ПРЕСТУПЛЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ: АНАЛИЗ, ПРОБЛЕМЫ КВАЛИФИКАЦИИ

А.С. Кузнецова, *студент*
Д.О. Николаев, *студент*
Д.А. Латыпов, *студент*
Научный руководитель: *Р.Н. Нурмухаметов, ассистент*
Уфимский университет науки и технологий
(Россия, г. Уфа)

DOI:10.24412/2500-1000-2023-1-3-26-29

Аннотация. *В настоящее время рост технологического прогресса, повсеместное распространение сети Интернет вывели множество преступлений на новый уровень. Преступления в сфере компьютерной информации имеют свою специфику, что обуславливает ряд проблем, возникающих при их квалификации. Данная статья посвящена анализу главы 28 УК РФ, рассматривающей преступления в сфере компьютерной информации, рассмотрены трудности, возникающих при квалификации преступлений в данной сфере, сформулированы предложения по совершенствованию действующего уголовного законодательства в области информационной безопасности.*

Ключевые слова: *уголовная ответственность, преступления в информационной сфере, квалификация, вредоносная программа, неправомерный доступ к компьютерной информации, состав преступления.*

Согласно аналитическому отчету МВД, в период с января по ноябрь 2022 года в России было зарегистрировано 470,1 тыс. преступлений, совершенных в сфере компьютерной информации или с использованием информационно-телекоммуникационных технологий [1]. Несмотря на то, что данный показатель по сравнению с показателем за аналогичный период 2021 года снизился на 4,9%, а в общем числе зарегистрированных преступлений их удельный вес уменьшился на 1,6% (с 26,7% в январе-ноябре 2021 года до 25,8% за аналогичный период в 2022 году), данная категория преступлений остается достаточно распространенной и представляет высокую угрозу для общества.

Ответственность за преступления в сфере компьютерной информации предусмотрена гл. 28 УК РФ, а именно ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»; ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»; ст. 274.2 «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» [2].

Вышеприведенные статистические данные свидетельствуют об уменьшении числа преступлений данного вида. Однако ввиду того, что преступления в информационной сфере характеризуются высокой латентностью, мы можем предположить, что их реальное число значительно превышает число, отраженное в статистических данных. Такая ситуация обусловлена, на наш взгляд, как спецификой самих преступных деяний и необходимостью выработки особых способов раскрытия фактов преступлений в информационной сфере, так и тем фактом, что нередко сами потерпевшие не желают обращаться в правоохранительные органы, предпочитая при-

бегать к иным способам восстановления нарушенных прав.

Рассмотрим ряд проблем, связанных с квалификацией преступлений в информационной сфере.

Согласно ст. 272 УК РФ, за «неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожений, блокирование, модификацию либо копирование компьютерной информации» предусмотрена уголовная ответственность. Компьютерная информация определена законодателем как «сведения (сообщения, данные), представляемые в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [2]. Однако отсутствует толкование термина «охраняемая законом компьютерная информация», что, на наш взгляд, представляет проблему при квалификации по ст. 272 УК РФ. Как отмечают некоторые авторы, действие ст. 272 УК РФ не распространяется на неправомерные манипуляции с открытой информацией. При этом судебная практика по данным делам свидетельствует, что данная статья может применяться и в отношении общедоступной информации. Так, суды, как правило, апеллируют к Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3]. Данный закон раскрывает понятие «защита информации» как принятие правовых, организационных и технических мер, направленных на: «обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации» [4].

Согласно ст. 273 УК РФ, за 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» предусмотрена уголовная ответственность. Преступления по данной статье являются одними из наиболее распространенных в категории преступлений в информационной сфере. Вредоносные программы, о которых идет речь в ст. 273 УК РФ, могут представлять собой: трояны, вирусы, черви, руткины, фишинг, кейлоггер, спам [5]. При этом единообразное толкование вредоносной программы в правовой науке отсутствует.

Согласно определению, данному в ГОСТе Р 50922-2006 «Защита информации. Основные термины и определения», вредоносной называется программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы [6]. Однако разнообразие программ, созданных с целью или способствующих выполнению несанкционированных действий в информационной системе, значительно шире содержания указанного определения. В частности, под данное определение не попадают вирусы, задачей которых является не принесение вреда операционной системе как таковое, а сбор данных о пользователях устройств без их уведомления.

Из содержания ст. 274 следует, что ответственность наступает за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Применительно к данной статье отметим, что общепринятых норм эксплуатации оборудования и обработки информации не существует, также отсутствует строгий перечень таких правил, поэтому данная ответственность должна закрепляться за правомочным лицом.

Ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» отсы-

лает нас к Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации» [7]. Особенность предмета преступления в том, что в качестве такового выступают программы, предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры.

Стоит отметить, что число преступлений в информационной сфере не ограничивается преступлениями, предусмотренными указанными статьями. Нередко преступления совершаются с использованием компьютерных и информационно-телекоммуникационных технологий, однако относящиеся к другим разделам УК РФ. Одним из распространенных является мошенничество в сфере информационных технологий, причем с развитием информационной среды появляются и новые способы совершения мошенничеств. Объектами мошеннических преступлений в информационной сфере чаще всего становятся: мобильное рекламное и компьютерное программное обеспечение; социальные сети; платежные операции в системе онлайн и интернет-банкинг; электронные кошельки; облачные носители информации.

Значительное число преступлений связано с использованием вредоносных программ с целью хищений денежных средств. Так, поводами для возбуждения уголовных дел по ст. 273 УК РФ являются заявления граждан или юридических лиц по фактам хищения у них денежных средств с использованием вредоносных программ или материалы, содержащие результаты оперативно-розыскных мероприятий, проведенных специализированными подразделениями МВД и ФСБ.

Изменение и совершенствования способов мошенничества, появление его новых форм обуславливает необходимость увеличения перечня составов преступлений, совершаемых в электронной среде и внесения поправок в действующий УК РФ. В настоящее время остается открытым вопрос определения перечня компьютерных преступлений. На наш взгляд, необходимо ввести в УК РФ способ совершения преступления, формулируемый как «с применением компьютерных средств» («в сфере компьютерной информации»). Также отметим необходимость определения дополнительных признаков в ст. 272 УК РФ, предусматривающих дифференциацию способа получения доступа к компьютерной информации, поскольку приведенное понятие «неправомерный доступ» в настоящее время не отвечает всем способам посягательств на информацию.

Таким образом, на сегодняшний день действующее законодательство в данной сфере нуждается в совершенствовании. В настоящее время 28 глава УК РФ во многом находится в тени законодателя. Несмотря на широкое распространение и высокую опасность для общества данной категории преступлений, отсутствует официальное толкование многих понятий. Специфика преступлений в сфере информационных технологий и сложность их расследования актуализирует необходимость восполнения пробелов в уголовном законе в данной сфере.

Библиографический список

1. Состояние преступности в России // Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр». – [Электронный ресурс]. – Режим доступа: https://d-russia.ru/wp-content/uploads/2022/12/mvd_22_11_.pdf (дата обращения 11.01.2023).

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с посл. изм. и доп. от 29 декабря 2022 г. № 586-ФЗ) // Официальный интернет-портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 12.01.2023).

3. Русскевич Е. А. Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. – 2018. – № 10 (94). – С. 46-50.

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с посл. изм. и доп. от 29 декабря 2022 г.

№ 604-ФЗ) // Официальный интернет–портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 12.01.2023).

5. Александров Л.П. Предупреждение и раскрытие оперативными подразделениями внутренних дел фактов мошенничества в сфере информационных технологий. Материалы XXIV Международной студенческой научной конференции «Молодежь, наука и цивилизация». – Красноярск: СибЮИ МВД России, 2022. – С. 365-368.

6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200058320 (дата обращения: 12.01.2023).

7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации» // Официальный интернет–портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 12.01.2023).

CRIMES IN THE INFORMATION SPHERE: ANALYSIS, PROBLEMS OF QUALIFICATION

A.S. Kuznetsova, *Student*
D.O. Nikolaev, *Student*
D.A. Latypov, *Student*
Supervisor: *R.N. Nurmukhametov, Assistant*
Ufa University of Science and Technology
(Russia, Ufa)

Abstract. *At present, the growth of technological progress, the ubiquity of the Internet have brought many crimes to a new level. Crimes in the field of computer information have their own specifics, which causes a number of problems that arise in their qualification. This article is devoted to the analysis of Chapter 28 of the Criminal Code of the Russian Federation, which considers crimes in the field of computer information, the difficulties that arise in the qualification of crimes in this area are considered, proposals are made to improve the current criminal legislation in the field of information security.*

Keywords: *criminal liability, crimes in the information sphere, qualification, malware, illegal access to computer information, corpus delicti.*