УДК 004.056.5:004.7

ПРОВЕДЕНИЕ ИНФОРМАЦИОННОЙ АТАКИ НА ЛОКАЛЬНУЮ ИНФОРМАЦИОННУЮ СЕТЬ

ЦЫМБАЛОВ А. Д., ГРИНКЕВИЧ А. В.

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

E-mail: grimjoy66@gmail.com

Аннотация. В работе рассмотрен один из сценариев проведения информационной атаки, такой, как сканирование ЛИС на всем диапазоне сети класса С для получения информации об организации сети, системе защиты информации, обнаружения уязвимостей.

Abstract. This paper considers one of the scenarios for conducting an information attack, such as scanning a LIC over the entire range of a class C network to obtain information about the network organization, information security system, and vulnerability detection.

В работе рассмотрен один из сценариев проведения информационной атаки, такой, как сканирование ЛИС на всем диапазоне сети класса *С* для получения информации об организации сети, системе защиты информации, обнаружения уязвимостей.

В качестве атакуемой ЛИС примем усредненные значения, полученные при проведении анализа на 5 разных ЛИС, результаты сканирования представлены в таблице *1*.

Таблица 1. Результаты анализа безопасности ЛИС

Результаты опыта / **ЛИС**	**Диапазон сканирования ЛИС СПО**	**Кол-во обнаруженных ресурсов ЛИС**	**Количество обнаруженных уязвимостей**	**Кол-во удачно эксплуатированных уязвимостей**
Сеть № 1	256 хостов	49	5	3
Сеть № 2	256 хостов	59	6	4
Сеть № 3	256 хостов	55	4	4
Сеть № 4	256 хостов	53	4	3
Сеть № 5	256 хостов	48	3	3
Итого	1280	264	22	17
Ср. значение	256	52,8≈53	4,4≈4	3,4≈3

Предположим что в начальный момент времени $P_z = 1$, а $P_a = 0$. Представим

$$\mathrm{P_z} = 1 - \mathrm{P_{ia}} = 1 - \sum_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{N} \times \mathrm{P_s} \times \mathrm{P_u}. \quad (1)$$

где P_z – вероятность работоспособности ЛИС;
P_s – вероятность найти хотя бы одну уязвимость в ЛИС, которую можно эксплуатировать;
P_u – вероятность что обнаруженные уязвимости будут удачно эксплуатированы СПО;
P_{ia} – вероятность проведения удачной информационной атаки на ресурсы ЛИС;
N – диапазон адресов поиска уязвимости;
P_s– рассчитываем по формуле локальной теоремы Муавра-Лапласа.

$$\mathrm{P_s} = \mathrm{P_n(m)} \approx \frac{1}{\sqrt{\mathrm{n \times p \times q}}} \times \varphi(\mathrm{x}) = \frac{1}{\sqrt{\mathrm{n \times p \times q}}} \times \varphi\left(\frac{\mathrm{m - n \times p}}{\sqrt{\mathrm{n \times p \times q}}}\right). \quad (2)$$

где m – количество ресурсов на которых обнаружена уязвимость, примем ранее высчитанное усредненное значение m = 4;
n – диапазон сканирования ресурсов сети, n = 256;

p – вероятность того, что на сканируемом диапазоне будет обнаружена хотя бы одна уязвимость которую можно эксплуатировать

$$p = \frac{m}{n} = \frac{17}{256} \approx 0{,}0664. \quad (3)$$

q – вероятность того, что не будет обнаружена хотя бы одна уязвимость, которую можно использовать на диапазоне сканирования ЛИС

$$q = 1 - p \approx 0{,}934. \quad (4)$$

P_u рассчитываем по формуле Бернулли

$$P_u = C_n^m \times p^n \times q^{n-m}, \quad (5)$$

где m – количество ресурсов на которых обнаружена уязвимость, примем ранее высчитанное усредненное значение m = 4;

n – диапазон сканирования ресурсов сети, n = 256;

p – вероятность того, что выявленную уязвимость получиться эксплуатировать p = 0,5;

q – вероятность того, что выявленную уязвимость не получиться эксплуатировать q = 1-p = 0,5.

Проведем расчеты для нашей усредненной сети для определения изменений зависимости P_z от количества ресурсов ЛИС при проведении атаки. Результаты расчета представлены в табл. *2*.

Таблица *2*. Зависимости P_z от количества определенных сетевых ресурсов ЛИС

Кол-во рес-ов ЛИС / ***P***	**3**	**5**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
P_s	0,0008	0,0042	0,0317	0,054	0,0863	0,1295	0,1826	0,242	0,3011	0,3485
P_u	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,75
P_z	0,9995	0,9960	0,9522	0,9085	0,8375	0,7318	0,5874	0,4077	0,2064	0,0158

Изобразим зависимость вероятности работоспособности (неудачи НСД) ЛИС от количества верно определенных ресурсов при сканировании на рис. 1.

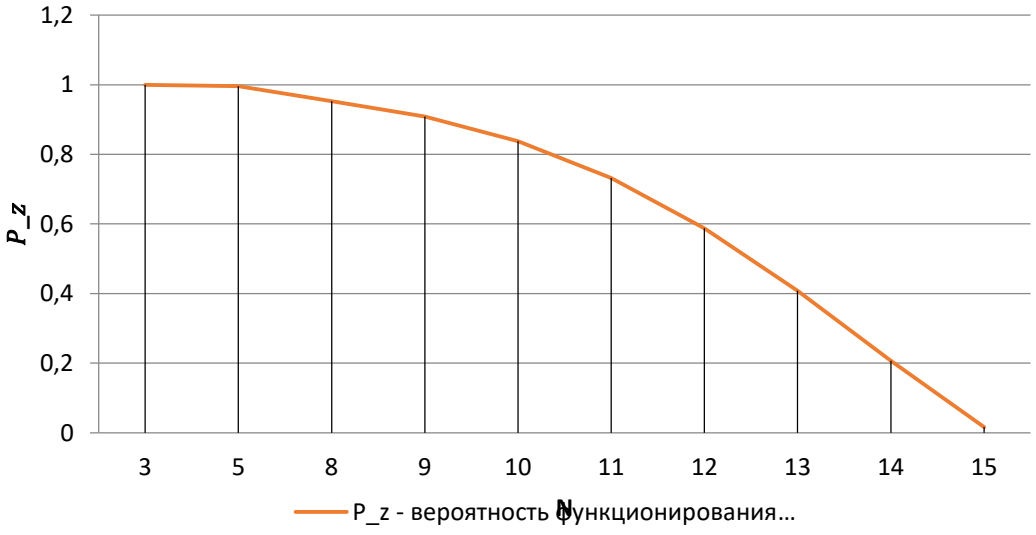

Рис. 1. Зависимость P_z от количества верно определенных ресурсов

Заключение

Анализ полученных результатов (рис. 1) показал, что вероятность удачного использования обнаруженной уязвимости P_u колеблется возле постоянной величины равной 0,75 соответственно с ростом обнаруженных уязвимостей вероятность проведения удачной информационной атаки увеличивается, а вероятность работоспособности ЛИС уменьшается и становиться практически равной нулю при 15 верно определенных хостах, что является 28% от общего количества хостов ЛИС. Проведя анализ формул по которым проводился расчет, можно сделать вывод, что для уменьшения эффективности информационной атаки необходимо влиять на следующие параметры:

1 Количество верно обнаруженных хостов сети и определенных на них уязвимостей;
2 Вероятность верного определения параметров хостов и реально существующих уязвимостей;
3 Вероятность успешной эксплуатации выявленной уязвимости.

Список использованных источников

1. Вентцель, Е. С. Теория вероятностей: 7-е изд. / Е. С. Вентцель. – М.: Высшая школа, 2001. – 575 с.
2. Андрончик, А.Н. Защита информации в компьютерных сетях практический курс / Андрончик, А.Н.,УГТУ-УПИ, 2008. – 248 с.