О малых возмущениях марковских моделей киберугроз

А.А. Магазев[1], В.Ф. Цырульник[1]

[1]Омский государственный технический университет, пр. Мира 11, Омск, Россия, 644050

Аннотация. В настоящей работе мы рассматриваем стохастическое моделирование киберугроз, действующих на компьютерные системы, основанное на использовании марковских цепей. В рамках данного подхода компьютерные системы рассматриваются как системы с отказами и восстанавлениями по аналогии с моделями технических систем в теории надежности. При предположении, что в различные моменты времени киберугрозы являются независимыми случайными событиями, мы выводим явные аналитические формулы для вероятностей состояний соответствующей марковской цепи и для среднего времени до отказа безопасности. Затем мы исследуем случай зависимых кибеугроз и вычисляем приближенные выражения для вероятностей состояний и среднего времени до отказа безопасности в рамках теории возмущений первого порядка. В качестве иллюстрации наших результатов мы рассматриваем несколько простых примеров.

1. Введение

Разработка и совершенствование современных систем защиты информации — это трудоемкий и сложный процесс, многие этапы которого до сих пор опираются не на какие-либо обоснованные научные принципы, а на профессиональный опыт специалистов. Во многом это связано с тем, что каждая защищаемая информационная система по-своему уникальна, что вкупе с большим многообразием используемых современных информационных технологий затрудняет построение единых унифицированных подходов к построению систем кибербезопасности. Однако, не смотря на существующие методологические трудности, внимание специалистов к теоретическим исследованиям в области защиты информации неуклонно растет, а спектр применяемых при этом математических моделей постоянно расширяется. Повышенный интерес при этом вызывают теоретико-вероятностные модели безопасности, а в особенности, модели, основанные на применении марковских процессов [1, 2, 3, 4].

В работе [5] была предложена модель киберугроз, формулируемая в терминах марковских цепей с дискретным временем. В данной модели компьютерная система, подвергающаяся воздействию киберугроз, описывается как система с отказами и восстанавлениями, по аналогии с моделями технических систем в теории надежности. В статьях [6, 7] авторы более подробно исследовали указанную модель, указав возможность ее использования для оценки эффективности и оптимизации используемых средств защиты информации.

Настоящая статья продолжает указанные исследования, обобщая исходную модель на случай, когда киберугрозы в различные моменты времени являются зависимыми случайными событиями. В частности, считая взаимные порождения одних киберугроз другими редкими случайными событиями, мы разрабатываем соответствующую теорию

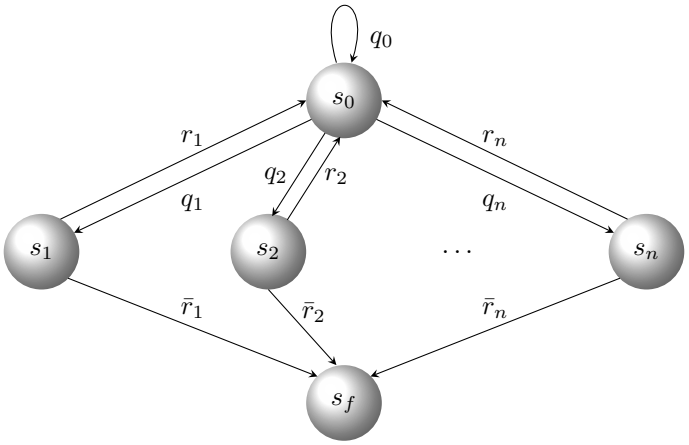


Рисунок 1. Диаграмма состояний системы

возмущений соответствующих марковских цепей. На основе этой теории возмущений мы получаем приближенные аналитические формулы для вероятностей состояний марковской цепи и для среднего времени до отказа безопасности. В заключении статьи приводится несколько примеров, иллюстрирующих полученные результаты.

2. Описание исходной модели киберугроз

В настоящем разделе мы напомним основные положения исходной марковской модели киберугроз и некоторые связанные с ней результаты, следуя работам [5, 6, 7].

Рассмотрим компьютерную систему (далее просто систему), на которую действует n независимых киберугроз. Примем следующие допущения.

1. Киберугрозы действуют на систему только в дискретные моменты времени: $t = 1, 2, \dots$.
2. В каждый момент времени может действовать только одна киберугроза.
3. Если в некоторый момент времени t действует одна из киберугроз, тогда в следующий момент времени $t + 1$ система пытается ее отразить.

В соответствие со сделанными допущениями мы можем полагать, что в произвольный момент времени система находится в одном из состояний $s_0, s_1, \dots, s_n, s_f$. В состоянии s_0, называемым *безопасным*, никакие киберугрозы не действуют. В случае, когда реализуется i-ая киберугроза, система осуществляет переход из состояния s_0 в состояние s_i, где $i = 1, 2, \dots, n$. Если система в данный момент времени t находится в состоянии s_i, тогда в момент времени $t + 1$ имеется две альтернативы:

- i-ая киберугроза устраняется с вероятностью r_i и система возвращается в состояние s_0;
- i-ая киберугроза не устраняется с вероятностью $\bar{r}_i \equiv 1 - r_i$ и система переходит в финальное состояние s_f, означающее *отказ безопасности*.

Ясно, что вероятность каждого состояния в произвольный момент времени зависит только от состояния, достигнутого в предыдущий момент времени. Это означает, что последовательность возможных состояний системы представляет собой простую марковскую цепь, диаграмма которой изображена на рисунке 1.

Динамика системы описывается в терминах величин $p_i(t)$, которые являются вероятностями состояний s_i в момент времени t. Эти вероятности могут быть вычислены

по формуле

$$p_i(t+1) = \sum_{j=0}^{n+1} p_j(t)\pi_{ji}, \tag{1}$$

где π_{ji} представляет собой вероятность перехода из состояния s_j в состояние s_i. Набор величин π_{ji} образует матрицу переходов Π, которая в нашем случае имеет вид

$$\Pi = \begin{pmatrix} q_0 & q_1 & q_2 & \dots & q_n & 0 \\ r_1 & 0 & 0 & \dots & 0 & \bar{r}_1 \\ r_2 & 0 & 0 & \dots & 0 & \bar{r}_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ r_n & 0 & 0 & \dots & 0 & \bar{r}_n \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \tag{2}$$

Здесь мы ввели обозначение $q_0 \equiv 1 - \sum_{i=1}^{n} q_i$. Естественно также предположить, что в начальный момент времени $t = 0$ система находится в безопасном состоянии:

$$p_0(0) = 1, \quad p_1(0) = \dots = p_n(0) = p_f(0) = 0. \tag{3}$$

Равенство (1) вместе с начальными условиями (3) однозначно определяет вероятности состояний системы в любой момент времени t.

Из (1) и (2) можно получить для вероятности $p_0(t)$ следующее линейное однородное рекуррентное соотношение 2-го порядка:

$$p_0(t) = p_0(t-1)q_0 + p_0(t-2)\sum_{i=1}^{n} r_i q_i.$$

Из общей теории линейных рекуррентных последовательностей известно, что явное выражение для $p_0(t)$ в этом случае имеет вид

$$p_0(t) = c_1\lambda_1^t + c_2\lambda_2^t,$$

где λ_1 и λ_2 — корни характеристического полинома $f(\lambda) = \lambda^2 - q_0\lambda - \sum_i q_i r_i$, а постоянные c_1 и c_2 определяются с помощью начальных условий $p_0(0) = 1$ и $p_0(1) = q_0$. Таким образом, получаем

$$p_0(t) = w^{-1}\left[\left(\frac{q_0 + w}{2}\right)^{t+1} - \left(\frac{q_0 - w}{2}\right)^{t+1}\right], \tag{4}$$

где $w^2 = q_0^2 + 4\sum_{i=1}^{n} q_i r_i$. Вероятности остальных состояний вычисляются через вероятность $p_0(t)$:

$$p_i(t) = q_i p_0(t-1), \quad i = 1, \dots, n; \quad p_f(t) = 1 - p_0(t) - p_0(t-1)\sum_{i=1}^{n} q_i. \tag{5}$$

Важнейшей характеристикой системы, отражающей эффективность работы защитных механизмов, является *время до отказа безопасности*, то есть число T переходов в соответствующей марковской цепи до первого достижения финального состояния s_f. Ясно, что T является дискретной случайной величиной, принимающей бесконечный ряд значений: $T = 2, 3, \dots$. Закон распределения $P(T)$ этой случайной величины может быть найден с использованием формулы (4):

$$P(T) = w^{-1}\left[\left(\frac{q_0 + w}{2}\right)^{T-1} - \left(\frac{q_0 - w}{2}\right)^{T-1}\right]\sum_{i=1}^{n} q_i \bar{r}_i. \tag{6}$$

Непосредственно проверяется условие нормировки: $\sum_{T=2}^{\infty} P(T) = 1$.

В задачах практического применения данной модели важно иметь конкретные числовые характеристики случайной величины T: ее математическое ожидание и дисперсию. В частности, математическое ожидание $\tau \equiv \mathbb{M}[T]$, означающее *среднее время до отказа безопасности*, определяется как

$$\tau = \sum_{T=2}^{\infty} TP(T) = \frac{1 + \sum_{i=1}^{n} q_i}{\sum_{i=1}^{n} q_i(1 - r_i)}. \tag{7}$$

Нетрудно видеть, что полученная нами формула вполне согласуется с ожидаемыми результатами в простейших частных случаях. Например, если все q_i равны нулю или все r_i равны единице, среднее время до отказа безопасности становится бесконечным. Эти предельные ситуации отвечают случаю полного отсутствия угроз или случаю абсолютной защиты соответственно.

Полученное выражение для τ может использоваться при оценке достаточности используемых средств защиты от киберугроз в контексте управления информационной безопасностью. На практике, например, мы можем наложить условие $\tau \geq \tau_{cr}$, означающее, что среднее время до отказа безопасности системы не должно быть меньше некоторого критического значения τ_{cr}. Нарушение этого требования будет означать недостаточную защиту системы и сигнализирует о том, что необходимо привлечь дополнительные средства кибербезопасности.

3. Возмущения модели: случай зависимых киберугроз

В реальных компьютерных системах киберугрозы редко являются независимыми; зачастую появление одной угрозы может порождать серию других киберугроз. Например, возникновение угрозы несанкционированного доступа может привести к появлению угрозы утечки данных, а угроза «отказ в обслуживании» может повлечь за собой появление угрозы несанкционированного использования вычислительных ресурсов. Исходя из сказанного, при моделировании киберугроз необходимо учитывать тот факт, что для соседних моментов времени t и $t+1$ они являются *зависимыми* случайными событиями.

В рамках настоящей статьи мы исследуем семейство малых возмущений описанной выше марковской модели, допустив возможность переходов между состояниями s_i, где $i = 1, 2, \ldots, n$. Для этого мы рассмотрим марковскую цепь, определяемую матрицей переходных вероятностей

$$\Pi_\epsilon = \begin{pmatrix} q_0 & q_1 & q_2 & \ldots & q_n & 0 \\ r_1 & \epsilon_{11} & \epsilon_{12} & \ldots & \epsilon_{1n} & \tilde{r}_1 \\ r_2 & \epsilon_{21} & \epsilon_{22} & \ldots & \epsilon_{2n} & \tilde{r}_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ r_n & \epsilon_{n1} & \epsilon_{n2} & \ldots & \epsilon_{nn} & \tilde{r}_n \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}. \tag{8}$$

Здесь $\tilde{r}_i = 1 - r_i - \sum_{j=1}^{n} \epsilon_{ij}$, причем естественно требовать, чтобы $0 \leq \sum_{j=1}^{n} \epsilon_{ij} \leq 1 - r_i$ для любого i. Величина ϵ_{ij} имеет смысл вероятности перехода из состояния s_i в s_j, то есть ϵ_{ij} — это вероятность появления j-ой киберугрозы в момент t при условии, что в предыдущий момент $t-1$ возникла i-ая киберугроза. Так же как и выше мы полагаем, что в начальный момент времени $t = 0$ система находится в безопасном состоянии, то есть имеют место равенства (3).

Динамика указанного марковского процесса как и в случае исходной модели задается рекуррентными соотношениями (1). Ее численный анализ не представляет особой

сложности, однако получить здесь точные аналитические результаты в общем случае уже довольно трудно. Исследуем, в связи с этим, частную ситуацию, когда переходы между состояниями s_i, где $i = 1, \ldots, n$, являются *редкими* случайными событиями. Математически указанное требование можно записать как

$$\epsilon_{ij} \ll 1 \quad \text{для всех } i, j = 1, \ldots, n.$$

В этом случае мы можем получить приближенные аналитические результаты, ограничиваясь первым приближением по коэффициентам ϵ_{ij}.

3.1. Формулы для вероятностей состояний в первом приближении

В рамках указанного приближения с помощью соотношений (1) мы получаем следующее линейное рекуррентное соотношение

$$p_0(t) \approx p_0(t-1)q_0 + p_0(t-2)\sum_{i=1}^{n} q_i r_i + p_0(t-3)\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}, \tag{9}$$

выполняющееся тем точнее, чем ближе значения величин ϵ_{ij} к нулю. Характеристический полином этой рекуррентной последовательности

$$f_\epsilon(\lambda) = \lambda^3 - q_0\lambda^2 - \lambda\sum_{i=1}^{n} q_i r_i - \sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}$$

при $\epsilon_{ij} = 0$ имеет три корня $\lambda_{1,2} = (q_0 \pm w)/2$ и $\lambda_3 = 0$, которые могут быть рассмотрены как нулевые приближения к соответствующим корням при произвольных ϵ_{ij}. В частности, в первом приближении эти корни имеют вид

$$\tilde{\lambda}_{1,2} \approx \frac{q_0 \pm w}{2} + \frac{2}{w(w \pm q_0)}\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}, \quad \tilde{\lambda}_3 \approx \frac{4}{q_0^2 - w^2}\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}.$$

Таким образом, формула, выражающая общий член рекуррентной последовательности (9), с точностью до членов по ϵ_{ij} первого порядка имеет вид

$$p_0(t) \approx c_1\tilde{\lambda}_1^t + c_2\tilde{\lambda}_2^t + c_3\tilde{\lambda}_3^t,$$

где постоянные c_1, c_2 и c_3 определяются из начальных условий $p_0(0) = 1$, $p_0(1) = q_0$ и $p_0(2) = q_0^2 + \sum_{i=1}^{n} q_i r_i$ и в указанном приближении записываются как

$$c_1 \approx \frac{q_0 + w}{2} - \frac{2}{w^3}\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}, \quad c_2 \approx \frac{q_0 - w}{2} + \frac{2}{w^3}\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}, \quad c_3 \approx 0.$$

Отсюда для вероятности безопасного состояния в первом приближении по ϵ_{ij} получаем следующее выражение:

$$p_0(t) \approx \frac{1}{w}\left(\frac{q_0 + w}{2}\right)^{t+1} - \frac{1}{w}\left(\frac{q_0 - w}{2}\right)^{t+1} + \left[\frac{t}{w^2}\left(\frac{q_0 + w}{2}\right)^{t-1} + \right.$$
$$\left. + \frac{t}{w^2}\left(\frac{q_0 - w}{2}\right)^{t-1} - \frac{2}{w^3}\left(\frac{q_0 + w}{2}\right)^{t} + \frac{2}{w^3}\left(\frac{q_0 - w}{2}\right)^{t}\right]\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}. \tag{10}$$

Напомним, что здесь $q_0 = 1 - \sum_{i=1}^{n} q_i$ и $w^2 = q_0^2 + 4\sum_{i=1}^{n} q_i r_i$.

Полученная формула (10) позволяет вычислить в том же приближении вероятности и остальных состояний системы:

$$p_i(t) \approx p_0(t-1)q_i + p_0(t-2)\sum_{j=1}^{n} q_j \epsilon_{ji}, \quad i = 1, \ldots, n; \quad p_f(t) \approx 1 - \sum_{i=0}^{n} p_i(t). \tag{11}$$

Легко видеть, что полученные формулы переходят в выражения (4) и (5) при $\epsilon_{ij} = 0$.

3.2. Вычисление среднего времени до отказа безопасности в первом приближении

Получим теперь в рассматриваемом приближении выражение для среднего времени τ до отказа безопасности.

Если в момент $t = T$ система в первый раз оказывается в финальном состоянии s_f, это означает, что в момент $t = T - 1$ она находилась в одном из состояний $s_1, s_2, \ldots, s_n$ (см. матрицу переходных вероятностей (8)). Таким образом, для распределения случайной величины τ получаем

$$P(T) = \sum_{i=1}^{n} p_i(T-1)\tilde{r}_i,$$

или, с использованием формул (11),

$$P(T) \approx p_0(T-2)\sum_{i=1}^{n} q_i \tilde{r}_i + p_0(T-3)\sum_{i=1}^{n}\sum_{j=1}^{n} q_j \epsilon_{ji} \tilde{r}_i \tag{12}$$

Среднее время до отказа безопасности τ определяется как математическое ожидание случайной величины T. Подставляя выражения (10) и (12) в формулу $\tau = \sum_{T=2}^{\infty} TP(T)$ и выполняя суммирование с точностью до первого порядка по ϵ_{ij} имеем

$$\tau \approx \frac{1 + \sum_{i=1}^{n} q_i \left(1 + \sum_{j=1}^{n} \epsilon_{ij}\right)}{\sum_{k=1}^{n} q_k (1 - r_k)} + \frac{\left(1 + \sum_{k=1}^{n} q_k\right)\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}}{\left(\sum_{k=1}^{n} q_k (1 - r_k)\right)^2}. \tag{13}$$

Нетрудно видеть, что при $\epsilon_{ij} = 0$ полученная формула совпадает с формулой (7).

4. Некоторые примеры

Приведем несколько примеров, иллюстрирующих корректность полученных результатов и их область применимости.

4.1. Случай одной киберугрозы

Рассмотрим случай одной киберугрозы: $n = 1$. Диаграмма переходов в марковской цепи для этого случая приведена на рисунке 2.

Нетрудно видеть, что матрица переходных вероятностей для данной марковской цепи имеет вид

$$\Pi_\epsilon = \begin{pmatrix} 1-q & q & 0 \\ r & \epsilon & 1-r-\epsilon \\ 0 & 0 & 1 \end{pmatrix}.$$

Зависимость вероятности безопасного состояния s_0 от времени в этом случае может быть найдена точно:

$$p_0(t) = \frac{q_0 + \delta - \epsilon}{2\delta}\left(\frac{q_0 + \delta + \epsilon}{2}\right)^t - \frac{q_0 - \delta - \epsilon}{2\delta}\left(\frac{q_0 - \delta + \epsilon}{2}\right)^t,$$

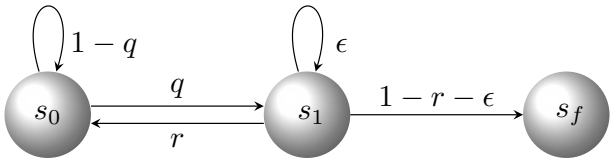
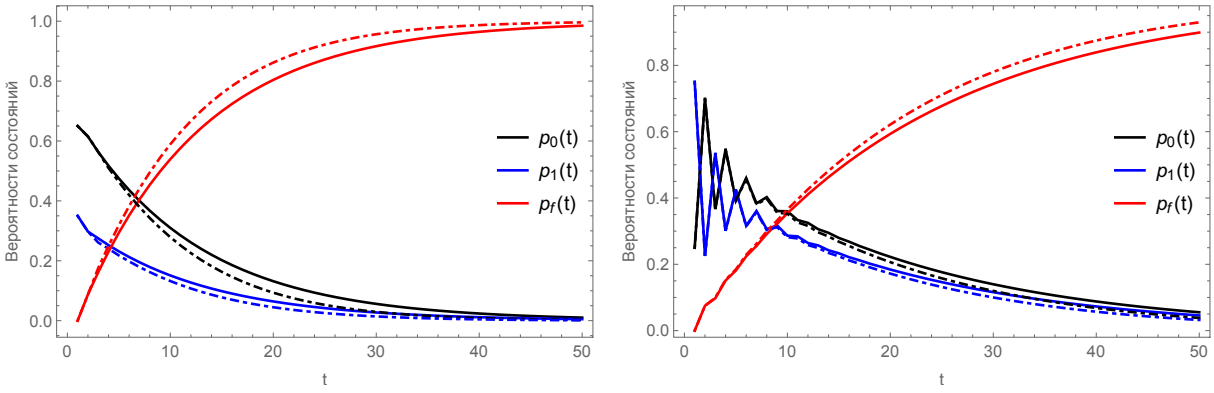


Рисунок 2. Диаграмма состояний системы в случае одной киберугрозы

где $q_0 = 1 - q$, $\delta^2 = q^2 + (1 - \epsilon^2) - 2q(1 - 2r - \epsilon)$. С другой стороны, согласно формуле (10) в первом приближении по ϵ получаем

$$p_0(t) \approx p_0^*(t) \equiv \frac{1}{w}\left(\frac{q_0 + w}{2}\right)^{t+1} - \frac{1}{w}\left(\frac{q_0 - w}{2}\right)^{t+1} + \left[\frac{t}{w^2}\left(\frac{q_0 + w}{2}\right)^{t-1} + \right.$$
$$\left. + \frac{t}{w^2}\left(\frac{q_0 - w}{2}\right)^{t-1} - \frac{2}{w^3}\left(\frac{q_0 + w}{2}\right)^{t} + \frac{2}{w^3}\left(\frac{q_0 - w}{2}\right)^{t}\right] qr\epsilon,$$

где $w^2 = q_0^2 + 4qr$. Для сравнения приближенного решения с точным, на рисунке 3 приведены графики функций $p_i(t)$ и $p_i^*(t)$ при различных наборах значений q, r и ϵ.



а) $q = 0.35$, $r = 0.55$, $\epsilon = 0.2$ б) $q = 0.55$, $r = 0.85$, $\epsilon = 0.02$

Рисунок 3. Графики функций $p_i(t)$ (сплошные линии) и $p_i^*(t)$ (прерывистые линии) для различных значений q, r и ϵ.

Среднее время до отказа безопасности в данном примере также может быть найдено точно. Приведем соответствующие точное выражение и приближенное выражение, получаемое с помощью формулы (13):

$$\tau = \frac{1 + q - \epsilon}{q(1 - r - \epsilon)}, \quad \tau \approx \tau^* \equiv \frac{1 + q}{q(1 - r)} + \frac{(q + r)}{q(1 - r)^2}\,\epsilon.$$

Соответствующий остаточный член $\Delta\tau \equiv \tau - \tau^*$ имеет вид

$$\Delta\tau = \frac{(q + r)\epsilon^2}{q(1 - r)^2(1 - r - \epsilon)}.$$

Отсюда нетрудно получить оценку для ϵ, при которой ошибка в вычислении среднего времени до отказа безопасности не будет превышать заданной величины $\sigma > 0$:

$$\epsilon < \frac{\sigma q (1-r)^2}{2(q+r)} \left(\sqrt{1 + \frac{4(q+r)}{\sigma q (1-r)}} - 1 \right).$$

Например, для значения $\sigma = 0.01$ при $q = 0.5$, $r = 0.90$ имеем $\epsilon < 0.00187$.

4.2. Случай двух киберугроз

Рассмотрим систему с двумя киберугрозами, диаграмма состояний которой показана на рисунке 4. Здесь $q_0 = 1 - q_1 - q_2$, $\tilde{r}_1 = 1 - r_1 - 3\epsilon$, $\tilde{r}_2 = 1 - r_2 - 4\epsilon$.

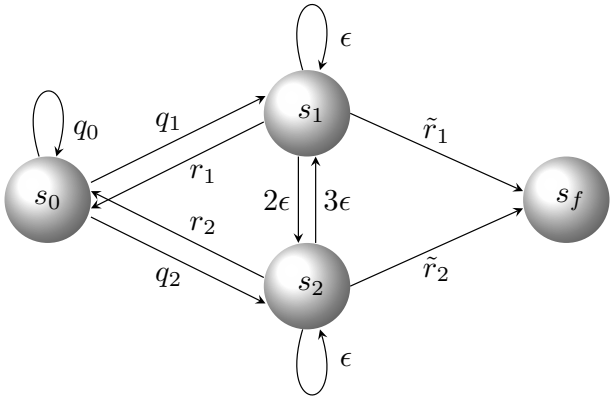


Рисунок 4. Диаграмма состояний системы в случае двух киберугроз

Матрица переходных вероятностей соответствующей марковской цепи имеет вид

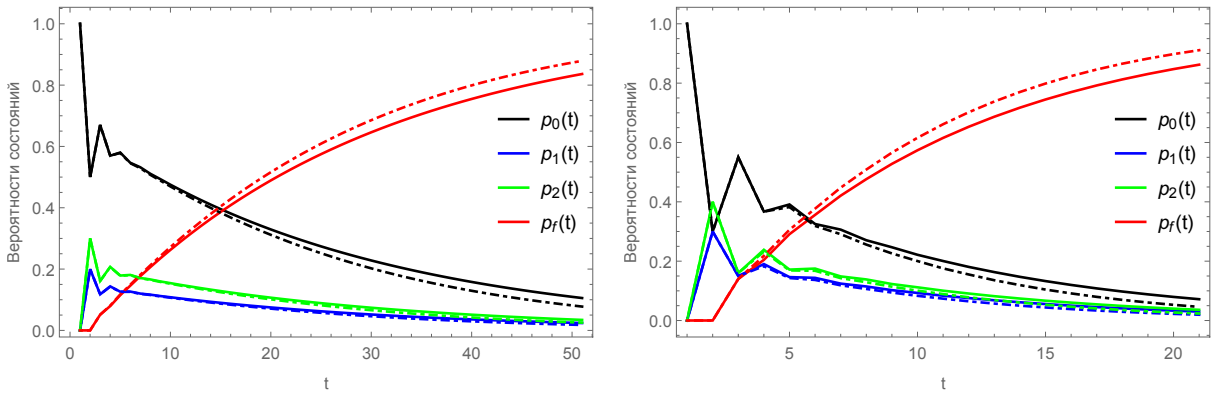
$$\Pi_\epsilon = \begin{pmatrix} q_0 & q_1 & q_2 & 0 \\ r_1 & \epsilon & 2\epsilon & \tilde{r}_1 \\ r_2 & 3\epsilon & \epsilon & \tilde{r}_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

По формуле (10) в первом приближении по ϵ для рассматриваемого случая получаем

$$p_0(t) \approx p_0^*(t) \equiv \frac{1}{w}\left(\frac{q_0+w}{2}\right)^{t+1} - \frac{1}{w}\left(\frac{q_0-w}{2}\right)^{t+1} + \left[\frac{t}{w^2}\left(\frac{q_0+w}{2}\right)^{t-1} + \right.$$
$$\left. + \frac{t}{w^2}\left(\frac{q_0-w}{2}\right)^{t-1} - \frac{2}{w^3}\left(\frac{q_0+w}{2}\right)^{t} + \frac{2}{w^3}\left(\frac{q_0-w}{2}\right)^{t}\right] (q_1 r_1 + 2q_1 r_2 + 3q_2 r_1 + q_2 r_2)\,\epsilon,$$

где $w^2 = q_0^2 + 4\,(q_1 r_1 + q_2 r_2)$. Остальные вероятности $p_i^*(t)$ в этом же приближении находятся согласно (11). Сравнение графиков функций $p_i(t)$ и $p_i^*(t)$ для некоторых наборов значений параметров q_i, r_i и ϵ приведено на рисунке 5.

Среднее время до отказа безопасности τ в данном примере также может быть вычислено точно (мы не приводим здесь соответствующую формулу ввиду ее громоздкости).



а) $q_1 = 0.2$, $q_2 = 0.3$, $r_1 = 0.9$, $r_2 = 0.8$, $\epsilon = 0.016$;

б) $q_1 = 0.3$, $q_2 = 0.4$, $r_1 = 0.6$, $r_2 = 0.7$, $\epsilon = 0.04$;

Рисунок 5. Графики функций $p_i(t)$ (сплошные линии) и $p_i^*(t)$ (прерывистые линии) для различных значений q, r и ϵ.

Приближенная формула для этой величины согласно (13) имеет вид

$$\tau \approx \tau^* \equiv \frac{1 + q_1(1+3\epsilon) + q_2(1+4\epsilon)}{q_1(1-r_1) + q_2(1-r_2)} + \frac{(1+q_1+q_2)(q_1r_1 + 2q_1r_2 + 3q_2r_1 + q_2r_2)\epsilon}{q_1(1-r_1) + q_2(1-r_2)}.$$

В таблице 1 приведены значения τ и τ^* для различных значений параметра ϵ при $q_1 = 0.3$, $q_2 = 0.4$, $r_1 = 0.6$, $r_2 = 0.7$, а также значения соответствующей относительной погрешности $\delta\tau \equiv |\tau - \tau^*|/\tau$. Из таблицы видно, что наша теория возмущений дает неплохую оценку для τ при $\epsilon = 0.01, 0.02, 0.03$. Напротив, при $\epsilon = 0.04$ и 0.05 относительная погрешность становиться большей 15%; в этом случае теория возмущений в первом порядке дает слишком грубую оценку и нужно либо привлекать члены более высокого порядка, либо использовать для нахождения τ другие приближенные методы.

Таблица 1. Сравнение τ и τ^* при $q_1 = 0.3$, $q_2 = 0.4$, $r_1 = 0.6$, $r_2 = 0.7$ для различных значений ϵ.

ϵ	τ	τ^*	$\delta\tau$
0.00	7.08333	7.08333	0.00
0.01	7.72447	7.65972	0.00838
0.02	8.52792	8.23611	0.03422
0.03	9.56435	8.81250	0.07861
0.04	10.9524	9.38889	0.14275
0.05	12.9077	9.96528	0.22796

5. Благодарности
Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90122.

6. Литература
[1] Jouini, M. Mean Failur-e Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study / M. Jouini, L.B.A. Rabai // JCP. – 2015. – Vol. 10(3). - P. 184-194.
[2] Le, N.T. A threat computation model using a Markov Chain and common vulnerability scoring system and its application to cloud security / N.T. Le, D.B. Hoang // Australian Journal of Telecommunications and the Digital Economy. – 2019. – Vol. 7(1). – P. 37.

[3] Almasizadeh, J. A stochastic model of attack process for the evaluation of security metrics / J. Almasizadeh, M.A. Azgomi // Computer Networks. - 2013. - Vol. 57(10). - P. 2159-2180.
[4] Щеглов, К.А. Математические модели эксплуатационной информационной безопасности / К.А. Щеглов, А.Ю. Щеглов // Вопросы защиты информации. – 2014. – Т. 3. – С. 52-65.
[5] Росенко, А.П. Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе / А.П. Росенко // Известия ЮФУ. Технические науки. – 2008. – Т. 85, № 8. – С. 71-81.
[6] Магазев, А.А. Исследование одной марковской модели угроз безопасности компьютерных систем / А.А. Магазев, В.Ф. Цырульник // Моделирование и анализ информационных систем. – 2017. – Т. 24, № 4. – С. 445-458.
[7] Magazev, A.A. Optimizing the selection of information security remedies in terms of a Markov security model / A. A. Magazev, V. F. Tsyiulnik // Journal of Physics: Conference Series. – 2018. – Vol. 1096(1). – P. 012160.

On small perturbations of Markov cyber threats models

A.A. Magazev[1], V.F. Tsyrulnik[1]

[1]Omsk State Technical University, Omsk, Russia, 644050

Abstract. In this work, we consider Markov chain-based stochastic modelling of cyber threats acting on computer systems. In the framework of this approach, computer systems are considered as systems with failures and recoveries by analogy with technical system models in reliability theory. Under the assumption that the cyber threats are independent random events, we derive the explicit analitical formulae for the state probabilities of the corresponding Markov chain and the mean time to security failure (MTSF). Then we investigate the case of dependent cyber threats and derive the approximate expressions for the state probabilities and MTSF within the framework of the first-order perturbation theory. As an illustration of our results, we consider a few simple examples.