УДК 343.9

Н. В. Павловская
заведующий лабораторией криминологического обеспечения прокурорской деятельности Научно-исследовательского института Университета прокуратуры Российской Федерации, кандидат юридических наук

БОРЬБА С АТАКАМИ НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ В РОССИИ

Результаты криминологических исследований свидетельствуют о значительном увеличении в последнее время масштабов неправомерного воздействия на информационные ресурсы как в России, так и во всем мире. По данным компаний, специализирующихся на информационной безопасности, в течение 2022 г. стремительно возрастало не только число разнообразных компьютерных атак, но и их мощность, интенсивность, длительность. Так, российские средства массовой информации сообщали об увеличении количества DDoS-атак на российские компании в 15 раз, а на государственный сектор в 17 раз, что связывалось, по мнению экспертов, с нестабильной политической ситуацией в России и во всем мире и, как следствие, активизацией «хактивистов», целью которых является нанесение вреда экономике и социальной сфере России [1]. Как правило, подобные атаки на российские ресурсы осуществляются с территории других государств, например, по данным Лаборатории Касперского, в третьем квартале 2022 г., большинство управляющих ботнетами серверов находились в США, Германии, Нидерландах [2], что значительно затрудняет борьбу с данным видом преступности.

Мнение экспертов соотносится с данными правовой статистики, согласно которым количество зарегистрированных преступлений, предусмотренных ст. 274.1 Уголовного Кодекса Российской Федерации («Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации») [4], за 2022 г. (519) в 3 раза превысило показатели 2021 г. (159). Существенно увеличилось и количество предварительно расследованных преступлений данного вида (с 50 до 437 соответственно). Представляется, что эти данные свидетельствуют об эффективности созданной в России, в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [4], государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации,

представляющей собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Силы, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, включают подразделения и должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (этим органом является Федеральная служба безопасности Российской Федерации); национальный координационный центр по компьютерным инцидентам; а также подразделения и должностные лица субъектов критической информационной инфраструктуры — государственных органов, государственных учреждений, российских юридических лиц и (или) индивидуальных предпринимателей, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также российских юридических лиц и (или) индивидуальных предпринимателей, которые обеспечивают взаимодействие указанных систем или сетей.

В то же время следует отметить, что при отсутствии в Уголовном кодексе Российской Федерации специальной нормы об ответственности непосредственно за действия, связанные с организацией и осуществлением DDoS-атак, в судебной практике пока не сложилось единого подхода к квалификации подобных деяний. Исследования показывают, что, помимо рассматриваемой нормы, в некоторых случаях судами применяются ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 272 «Неправомерный доступ к компьютерной информации» Уголовного кодекса Российской Федерации, а иногда и их совокупность [5].

При этом ни одна из упомянутых уголовно-правовых норм не охватывает всех возможных действий, связанных с организацией и осуществлением DDoS-атак. Так, в ст. 273 Уголовного кодекса Российской Федерации не упоминаются заказчики такого рода атак, которые сами не создают и не используют

вредоносные программы, предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, а только оплачивают соответствующие услуги хакеров. Кроме того, распространены случаи, когда для совершения компьютерных атак вредоносное программное обеспечение приобретается на различных хакерских страницах, сайтах, форумах, что также не охватывается указанной нормой. В связи с этим в науке широко обсуждаются различные варианты совершенствования действующего уголовного законодательства. Так, предлагается дополнить Уголовного кодекса Российской Федерации новой статьей, предусматривающей уголовную ответственность за незаконное ограничение доступа к информации, находящейся в телекоммуникационных сетях, нарушающее права граждан на получение информации, свободу распространения информации законным способом [6, с. 306]. Высказываются предложения о введении уголовной ответственности за создание и использование «ботнетов», «ботнет-сетей» [7, с. 406].

В декабре 2022 г. Пленум Верховного Суда Российской Федерации разъяснил, что действия лица квалифицируются по ч. 1 ст. 274.1 Уголовного кодекса Российской Федерации, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, а в ином случае при наличии на то оснований — по ст. 273 Уголовного кодекса Российской Федерации [8]. При этом воздействие не только на саму информацию, но и на средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением) следует считать блокированием компьютерной информации. Представляется, что разъяснения могут способствовать формированию единообразной судебной практики и совершенствованию борьбы с данным видом преступности.

Список основных источников:

1. Число DDoS-атак на российские компании в I полугодии 2022 года выросло в 15 раз [Электронный ресурс] // Информационное агентство ТАСС. URL: https://tass.ru/ekonomika/15211801 (дата обращения: 11.11.2022). Перейти к источнику Вернуться к статье

2. DDoS-атаки в третьем квартале 2022 г. [Электронный ресурс] // https://securelist.ru/ddos-report-q3-2022/106012/ (дата обращения: 11.11.2022). Перейти к источнику Вернуться к статье

3. Уголовный кодекс Российской Федерации [Электронный ресурс] : 13 июня 1996 г., № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. от 18.03.2023 г. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

4. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : Федер. закон, 26 июля 2017 г., № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

5. Евдокимов К. Н., Таскаев Н. Н. Проблемные вопросы квалификации преступлений, предусмотренных статьей 273 УК РФ, на стадии возбуждения уголовного дела // Всерос. криминолог. журн. 2018. Т. 12, № 4. С. 590–600. Вернуться к статье

6. Родивилин И. П. Современная специфика детерминации преступлений в сфере обращения охраняемой законом информации // Вестн. Удмурт. ун-та. Сер. Экономика и право. 2021. № 2. С. 301–307. Вернуться к статье

7. Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика : дис. … д-ра юрид. наук : 12.00.08. М., 2021. 557 с. Вернуться к статье

8. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [Электронный ресурс] : постановление Пленума Верхов. Суда Рос. Федерации, 15 дек. 2022 г., № 37. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье