Широкий А.А.

Метод экспресс-оценки рисков компьютерной сети с топологией «звезда»

Аннотация: При решении задач выбора оптимального набора мер для обеспечения безопасности компьютерных сетей влияние их топологии на итоговый уровень безопасности (или же интегральный риск) обычно не рассматривается. В предшествующих работах был предложен алгоритм проектирования минимизирующей риск топологии компьютерной сети и представлено частное решение для топологии «шина». В настоящей работе предлагается метод экспресс-оценки рисков компьютерной сети с топологией «звезда».

Ключевые слова: управление рисками, оценка рисков, интегральный риск, компьютерные сети, топология сети

Стандартным подходом к оценке информационного риска является определение тем или иным методом рисков конфиденциальности, целостности и доступности информации [1]. Концептуально такой подход вполне показал свою работоспособность. При этом вопрос о получении количественных оценок как уровня самого риска, так и результативности предпринимаемых контрмер он не затрагивает в силу высокого уровня абстракции.

При попытке реализовать стандарт на практике, специалист по информационной безопасности имеет дело с вполне конкретными информационными системами, характеризующимися спецификой применяемых программно-аппаратных средств, а также внутренними связями между ними, образующими сложные взаимодействующие между собой гетерогенные структуры. Базовой структурой при этом является топология компьютерной сети, внутри которой развернута защищаемая информационная система.

Несмотря на это, возможность повышения безопасности системы через изменение топологии сети рассматривается крайне редко. Более того, за рамками внимания исследователей остается даже вопрос о степени ее влияния на риск защищаемой системы.

Например, в обзорах [2-3], посвящённых информационной безопасности программно-определяемых сетей, риски, связанные с физической топологией, обсуждаются лишь в смысле возможности её выявления злоумышленником. При этом встречаются ссылки на работы, где вмешательство в топологию рассматривается как атака [4], но не как мера защиты.

В обзоре [5] упоминается сравнительно давнее исследование [6], посвящённое моделям киберстрахования, где топология сети подробно рассматривается как важный атрибут при моделировании особенностей киберриска. Авторы при этом отметили, что хотя топология сети может быть использована в рыночных моделях путем определения процесса возникновения рисков, в литературе подобный подход не представлен. Судя по [5], к 2021 году ситуация не изменилась.

В настоящей работе представлен алгоритм экспресс-оценки интегрального риска компьютерной сети с топологией «звезда». Показана зависимость поведения верхней и нижней оценок риска в зависимости от числа лучей.

1. Обозначения и определения

Предположим, что компьютерная сеть включает в себя n узлов $s_1, \dots, s_n \in S$, $n \in \mathbb{N}$. Предположим также, что каждому узлу поставлены в соответствие два числа:

$p_i^0 \in (0,1]$ – удельная вероятность успешной атаки -го узла;

$u_i > 0, u \in \mathbb{R}^+$ – ущерб, который будет нанесён, если -й узел будет успешно атакован.

Определение 1. Удельный риск -го узла определяется следующей величиной:

$$\rho_{s_i}^0 = u_i p_i^0. \quad (1)$$

Зададим топологию сети $W = \langle G(V,E), T \rangle, T \subseteq V$, где $G(V,E)$ – граф со множеством вершин V и множеством рёбер E, а T – подмножество V, называемое периметром. Как правило, соединение компьютерной сети с внешней сетью осуществляется через центральный узел, поэтому в данной работе будем считать, что периметр включает в себя одну-единственную вершину v_0.

Определение 2. Топологией «звезда с m лучами» будем называть такую структуру $W_m = \langle G(V,E), T\rangle$, что:

$$V = \left\{ v_0 \cup \bigcup_{b=1}^{m} \bigcup_{l=1}^{l_b} \{v_{bl}\} \right\},$$
$$E = \left\{ \bigcup_{b=1}^{m} \left\{ (v_0, v_{b1}) \cup \bigcup_{l=2}^{l_b} \left(v_{b(l-1)}, v_{bl}\right) \right\} \right\}, \quad (2)$$
$$T = \{v_0\}.$$

Здесь $l_b \in \mathbb{N}$ – число вершин в -м луче, представляющем собой простую цепь с началом в вершине v_{b1}. Для всех таких вершин периметр v_0 является смежной вершиной. В общем случае l_b не ограничены.

Определение 3. Если для топологии $W_m = \langle G(V,E), T\rangle$ существует взаимно-однозначное отображение $M: V \to S$, то будем называть его отображением топологии W_m на множество узлов S.

Определение 4. Взаимно-однозначное отображение $M^{-1}: S \to V$, обратное ранее определённому отображению $M: V \to S$, будем называть размещением узлов S в топологии W_m.

В настоящей работе мы рассматриваем случай, когда нам неизвестны точные значения ущерба при успешной атаке того или иного узла, поэтому далее будем считать, что $u_1 = u_2 = \ldots = u_n = u$.

Определение 5. Локальным риском узла защищаемой сети, отображённого в вершину v_{bl} топологии W_m, будем называть величину:

$$\rho_{M(v_{bl})} = u_{M(v_{bl})} \prod_{v \in \langle v_0, v_{bl}\rangle} p_{M(v)}, \quad (3)$$

где $\langle v_0, v_{bl}\rangle$ – простой путь, соединяющий вершину-периметр v_0 с вершиной v_{bl}. Локальный риск узла, отображённого в вершину v_0, равен его удельному локальному риску. Отметим, что в

рассматриваемом случае простой путь существует и является единственным.

Определение 6. Интегральным риском компьютерной сети со множеством узлов S и топологией W_m, расположение которых определено взаимно-однозначным отображением $M^{-1}: S \to W_m$, будем называть величину:

$$\rho(S, W_m, M^{-1}) = \rho_{M(v_0)} + \sum_{b=1}^{m} \sum_{l=1}^{l_b} \rho_{M(v_{bl})}. \quad (4)$$

Для оценки влияния топологии компьютерной сети на её интегральный риск сформулируем следующую постановку задачи. Пусть защищаемая компьютерная сеть включает в себя множество узлов $S = \{s_1, s_2, \ldots, s_n\}, n \in \mathbb{N}$ с соответствующими им вероятностями успешной атаки $P = \{p_{s_1}, p_{s_2}, \ldots, p_{s_n}\}$ и ущербами $U = \{u_{s_1}, u_{s_2}, \ldots, u_{s_n}\}$. Предположим, что задана топология типа «звезда с m лучами» $W_m = \langle G(V, E), T \rangle$, причём $\sum_{b=1}^{m} l_b = n - 1$. Тогда задача построения минимизирующей риск топологии компьютерной сети состоит в поиске такого размещения узлов S в топологии W_m, что:

$$\rho(S, W_m, M^{-1}) \to \min. \quad (5)$$

Для частного случая $m = 1$ решение в общем виде приведено в работе [7]. Для $m = 2$ в работе [8] были найдены решения задачи (5) с верхними оценками максимальной погрешности. Далее будет предложен метод быстрой оценки интегрального риска компьютерной сети в зависимости от её топологии.

2. Метод экспресс-оценки рисков компьютерных сетей с топологией «звезда»

Вначале введём ещё два дополнительных определения.

Определение 7. Предельно допустимым удельным локальным риском узла компьютерной сети с топологией $W_m = \langle G(V, E), T \rangle$ будем считать величину:

$$\rho_{max}^{0} = u \cdot p_{max} = \frac{u}{1+\sqrt{m}}. \quad (6)$$

Содержательная интерпретация величины (6) подробно обсуждается в [8].

Определение 8. Остаточным удельным риском компьютерной сети, включающей в себя $n \in \mathbb{N}$ *узлов* $s_1, \ldots, s_n \in S$ будем называть величину:

$$\rho_{min}^{0} = u \cdot p_{min} : p_{s_i}^{0} \geq p_{min} \; \forall i \in 1, \ldots, n. \quad (7)$$

Рассмотрим компьютерную сеть, включающую в себя множество узлов S и имеющую топологию W_m. Предположим, что нам неизвестны ни удельные вероятности успешной атаки каждого из узлов, ни значения ущерба, наносимого злоумышленником в случае успешной атаки какого-либо узла. В то же время, будем считать, что нам известны величины p_{min} и p_{max}, $0 < p_{min} < \frac{1}{1+\sqrt{m}}$, $0 < p_{max} \leq \frac{1}{1+\sqrt{m}}$, причём:

$$p_{min} \leq p_i^0 \leq p_{max} \;\; \forall i = 1, 2, \ldots, n, n \in \mathbb{N}. \quad (8)$$

Тогда при $m = 1$ оценка интегрального риска ρ_1 данной сети будет иметь следующий вид:

$$\rho_1^- = u \sum_{l=1}^{n} (p_{min})^l \leq \rho_1 \leq u \sum_{l=1}^{n} (p_{max})^l = \rho_1^+, \quad (9)$$

где u – некоторая оценка «среднего» ущерба. Заметим, что эти суммы будут конечны даже для сети со счётным множеством узлов при условии, что $p_{max} \leq \frac{1}{1+\sqrt{m}} \leq \frac{1}{2}$.

Предположим теперь, что топология рассматриваемой компьютерной сети имеет два луча с примерно одинаковыми длинами l_1 и l_2, то есть $n - 1 \leq l_1 + l_2 \leq n$. Тогда величину интегрального риска ρ_2 такой сети можно оценить снизу и сверху через p_{min} и p_{max} соответственно. Запишем вначале выражение для нижней оценки:

$$\rho_2^- = u\left(p_{min} + 2p_{min} \cdot \sum_{l=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} (p_{min})^l + p_{min}\left(n - 1 - 2\left\lfloor \frac{n-1}{2} \right\rfloor\right)(p_{min})^{\left\lfloor \frac{n}{2} \right\rfloor} \right) = u\left(p_{min} + 2\sum_{l=2}^{\left\lfloor \frac{n}{2} \right\rfloor} (p_{min})^l + \left(n - 1 - 2\left\lfloor \frac{n-1}{2} \right\rfloor\right)(p_{min})^{\left\lfloor \frac{n}{2} \right\rfloor + 1} \right). \quad (10)$$

Запись $\lfloor n \rfloor$ здесь и далее означает выделение целой части числа n. Величина $n - 1 - 2\left\lfloor \frac{n-1}{2} \right\rfloor$ будет равна нулю для нечётных n и 1 – для чётных. При этом в первом случае мы получим два луча одинаковой длины, а во втором их длины будут отличаться на единицу. Запись выражения для верхней оценки будет такой же с точностью до замены p_{min} на p_{max}.

Теперь запишем выражение для нижней оценки интегрального риска сети с топологией, включающей в себя произвольное конечное число лучей m:

$$\rho_m^- = u\left(p_{min} + m\sum_{l=2}^{\left\lfloor\frac{n-1}{m}\right\rfloor+1}(p_{min})^l + \left(n-1-m\left\lfloor\frac{n-1}{m}\right\rfloor\right)(p_{min})^{\left\lfloor\frac{n-1}{m}\right\rfloor+2}\right). \quad (11)$$

Посмотрим, насколько изменяется оценка (11) при увеличении числа лучей до $(m+1)$. Для этого запишем выражение для нижней оценки интегрального риска при новой топологии сети:

$$\begin{aligned}\rho_{m+1}^- &= u\left(p_{min} + (m+1)\sum_{l=2}^{\left\lfloor\frac{n-1}{m+1}\right\rfloor+1}(p_{min})^l + \left(n-1-(m+1)\left\lfloor\frac{n-1}{m+1}\right\rfloor\right)(p_{min})^{\left\lfloor\frac{n-1}{m+1}\right\rfloor+2}\right)\\ &= u\left(p_{min} + m\sum_{l=2}^{\left\lfloor\frac{n-1}{m+1}\right\rfloor+1}(p_{min})^l + \sum_{l=2}^{\left\lfloor\frac{n-1}{m+1}\right\rfloor+1}(p_{min})^l + \left(n-1-(m+1)\left\lfloor\frac{n-1}{m+1}\right\rfloor\right)(p_{min})^{\left\lfloor\frac{n-1}{m+1}\right\rfloor+2}\right).\end{aligned} \quad (12)$$

Оценка величины $|\rho_{m+1}^{-} - \rho_{m}^{-}|$ подробно обсуждается в [8]. Здесь лишь отметим, что верхние и нижние оценки интегрального риска компьютерной сети монотонно возрастают с ростом числа лучей в её топологии. Заметив, что:

$$\forall z = \text{const}, l > 1 \; (p_{min})^{l} - (p_{min})^{l+z} \leq \leq (p_{max})^{l} - (p_{max})^{l+z}, \tag{13}$$

получаем, что величина $\rho_{m}^{+} - \rho_{m}^{-}$ при $p_{min} < p_{max}$ также монотонно возрастает с ростом m. При $p_{min} = p_{max}$ достигается равенство верхней и нижней оценок.

Таким образом, чем больше лучей включает в себя топология компьютерной сети, тем сложнее построить оценку её интегрального риска. Это хорошо согласуется с полученными в работе [8] приближёнными решениями задачи оптимального размещения элементов сложной системы в заданной структуре. Дальнейшее развитие результатов видится в их обобщении на случай сетей более сложных топологий – в первую очередь, древовидных, – где можно выбирать, к какому концентратору подключить новый узел (или множество новых узлов) с тем, чтобы интегральный риск компьютерной сети возрастал минимально.

Заключение

Предлагаемая работа является частью исследования, посвящённого изучению влияния структуры сложной системы на её интегральный риск. Применительно к информационным системам и, в частности, компьютерным сетям, полученные результаты могут быть использованы для решения задач управления рисками как при проектировании топологии новой сети, так и при эксплуатации уже существующих сетей.

В настоящей работе представлен алгоритм быстрой оценки интегрального риска компьютерной сети с довольно часто встречающейся на практике звездообразной топологии. Показано, что увеличение числа лучей увеличивает разницу между верхней и нижней оценками и, как следствие, усложняет проведение оценки.

В сочетании с ранее полученными решениями задачи рационального размещения элементов сложной системы в звездообразной структуре, полученный результат формирует задел

для изучения влияния топологии на риск компьютерных сетей более сложных топологий.

Литература:

1. ISO/IEC 27005:2022(en) Information security, cybersecurity and privacy protection – Guidance on managing information security risks. – URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en. (дата обращения 13.05.2024).

2. *Deb R., Roy S.* A comprehensive survey of vulnerability and information security in SDN // Computer Networks. – 2022. – Vol. 206. – e108802.

3. *Priyadarsini M., Bera P.* Software defined networking architecture, traffic management, security, and placement: A survey // Computer Networks. – 2021. – Vol. 192. – e108047.

4. *Skowyra R., Xu L., Gu G., Dedhia V., Hobson T., Okhravi H., Landry J.* Effective topology tampering attacks and defenses in software-defined networks / 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Luxembourg, June 2018. – 2018. – P. 374-385.

5. *Eling M., McShane M., Nguyen T.* Cyber risk management: History and future research directions // Risk Management and Insurance Review. – 2021. – Vol. 24(1). – P. 93-125.

6. *Böhme R., Schwartz G.* Modeling cyber-insurance: towards a unifying framework / Workshop on the Economics of Information Security (WEIS), June 2010. – Cambridge, MA, USA, 2010. – P. 1-36.

7. *Shiroky A., Kalashnikov A.* Mathematical problems of managing the risks of complex systems under targeted attacks with known structures // Mathematics. – 2021. – Vol. 9(19). – e2468.

8. *Shiroky A., Kalashnikov A.* Influence of the Internal Structure on the Integral Risk of a Complex System on the Example of the Risk Minimization Problem in a “Star” Type Structure // Mathematics. – 2023. – Vol. 11(4). – e998.