предусмотренные ст. 272–274.1 УК РФ, не включают в качестве конструктивного или квалифицирующего признака цель скрыть другое преступление или облегчить его совершение. Полагаем возможным согласиться с мнением о том, что отсутствие в уголовном законе прямого указания на обязательность анализа мотивов и целей совершения компьютерных преступлений является пробелом в законодательстве [8, с. 155]. Если первые случаи неправомерного доступа к компьютерной информации и создания вредоносных программ осуществлялись из хулиганских побуждений, то в настоящее время они направлены на достижение конкретных целей, и это необходимо учитывать при диффе-

[2] Приговор от 9 ноября 2018 г. по делу № 1-588/2018 по обвинению Р. А. Г. в совершении преступлений, предусмотренных пунктом «в» части 3 статьи 158, частью 2 статьи 273 УК РФ // СПС «КонсультантПлюс».

[3] Приговор от 13 декабря 2019 г. по делу № 1-268/2019 по обвинению М. Я. В и Г. В. Р. в совершении преступлений, предусмотренных частью 2 статьи 272, частью 3 статьи 183 УК РФ и пунктом «г» части 3 статьи 158 УК РФ // СПС «КонсультантПлюс».

ренциации уголовной ответственности. Достаточно обратить внимание на сферу электронной коммерции, с развитием которой неизбежно возрастают риски компьютерных атак, направленных на клиентов [9, с. 96].

Цель скрыть другое преступление или облегчить его совершение давно известна уголовному праву. Это явление выступает в качестве обстоятельства, отягчающего наказание (п. «е.1» ч. 1 ст. 63 УК РФ). Но в ряде случаев законодатель обоснованно посчитал необходимым закрепить такой признак в качестве квалифицирующего, например, при совершении убийства (п. «к» ч. 2 ст. 105 УК РФ) или подделки документов, государственных наград, штампов, печатей или бланков (ч. 4 ст. 327 УК РФ). Закрепление указанной цели в киберпреступлениях также представляется оправданным.

В законодательстве отдельных стран конструкция диспозиции составов компьютерных преступлений предусматривает цели, связанные с совершением иных противоправных деяний. Например, Уголовный кодекс Австралии 2002 г. запрещает как простой незаконный доступ к компьютерному устройству, так и незаконный доступ с целью дальнейшего совершения преступления (ст. 415). Отдельным деликтом признается получение электронной информации с целью совершения преступления (ст. 418). Как отмечается в зарубежной литературе, доступ в основном предоставляется злоумышленникам вследствие использования инструментов социальной инженерии. И чаще всего после получения доступа следует совершение мошенничества [10, p. 221].

В Великобритании уголовная ответственность за киберпреступления регулируется, помимо прочего, Законом о неправомерном использовании компьютеров 1990 г. (Computer Misuse Act 1990). Закон прямо запрещает несанкционированный доступ с целью совершения или облегчения совершения дальнейших правонарушений, что наказывается строже, нежели простой нелегальный доступ. Учеными подчеркивается, что такой подход позволяет дифференцировать случаи компьютерного хулиганства и более тяжкие преступления [11, p. 53].

Положения ст. 230 Уголовного кодекса Чешской Республики предусматривают ответственность за незаконный доступ к компьютерной системе или иному носителю информации. Более строго (лишением свободы на срок до четырех лет) наказывается аналогичное деяние, совершенное с целью нанесения другого вреда [12, p. 2]. Думается, это можно истолковать как аналог цели совершения другого преступления.

Как отмечается в компаративистских исследованиях, подход к криминализации деяний, посягающих на информационную безопасность, в законодательстве зарубежных стран нельзя признать идентичным, он различен и в определении объекта преступления, и в установлении видов деяний, и в закреплении способов совершения таких посягательств [13, с. 112–113]. Разумеется, закрепление целей, связанных с иными преступлениями, также не является единообразным для государств. Во многих странах такой подход отсутствует. Тем не менее успешное применение в рассмотренных странах такого признака на практике может свидетельствовать о потенциальной эффективности в случае заимствования его в отечественное законодательство.

Следует отметить, что указанный подход носит дискуссионный характер, поскольку учитывает и предикатное, и последующее деяние, что в теории уголовного права может оцениваться как повторность уголовной ответственности. Однако цели, связанные с совершением иных преступлений, уже длительное время закреплены в качестве признаков отдельных составов преступлений, проверены практикой и положительно оцениваются рядом ученых. Например, К.Н. Евдокимов [14] и В.Г. Степанов-Егиянц [15] в научных трудах высказывались в пользу установления цели, связанной с совершением иных преступлений, в качестве квалифицирующего признака деяний, посягающих на безопасность компьютерной информации. Авторами была убедительно доказана необходимость таких изменений.

Таким образом, обзор зарубежного законодательства, научных трудов отечественных и зарубежных авторов, а также анализ судебных решений позволили разработать аргументированную рекомендацию по совершенствованию уголовного законодательства путем закрепления цели скрыть другое преступление или облегчить его совершение в качестве квалифицирующего признака в составах преступления, предусмотренных ст. 272 и 273 УК РФ.

Исследование судебно-следственной практики дало возможность выявить еще одну проблему уголовно-правового регулирования противодействия компьютерным преступлениям. В настоящее время диспозиция ст. 273 УК РФ

предусматривает такие виды деяний, как создание, распространение или использование вредоносных программ. Поскольку основной состав данного преступления по конструкции объективной стороны является формальным, момент его окончания связывается с совершением вышеуказанных действий.

Существует множество авторских определений создания вредоносной программы. Например, под данным действием понимается комплекс операций, состоящий из подготовки исходных данных, предназначенных для управления конкретными компонентами системы обработки данных в целях уничтожения, блокирования, модификации или копирования информации [16, с. 1318]. Встречаются иные определения, в том числе довольно дискуссионного характера. Однако все формулировки сводятся к тому, что описываются деяния, направленные на возникновение вредоносной программы, которая ранее не существовала или не обладала вредоносными функциями. По мнению законодателя, сам факт создания программы уже является общественно опасным поведением, хотя ее использование или распространение могло не осуществляться.

В то же время владение лицом вредоносным программным обеспечением может быть осуществлено не только посредством его создания, но и с использованием других способов, не отраженных в уголовном законодательстве. Так, в частности, возможны покупка, обмен, получение в дар, скачивание и другие варианты.

Например, приговором Советского районного суда г. Самары С. Д. Ю. был признан виновным в совершении преступлений, предусмотренных ч. 2 ст. 273 УК РФ и ч. 2 ст. 272 УК РФ. Он, обладая специальными познаниями в области компьютерной техники и программного обеспечения, решил воспользоваться специальными программами для того, чтобы с их с помощью вносить изменения в системное программное обеспечение игровых устройств по просьбе третьих лиц за плату. Затем С. Д. Ю. в сети Интернет разместил объявление об осуществлении им за вознаграждение «прошивки» и «чиповки» игровых приставок с указанием номера контактного телефона. После этого он приобрел специализированное программное обеспечение, которое, согласно заключению эксперта, было предназначено для несанкционированного блокирования, модификации компьютерной информации и нейтрализации средств защиты компьютерной информации[4].

В зарубежной литературе обращается внимание на то, что вредоносное программное обеспечение или инструкции по его созданию легко загружаются из Интернета. Точно так же существует масса возможностей приобрести вредоносную программу онлайн [17, p. 145].

Таким образом, отдельные лица совершают приобретение вредоносных программ, которое само по себе не является преступным деянием. В связи с этим не в полной мере понятно, почему создание вредоносных программ влечет наступление уголовной ответственности, а их приобретение — нет. Итоговым результатом обоих действий выступает наличие у лица определенной компьютерной программы.

Разница заключается в следующем. Во-первых, при создании вредоносной программы задействуются навыки программирования. Но лицо, приобретающее подобную программу, тоже может обладать такими навыками, как было отражено в вышеуказанном примере из судебной практики.

Во-вторых, создание означает возникновение, как правило, новой программы, которую средства защиты компьютерной информации могут не распознать. Но в случае создания по существующей инструкции это приведет к возникновению еще одной версии программы, а не ее нового вида. И такое деяние вновь будет являться наказуемым.

Исходя из изложенного, думается, что приобретение вредоносной программы представляет собой не менее общественно опасное деяние, чем ее создание. Кроме того, это одинаково может привести к дальнейшему ее распространению или использованию. Следовательно, полагаем оправданной и целесообразной криминализацию приобретения вредоносной компьютерной программы. В дополнение отметим, что такое направление совершенствования законодательства находит поддержку в научной среде [18, с. 75; 19, с. 98].

Вместе с тем как создание, так и приобретение вирусов может осуществляться в научных, учебных, экспертных и иных некриминальных целях. Буквальное толкование ст. 273 УК РФ (а тем более с учетом возможной криминализа-

[4] Приговор от 30 января 2017 г. по делу № 1-32/2017 по обвинению С. Д. Ю. в совершении преступлений, предусмотренных частью 2 статьи 273 УК РФ, частью 2 статьи 272 УК РФ // СПС «КонсультантПлюс».

ции приобретения) не исключает уголовной ответственности в таких случаях, хотя общественная опасность отсутствует. То есть запрещено любое умышленное создание, использование и распространение вредоносных программ. Положения о малозначительности деяния (ч. 2 ст. 14 УК РФ) также не всегда применимы, поскольку не имеют четко выраженных критериев и используются на практике чрезвычайно редко. В европейском законодательстве, к слову, такая проблема тоже имеет место. Исследователи отмечают необходимость какой-либо правовой защиты в случае хакерства в общественно полезных целях [20].

С другой стороны, отечественному уголовному праву уже известны способы регулирования оборота запрещенных предметов. Так, в частности, ст. 228 и 228.1 УК РФ, запрещая оборот наркотических средств, указывают на незаконный характер таких действий. Это необходимо, поскольку существует легальный оборот.

Возвращаясь к вопросу уголовно-правового регулирования преступлений в сфере компьютерной информации, считаем целесообразным включить в диспозицию ст. 273 УК РФ указание на противоправность действий с помощью прилагательного «незаконные».

Проведенное исследование позволило вывести ряд закономерностей в совершении преступлений в сфере компьютерной информации, а также дополнительно обосновать их специфические особенности, установленные другими учеными.

Не возникает сомнений, что цель скрыть другое преступление или облегчить его совершение повышает общественную опасность преступлений в сфере компьютерной информации, как и лиц, их совершающих. Изучение актуальной судебной практики показало, что такая цель имеет место достаточно часто. В науке уголовного права уже предлагались рекомендации по совершенствованию ст. 272 УК РФ с дополнением ее признаком, учитывающим цель скрыть другое преступление или облегчить его совершение [15]. Проведенное нами исследование, основанное на новой эмпирической базе, подтверждает необходимость таких изменений. Более того, для обеспечения системности совершенствования уголовного закона таким изменениям должна подвергнуться и ст. 273 УК РФ.

Приобретение вредоносных программ не менее общественно опасное деяние, чем их создание. В правоприменительной деятельности такие случаи имеют место и не являются редкостью. В связи с этим представляется необходимой криминализация приобретения вредоносных программ в качестве еще одного из альтернативных действий, образующих состав преступления, предусмотренного ст. 273 УК РФ.

Приобретение, создание и использование вредоносных программ могут осуществляться не в криминальных целях. Однако уголовный закон не содержит исключений, поэтому такая деятельность может повлечь наступление уголовной ответственности. Думается, что прямое указание на незаконный характер действий, предусмотренных ст. 272 и 273 УК РФ, позволит отграничить общественно опасное поведение от иного, не нуждающегося в применении уголовно-правовых мер.

Таким образом, действующие положения уголовного закона о преступлениях в сфере компьютерной информации нуждаются в изменениях. Относительно совершенствования ст. 272 УК РФ согласимся с редакцией ч. 2 ст. 272 УК РФ, разработанной В.Г. Степановым-Егиянцем [15, с. 16]. Развивая и дополняя идеи, высказанные ученым, считаем возможным предложить вариант ч. 1 и 2 ст. 273 УК РФ с учетом разработанных нами изменений:

«1. Незаконные приобретение, создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, — …»

В свою очередь, квалифицированный состав, предусмотренный ч. 2 ст. 273 УК РФ, примет следующий вид:

«2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности либо совершенные с целью скрыть другое преступление или облегчить его совершение, — …»

Изложенные рекомендации призваны обратить внимание на проблемы регулирования киберпреступлений со стороны законодателя и представителей науки уголовного права. Несомненно, совместными усилиями будут найдены правильные решения вопросов совершенствования уголовного закона.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Li X. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime / X. Li // International Journal of Cyber Criminology. — 2015. — Vol. 9, iss. 2. — P. 185–204.

2. Евдокимов К.Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями / К.Н. Евдокимов // Вестник Казанского юридического института МВД России. — 2016. — № 2 (24). — С. 62–66.

3. Литвинов Д.А. Киберпреступность в банковской сфере России: характер, масштабы, последствия / Д.А. Литвинов // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. — 2017. — № 1. — С. 35–42.

4. Gupta P. Cybercrime: in Disguise Crimes / P. Gupta, R.A. Mata-Toledo // Journal of Information Systems & Operations Management. — 2016. — Vol. 10, iss. 1. — P. 1–10.

5. Measuring the changing cost of cybercrime / R. Anderson, C. Barton, R. Bölme [et al.] // The 18th Annual Workshop on the Economics of Information Security (WEIS 2019). — Boston, 2019. — URL: https://www.repository.cam.ac.uk/handle/1810/294492.

6. Gordon S. On the definition and classification of cybercrime / S. Gordon, R. Ford // Journal in Computer Virology. — 2006. — Vol. 2, iss. 1. — P. 13–20.

7. Fortes B.V. An analysis of cybercrimes from a global perspective on penal law / B.V. Fortes, S.O. Boff // Revista Brasileira de Direito, Passo Fundo. — 2017. — Vol. 13, iss. 1. — P. 7–24.

8. Евдокимов К.Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты / К.Н. Евдокимов. — Иркутск : Изд-во ИЮИ (ф) УП РФ, 2016. — 267 с.

9. Девиации в цифровом мире: уголовно-правовое измерение : науч.-практ. пособие. В 2 ч. Ч. 1 / под ред. Ю.В. Грачевой. — Москва : Контракт, 2019. — 160 с.

10. The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice / ed. A. Deckert, R. Sarre. — Cham : Palgrave Macmillan, 2017. — 916 p.

11. Sallavaci O. Combating Cyber Dependent Crimes: The Legal Framework in the UK / O. Sallavaci // Global Security, Safety and Sustainability — The Security Challenges of the Connected World : 11th International Conference, ICGS3 January 18–20, 2017. — London, 2017. — P. 53–56.

12. Gřivna T. Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic / T. Gřivna, J. Drápal // Digital Investigation. — 2019. — Vol. 28. — P. 1–13.

13. Семыкина О.И. Противодействие киберпреступности за рубежом / О.И. Семыкина // Журнал зарубежного законодательства и сравнительного правоведения. — 2016. — № 6 (61). — С. 104–113.

14. Евдокимов К.Н. Субъективная сторона неправомерного доступа к компьютерной информации / К.Н. Евдокимов // Вестник Академии Генеральной прокуратуры Российской Федерации. — 2009. — № 4 (12). — С. 53–58.

15. Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) : дис. ... д-ра юрид. наук : 12.00.08 / В.Г. Степанов-Егиянц. — Москва, 2016. — 389 с.

16. Энгельгардт А.А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) / А.А. Энгельгардт // Lex Russica. — 2014. — Т. 96, № 11. — С. 1316–1325.

17. Li X. Crucial Elements in Law Enforcement against Cybercrime / X. Li // International Journal of Information Security Science. — 2018. — Vol. 7, № 3. — P. 140–158.

18. Гребенкин Ф.Б. Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ / Ф.Б. Гребенкин, Л.А. Коврижных // Вестник гуманитарного образования. — 2017. — № 2. — С. 71–77.

19. Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания : дис. ... канд. юрид. наук : 12.00.08 / В.Ю. Максимов. — Краснодар, 1998. — 169 с.

20. Guinchard A. The Computer Misuse Act 1990 to Support Vulnerability Research? Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime / A. Guinchard // Journal of Information Rights, Policy and Practice. — 2017. — Vol. 2, iss. 1. — URL: https://ssrn.com/abstract=2946763

REFERENCES

1. Li X. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology*, 2015, vol. 9, iss. 2, pp. 185–204.

2. Evdokimov K.N. Actual Issues of Improving Criminal Legal Means of Combating Computer Crime. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia*, 2016, no. 2 (24), pp. 62–66. (In Russian).

3. Litvinov D.A. Cybercrime in the Banking Sector of Russia: the Nature, Extent, Consequences. *Prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologii: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestuplenii = Crime in the Sphere of Information and Telecommunication technologies: Problems of Prevention, Detection and Investigation of Crimes*, 2017, no. 1, pp. 35–42. (In Russian).

4. Gupta P., Mata-Toledo R.A. Cybercrime: in Disguise Crimes. *Journal of Information Systems & Operations Management*, 2016, vol. 10, iss. 1, pp. 1–10.

5. Anderson R., Barton C., Bölme R., Clayton R., Ganan C. Measuring the changing cost of cybercrime. *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)*. Boston, 2019. Available at: https://www.repository.cam.ac.uk/handle/1810/294492.

6. Gordon S., Ford R. On the definition and classification of cybercrime. *Journal in Computer Virology*, 2006, vol. 2, iss. 1, pp. 13–20.

7. Fortes B.V., Boff S.O. An analysis of cybercrimes from a global perspective on penal law. *Revista Brasileira de Direito, Passo Fundo*, 2017, vol. 13, iss. 1, pp. 7–24.

8. Evdokimov K.N. *Countering Computer Crime in the Russian Federation: Criminological and Criminal Law Aspects*. Irkutsk, ILI (b) UP RF Publ., 2016. 267 p.

9. Gracheva Yu.V. (ed.). *Deviatsii v tsifrovom mire: ugolovno-pravovoe izmerenie* [Deviation in the Digital World: a Criminal-law Dimension]. Moscow, Kontrakt Publ., 2019. Pt. 1. 160 p.

10. Deckert A., Sarre R. (eds.). *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*. Cham, Palgrave Macmillan, 2017. 916 p.

11. Sallavaci O. Combating Cyber Dependent Crimes: The Legal Framework in the UK. *Global Security, Safety and Sustainability — The Security Challenges of the Connected World. 11th International Conference, ICGS3 January 18–20, 2017*. London, 2017, pp. 53–56.

12. Gřivna T., Drápal J. Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. *Digital Investigation*, 2019, vol. 28, pp. 1–13.

13. Semykina O.I. Combating Cybercrime in Foreign Countries. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law*, 2016, no. 6 (61), pp. 104–113. (In Russian).

14. Evdokimov K.N. Mental Element of a Crime Regarding an Illegal Access to Data. *Vestnik Akademii General'noi prokuratury Rossiiskoi Federatsii = Bulletin of the Academy of the RF Prosecutor General's Office*, 2009, no. 4 (12), pp. 53–58. (In Russian).

15. Stepanov-Egiyants V.G. *Metodologicheskoe i zakonodatel'noe obespechenie bezopasnosti komp'yuternoi informatsii v Rossiiskoi Federatsii (ugolovno-pravovoi aspekt). Dokt. Diss.* [Methodological and legislative support of digital security in the Russian Federation (a criminal law aspect). Doct. Diss.]. Moscow, 2016. 389 p.

16. Engelgardt A.A. Criminal Legal Evaluation of Creation, Application and Expansion of Harmful Computer Programs (Information). *Lex Russica*, 2014, vol. 96, no. 11, pp. 1316–1325. (In Russian).

17. Li X. Crucial Elements in Law Enforcement against Cybercrime. *International Journal of Information Security Science*, 2018, vol. 7, no. 3, pp. 140–158.

18. Grebenkin F.B., Kovrizhnykh L.A. Some of the Problems of Objective Evidence of a Crime under Article 273 of the Criminal Code of Russian Federation. *Vestnik gumanitarnogo obrazovaniya = Herald of Humanitarian Education*, 2017, no. 2, pp. 71–77. (In Russian).

19. Maksimov V.Yu. *Nezakonnoe obrashchenie s vredonosnymi programmami dlya EVM: problemy kriminalizatsii, differentsiatsii otvetstvennosti i individualizatsii nakazaniya. Kand. Diss.* [[Illegal use of harmful software for computers: problems of criminalization, differentiation of liability and individualization of punishment. Cand. Diss.]. Krasnodar, 1998. 169 p.

20. Guinchard A. The Computer Misuse Act 1990 to Support Vulnerability Research? Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime. *Journal of Information Rights, Policy and Practice*, 2017, vol. 2, iss. 1. Available at: https://ssrn.com/abstract=2946763.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Гладких Виктор Иванович — главный научный сотрудник Всероссийского научно-исследовательского института МВД России, доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: gladkich04@mail.ru.

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

Гладких В.И. Проблемы совершенствования уголовно-правовых мер противодействия преступлениям в сфере компьютерной информации / В.И. Гладких, И.Н. Мосечкин. — DOI 10.17150/2500-4255.2021.15(2).229-237 // Всероссийский криминологический журнал. — 2021. — Т. 15, № 2. — С. 229–237.

INFORMATION ABOUT THE AUTHORS

Gladkikh, Viktor I. — Chief Researcher, All-Russian Research Institute of the Ministry of Internal Affairs of Russia, Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: gladkich04@mail.ru.

Mosechkin, Ilya N. — Ass. Professor, Chair 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

Gladkikh V.I., Mosechkin I.N. Problems of improving criminal law measures of counteracting crimes in the sphere of computer information. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2021, vol. 15, no. 2, pp. 229–237. DOI: 10.17150/2500-4255.2021.15(2).229-237. (In Russian).