УДК 343.3

М. В. Рубцова
старший научный сотрудник Научно-исследовательского института Университета прокуратуры Российской Федерации

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНЫМ АТАКАМ НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

В последнее время наблюдается увеличение количества компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств. Компьютерная атака — целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации [1, с. 210]. Государственная политика в области международной информационной безопасности представляет собой совокупность скоординированных мер, направленных на формирование с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности [2]. В связи с увеличением роста преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее — ИКТ), вопросы, касающиеся защиты информационных ресурсов, вошли в перечень стратегических национальных приоритетов Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 года № 400.

В 2022 году количество кибератак на Россию выросло на 80 %, которые были успешно ликвидированы. В России действуют оперативные штабы по защите от киберугроз, Национальный координационный центр по компьютерным инцидентам (далее — НКЦКИ), созданный ФСБ России [3]. На фоне специальной военной операции предпринимается массированная кибероперация против России. Так, по сообщению НКЦКИ, в сложившейся напряженной геополитической обстановке ожидается увеличение интенсивности компьютерных атак на информационные ресурсы, объекты критической информационной структуры, направленные на нарушение функционирования важных информационных ресурсов и сервисов, причинение ущерба, в том числе и политических целях. При этом используется следующая тактика атак: блокируется доступ к российским интернет-ресурсам, становится недоступной информация или

подменяется фейками, фальшифками. Применяются самые современные алгоритмы и комбинированные технологии, сложное программное обеспечение, способное поражать устройства, использующие различные операционные системы.

Однако уже сегодня можно сказать, что кибератрессия против России не увенчалась успехом, поскольку определенная системная работа проводилась все последние годы. Специалистами осуществлялась необходимая работа в сфере защиты информационной инфраструктуры, обеспечивалась устойчивость работы и безопасность сетей и каналов связи. Принимались документы стратегического характера, которые определяли основные угрозы и риски в данной области, а также пути их нейтрализации. В связи с чем принят Указ Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», который регламентирует новые направления и требования в рассматриваемой сфере деятельности. Между тем характер вызовов и угроз стремительно меняется с быстрым развитием информационной сферы.

В текущем году (январь – февраль 2023 года) зарегистрировано 93 372 преступления с использованием ИКТ и в сфере компьютерной информации, рост по сравнению с аналогичным периодом прошлого года составил 17,1 %. Наблюдается увеличение удельного веса таких преступлений на 30,6 % (26,3 % аналогичный период 2022 года). Несмотря на принимаемые государством все необходимые предупреждающие меры, остается повышенная активность компьютерных атак на информационные ресурсы государственной власти, которая фиксируется Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак. Так, по мнению секретаря Совета безопасности Российской Федерации Н. П. Патрушева, данная ситуация осложняется тем, что в органах публичной власти в ходе проверок защиты информации выявлено около 670 уязвимостей информационных систем (лишь 8 % региональных информационных ресурсов подключены к системе обнаружения, предупреждения и ликвидации последствий компьютерных атак) [4]. По мнению некоторых авторов, которые безопасность компьютерных сетей определяют как действие, позволяющее защитить данные сети от различных угроз киберпреступников. К примеру, таких как атаки при помощи вредоносных программ [5, с. 25]. Также сетевая атака рассматривается как вторжение злоумышленников в операционную систему удаленного компьютера для захвата управления над ней, приведения ее к отказу в обслуживании и получении доступа к защищенной информации [6, с. 333]. В свою очередь, под защитой от компьютерных атак понимается совокупность методов, процессов и

технологий, предназначенных для защиты целостности программного обеспечения, информационных инфраструктур и информации, ИКТ [7, с. 126]. Система безопасности должна обеспечивать недопущение хакерских атак, и для решения этой задачи необходимы совместные усилия как правоохранительных органов, так и банковского сектора, специальных служб, специалистов в сфере высоких технологий [8, с. 253].

Список основных источников

1. Соболева Е. С., Сапожникова А. В. Обнаружение компьютерных атак на критически важную информационную систему и противодействие компьютерному нападению // Современные проблемы радиоэлектроники и телекоммуникаций / Федер. гос. автоном. образоват. учреждение высшего образования «Севастопольский государственный университет». Севастополь : Россия № 1, 2018. С. 210. Вернуться к статье

2. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности [Электронный ресурс] : Указ Президента Рос. Федерации, 12 апр. 2021 г., № 213. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

3. Война в киберпространстве: как Россия защищает свой цифровой суверенитет [Электронный ресурс] // Профиль. Наука и Технологии. URL: https://profile.ru/scitech/vojna-v-kiberprostranstve-kak-rossiya-zashhishhaet-svoj-cifrovoj-suverenitet-1193878/?ysclid=ldu4lqu8ym377529516 (дата обращения: 07.02.2023). Перейти к источнику Вернуться к статье

4. Патрушев: Растет число кибератак атак на информационные государственные ресурсы [Электронный ресурс] // Российская газета. URL: https://rg.ru/2022/07/05/reg-dfo/patrushev-rastet-chislo-kiberatak-atak-na-informacionnye-gosudarstvennye-resursy.html?ysclid=lg4y03mnat239027971 (дата обращения: 06.04.2023). Перейти к источнику Вернуться к статье

5. Зык А. В. Киберпреступники в современном обществе. Мотивы преступлений с использованием информационных технологий // Науч. дайджест Вост.-Сибир. ин-та МВД России. 2022. № 3 (17). С. 25. Вернуться к статье

6. Демченко Р. О., Богданов В. В., Василенко Н. В. Выявление сетевых атак // Науч. чтения им. проф. Н. Е. Жуковского : сб. науч. ст. XII Междунар. науч.-практ. конф. / Краснодар. высш. воен. авиацион. училище летчиков им. Героя Советского Союза А. К. Серова. Краснодар, 2022. С. 333. Вернуться к статье

7. Жарова А. К. Обеспечение защиты государства от компьютерных атак в ИТК-сфере // Тр. Ин-та государства и права РАН. 2022. Т. 17. № 4. С. 126. Вернуться к статье

8. Абидов Р. Р. Кибератаки на критическую информационную инфраструктуру, как угроза национальной безопасности // Пробелы в рос. законодательстве. 2022. Т. 15. № 4. С. 253. Вернуться к статье