ВЕРОЯТНОСТНЫЙ МЕТОД ОЦЕНКИ ЭФФЕКТИВНОСТИ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

A PROBABILISTIC METHOD FOR EVALUATING THE EFFECTIVENESS OF AN ADAPTIVE INFORMATION SECURITY SYSTEM OF A CORPORATE NETWORK OF DATA TRANSMISSION

L. Gruzdeva

Summary. The article presents statistical data on the most popular attack methods, the objects of which were government institutions and financial organizations. The share of cyberattacks on government resources in the third quarter of 2019 increased to 23%. Three quarters of attacks on corporate networks and 62% of individuals were carried out using malicious software. An algorithm is proposed for evaluating the characteristics of an adaptive information protection system using the example of a corporate network operating in conditions of attacks accompanied by infection of nodes of various kinds by malicious programs.

Keywords: corporate network of data transmission, information security system, malicious software, information security.

Груздева Людмила Михайловна
К.т.н., доцент, Российский университет транспорта (РУТ-МИИТ), Москва
docentglm@gmail.com

Аннотация. В статье представлены статистические данные наиболее популярных методов атак, объектами которых становились государственные учреждения и финансовые организации. Доля кибератак на правительственные ресурсы в третьем квартале 2019 г. выросла до 23%. Три четверти атак на сети юридических лиц и 62% частных лиц осуществлялись с применением вредоносного программного обеспечения. Предложен алгоритм оценки характеристик адаптивной системы защиты информации на примере корпоративной сети, функционирующей в условиях атак, сопровождающихся заражениями узлов различного рода вредоносными программами.

Ключевые слова: корпоративная сеть передачи данных, система защиты информации, вредоносное программное обеспечение, информационная безопасность.

Введение

В [1] предложена модель адаптивной системы защиты информации (СЗИ), реализация которой в корпоративной сети передачи данных (КСПД) способна обеспечить необходимый уровень производительности сети [2, 3] путем выбора алгоритма для раннего и надежного обнаружения информационных угроз [4] и быстрого запуска доступных средств противодействия угрозам информационной безопасности в наиболее уязвимых узлах сети.

В адаптивной СЗИ выделено два уровня организации защитных механизмов: (1) уровень обнаружения (на основе его показаний принимается решение о наличии / отсутствии угрозы информационной безопасности в сети); (2) уровень противодействия (инициируется только при обнаружении информационной угрозы) [5].

Рассмотрим метод количественных оценок характеристик адаптивной СЗИ на примере корпоративной сети, функционирующей в условиях атак, совершаемых с использованием вредоносного программного обеспечения (ПО). Данный метод атак является одним из самых распространенных, в частности, вредоносное ПО во III квартале 2019 г. применялось в 74% уникальных кибератак на сети юридических лиц, таких как государственные учреждения (рис. 1), финансовые организации (рис. 2) и промышленные компании [6–8]. При этом в 79% объектами для атак становились компьютеры, серверы и сетевое оборудование [6].

Частные лица за тот же период были атакованы с использованием вредоносного ПО в 62% случаев от общего числа инцидентов информационной безопасности [9]. При этом тремя основными путями распространения вредоносного программного обеспечения являлись [6]:

- электронная почта: вредоносное вложение или ссылка на зараженный ресурс отправлялись жертве в письме (23% случаев);
- официальные магазины приложений (26%) и сайты, при посещении которых вредоносное ПО устанавливалось на устройство жертвы (35%).

По мнению специалистов, нарушители информационной безопасности будут искать новые пути распространения вредоносного программного обеспечения и совершенствовать старые. Злоумышленники будут

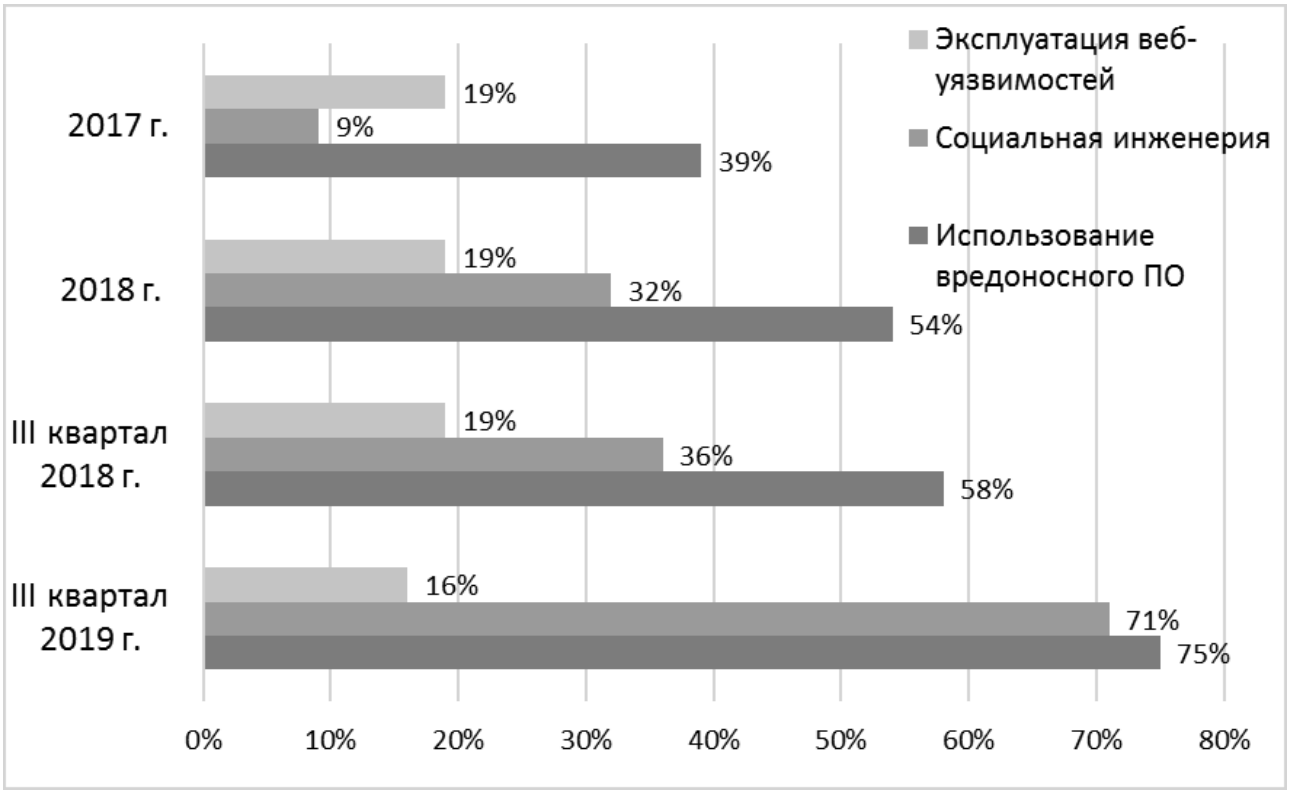

Рис. 1. Наиболее популярные методы атак на государственные учреждения

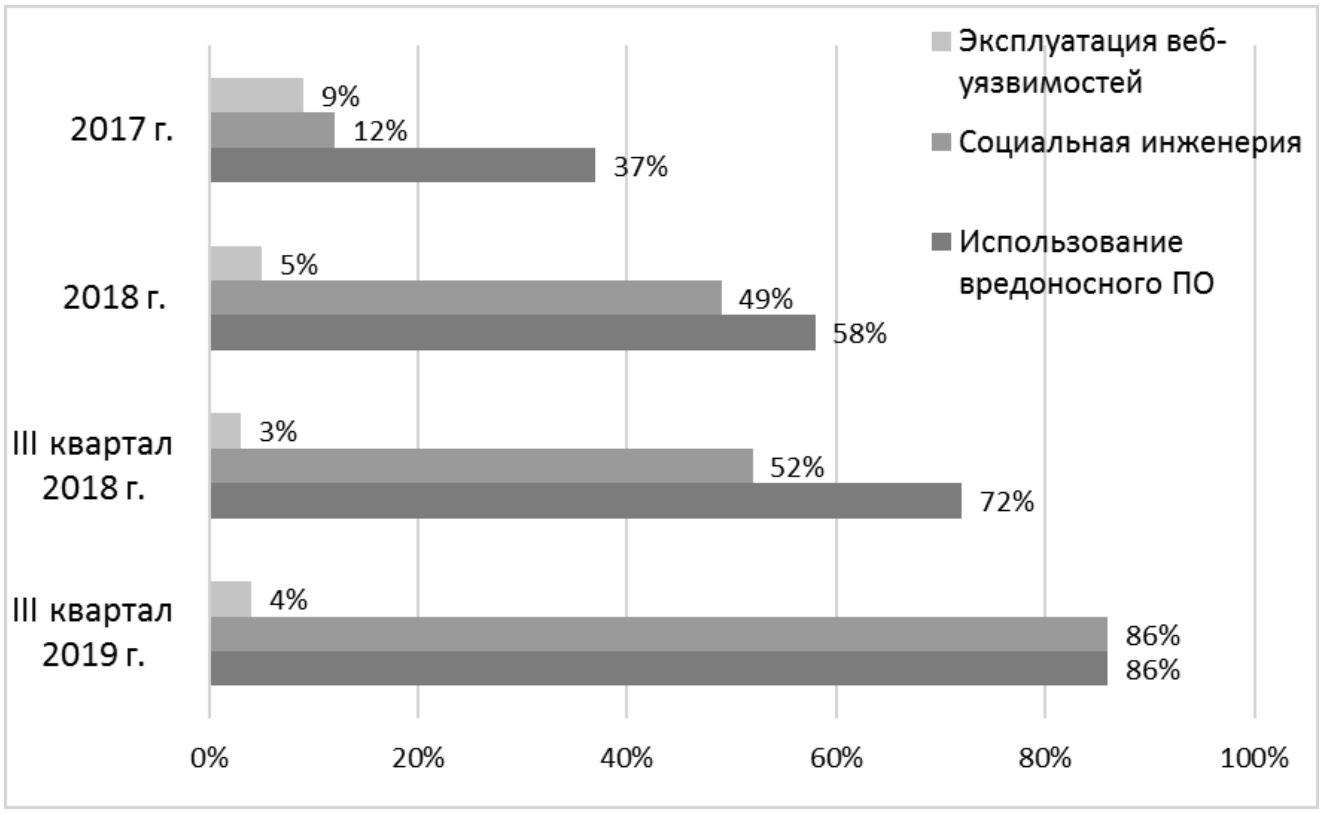

Рис. 2. Наиболее популярные методы атак на финансовые организации

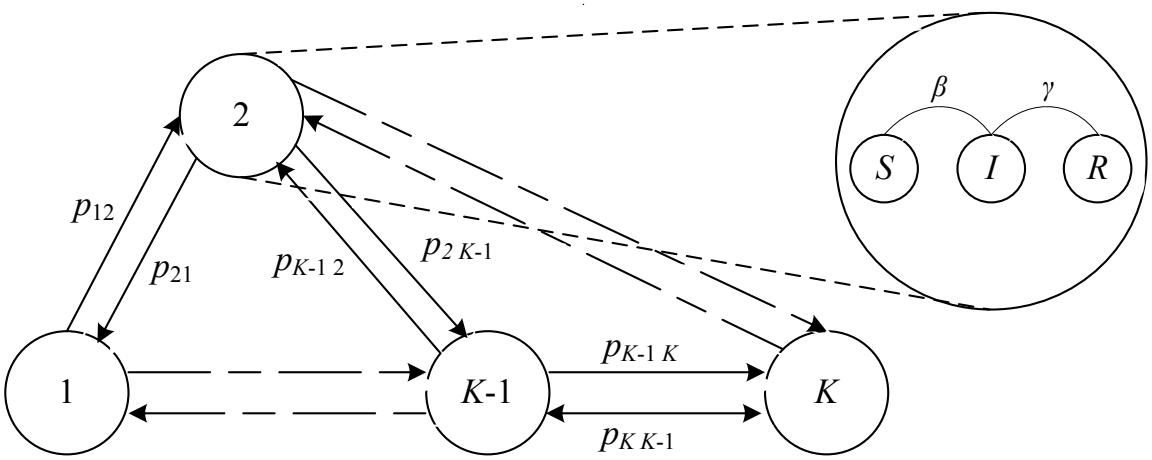

Рис. 3. Граф замкнутой сети массового обслуживания [10]

продолжать атаковать слабо защищенные ресурсы для хищения данных (персональных, медицинских и платежных), поэтому задача обеспечения эффективного функционирования систем защиты информации в КСПД актуальна и будет оставаться таковой в дальнейшем.

Модель корпоративной сети. Основой модели является сеть из K связанных узлов, образующих графовую структуру (рис. 3). Каждая пара узлов связана вероятностью p_{ij} пересылки пакета трафика из i-го в j-й узел, причем пакет может быть вредоносным (ВП).

В исследовании динамики распространения вредоносных программ в компьютерных сетях, в которых происходит два противоборствующих подпроцесса атаки и защиты узлов, нашли широкое применение претерпевшие различные модификации эпидемиологические математические модели. Наиболее релевантной для подобных исследований является SIR-модель Кермака-Маккендрика [11]. Каждый узел сети может прибывать в одном из трех состояний: «восприимчивый» (S), «заражённый» (I) или «не восприимчивый» (R), при этом β — скорость заражения, а γ — скорость восстановления (как только узел избавляется от вредоносной программы, он приобретает к ней иммунитет).

Если вредоносный пакет обнаружен в i-ом узле, то необходимо инициировать средства противодействия в узлах сети, с которыми он связан. Используя вероятности p_{ij} можно оценить общее число вредоносных пакетов в сети и количество процессов обнаружения и устранения ВП, необходимых для полного восстановления сети.

Результатом работы уровня обнаружения является вектор-строка $V = (V_1, V_2, \ldots, V_K)$ — общее число вредоносных пакетов в начальный момент времени. Так как V_i — общее число обнаруженных вредоносных пакетов для каждого i-го узла сети, то $V_i P$ — общее число ВП, поиск и устранение которых необходимо осуществлять в сети после восстановления i-го узла в начальный цикл. Элемент (i, j) матрицы P^2 есть сумма вероятностей того, что процесс восстановления узла i вызовет запуск средств противодействия в узле k, а затем в узле j.

Алгоритм оценки характеристик адаптивной СЗИ

Шаг 1. Оценить для каждой пары узлов i, j вероятность p_{ij}.

Шаг 2. Если уровень обнаружения принимает решение о наличии угрозы [1, 3], то зафиксировать начальное число вредоносных пакетов в каждом узле сети — V_i (генерируются средствами обнаружения) и инициализировать уровень противодействия [1, 5].

Шаг 3. Определить общее число инициализаций средств противодействия, вызываемых i-м модулем: $SP_i = V_i (\mathrm{I} - P)^{-1}$, где I — единичная матрица, а $P = ||p_{ij}||$.

Шаг 4. Суммировать элементы вектор-столбцов SP_i для нахождения общего числа процессов поиска и устранения ВП в сети:

$$SP = SP_1 + SP_2 + \ldots + SP_K.$$

Шаг 5. Оценить время, необходимое системе защите информации на полное восстановление сети: $T=SP/C$, где C — постоянная скорость поиска и устранения ВП. Конец алгоритма.

Для наглядности произведем вычисления для сети, переходы в которой заданы следующей матрицей:

$$P = \begin{Vmatrix} 0.13 & 0.10 & 0.20 & 0.00 & 0.20 \\ 0.20 & 0.15 & 0.05 & 0.20 & 0.15 \\ 0.20 & 0.00 & 0.00 & 0.30 & 0.00 \\ 0.26 & 0.00 & 0.24 & 0.00 & 0.10 \\ 0.27 & 0.20 & 0.00 & 0.23 & 0.30 \end{Vmatrix},$$

а начальное число вредоносных пакетов, обнаруженных в каждом узле задано вектором-строкой V = (3, 5, 8, 4, 2).

Общее число процессов поиска и устранения ВП, которые необходимо запустить во узлах сети, определенное с помощью предложенного алгоритма, равно

$$SP = \begin{vmatrix} 4.766 & 0.962 & 1.230 & 0.953 & 1.704 \\ 3.681 & 7.003 & 1.707 & 2.585 & 2.922 \\ 4.074 & 0.918 & 9.707 & 3.524 & 1.864 \\ 2.554 & 0.675 & 1.751 & 5.027 & 1.593 \\ 2.066 & 1.159 & 0.799 & 1.366 & 3.891 \end{vmatrix} \begin{matrix} 9.615 \\ 17.898 \\ 20.087 \\ 11.600 \\ \overbrace{9.281} \\ 68.481 \end{matrix}$$

и целая часть этого числа есть искомая оценка (68).

Заключение

Анализ статистических данных позволил определить, что вредоносное программное обеспечение вместе с социальной инженерией наибольшее число раз используется злоумышленниками для атак на ресурсы корпоративных сетей передачи данных. В связи с этим была выбрана модель корпоративной сети, в которой происходит обработка как полезного, так и вредоносного трафика.

Для оценки характеристик адаптивной системы защиты информации, которая включает уровни обнаружения и противодействия, чьи объекты инициируются только после обнаружения информационных угроз, разработан алгоритм, базирующийся на теории сетей массового обслуживания. На практике его применение позволит определить общее число процессов поиска и устранения вредоносных пакетов в сети, а также время, необходимое СЗИ на полное восстановление сети.

ЛИТЕРАТУРА

1. Gruzdeva L. M. Model of adaptive information security system of a computer-based data transmission network // Cloud of Science. 2018. Vol. 5. № 3. P. 563–575.
2. Вишневский В. М. Теоретические основы проектирования компьютерных сетей.— М.: Техносфера, 2003.— 512 с.
3. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий: монография / под ред. П. П. Парамонова.— СПб: Изд-во ООО «Студия «НП-Принт», 2012.— 115 с.
4. Gruzdeva L.M., Monakhov M. Yu. Early detection algorithm for attacks against information resources of automatic manufacturing control systems//Automation and Remote Control. 2011. Vol.72. № 5. P. 1075–1079.
5. Груздева Л. М. Модель распределенной системы противодействия угрозам информационной безопасности в корпоративной сети // Математические методы в технике и технологиях: сб. тр. междунар. науч. конф.: в 12 т. Т. 4 / под общ. ред. А. А. Большакова.— СПб.: Изд-во Политехн. ун-та, 2018.— С. 129–132.
6. Актуальные киберугрозы: III квартал 2019 года [Электронный ресурс] // Positive Technologies: сайт.— URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q3/.
7. Актуальные киберугрозы — 2018: тренды и прогнозы [Электронный ресурс] // Positive Technologies: сайт.— URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/.
8. Актуальные киберугрозы — 2017: тренды и прогнозы [Электронный ресурс] // Positive Technologies: сайт.— URL: https://www.ptsecurity.com/ru-ru/research/analytics/.
9. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин.— М.: ДМК, 2014.— 702 с.
10. Клейнрок Л. Теория массового обслуживания / Л. Клейнрок.— М.: Книга по Требованию, 2013.— 429 с.
11. Абрамов К. Г. Модели угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях — Диссертация на соискание ученой степени к.т.н. Владим. Гос.ун-т.— Владимир: Изд-во Владим. Гос. Ун-та, 2014.

Журнал «Современная наука: актуальные проблемы теории и практики»