Математические структуры и моделирование 2020. № 2(54). С. 129–144

УДК 004.056 : 519.217
DOI 10.24147/2222-8772.2020.2.129-144

ПРИМЕНЕНИЕ ОДНОЙ МАРКОВСКОЙ МОДЕЛИ КИБЕРАТАК ДЛЯ ОЦЕНКИ МЕТРИК БЕЗОПАСНОСТИ

А.А. Касенов
магистрант, e-mail: kassenov_adil@mail.ru
А.А. Магазев
д. ф.-м. н. профессор, e-mail: magazev@omgtu.ru
Е.В. Трапезников
старший преподаватель, e-mail: evtrapeznikov@yandex.ru

Омский государственный технический университет, Омск, Россия

Аннотация. В настоящей работе представлено описание одной марковской модели кибератак, с помощью которой сконструированы две метрики безопасности. Даётся алгоритм оценки входных параметров модели на основе ограниченного числа эмпирических данных. Приводится пример, иллюстрирующий применение предложенных метрик безопасности.

Ключевые слова: метрика безопасности, модель кибератак, марковская цепь.

Введение

В настоящее время *метрики безопасности* представляют собой удобный инструмент для количественной оценки достаточности и эффективности мер по обеспечению информационной безопасности. Регулярный мониторинг метрик безопасности позволяет своевременно обнаруживать недостатки систем защиты информации и вовремя принимать меры по их устранению. В то же время выбор той или иной метрики — далеко не тривиальная задача, решение которой во-многом зависит от специфики рассматриваемой защищаемой информационной системы. Возможно поэтому на сегодняшний день существует довольно большое число различных метрик безопасности, часть из которых даже закреплена в российских и зарубежных стандартах.

При разработке метрик безопасности чаще всего основываются на различных *моделях безопасности*. При таком подходе, метрики — это фактически некоторые функции от параметров выбранной модели. В подобном контексте чаще всего используются различные теоретико-вероятностные модели, основанные на применении математического аппарата теории вероятностей и случайных процессов [1, 2].

Среди теоретико-вероятностных моделей безопасности особую роль играют модели, построенные с применением положений теории марковских процессов, что, по-видимому, связано с чрезвычайно широким спектром их применимости (см., например, [3–5]). Так, в работе [6] была предложена модель кибератак,

сформулированная на языке марковских цепей с дискретным временем. Важной особенностью этой модели является возможность её строгого аналитического исследования, что было осуществлено в работе [7]. В дальнейшем эта модель была существенно модифицирована [8], а также с её помощью удалось сформулировать оптимизационную задачу выбора средств защиты информации [9, 10].

В настоящей работе предлагаются две новые метрики безопасности, конструкция которых основана на модели кибератак, предложенной в [6]. Это так называемые *среднее время до отказа безопасности* и *средний риск при отказе безопасности*. В статье мы приводим строгие определения этих метрик, а также получаем явные аналитические формулы для их вычисления. Кроме того, в статье также обсуждается проблема получения входных параметров данной модели, в частности мы описываем оригинальный алгоритм их оценки с применением общей системы оценки уязвимостей CVSS. В заключении работы рассматривается пример гипотетической локальной сети организации, в рамках которого проводится оценка входных параметров, а также осуществляются вычисление и анализ предложенных нами двух метрик безопасности.

1. Описание марковской модели кибератак

Рассмотрим модель компьютерной системы, в соответствии с которой последняя может находиться в $2n+1$ состояниях $S_0, S_1, \ldots, S_{2n}$. Состояние S_0, называемое *безопасным*, означает отсутствие каких-либо кибератак на систему. Состояние S_i, где $i = 1, \ldots, n$, отвечает появлению i-ой кибератаки, а соответствующее ему состояние S_{n+i}, называемое *i-ым финальным состоянием*, символизирует её успешное завершение с последующими негативными последствиями для компьютерной системы.

Естественно считать, в начальный момент времени $t = 0$ система находится в безопасном состоянии S_0, а все переходы между состояниями системы могут происходить только в строго определённые промежутки времени $t = 1, 2, \ldots$ (дискретное время). Мы также принимаем возможность только следующих переходов:

- если в момент t система находится в состоянии S_0, в следующий момент $t+1$ с вероятностью q_i она может оказаться в состоянии S_i или с вероятностью $q_0 \equiv 1 - \sum_{i=1}^{n} q_i$ останется в том же состоянии S_0;

- если в момент t система находится в одном из состояний S_i, где $i = 1, \ldots, n$, то в следующий момент $t+1$ она с вероятностью r_i может перейти в состояние S_0 (кибератака отражена), остаться в том же состоянии S_i с вероятностью d_i (кибератака продолжается) или перейти в i-ое финальное состояние S_{n+i} с вероятностью $\tilde{r}_i = 1 - r_i - d_i$ (кибератака успешно осуществилась);

- оказавшись в момент t в одном из финальных состояний S_{n+i}, система будет оставаться в нём бесконечно долго.

В соответствии со сделанными предположениями состояние системы в каждый момент времени определяется только её состоянием в предыдущий момент времени. Это означает, что последовательность состояний системы представляет собой простую марковскую цепь, граф переходов которой изображен на рис. 1. Таким образом, входными параметрами нашей модели компьютерной системы являются три n-мерных вектора: вектор вероятностей появления кибератак $\mathbf{q} = (q_1, \ldots, q_n)$, вектор вероятностей их отражений $\mathbf{r} = (r_1, \ldots, r_n)$ и вектор вероятностей задержки кибератак $\mathbf{d} = (d_1, \ldots, d_n)$. По своему смыслу компоненты этих векторов являются неотрицательными вещественными числами, удовлетворяющими следующим ограничениям:

$$\sum_{i=1}^{n} q_i \leqslant 1 \quad \text{и} \quad d_i + r_i \leqslant 1 \text{ для всех } i = 1, \ldots, n. \tag{1}$$

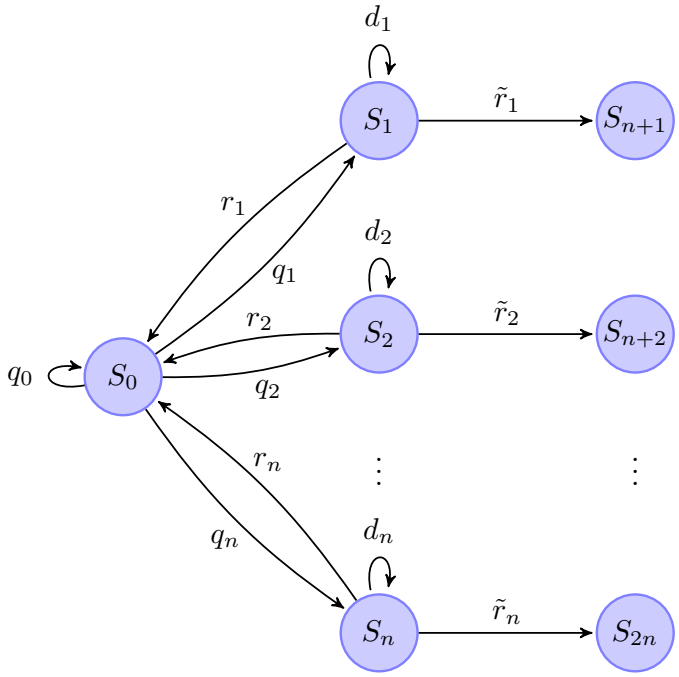

Рис. 1. Граф переходов марковской цепи

Полное описание марковской цепи заключается в вычислении вероятностей её состояний в произвольный момент времени t. Обозначим через $p_i(t)$ вероятность i-го состояния цепи в момент t, а через $\mathbf{p}(t) = (p_0(t), \ldots, p_{2n}(t))$ — вектор всех таких вероятностей. Из общей теории марковских цепей хорошо известно, что вектор $\mathbf{p}(t)$ может быть рассчитан в соответствии с матричной формулой

$$\mathbf{p}(t) = \mathbf{p}(0) \cdot \Pi^t, \tag{2}$$

где Π — *матрица переходных вероятностей* марковской цепи, которая в на-

шем случае имеет вид (см. рис. 1):

$$\Pi = \begin{pmatrix} q_0 & q_1 & q_2 & \dots & 0 & 0 & 0 & \dots & 0 \\ r_1 & d_1 & 0 & \dots & 0 & \tilde{r}_1 & 0 & \dots & 0 \\ r_2 & 0 & d_2 & \dots & 0 & 0 & \tilde{r}_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ r_n & 0 & 0 & \dots & d_n & 0 & 0 & \dots & \tilde{r}_n \\ 0 & 0 & 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}. \tag{3}$$

К сожалению, в общем случае вывод явных аналитических формул для вероятностей $p_i(t)$ затруднён ввиду вычислительных трудностей, связанных с возведением Π в произвольную степень t. Однако в некоторых частных ситуациях подобные формулы могут быть получены. Рассмотрим два таких случая.

1. Случай отсутствия защиты: $r_i = 0$, $i = 1, \dots, n$. В этом случае вероятности состояний системы как функции t имеют вид:

$$p_0(t) = q_0^t, \quad p_i(t) = q_i \frac{q_0^t - d_i^t}{q_0 - d_i}, \tag{4}$$

$$p_{n+i}(t) = q_i \frac{(1-q_0)(d_i^t - 1) - (1-d_i)(q_0^t - 1)}{(1-q_0)(q_0 - d_i)}, \quad i = 1, \dots, n. \tag{5}$$

2. Случай отсутствия задержек атак: $d_i = 0$, $i = 1, \dots, n$. При данном ограничении получаем

$$p_0(t) = \frac{1}{w}\left(\lambda_+^{t+1} - \lambda_-^{t+1}\right), \tag{6}$$

$$p_i(t) = \frac{q_i}{w}\left(\lambda_+^t - \lambda_-^t\right), \quad p_{n+i}(t) = \frac{(1-r_i)q_i}{w}\left(\frac{1-\lambda_+^t}{1-\lambda_+} - \frac{1-\lambda_-^t}{1-\lambda_-}\right), \quad i = 1, \dots, n, \tag{7}$$

где $\lambda_\pm = (q_0 \pm w)/2$, $w = \left(q_0 + 4\sum_{i=1}^n q_i r_i\right)^{1/2}$.

Нетрудно проверить, что формулы (4) и (5) при $d_i \to 0$ совпадают с формулами (6) и (7) при $r_i \to 0$.

Несложный анализ приведённых формул показывает, что в обеих частных ситуациях имеют место предельные соотношения

$$\lim_{t\to\infty} p_0(t) = \lim_{t\to\infty} p_1(t) = \dots = \lim_{t\to\infty} p_n(t) = 0,$$

то есть на больших временах вероятности обнаружить систему в состояниях $S_0, \dots, S_n$ являются бесконечно малыми величинами. Для остальных состояний в случае 1 получаем

$$\lim p_{n+i}(t) = \frac{q_i}{1-q_0}, \quad i = 1, \dots, n,$$

а в случае 2 имеем

$$\lim p_{n+i}(t) = \frac{(1-r_i)q_i}{(1-\lambda_+)(1-\lambda_-)}, \quad i = 1, \ldots, n,$$

то есть предельные вероятности для совокупности финальных состояний $S_{n+1}, \ldots, S_{2n}$ распределяются в зависимости от значений исходных параметров модели.

Возвращаясь к общему случаю, следует отметить, что, не смотря на отсутствие здесь для $p_i(t)$ явных аналитических формул, качественное описание динамики соответствующей марковской цепи выглядит относительно просто (см. рис. 1). Находясь в момент $t = 0$ в безопасном состоянии S_0, система в последующие случайные моменты времени будет подвергаться атакам, отражение которых имеющейся системой защиты будет осуществляться с определённой долей успеха. Таким образом, рано или поздно система окажется в одном из поглощающих состояний $S_{n+1}, \ldots, S_{2n}$, что будет означать отказ безопасности вследствие соответствующей кибератаки.

2. Две метрики безопасности

2.1. Среднее время до отказа безопасности

Напомним некоторую терминологию. Состояние S_i марковской цепи называется *поглощающим*, если, попав в это состояние, марковская цепь не сможет его покинуть. Соответственно, марковская цепь называется *поглощающей*, если из каждого её состояния можно достичь поглощающего состояния. Состояние S_i называется *переходным*, если с вероятностью 1 марковская цепь посетит это состояние только конечное число раз. Очевидно, что марковская цепь с матрицей переходных вероятностей (3) является поглощающей. При этом состояния $S_0, S_1, \ldots, S_n$ для нее являются переходными, а состояния $S_{n+1}, \ldots, S_n$ — поглощающими.

Обозначим через Q подматрицу в матрице переходных вероятностей (3), содержащую только строки и столбцы, соответствующие переходным состояниям:

$$Q = \begin{pmatrix} q_0 & q_1 & q_2 & \ldots & 0 \\ r_1 & d_1 & 0 & \ldots & 0 \\ r_2 & 0 & d_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_n & 0 & 0 & \ldots & d_n \end{pmatrix}. \tag{8}$$

Данную матрицу будем называть *матрицей переходных состояний*. Таким образом, матрица переходных вероятностей Π всей марковской цепи имеет блочный вид

$$\Pi = \begin{pmatrix} Q & R \\ 0 & I \end{pmatrix}, \tag{9}$$

где Q — матрица переходных состояний (8), R — так называемая *матрица поглощающих состояний*, I — единичная $n \times n$-матрица.

В силу того что марковская цепь с матрицей переходных вероятностей (3) является поглощающей, вероятность попадания в какое-либо поглощающее состояние равна единице. Таким образом, мы имеем

$$Q^t \to 0 \text{ при } t \to \infty.$$

Отсюда следует, что модули всех собственных чисел матрицы Q строго меньше единицы. Это значит, что матрица $I - Q$ невырожденна и мы можем вычислить её обратную матрицу:

$$A \equiv (Q - I)^{-1} = I + Q + Q^2 + Q^3 + \dots. \tag{10}$$

Матрица A называется фундаментальной матрицей поглощающей марковской цепи [11]. Важное значение матрицы A объясняется следующим фактом: если в начальный момент времени марковская цепь стартует из состояния S_j, то среднее число раз, которое она посетит состояние S_i, равно A_{ij}.

Пусть марковская цепь с матрицей переходных вероятностей (3) стартует из состояния S_0. Тогда *временем до отказа безопасности* будем называть число T переходов между состояниями в марковской цепи до её первого попадания в одно из поглощающих состояний S_{n+i}, $i = 1, \dots, n$. Ясно, что T является случайной величиной с некоторым законом распределения. Из указанных выше фактов о матрице (10) следует, что среднее время до отказа безопасности $\tau = \langle T \rangle$ будет равно сумме элементов первой строки матрицы A:

$$\tau = \sum_{j=1}^{n+1} A_{1j}.$$

После некоторых вычислений можно показать, что эта величина выражается следующей формулой:

$$\tau = \frac{\prod\limits_{j=1}^{n}(1 - d_j) + \sum\limits_{i=1}^{n} q_i \prod\limits_{j=1}^{n} [1 - (1 - \delta_{ij}) d_j]}{\sum\limits_{i=1}^{n} q_i \prod\limits_{j=1}^{n} (1 - \delta_{ij} r_j - d_j)}, \tag{11}$$

где δ_{ij} — символ Кронеккера. Ясно, что в заданном пространстве потенциальных кибератак с фиксированными вероятностями q_i среднее время до отказа безопасности представляет собой функцию $2n$ переменных $\mathbf{r} = (r_1, \dots, r_n)$ и $\mathbf{d} = (d_1, \dots, d_n)$, непрерывную на всей области их определения. Нетрудно видеть, что множество возможных значений величины $\langle \tau \rangle$ есть полуотрезок $[\tau_{\min}, +\infty)$, где $\tau_{\min}$ — среднее время до отказа безопасности в случае, когда все d_i и r_i равны нулю:

$$\tau_{\min} = 1 + \left(\sum_{i=1}^{n} q_i \right)^{-1}. \tag{12}$$

2.2. Средний риск при отказе безопасности

Допустим, что при реализации i-ой атаки ущерб, нанесённый системе, составляет U_i условных единиц. Если вероятность реализоваться данной атаке равна P_i, то мы можем оценить связанный с этим событием *риск*: $R_i = P_i U_i$. *Средний риск*, связанный с отказом безопасности системы, это величина

$$R = \sum_{i=1}^{n} P_i U_i.$$

Получим явную формулу для вычисления среднего риска, выраженную через исходные параметры марковской цепи.

Нетрудно видеть, что t-ая степень блочной матрицы (9) имеет вид

$$\Pi^t = \begin{pmatrix} Q^t & \left(\sum\limits_{k=0}^{t-1} Q^k\right) R \\ 0 & I \end{pmatrix}.$$

Как уже отмечалось, абсолютные значения собственных чисел матрицы Q строго меньше единицы, поэтому при $t \to \infty$ получаем

$$Q^t \to 0 \quad \text{и} \quad \sum_{k=0}^{t} Q^k \to A,$$

где $A \equiv (I - Q)^{-1}$ — фундаментальная матрица марковской цепи. Таким образом, предел матрицы Π^t при $t \to \infty$ записывается как

$$\lim_{t\to\infty} \Pi^t = \begin{pmatrix} 0 & AR \\ 0 & I \end{pmatrix}.$$

Так как марковская цепь в начальный момент времени $t = 0$ находится в состоянии S_0, для предельных вероятностей $P_i = \lim\limits_{t\to\infty} p_{n+i}(t)$, где $i = 1, \ldots, n$, получаем

$$P_i = \frac{q_i \prod\limits_{j=1}^{n} (1 - \delta_{ij} r_j - d_j)}{\sum\limits_{k=1}^{n} q_k \prod\limits_{j=1}^{n} (1 - \delta_{kj} r_j - d_j)}.$$

Отсюда для среднего риска R получаем выражение

$$R = \frac{\sum\limits_{i=1}^{n} q_i U_i \prod\limits_{j=1}^{n} (1 - \delta_{ij} r_j - d_j)}{\sum\limits_{k=1}^{n} q_k \prod\limits_{j=1}^{n} (1 - \delta_{kj} r_j - d_j)}. \tag{13}$$

Таким образом, основываясь на марковской модели кибератак, описанной в разделе 1, мы предложили две метрики безопасности — среднее время до отказа безопасности (11) и средний риск при отказе безопасности (13). Обе эти метрики вычисляются через исходные параметры модели: векторы $\mathbf{q}$, $\mathbf{d}$ и $\mathbf{r}$.

3. Оценка параметров модели

Для вычисления предложенных метрик безопасности требуется знать величины исходных параметров модели. Этими параметрами являются:

- вектор вероятностей возникновения кибератак $\mathbf{q} = (q_1, \ldots, q_n)$;
- вектор вероятностей отражений кибератак $\mathbf{r} = (r_1, \ldots, r_n)$;
- вектор вероятностей задержки кибератак $\mathbf{d} = (d_1, \ldots, d_n)$;
- вектор ущербов от кибератак: $\mathbf{U} = (U_1, \ldots, U_n)$.

Кроме того, требуется явно указать временной интервал Δt, который задаёт минимальное время, по истечении которого компьютерная система может изменить своё состояние (такт времени). В соответствии с этим все требуемые вероятности должны быть отнесены к данному временному интервалу; например, величина q_i задаёт вероятность возникновения i-ой кибератаки в течение промежутка времени Δt. Таким образом, нам фактически требуется задать $4n + 1$ исходных параметров нашей модели, где n — количество рассматриваемых видов кибератак. Можно, однако, немного снизить число свободных параметров, если учесть, что всякая кибератака осуществляется с помощью эксплуатации некоторой уязвимости, присутствующей в системе, и использовать для оценки вероятностей появления кибератак общую систему оценки уязвимостей CVSS.

Допустим, что в результате предварительного анализа рассматриваемой компьютерной системы было обнаружено m незакрытых уязвимостей. Считая, что каждая уязвимость может быть задействована для реализации *только одной* кибератаки, для обозначения a-ой уязвимости, приводящей к i-ой кибератаке, мы будем использовать нотацию $V_{a,i}$. Здесь $a = 1, 2, \ldots, m_i$, $i = 1, 2, \ldots, n$, причём $m_1 + m_2 + \cdots + m_n = m$. Обозначим $v_{a,i}$ значение базовой CVSS-метрики для уязвимости $V_{a,i}$. Разумно предположить, что вероятность q_i возникновения i-ой кибератаки является некоторой функцией от этих метрик, причём эта вероятность тем больше, чем больше суммарная доля CVSS-метрик для уязвимостей, приводящих к данной атаке, по отношению к общей сумме всех CVSS-метрик всех уязвимостей системы. Таким образом, в линейном приближении мы можем записать

$$q_i = \alpha \cdot k_i, \tag{14}$$

где α — некоторый положительный коэффициент, а величины k_i определяются как

$$k_i = \frac{\sum_{a=1}^{m_i} v_{a,i}}{\sum_{j=1}^{n} \sum_{b=1}^{m_j} v_{j,b}}, \quad i = 1, \ldots, n. \tag{15}$$

Предположим также, что и вероятность успешного отражения i-ой кибератаки пропорциональна числу k_i. Так как в рамках нашей марковской модели эта вероятность равна $r_i/(1 - d_i)$, мы имеем

$$r_i = \beta \cdot k_i(1 - d_i), \tag{16}$$

где β_i — ещё один положительный коэффициент.

С учётом формул (14) и (16), а также условия нормировки $\sum_{i=1}^{n} k_i = 1$, для метрик безопасности (11) и (13) получаем следующие выражения:

$$\tau = \frac{1/\alpha + \sum_{i=1}^{n} k_i/(1-d_i)}{1 - \beta \sum_{i=1}^{n} k_i^2}, \quad R = \frac{\sum_{i=1}^{n} k_i U_i (1 - \beta k_i)}{1 - \beta \sum_{j=1}^{n} k_j^2}. \tag{17}$$

Интересно отметить, что в подобном приближении метрика R не зависит от параметров α и d_i.

Оценка параметров α и β, а также d_i возможна, например, с помощью экспертных оценок или на основе некоторой заранее накопленной статистики о данной системе. Рассмотрим более подробно последний вариант. Допустим, что за достаточно длительное время наблюдения за системой нам удалось собрать следующие эмпирические данные:

- среднее время до очередной кибератаки $T^*_{\text{ат}}$ (в единицах Δt);
- средняя длительность i-ой кибератаки с момента её начала до момента отражения или успешной реализации θ^*_i (в единицах Δt);
- доля успешно отражённых кибератак $p^*_{\text{отр}}$.

Эти же параметры могут быть вычислены теоретически с помощью нашей марковской модели; соответствующие оценки имеют вид:

$$T_{\text{ат}} = \frac{1}{\sum_{i=1}^{n} q_i}, \quad \theta_i = \frac{1}{1-d_i}, \quad p_{\text{отр}} = \frac{\sum_{i=1}^{n} q_i r_i/(1-d_i)}{\sum_{i=1}^{n} q_i}.$$

Подставляя в эти формулы равенства (14) и (16), получаем оценки для величин α, β и d_i:

$$\alpha \approx \frac{1}{T^*_{\text{ат}}}, \quad \beta \approx \frac{p^*_{\text{отр}}}{\sum_{i=1}^{n} k_i^2}, \quad d_i \approx 1 - \frac{1}{\theta^*_i}.$$

Отсюда для метрик безопасности (17) получаем следующие оценки

$$\tau \approx \frac{T^*_{\text{ат}} + \sum_{i=1}^{n} k_i \theta^*_i}{1 - p^*_{\text{отр}}}, \quad R \approx \frac{1}{1 - p^*_{\text{отр}}} \left(\sum_{i=1}^{n} k_i U_i - p^*_{\text{отр}} \frac{\sum_{i=1}^{n} k_i^2 U_i}{\sum_{i=1}^{n} k_i^2} \right). \tag{18}$$

Важно отметить, что в силу ограничений (1) у нас имеется следующее условие применимости принятого приближения:

$$p^*_{\text{отр}} \lesssim \min_i \left\{ \frac{\sum_{j=1}^{n} k_j^2}{k_i} \right\}. \tag{19}$$

Наконец, оценка параметров U_i, характеризующих степень влияния кибератак на систему с точки зрения возможного ущерба, может быть проведена исключительно экспертными методами.

4. Пример

Рассмотрим гипотетическую локальную сеть организации с набором серверов, коммутационного оборудования, рабочих станций и программного обеспечения. Так как большинство современных кибератак возникают извне через глобальную сеть Интернет, мы предполагаем, что наша локальная сеть к ней подключена. Также будем предполагать, что в сети циркулирует конфиденциальная информация, хранящаяся и обрабатываемая некоторой базой данных на основе MySQL. Для взаимодействия с базой данных имеется веб-сервер.

В связи с тем, что пример носит гипотетический характер, предположим, что злоумышленник будет пытаться получить необходимую информацию о топологии сети, серверах, рабочих станциях, операционных системах, учётных данных пользователя и т. д. Эта информация будет призвана помочь ему обнаружить уязвимости сети как программные, так и технические, причём часть уязвимостей может быть известна, и для них могут быть или отсутствовать средства защиты.

Для конкретизации мы допустим, что в случае описанной нами локальной сети возможны только три типа кибератак: *переполнение буфера*, *SQL-инъекция* и *анализ сетевого трафика*. (Конечно, в реальных ситуациях их число гораздо больше, однако для наших иллюстративных целей этих трёх будет достаточно.) В частности отметим, что возможность анализа сетевого трафика может возникнуть как изнутри системы, так и в виде попытки анализа трафика, исходящего из системы. Мы также предположим, что атака «анализ сетевого трафика» может возникнуть из-за уязвимости получения удалённого доступа к рабочей машине внутри сети.

Допустим, в результате анализа системы мы пришли к выводу, что к названным трём кибератакам может привести эксплуатация следующих незакрытых уязвимостей системы.

1. Переполнение буфера:
   (a) `CVE-2019-8166`: переполнение буфера в Adobe Acrobat и Reader;
   (b) `CVE-2019-5871`: переполнение буфера динамической памяти в Skia в Google Chrome;
   (c) `CVE-2019-5439`: переполнение буфера в VLC Media Player;
   (d) `CVE-2020-7450`: переполнение буфера в FreeBSD;
   (e) `CVE-2018-3932`: переполнение буфера в Microsoft Word.
2. SQL-инъекция:
   (a) `CVE-2020-5504`: в phpMyAdmin существует возможность SQL-инъекции на странице учётных записей пользователей;
   (b) `CVE-2019-10752`: все Sequelize до версий 4.44.3 и 5.15.1 уязвимы для SQL-инъекций;

(c) CVE-2018-18476: mysql-binuuid-rails 1.1.0 и более ранние версии позволяют осуществить SQL-инъекцию;

(d) CVE-2020-10802: в phpMyAdmin 4.x версий до 4.9.5 и версий 5.x до 5.0.2 была открыта возможность SQL-инъекции при поисковых запросах;

(e) CVE-2019-9083: SQLiteManager версий 1.20 и 1.24 позволяет осуществить SQL-инъекцию через '/sqlitemanager/main.php?dbsel' параметр.

3. Анализ сетевого трафика:

(a) CVE-2020-0612: уязвимость отказа в обслуживании в шлюзе удалённых рабочих столов Windows;

(b) CVE-2020-0610: в удалённом настольном шлюзе Windows (шлюз удалённых рабочих столов) существует уязвимость удалённого выполнения кода;

(c) CVE-2019-9510: уязвимость в системе Microsoft Windows 10 позволяет клиентам, подключённым по протоколу RDP, получать доступ к сеансам пользователя без необходимости взаимодействия с экраном блокировки Windows;

(d) CVE-2017-7406: устройство D-Link DIR-615 не использует SSL для страниц, прошедших проверку подлинности;

(e) CVE-2015-2476: WebDAV клиент в Microsoft Windows поддерживает SSL 2.0, что делает его пригодным для обхода криптографических механизмов защиты от перехвата сети.

В таблице 1 приведены значения $v_{i,a}$ базовых CVSS-метрик для указанных уязвимостей. Используя эти значения для коэффициентов k_i в соответствии с формулой (15), получаем:

$$k_1 = 0.3331, \quad k_2 = 0.3910, \quad k_3 = 0.2764.$$

Для дальнейших оценок необходимо определить характерный для системы временной интервал Δt, по истечении которого система может изменять своё состояние (временной масштаб). В нашем случае положим его равным суткам: $\Delta t = 1$ сут. Кроме того, мы допустим, что либо в результате опроса экспертов, либо имея некоторую статистику, мы выяснили, что средние продолжительности θ_i^* наших трёх типов кибератак, а также оценки соответствующих ущербов U_i равны:

$$\theta_1^* = 1.0 \text{ сут.}, \quad \theta_2^* = 2.5 \text{ сут.}, \quad \theta_3^* = 4.0 \text{ сут.}.$$

$$U_1 = 0.2, \quad U_2 = 0.6, \quad U_3 = 0.2.$$

Подставляя данные величины, а также значения коэффициентов k_i в формулы (18), получаем для метрик безопасности выражения, являющиеся функциями

Таблица 1. Базовые CVSS-метрики существующих уязвимостей

Кибератака	**Уязвимость**	**Базовая CVSS-метрика** $v_{a,i}$
Переполнение буфера	CVE-2019-8166	8.8
	CVE-2019-5871	8.8
	CVE-2019-5439	6.5
	CVE-2020-7450	7.5
	CVE-2018-3932	7.8
SQL-инъекция	CVE-2020-5504	8.8
	CVE-2019-10752	9.8
	CVE-2018-18476	9.8
	CVE-2020-10802	8.0
	CVE-2019-9083	9.8
Анализ трафика	CVE-2020-0612	7.5
	CVE-2020-0610	9.8
	CVE-2019-9510	7.8
	CVE-2017-7406	5.0
	CVE-2015-2476	2.6

от $T^*_{\text{ат}}$ и $p^*_{\text{отр}}$:

$$\tau \approx \frac{2.4151 + T^*_{\text{ат}}}{1 - p^*_{\text{отр}}}, \quad R \approx \frac{0.3562 - 0.3795\, p^*_{\text{отр}}}{1 - p^*_{\text{отр}}}.$$

В соответствии с (19) условие применимости данных оценок имеет вид

$$p^*_{\text{отр}} \lesssim p^*_{\max} = 0.8702.$$

На рис. 2 приведены несколько графиков функции $\tau = \tau(p^*_{\text{отр}})$ при различных значениях параметра $T^*_{\text{ат}}$. Видно, что при увеличении $T^*_{\text{ат}}$ среднее время до отказа безопасности увеличивается, так как увеличивается средний интервал между кибератаками. Время τ также быстро растёт с увеличением $p^*_{\text{отр}}$: эффективность системы защиты приводит к удлинению среднего промежутка времени до отказа безопасности. Зависимость $\tau = \tau(p^*_{\text{отр}})$ может быть использована на практике для установления минимального порогового значения $p^*_{\text{отр}}$, при котором метрика τ не будет меньшей заранее фиксированной величины τ_0. В нашем случае будем иметь

$$p^*_{\text{отр}} \geqslant 1 - \frac{T^*_{\text{ат}} + 2.4152}{\tau_0}.$$

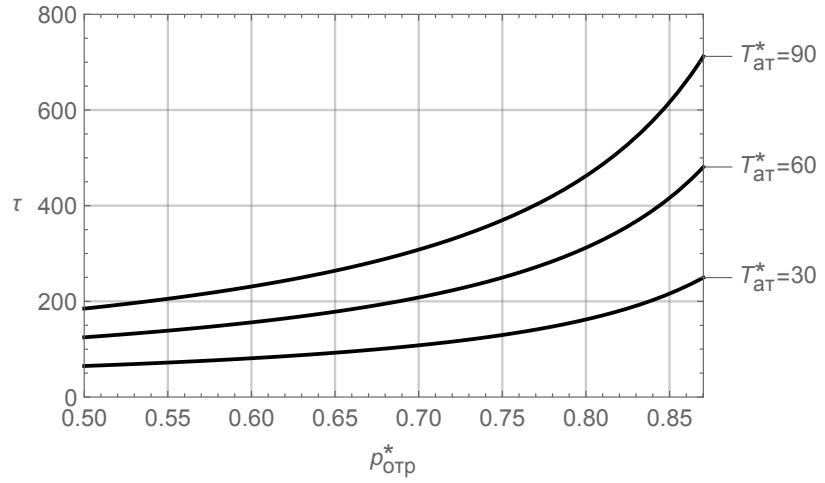

Рис. 2. Графики функции $\tau(p^*_{\text{отр}})$ на интервале $[0.5, p^*_{\max}]$ при различных значениях $T^*_{\text{ат}}$.

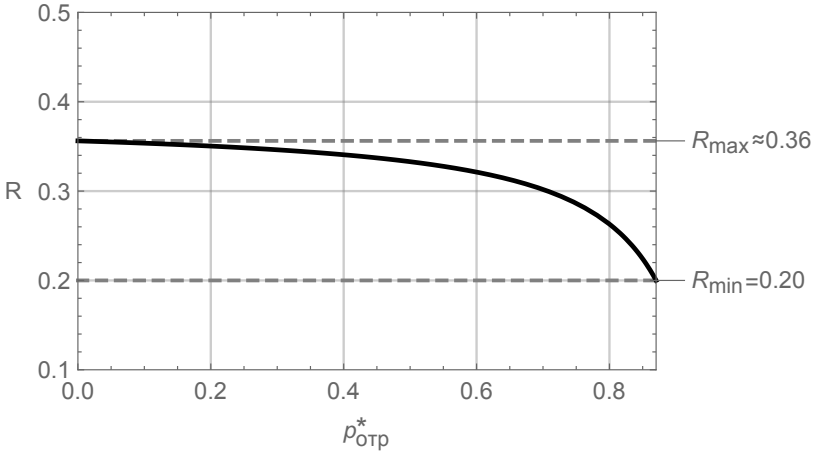

Рис. 3. График функции $R(p^*_{\text{отр}})$ на интервале $[0.5, p^*_{\max}]$.

При этом, если мы хотим, чтобы значение метрики τ было большим, чем $\tau_0 = 200$ суток, то необходимо, чтобы $p^*_{\text{отр}}$ была не менее, чем $0.9879 - 0.005 \cdot T^*_{\text{ат}}$. Например, при $T^*_{\text{ат}} = 30$ должно быть $p^*_{\text{отр}} \geqslant 0.8379$, а при $T^*_{\text{ат}} = 60$ получаем $p^*_{\text{отр}} \geqslant 0.6879$.

На рис. 3 изображена зависимость метрики R от $p^*_{\text{отр}}$ (напомним, что от параметра $T^*_{\text{ат}}$ эта метрика не зависит). Как видно из графика, своё максимальное значение $R_{\max} \approx 0.3562$ риск принимает при $p^*_{\text{отр}} = 0$, в то время как при $p^*_{\text{отр}} = p_{\max} \approx 0.8702$ риск минимален: $R = R_{\min} = 0.2$. Так же, как и в случае с предыдущей метрикой, мы можем определить пороговый уровень R_0 среднего риска, связанного с отказом безопасности системы, и подбирать параметры эффективности системы защиты от кибератак исходя из условия $R \geqslant R_0$:

$$p^*_{\text{отр}} \geqslant \frac{R_0 - 0.3562}{R_0 - 0.3795}.$$

Например, при $R_0 = 0.3$ должно быть $p^*_{\text{отр}} \geqslant 0.707$.

Заключение

В настоящей статье мы описали две метрики безопасности, основанные на модели кибератак, предложенной в работе [6]. Мы также показали, что с помощью применения общей системы уязвимостей CVSS параметры данной модели могут быть эффективно оценены на основе малого числа эмпирических данных, что является несомненным преимуществом по сравнению, например, с методом экспертных оценок. Конечно, рассмотренная нами модель кибератак имеет ряд допущений, связанных, в частности, с невозможностью одновременного появления нескольких кибератак, а также с их независимостью друг от друга. Дальнейшая наша работа будет направлена на ослабление данных допущений и получение более комплексной и обобщённой модели, динамика которой будет максимально приближена к поведению реальных компьютерных систем.

Литература

1. Wang A.J.A. Information security models and metrics // Proceedings of the 43rd annual Southeast regional conference. 2005. V. 2. P. 178–184.
2. Purboyo T.W. et al. Security metrics: A brief survey // 2011 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering. IEEE. 2011. P. 79–82.
3. Almasizadeh J., Azgomi M.A. A stochastic model of attack process for the evaluation of security metrics : Towards a Science of Cyber Security // Computer Networks. 2013. V. 57(10). P. 2159–2180.
4. Lalropuia K.C., Gupta V. Modeling cyber-physical attacks based on stochastic game and Markov processes // Reliability Engineering & System Safety. 2019. V. 181. P. 28–37.
5. Lei C. et al. Incomplete information Markov game theoretic approach to strategy generation for moving target defense // Computer Communications. 2018. V. 116. P. 184–199.
6. Росенко А.П., Бордак И.В. Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения // Известия ЮФУ. Технические науки. 2015. № 7(168). С. 6–19.
7. Magazev A.A., Tsyrulnik V.F. Investigation of a Markov model for computer system security threats // Automatic Control and Computer Sciences. 2018. V. 52, No. 7. P. 615–624.
8. Касенов А.А., Магазев А.А., Цырульник В.Ф. Марковская модель совместных киберугроз и её применение для выбора оптимального набора средств защиты информации // Моделирование и анализ информационных систем. 2020. № 27(1). С. 108–123.
9. Magazev A.A. and Tsyrulnik V.F. Optimizing the selection of information security remedies in terms of a Markov security model // Journal of Physics: Conference Series. 2018. V. 1096. P. 012–160.

10. Kasenov A.A., Kustov E.F., Magazev A.A., Tsyrulnik V.F. A Markov model for optimization of information security remedies // Journal of Physics: Conference Series. 2020. V. 1441. P. 012–043.
11. Феллер В. Введение в теорию вероятностей и её приложения. В 2-х томах. Т. 1. М. : Мир, 1984. 528 с.

USING A MARKOV CYBERATTACK MODEL FOR EVALUATION OF SECURITY METRICS

A.A. Kassenov
Undergraduate, e-mail: kassenov_adil@mail.ru
A.A. Magazev
Dr.Sc. (Phys.), Professor, e-mail: magazev@omgtu.ru
E.V. Trapeznikov
Senior Lecturer, e-mail: evtrapeznikov@yandex.ru

Omsk State Technical University, Omsk, Russia

Abstract. This paper presents a description of a Markov model of cyberattacks by which two security metrics are constructed. An algorithm is given for estimating the input parameters of the model based on a limited number of empirical data. An example that illustrates the use of the proposed security metrics is considered.

Keywords: security metric, cyberattack model, Markov chain.

References

1. Wang A.J.A. Information security models and metrics. Proceedings of the 43rd annual Southeast regional conference, 2005, vol. 2, pp. 178–184.
2. Purboyo T.W. et al. Security metrics: A brief survey. 2011 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering, IEEE, 2011, pp. 79–82.
3. Almasizadeh J. and Azgomi M.A. A stochastic model of attack process for the evaluation of security metrics : Towards a Science of Cyber Security. Computer Networks, 2013, vol. 57(10), pp. 2159–2180.
4. Lalropuia K.C. and Gupta V. Modeling cyber-physical attacks based on stochastic game and Markov processes. Reliability Engineering & System Safety, 2019, vol. 181, pp. 28–37.
5. Lei C. et al. Incomplete information Markov game theoretic approach to strategy generation for moving target defense. Computer Communications, 2018, vol. 116, pp. 184–199.
6. Rosenko A.P. and Bordak I.V. Matematicheskaya model' opredeleniya veroyatnosti posledstvii ot realizatsii zloumyshlennikom ugroz bezopasnosti informatsii ogranichennogo rasprostraneniya. Izvestiya YuFU, Tekhnicheskie nauki, 2015, no. 7(168), pp. 6–19. (in Russian)

7. Magazev A.A. and Tsyrulnik V.F. Investigation of a Markov model for computer system security threats. Automatic Control and Computer Sciences, 2018, vol. 52, no. 7, pp. 615–624.
8. Kasenov A.A., Magazev A.A., and Tsyrul'nik V.F. Markovskaya model' sovmestnykh kiberugroz i ee primenenie dlya vybora optimal'nogo nabora sredstv zashchity informatsii. Modelirovanie i analiz informatsionnykh sistem, 2020, no. 27(1), pp. 108–123. (in Russian)
9. Magazev A.A. and Tsyrulnik V.F. Optimizing the selection of information security remedies in terms of a Markov security model. Journal of Physics: Conference Series, 2018, vol. 1096, pp. 012–160.
10. Kasenov A.A., Kustov E.F., Magazev A.A., and Tsyrulnik V.F. A Markov model for optimization of information security remedies. Journal of Physics: Conference Series, 2020, vol. 1441, pp. 012–043.
11. Feller V. Vvedenie v teoriyu veroyatnostei i ee prilozheniya. V 2-kh tomakh, vol. 1, Moscow, Mir Publ., 1984, 528 p. (in Russian)

Дата поступления в редакцию: 29.07.2020