УДК 343.3/.7
DOI: https://doi.org/10.17308/law/1995-5502/2024/2/294-300

О СОВРЕМЕННЫХ ТЕНДЕНЦИЯХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В. А. Шестак

Московская академия Следственного комитета Российской Федерации

А. С. Чеботарь

Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации

ABOUT THE CURRENT TRENDS OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AND IN THE FIELD OF COMPUTER INFORMATION IN THE RUSSIAN FEDERATION

V. A. Shestak

Moscow Academy of the Investigative Committee of the Russian Federation

A. S. Chebotar

Moscow State Institute of International Relations (MGIMO)

Аннотация: рассматриваются современные тенденции преступлений, совершенных посредством информационно-телекоммуникационных технологий или в сфере компьютерной информации в Российской Федерации. Актуальность исследования обусловливается колоссальным ростом числа рассматриваемых преступлений, позволяющим говорить о них как о новой угрозе национальной безопасности.

Проведенный авторами анализ позволяет сделать выводы о том, что в современных условиях существует ряд юридических и технических проблем, связанных с недостаточным правовым регулированием противодействия рассматриваемой группе преступлений. Действующее законодательство России, криминализирующее отдельные совершаемые в киберпространстве противоправные деяния, находится лишь на этапе своего формирования и не соответствует современным вызовам и угрозам.

Недостатки в существующем правовом регулировании обусловлены рядом негативных факторов, в частности, недостатками юридической техники и многочисленными нарушениями ее правил; отсутствием понимания, что представляет собой современная киберпреступность, каковы ее основные проявления, цели и задачи; факторы воздействия и мотивы, подталкивающие лиц к совершению противоправных деяний в виртуальном пространстве и др.

Ключевые слова: киберпреступность, уголовно-правовое регулирование, состояние преступности, преступления, совершаемые с использованием ИКТ.

Abstract: the article examines current trends in crimes committed through information and telecommunication technologies or in the field of computer information in the Russian Federation. The relevance of the study is determined by the colossal increase in the number of crimes under consideration, which allows us to talk about them as a new threat to national security.

The analysis carried out by the authors allows us to draw conclusions that in modern conditions there are a number of legal and technical problems associated with insufficient legal regulation of combating the group of crimes under consideration. The current legislation of Russia, which criminalizes certain illegal acts committed in cyberspace, is only at the stage of its formation and does not correspond to modern challenges and threats.
The shortcomings in the existing legal regulation are due to a number of negative factors, in particular, shortcomings of legal technology and numerous violations of its rules; lack of understanding of what modern cybercrime is, what its main manifestations, goals and objectives are; influencing factors and motives pushing individuals to commit illegal acts in the virtual space, etc.
Key words: cybercrime, criminal law regulation, criminal situation, ICT-crime.

Согласно статистическим сведениям ГИАЦ МВД России о состоянии преступности в стране, за период с января по ноябрь 2023 г. зарегистрировано 1804,8 тыс. преступлений, из них 614,8 тыс. были совершены посредством использования информационно-телекоммуникационных технологий или в сфере компьютерной информации, 312,9 тыс. относятся к категориям «тяжкие» и «особо тяжкие» (рис. 1).

За аналогичный отчетный период 2022 г. на территории Российской Федерации было зарегистрировано 1823,3 тыс. преступлений, 470,1 тыс. из которых были совершены посредством использования ИКТ или в сфере компьютерной информации[2]. Следовательно, состояние преступности в России находится на стабильном уровне, однако за прошедший год отмечается тенденция увеличения количества преступлений, совершаемых посредством использования информационно-телекоммуникационных технологий или в сфере компьютерной информации (на 30,8 %) (рис. 2).

Рис. 1. Состояние преступности в России за период с января по ноябрь 2023 г.[1]

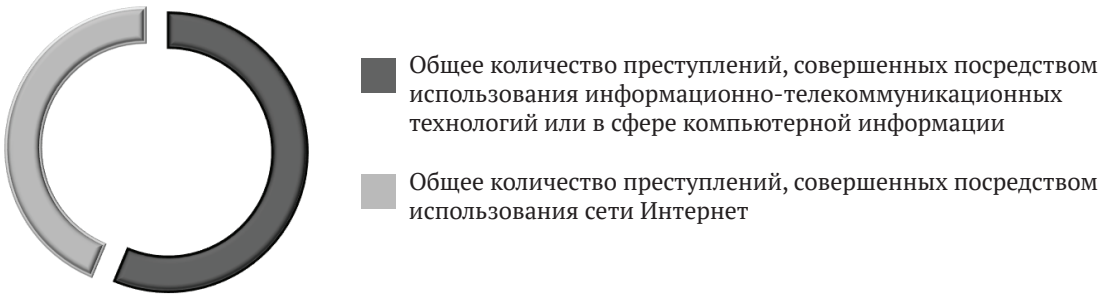

Рис. 2. Общее количество зарегистрированных преступлений, совершенных посредством использования сети Интернет[3]

[1] Состояние преступности в России за январь–ноябрь 2023 г. // ФКУ «Главный информационно-аналитический центр» МВД РФ : официальный сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/45293174/ (дата обращения: 06.01.2024).

[2] См.: Состояние преступности в России за январь–ноябрь 2022 г. // ФКУ «Главный информационно-аналитический центр» МВД РФ : официальный сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/34307225/ (дата обращения: 08.01.2024).

[3] Состояние преступности в России за январь–ноябрь 2023 г. // ФКУ «Главный информационно-аналитический центр» МВД РФ : официальный сайт.

Рис. 3. Количество зарегистрированных преступлений, совершенных посредством использования или применения различных технологий и средств[4]

За исследуемый отчетный период 2023 г. 477,3 тыс. противоправных деяний были совершены киберзлоумышленниками посредством использования сети Интернет, что составляет 77,6 % от общего числа всех преступлений, совершенных посредством использования информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Вместе с тем современные преступления рассматриваемой группы совершаются не только при помощи сети Интернет, но и посредством использования или применения расчетных карт (122 191), компьютерной техники (31 766), программных средств (10 724), фиктивных электронных платежей (1595) и средств мобильной связи (275 382) (рис. 3).

При этом среди них в 2023 г. зарегистрировано на 56,4 % меньше фактов мошенничества с использованием электронных платежных средств (2949), что является свидетельством эффективности мер, предпринимаемых правоприменителями в рамках противодействия таким преступлениям. В качестве негативных тенденций правоохранительными органами Российской Федерации отмечается увеличение числа фактов незаконного производства, сбыта или пересылки наркотических средств посредством сети Интернет, в частности, на 30,7 % (т. е. каждое восьмое преступление). Кроме того, 50,9 % преступлений, совершаемых посредством использования ИКТ или в сфере компьютерной информации, относятся к категориям «тяжкие» и «особо тяжкие»[5].

Полагаем, что увеличение числа преступлений, совершаемых с использованием ИКТ, объясняется не только непосредственной противоправной активностью киберпреступников, но и повышением эффективности работы правоохранительных органов, направленной на практическую реализацию основных мер реагирования на современные преступления, совершаемые посредством использования ИКТ или в сфере компьютерной информации. Так, по данным МВД России, раскрываемость преступлений, совершаемых с использованием ИКТ или в сфере компьютерной информации, составляет 98,8 %[6].

С принятием Уголовного кодекса РФ правоохранительными органами было зафиксировано и увеличение числа противоправных деяний, совершаемых в сфере компьютерной информации. Так, в 1997 г. было зарегистрировано всего 30 противоправных деяний, тогда как в 2017 и 2018 гг. была достигнута отметка в 1883 и 90 тыс. соответственно. Подобный всплеск рассматриваемых преступлений обусловлен в первую очередь созданием и использованием все более изощренных методов совершения преступлений в киберпространстве со стороны злоумышленников, а также обеспечением правоохранительных органов необходимыми навыками и техническими средствами в целях обнаружения и оказания противодействия рассматриваемому негативному явлению[7].

[4] Состояние преступности в России за январь–ноябрь 2023 г. // ФКУ «Главный информационно-аналитический центр» МВД РФ : официальный сайт.

[5] См.: Там же.

[6] См.: Там же.

[7] См.: *Эткина А. Д.* Об определении киберпреступления, компьютерного преступления и преступления в сфере компьютерной информации // Актуальные проб-

Большинство противоправных деяний, совершенных в сфере компьютерной информации в указанный период, квалифицировались по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» и по ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»[8]. При этом общество не признавало опасность, исходящую от киберпространства, ввиду низкого уровня интернетизации населения, отсутствия эффективного правового регулирования и должного противодействия со стороны правоохранительных органов. Хакеры и иные злоумышленники считались гениями, а их противоправная деятельность не признавалась таковой, поскольку резкий рост насильственных преступлений в стране в большей степени доставлял неудобства местному населению, а все силы правоохранительных органов были брошены на борьбу с организованной преступностью[9].

Подобная негативная тенденция изменилась лишь к 2008 г. с учреждением *Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)* во исполнение Указа Президента Российской Федерации от 3 декабря 2008 г. № 1715.[10] Этот федеральный орган исполнительной власти осуществляет контроль и надзор за соблюдением законодательства в области связи, информационных технологий и массовых коммуникаций, регистрации и контроля за деятельностью СМИ, ведения реестров сайтов с незаконным контентом и ограничения доступа к ней, участия в разработке государственной политики в области информационных технологий, проведения проверок и т. д.[11]

Кроме того, в целях недопущения незаконного распространения информации и ограничения доступа к противоправному контенту был разработан и размещен в открытом доступе *Единый реестр доменных имен, индексов страниц сайтов в Интернете и сетевых адресов*[12]. На основании соответствующего решения суда в данный реестр вносятся веб-адреса сайтов, содержащих информацию, распространение которой запрещено на территории Российской Федерации, что позволяет осуществлять фильтрацию вредоносной информации.

В соответствии со ст. 18 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» на оператора при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, возложена обязанность по обеспечению записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных действующим законодательством[13]. Важность нормативного закрепления приведенного выше положения была обусловлена необходимостью преодоления юрисдикционных вопросов, возникающих относительно цифровых данных, принадлежащих гражданам РФ[14].

В 2017 г. в Уголовный кодекс РФ были внесены изменения: имплементирована норма, предусматривающая уголовную ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на

лемы теории и практики применения уголовного закона. 2022. С. 208.

[8] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 18.02.2020). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 08.01.2024).

[9] Среднегодовой рост числа убийств составлял 20 %, а реальную угрозу представляла организованная преступность – более 150 преступных объединений контролировали до 40 тыс. государственных предприятий.

[10] См.: О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций : указ Президента РФ от 3 декабря 2008 г. № 1715 (в ред. от 21.05.2012). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 09.01.2024).

[11] См.: Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) : официальный сайт. URL: https://rkn.gov.ru/about/ (дата обращения: 09.01.2024).

[12] См.: Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено : официальный сайт. URL: https://eais.rkn.gov.ru (дата обращения: 08.01.2024).

[13] См.: О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ (последняя редакция). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 10.01.2024).

[14] См.: *Сулейманова С. Т., Еникеев Т. А.* Правовое регулирование компьютерной информации в Российской Федерации // Электронный научный журнал «Наука. Общество. Государство». 2019. Т. 7, № 2 (26). С. 4.

критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации[15]. В настоящее время в главе 28 УК РФ содержатся и иные нормы, предусматривающие уголовную ответственность за совершение следующих противоправных деяний.

Как можно увидеть, российский законодатель, в отличие от большинства европейских государств, не использует понятие «киберпреступление». Данный подход обусловлен тем фактом, что в широком смысле термин «киберпреступление» охватывает составы, предусмотренные не только главой 28 УК РФ, но и закрепленные в иных главах Уголовного кодекса РФ, например, п. «д» ч. 2 ст. 110, п. «б» ч. 3 ст. 133 и др. Следовательно, понятие «киберпреступление» охватывает не только преступления, совершаемые посредством использования информационно-телекоммуникационных технологий и в сфере компьютерной информации, но и учитывает квалифицирующие признаки и способы совершения таких уголовно наказуемых деяний.

Квалифицированные и особо квалифицированные составы образуют те же деяния, но совершенные из корыстной заинтересованности группой лиц по предварительному сговору, лицом с использованием своего служебного положения, причинившие крупный ущерб (свыше 1 млн рублей), повлекшие тяжкие последствия или создавшие угрозу их наступления[16].

Вместе с тем в процессе квалификации преступных посягательств встречается немало затруднений, в том числе относительно правомерности самой квалификации[17]. К примеру, правомерно ли квалифицировать хищение денежных средств с использованием компьютерных сетей по ст. 158 и 159 УК РФ, или же требуется привлечение к ответственности и по статьям главы 28 УК РФ? Единого практического подхода так и не было выработано. Так, в ряде ситуаций признается, что в данном случае компьютерное устройство выступает лишь в качестве средства совершения противоправного деяния, тогда как в иных требуется дополнительное вменение[18]. Авторы же придерживаются точки зрения той немногочисленной группы ученых, которые считают, что в описанной выше ситуации возможно вести речь о совокупности преступлений, поскольку имеет место посягательство не только на отношения собственности, но и на отношения, связанные с обеспечением конфиденциальности компьютерной информации[19].

По мнению авторов, в современных условиях сформировалась общественная потребность законодательного закрепления термина «киберпреступления», под которым следует рассматривать группу преступлений, совершение которых возможно не только посредством применения таких предметов материального мира, как расчетные банковские карты или использование компьютерной техники, но и посредством эксплуатации виртуального пространства в противоправных целях.

Помимо этого, авторы полагают возможным предложить рассмотреть ряд изменений в действующий уголовный закон. Так, в связи с ростом преступлений, предусмотренных ст. 242, 242.1, 242.2 УК РФ, и участившимися случаями применения сексуального насилия в отношении несовершеннолетних авторы полагали бы целесообразным дополнить диспозицию нормы, предусмотренной ч. 1 ст. 242.1 УК РФ, следующей формулировкой: «…публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно изображениями сексуального насилия над несовершеннолетними –».

Кроме того, полагаем возможным дополнить содержание примечания 1 к ст. 242.1 УК РФ в части: «…совершеннолетнего лица, осуществляющего сексуальное насилие или ими-

[15] См.: Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 18.02.2020). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 03.01.2024).

[16] См.: *Евдокимов К. Н.* Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. 2016. № 2 (24). С. 65.

[17] См.: *Маякова А. С., Шелепова С. А.* Компьютерные преступления : отдельные вопросы квалификации // Проблемы экономики и юридической практики. 2017. № 6. С. 194.

[18] См.: *Лавицкая М. И.* Структурно-содержательная характеристика главы 28 УК РФ : юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации // Российский следователь. 2021. № 6. С. 36.

[19] См.: *Ляпунов Ю., Максимов В.* Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 10.

тирующего сексуальное насилие над несовершеннолетним».

Авторам представляется возможным обсудить среди научной общественности целесообразность дополнения главы 28 УК РФ новыми составами, а именно: «Кибербуллинг», «Киберсталкинг», «Груминг в отношении несовершеннолетних», а в связи с возросшей угрозой заведомо ложных сообщений о террористических актах – и новым составом: «Захват интернет-сайтов и подмена их текущего содержания в целях дезинформации и дестабилизации обстановки в стране, уничтожения или широкомасштабного повреждения инфраструктуры, обладающей широкой общественной значимостью, в том числе финансовых систем и систем управления».

Библиографический список

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

Лавицкая М. И. Структурно-содержательная характеристика главы 28 УК РФ : юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации // Российский следователь. 2021. № 6. С. 35–41.

Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 10–15.

Маякова А. С., Шелепова С. А. Компьютерные преступления : отдельные вопросы квалификации // Проблемы экономики и юридической практики. 2017. № 6. С. 191–194.

Сулейманова С. Т., Еникеев Т. А. Правовое регулирование компьютерной информации в Российской Федерации // Электронный научный журнал «Наука. Общество. Государство». 2019. Т. 7, № 2 (26). С. 1–6.

Эткина А. Д. Об определении киберпреступления, компьютерного преступления и преступления в сфере компьютерной информации // Актуальные проблемы теории и практики применения уголовного закона. 2022. С. 204–210.

References

Evdokimov K. N. Current issues of improving criminal legal means of combating computer crimes // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2016. No. 2 (24). P. 62–66.

Lavitskaya M. I. Structural and content characteristics of Chapter 28 of the Criminal Code of the Russian Federation : Legal, technical and legal implementation problems of crimes in the field of computer information // Russian investigator. 2021. No. 6. P. 35–41.

Lyapunov Yu., Maksimov V. Responsibility for computer crimes // Legality. 1997. No. 1. P. 10–15.

Mayakova A. S., Shelepova S. A. Computer crimes : selected qualification issues // Problems of economics and legal practice. 2017. No. 6. P. 191–194.

Suleymanova S. T., Enikeev T. A. Legal regulation of computer information in the Russian Federation // Electronic scientific journal "Science. Society. State". 2019. Vol. 7, No. 2 (26). P. 1–6.

Etkina A. D. On the definition of cybercrime, computer crime and crime in the field of computer information // Current problems of the theory and practice of applying criminal law. 2022. P. 204–210.

Московская академия Следственного комитета Российской Федерации

Шестак В. А., доктор юридических наук, доцент, профессор кафедры криминалистики

E-mail: viktor_shestak@mail.ru

Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации

Чеботарь А. С., аспирант кафедры уголовного права, уголовного процесса и криминалистики

E-mail: chebotar.a.s@mail.ru

Moscow Academy of the Investigative Committee of the Russian Federation

Shestak V. A., Doctor of Legal Sciences, Associate Professor, Professor of the Department of Criminalistics

E-mail: viktor_shestak@mail.ru

Moscow State Institute of Internation Relations (MGIMO)

Chebotar A. S., Post-graduate Student of the Department of Criminal Law, Criminal Procedure and Criminalistics

E-mail: chebotar.a.s@mail.ru

Поступила в редакцию: 11.01.2024

Для цитирования:
Шестак В. А., Чеботарь А. С. О современных тенденциях преступлений, совершенных посредством использования информационно-телекоммуникационных технологий или в сфере компьютерной информации в Российской Федерации // Вестник Воронежского государственного университета. Серия: Право. 2024. № 2 (57). С. 294–300. DOI: https://doi.org/10.17308/law/1995-5502/2024/2/294-300.

Received: 11.01.2024

For citation:
Shestak V. A., Chebotar A. S. About the current trends of crimes committed using information and telecommunication technologies and in the field of computer information in the Russian Federation // Proceedings of Voronezh State University. Series: Law. 2024. No. 2 (57). P. 294–300. DOI: https://doi.org/10.17308/law/1995-5502/2024/2/294-300.