УДК 343.9
DOI 10.18101/978-5-9793-1659-8-111-115

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ОБРАЩЕНИЯ ОХРАНЯЕМОЙ ЗАКОНОМ ИНФОРМАЦИИ

© **Репецкая Анна Леонидовна**
доктор юридических наук, профессор,
профессор кафедры уголовного права и криминологии,
Восточно-Сибирский институт МВД РФ
Россия, г. Иркутск
repetsk@mail.ru

© **Родивилин Иван Петрович**
старший оперуполномоченный по особо важным деламотдела «К»,
ГУ МВД России по Иркутской области
Россия, г. Иркутск
377a@bk.ru

Предметом работы являются нормы уголовного закона, а также иных законов Российской Федерации, регламентирующие ответственность, возникающую при неправомерном доступе к охраняемой законом информации, нарушении правил эксплуатации средств хранения, обработки или передачи информации и информационно-телекоммуникационных сетей; состояние и структура преступлений в сфере обращения охраняемой законом информации, факторы их детерминирующие, личность преступника, совершающего названные преступления, а также существующая система противодействия указанным преступлениям.
Цель работы состоит в выявлении особенностей и определении тенденций преступлений в сфере обращения охраняемой законом информации, основных факторов, влияющих на выявляемые тренды и выработке новых научно обоснованных предложений по совершенствованию уголовного законодательства, а также иных мер противодействия рассматриваемым преступлениям в сфере обращения охраняемой законом информации.
Методологическую основу работы составляют общенаучные и частнонаучные методы познания — метод системного анализа, сравнительно-правовой, формально-логический, логико-юридический и другие методы, широко используемые в юридической науке.
Результаты работы. Сформулировано определение понятия «преступление в сфере обращения охраняемой законом информации» в соответствии с действующим законодательством, проанализированы факторы, детерминирующие совершение преступлений в сфере обращения охраняемой законом информации; исследовано состояние, структура и динамика совершения преступлений в сфере обращения охраняемой законом информации
Область применения результатов. Практическая значимость исследования заключается в возможности использования его результатов для развития государственной политики противодействия киберпреступности, а также практического применения предложенных рекомендаций в правоприменительной деятельности по обеспечению информационной безопасности.
Вывод. Детерминанты преступлений в сфере обращения охраняемой законом информации имеют многофакторный характер, к ним относятся: факторы правового характера, технические, социально-экономические, организационные, виктимологические. На основе проведенных авторами исследований выявлено, что в потерпевшие сами создают условия для совершения преступлений в сфере обращения охраняемой зако-

ном информации и их можно было бы не допустить при должной осмотрительности со стороны потерпевших. Также делается вывод о том, что основное внимание в предупреждении преступлений в сфере обращения охраняемой законом информации должно уделяться виктимологической профилактике, заключающейся в обеспечении надежной защиты информации.
Ключевые слова: преступления в сфере компьютерной информации, факторы преступности, ddos-атака, кибератака, информационная безопасность.

Процесс оборота информации в Российской Федерации регулируется Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [7] (далее — ФЗ № 149-ФЗ), в котором закрепляются основные понятия: информация, электронный документ и др. Вместе с тем, отсутствие четкого понятийного аппарата, имеющего отношение к охраняемой законом информации и совершение в отношении нее преступлений, дает возможность манипулировать понятиями, вводить в заблуждение следствие и суд, тем самым уходить от уголовной ответственности.

В ст. 2 ФЗ № 149-ФЗ закреплено понятие информации — это сведения (сообщения, данные) независимо от формы их представления, а в примечании 1 к ст. 272 УК РФ дается понятие именно компьютерной информации — сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Слово компьютер упоминается еще в 1897 году в Оксфордском словаре английского языка [4]. Российское законодательство не содержит легальной дефиниции данного понятия. Подобного рода пробел усложняет толкование и использование правоприменителем понятия «компьютерная информация». Термин «компьютерная информация» в современном научном словоупотреблении весьма многозначен и уже не относится к одному понятию компьютер, а распространяется на многие другие современные электронные устройства. Стоит обратить внимание на то, что компьютерная информация может находиться не только в компьютере, но и в периферийных устройствах (принтеры, сканеры и т. д.), телефонных аппаратах, планшетах, а также в киберпространстве (на сервере хостинг-провайдера или социальной сети).

Законодатели называют информацию и компьютерной, и цифровой, и электронной, и электронно-цифровой, как пример, отражение в федеральных законах понятия электронно-цифровой подписи или электронный документ.

Ряд ученых [2, 3] подвергают определение компьютерной информации, данное в Уголовном кодексе Российской Федерации критике, обосновывая это тем, что для передачи электронной информации могут быть использованы не только электрические сигналы, но и световые сигналы или электромагнитное излучение, имея ввиду оптоволоконный кабель, с помощью которого возможна передача данных. Однако, у определения «компьютерная информация», данного в Уголовном Кодексе Российской Федерации есть другие недостатки, подробно описанные в работах российских ученых [6, 8], исправить которые можно, если заменить указанную дефиницию на «цифровую информацию», изучение которой наблюдается в последние годы в работах некоторых ученых [1, 5].

Термин «электронная информация» расширяет количество устройств, в которых может находиться информация. Таким образом, аналоговый телевизор, микроволновую печь и т.п. тоже можно отнести к устройствам, в которых может обращаться электронная информация. Однако совершить неправомерный доступ к

ним невозможно, а также там, как правило, отсутствует охраняемая законом информация, к которой ограничили доступ.

Разделять информация на цифровую и аналоговую тоже не совсем верно в рамках юридических наук, так как это опять вызывает зависимость определения информации от устройства, в котором она находится.

На наш взгляд, необходимо отказаться от определения охраняемой законом информации через место ее нахождения, зависимость от какого-либо технического устройства, способ обработки. Охраняемая законом информация ограниченного доступа как предмет преступного посягательства — это сведения, на которые распространяется режим ограниченного доступа, установленный Конституцией РФ и Федеральными законами и ограниченные владельцем информации от неправомерного доступа. Собственно говоря, можно выделить два главных свойства охраняемой законом информации:

1. Владелец информации предпринял действия по ее защите, например, установил пароль.

2. Информация подпадает под сведения ограниченного доступа, режим оборота которых регулируется федеральным законом.

Совершение преступлений в сфере обращения охраняемой законом информации, направленных на получение информации, находящейся в мобильных устройствах, связано с увеличением в России количества мобильных телефонов и другой носимой электроники. Пользователи фотографируют бумажные документы, экран рабочего монитора, отправляют фотографии и файлы с помощью мессенджеров и облачных сервисов.

Неправомерный доступ к охраняемой законом информации зачастую имеет схожий предмет преступного посягательства — охраняемую законом информацию и становится способом совершения иных преступлений, таких как нарушений тайны переписки, личной или семейной тайны, собирание сведений, составляющих банковскую или коммерческую тайну. Указанные преступления имеют другой основной непосредственный объект, а в диспозиции соответствующей статьи Особенной части УК РФ отсутствует указание на такой способ совершения преступления. Однако практика показывает, что неправомерный доступ к информации зачастую рассматривается как способ совершения иного преступления и не выделяет реальную совокупность преступления, что, по нашему мнению, влечет недооценку общественной опасности содеянного.

В частности, в чем заключается и в чем выражается неправомерность доступа к охраняемой законом информации? Доступ к информации можно разделить на 2 группы:

1) доступ с использованием методов обхода средств защиты информации;

2) доступ в систему, хотя и правомерный, но осуществляемый неправомерно.

Исходя из изложенного, предлагаем под неправомерным доступом к охраняемой законом информации понимать возможность воздействия на информацию лицом, не имеющим легального права на ознакомление с ней, а также лицом, хотя и имеющим право на правомерный доступ к информации, но использующим это право в нарушение правил доступа к информации.

Количество регистрируемых преступлений в сфере обращения охраняемой законом информации с каждым годом увеличивается. 25% всех зарегистрированных преступлений совершаются либо с незаконным использованием охраняемой законом информации, либо она сама становиться предметом преступления. Однако наблюдается снижение преступлений в сфере компьютерной информа-

ции, что обусловлено, с одной стороны, появлением новых схем противоправных деяний, с другой, изменением отношения пользователей к своей информации ограниченного доступа.

Существование преступности в сфере оборота охраняемой законом информации определяются несколькими специфическими факторами, которые не совпадают с факторами, порождающими преступность в целом. К таким факторам можно отнести:

1) факторы правового характера (отсутствие единого понятийного аппарата, регламентирующего преступления в сфере обращения охраняемой законом информации, отсутствие уголовной ответственности за ограничение доступа к охраняемой законом информации);

2) технические факторы (рост числа компьютерной техники, увеличение объемов информации, недостаточность защиты самих технических средств защиты компьютерной техники);

3) организационные факторы (усиление цифрового неравенства в России, под которым понимается, с одной стороны, различие в уровнях развития информационных технологий между различными странами и регионами, внутри страны, возрастными и социальными группами, различными государственными учреждениями, между институтами гражданского общества, с другой — как разрыв в возможностях доступа к информации между богатыми и бедными).

Методы противодействия преступлениям должны соответствовать современным реалиям. Преступления в сфере обращения охраняемой законом информации постоянно пополняются новыми способами совершения преступлений, новой техникой, устройствами. На данном этапе необходимо поменять подход к профилактике и борьбе с преступлениями в данной сфере

Формулируя выводы, следует отметить, что применение иных специальных мер противодействия преступлениям в сфере обращения охраняемой законом информации, должны основываться на положении о проведении преобразований в обществе, нацеленных на повышение компьютерной и сетевой грамотности, сокращения цифрового неравенства.

Литература

1. Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юр. наук. Москва, 2017. 204 с.

2. Богданова Т. Н. К вопросу об определении понятия «Преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. 2012. № 37 (291). С. 64–67.

3. Жиделев В. Г. Некоторые аспекты квалификации преступлений в сфере компьютерной информации в российском и зарубежном законодательстве // Человек: преступление и наказание. 2012. № 2. С. 3–25.

4. Оксфордский словарь английского языка (Oxford English Dictionary) // oed.com. URL: http://www.oed.com/view/Entry/37975.

5. Рудых А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юр. наук. Ростов-на-Дону, 2020. 239 с.

6. Смагин П. Г. О понятии «компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД // Вестник Воронежского института МВД России. 2008. № 1. С. 80–81.

7. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защиты информации»: в ред. Федерального закона от 3 апреля 2020 г. № 105-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

8. Чупрова А.Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 131–134.

COUNTERING CRIMES IN THE SPHERE OF INFORMATION PROTECTED BY LAW

Anna L. Repetskaya
Doctor. Jur. Sciences, Professor,
Professor of the Department of Criminal Law and Criminology
East Siberian Institute of the Ministry of Internal Affairs of Russia
Russia, Irkutsk
repetsk@mail.ru

Ivan P. Rodivilin
Senior operative for the internal affairs department of the "K" department
Main Directorate of the Ministry of Internal Affairs of Russia for the Irkutsk Region
Russia, Irkutsk
377a@bk.ru

The subject of the work is the norms of the criminal law, as well as other laws of the Russian Federation, regulating liability arising from improper access to information protected by law, violation of the rules for the operation of means of storing, processing or transmitting information and information and telecommunication networks; the state and structure of crimes in the field of circulation of information protected by law, their determinant factors, the personality of the offender who commits these crimes, as well as the existing system of counteraction to these crimes.
The purpose of the work is to identify the features and determine the trends of crimes in the field of circulation of information protected by law, the main factors affecting the identified trends and the development of new scientifically substantiated proposals for improving the criminal legislation, as well as other measures to counteract the considered crimes in the field of circulation of information protected by law**.**
The methodological basis of the work is formed by general scientific and specific scientific methods of cognition — the method of system analysis, comparative legal, formal logical, logical legal and other methods widely used in legal science**.**
Results of work. The definition of the concept "crime in the sphere of circulation of information protected by law" has been formulated in accordance with the current legislation, the factors that determine the commission of crimes in the field of circulation of information protected by law have been analyzed; investigated the state, structure and dynamics of the commission of crimes in the field of circulation of information protected by law**.**
Scope of the results. The practical significance of the study lies in the possibility of using its results for the development of state policy on countering cybercrime, as well as the practical application of the proposed recommendations in law enforcement activities to ensure information security.
Output. The determinants of crimes in the sphere of circulation of information protected by law are multifactorial in nature, they include: factors of a legal nature, technical, socio-economic, organizational, victimological. On the basis of the research conducted by the authors, it was revealed that victims themselves create conditions for committing crimes in the field of circulation of information protected by law, and they could have been prevented with due diligence on the part of the victims. It is also concluded that the main attention in the prevention of crimes in the sphere of circulation of information protected by law should be paid to victimological prevention, which consists in ensuring reliable protection of information.
Keywords: crimes in the field of computer information, crime factors, ddos-attack, cyberattack, information security.