УДК 381.3

ФОРМАЛИЗАЦИЯ ЦЕННОСТИ НЕГАТИВНОЙ ИНФОРМАЦИИ В ВИДЕ УЩЕРБА, НАНЕСЁННОГО В РЕЗУЛЬТАТЕ СПАМ-АТАКИ НА УЗЕЛ СЕТИ

© 2020 В. В. Кабылин, Ю. П. Преображенский, О. Н. Чопоров

Министерство внутренних дел (Москва, Россия)
Воронежский институт высоких технологий (Воронеж, Россия)
Воронежский государственный технический университет (Воронеж, Россия)

В статье дается анализ возможности решения задачи противодействия СПАМ-атакам. Подобные задачи возникают в разных организациях, в которых эксплуатируются распределенные информационные сети.
Ключевые слова: спам-атака, защита информации, информационная безопасность.

Спам (англ. spam) – массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания ее получить, а также рассылка массовых сообщений [1].

В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем.

Рассмотрим подробнее отрицательный ресурс сети [2].

Для более точной оценки негативной части ресурса необходимо выражение представить в виде суммы произведений ценности информации и потока информации по каждому виду СПАМа, а именно «фишинга», СПАМ-атаки с вредоносными вложениями, мошеннический СПАМ и СПАМ-сообщения рекламного характера. При анализе СПАМ-атак с вредоносными вложениями выражение для негативного ресурса имеет вид: $Res\_(x_i) = C_{s_v}(x_i)V_{s_v}(x_i) + Res\_{}_o(x_i)$.

Величина ресурса зависит от двух значений: ценность и объем информации. Рассмотрим каждую из этих составляющих отдельно.

Ценность информации. В данном случае ценность негативная и будет, в первую очередь, зависеть от типа СПАМа. СПАМ, который несет в себе исключительно рекламные цели, будет обладать наименьшей негативной ценностью, а СПАМ, целью которого является нанесение ущерба жертве или же получение собственной выгоды, имеет наибольшую негативную ценность.

Кабылин Виталий Викторович – Министерство внутренних дел, специалист, ggroshev074@yandex.ru.
Преображенский Юрий Петрович – Воронежский институт высоких технологий, профессор, it_pro@vivt.ru.
Чопоров Олег Николаевич – Воронежский государственный технический университет, профессор, choporov_oleg@mail.ru.

Относительно математической оценки, сделаем допущение о том, что ценность информации может быть трактована как ущерб, нанесенный в результате успешной реализации СПАМ-атаки с вредоносным вложением на узел сети.

Объем негативной информации можно рассматривать как количество СПАМ-атак, успешно реализованных за определенный промежуток времени. Количество атак – случайная величина [3, 4].

В работах было доказано, что количество СМАП-атак с вредоносными вложениями имеет логнормальное распределение.

Однако анализ статистики показал, что в рассматриваемый промежуток времени можно выделить некоторую постоянную составляющую количества атак, определяющую ее минимальное значение. В результате, доказывается [5, 6], что случайная величина количества атак складывается из двух составляющих: постоянной величины n_{min} и собственно случайной составляющей n_{rand}.

Используя полученные данные, можно получить значение количества СПАМ-сообщений с вредоносными вложениями, которое поступает на узел сети. Для того, чтобы найти количество успешно реализованных атак, необходимо учитывать элементы системы защиты рассматриваемого узла.

В работе рассмотрены применяемые системы защиты [7, 8] от СПАМ-атак с вредоносными вложениями, а также критерии оценки их эффективности, которые выражаются в вероятности реализации атаки.

Ущерб рассмотрен в работах по СПАМ-атакам с вредоносным вложением при нерегулярном распределении ущерба и описывается выражением:

$$u_i(n) = u_{imin} + u_{ir}(n),$$
$$u_{imin} = n_{imin} \cdot \left(t_{imin} c_i + (t_{ir}\lambda_{iз} + \exp(-\lambda_{iз} t_{ir}) - 1)\right),$$
$$u_{ir}(n) = (n - n_{imin}) \cdot \left(t_{iо} \cdot c_i + \exp\left(-\lambda_{iи} \cdot (t_{iи} - t_{ir})\right) - \exp(-\lambda_{iз} t_{ir})\right),$$

где: u_i – ущерб от СПАМ-атак, u_{imin} – минимальный ущерб от СПАМ-атак, n_{imin} - минимальное количество СПАМ-атак, t_{imin} – минимальное время, затраченное на обработку пользователем СПАМ-сообщения, c_i – ценность единицы времени (у.е.), $\lambda_{iз}$ – интенсивность заражения вредоносного ПО, λ_{iu} – интенсивность лечения от вредоносного ПО, t_{ir} – период реакции системы на внедрение вредоносного ПО, $t_{iи}$ – момент времени лечения системы от вредоносного ПО, $t_{iо}$ – время, затраченное на обработку пользователем СПАМ-сообщения.

Отрицательный ресурс узла вершины сети будет определяться следующим выражением:

$$Res_{lay} = \sum_{i=0}^{n} Res_{+}(x_i) - Res\_(x_i)$$
$$= \sum_{i=0}^{n} Res_{+}(x_i) - - \left(t_{iо} \cdot c_i + \exp\left(-\lambda_{iи} \cdot (t_{iи} - t_{ir})\right) - \exp(-\lambda_{iз} t_{ir})\right) \cdot n_i^* \cdot p_{iantiv}$$
$$\cdot p_{iantis} \cdot p(l_i) - Res_{-o}(x_i).$$

В результате, получено выражение оценки ресурса слоя и ресурса отдельных узлов сети. Подобное представление позволяет произвести адекватную оценку состояния узла сети, а также производить управление ресурсом, используя параметры системы защиты.

Основная задача заключается в повышении общего ресурса узла. Для его увеличения необходимо снизить отрицательный ресурс [9, 10].

Проанализируем выражение на предмет изменяющихся величин:

$t_{iо}$ – величина времени, затраченного пользователем на обработку одного СПАМ-сообщения. Данное значение может быть подвержено изменению с помощью организационных мер.

В частности, информирование пользователей о наиболее характерных признаках СПАМ-сообщения, с целью уменьшения времени анализа его содержимого;

c_i – стоимость единицы времени. Данное значение определяется для каждого узла сети индивидуально и как таковому регулированию подвержено быть не может;

n_i^* – наиболее вероятное значение количества атак, направленных на узел сети. Данное значение определяется статистическими методами, поэтому для фиксации изменения этого параметра необходимо провести длительный эксперимент;

p_{iantiv} – вероятность срабатывания антивирусной системы защиты. Величина определяется статистически независимыми экспертами, зависит от конкретной системы защиты, используемой узлом сети. Изменение системы защиты влечет за собой и изменение этой величины [11, 12].

В качестве защиты от вредоносного программного обеспечения является одной из основополагающих технических мер;

p_{iantiv} – вероятность срабатывания анти СПАМ-фильтра. Величина оценивается аналогично антивирусным системам защиты;

$t_{ir}, \lambda_{iи}, t_{iи}$ – величины, характеризующие процесс излечения узла от деструктивного воздействия вредоносного ПО. Зависит от используемой системы защиты, поэтому может быть подвергнуто влиянию;

$\lambda_{iз}$ – интенсивность заражения. Это значение является характеристикой атакующей стороны, поэтому может быть принято за неизменяемую величину.

Таким образом, полученное выражение позволяет оценить текущий ресурс сети, а также его динамику путем отслеживания изменения величин, характеризующих систему защиты.

ЛИТЕРАТУРА

1. Выборнова О. Н. Система обнаружения вредоносного программного обеспечения на основе технологии машинного обучения / О. Н. Выборнова, И. А. Пидченко // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. – № 2 (29). – С. 42-43.

2. Космачева И. М. Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов / И. М. Космачева, Н. В. Давидюк, И. В. Сибикина, И. Ю. Кучин // Моделирование, оптимизация и информационные

технологии. – 2020. – Т. 8. – № 2 (29). – С. 40-41.

3. Львович Я. Е. Исследование методов оптимизации при проектировании систем радиосвязи / Я. Е. Львович, И. Я. Львович, А. П. Преображенский, С. О. Головинов // Теория и техника радиосвязи. – 2011. – № 1. – С. 5-9.

4. Львович Я. Е. Проблемы построения корпоративных информационных систем на основе web-сервисов / Я. Е. Львович, И. Я. Львович, Н. В. Волкова // Вестник Воронежского государственного технического университета. – 2011. – Т. 7. – № 6. – С. 8-10.

5. Чопоров О. Н. Анализ затухания радиоволн беспроводной связи внутри зданий на основе сравнения теоретических и экспериментальных данных / О. Н. Чопоров, А. П. Преображенский, А. А. Хромых // Информация и безопасность. – 2013. – Т. 16. – № 4. – С. 584-587.

6. Львович И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. – Т. 14. – № 3. – С. 469-470.

7. Преображенский Ю. П. Проблемы кодирования информации в каналах связи / Ю. П. Преображенский // Современные инновации в науке и технике. Сборник научных трудов 8-й Всероссийской научно-технической конференции с международным участием. Ответственный редактор А. А. Горохов. – 2018. – С. 180-182.

8. Мэн Ц. Анализ методов классификации 8нформации в интернете при решении задач информационного поиска / Ц. Мэн // Моделирование, оптимизация и информационные технологии. – 2016. – № 2 (13). – С. 19.

9. Львович И. Я. Разработка подсистемы САПР для проектирования средних характеристик рассеяния объектов / И. Я. Львович, А. П. Преображенский, К. Ю. Родионова // Фундаментальные исследования. –2013. – № 4-4. – С. 823-826.

10. Гвоздев В. Е. Информационная поддержка проактивного управления функциональной безопасностью компонентов киберфизических систем / В. Е. Гвоздев, М. Б. Гузаиров, О. Я. Бежаева, Р. Р. Курунова, Р. А. Насырова // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. № 2 (29). С. 36-37.

11. Подольцев В. В. Исследование вероятностных характеристик методов синхронизации ПСП: мажоритарного метода обработки синхронизирующей информации в мас протоколах множественного доступа и метода последовательной оценки Уорда / В. В. Подольцев, И. М. Ажмухамедов // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. – № 2 (29). – С. 37-38.

12. Токарев В. Л. Метод оценки уровня рисков безопасности узлов сети для повышения эффективности размещения иммунных детекторов / В. Л. Токарев, А. А. Сычугов // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. – № 2 (29). – С. 39-40.

FORMALIZATION OF THE VALUE OF NEGATIVE INFORMATION IN THE FORM OF DAMAGE AS A RESULT OF A SPAM ATTACK ON A NETWORK NODE

© 2020 V. V. Kabylin, Yu. P. Preobrazhenskiy, O. N. Choporov

Ministry of Internal Affair (Moscow, Russia)
Voronezh Institute of High Technologies (Voronezh, Russia)
Voronezh State Technical University (Voronezh, Russia)

The article analyzes the possibility of solving the problem of countering SPAM attacks. Similar tasks arise in different organizations that operate distributed information networks.

Keywords: spam attack, information protection, information security.