

УДК 004.056

Евгений В. Трапезников
Омский государственный технический университет,
пр-кт Мира, 11, Омск, 644050, Россия
e-mail: evtrapeznikov@yandex.ru, <https://orcid.org/0000-0003-3205-193X>

ВЫБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ
СИСТЕМАХ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ КИБЕРАТАК*

DOI: <http://dx.doi.org/10.26583/bit.2023.4.06>

Аннотация. Одной из основных проблем обеспечения информационной безопасности автоматизированных систем является отсутствие универсальных подходов к количественной оценке их эффективности. В статье рассматривается один из возможных подходов к этой проблеме, основанный на использовании моделей кибератак, описываемых в терминах марковских цепей с поглощающими состояниями. Разработана модель, в которой, в отличие от подобных моделей других авторов, предусмотрено, что атаки могут иметь различную длительность. Кроме этого, в модели предусмотрено несколько поглощающих состояний, ассоциированных с успешными реализациями каждой из атак. Указанные особенности позволили ввести две метрики безопасности, которые могут быть использованы для оценки эффективности используемых средств защиты: среднее время до отказа безопасности и средний риск при реализации атаки. С использованием этих метрик в статье формулируется ряд оптимизационных задач, представляющих практический интерес при разработке и проектировании защищённых автоматизированных систем. Показано, что эти задачи принадлежат классу задач нелинейного целочисленного программирования и предложен эффективный алгоритм их решения, основанный на концепции последовательного анализа вариантов. Разработана программа для исследования марковских моделей безопасности с учетом длительности компьютерной атаки и приведен пример решения одной из оптимизационных задач, решением которой является оптимальный набор средств защиты, минимизирующий стоимость затрачиваемых на защиту средств при имеющихся ограничениях на среднее время до отказа безопасности.

Ключевые слова: марковская модель, кибератаки, метрики безопасности, оптимизация средств защиты, автоматизированная система, метод последовательного анализа вариантов.

Для цитирования: ТРАПЕЗНИКОВ Евгений В. ВЫБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ КИБЕРАТАК. Безопасность информационных технологий, [S.l.], т. 30, № 4, с. 102–113, 2023. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1548>. DOI: <http://dx.doi.org/10.26583/bit.2023.4.06>.

**Благодарности.* Автор выражает особую благодарность научному руководителю, д.ф.-м.н. профессору Магазеву Алексею Анатольевичу.

Evgeny V. Trapeznikov
Omsk state technical university,
Mira Ave., 11, Omsk, 644050, Russia
e-mail: evtrapeznikov@yandex.ru, <https://orcid.org/0000-0003-3205-193X>

Optimal choice of information security in automated systems via Markov cyber-attack models*

DOI: <http://dx.doi.org/10.26583/bit.2023.4.06>

Abstract. One of the main problems to provisioning the information security of automated systems is the absence of unify approaches to the quantitative evaluation of their efficiency and reliability. In this article, we consider one of the approaches to this problem, which is based on the use of cyber-attack models described in terms of Markov chains with absorbing states. In particular, we describe one of these models in detail, in which, in contrast to the similar models of other authors, the different duration of attacks is

provided. Moreover, we also have provided for this model the different absorbing states that are associated with the successful implementations for every of cyber-attacks. These features allow us to introduce two security metrics, which can be use for evaluating efficiency of the security remedies applied: the mean time to security failure and the mean risk of the attack implementation. Using these metrics, we formulate, in this article, a few optimization problems, which are of interest in the development and design of the secured automated systems. It has shown that these problems belong to the class of non-linear integer programming problems, and therefore we also suggest an efficient algorithm of their solving based on the concept of sequent analysis of variants. A program has been developed for studying Markov security models taking into account the duration of a computer attack and an example of solving one is given optimization problems whose solution is some optimal set of security remedies. This solution minimizes the cost and expenses sent on the security remedies at some constraints on the mean time to security failure.

Keywords: Markov model, cyber-attack, security metrics, protection optimization, automated system, method of sequential analysis of variants.

For citation: TRAPEZNIKOV Evgeny V. Optimal choice of information security in automated systems via Markov cyber-attack models. *IT Security (Russia)*, [S.l.], v. 30, no. 4, p. 102–113, 2023. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1548>. DOI: <http://dx.doi.org/10.26583/bit.2023.4.06>.

**Acknowledgement.* The author expresses special gratitude to the supervisor of sciences, Dr. Sci. Professor Magazev Alexey Anatolyevich.

Введение

Анализ нормативной документации в области защиты информации автоматизированных систем показывает, что существующие подходы к оценке эффективности применяемых мер защиты в большинстве случаев имеют качественный характер. Подобные подходы, обеспечивая необходимые условия по обеспечению информационной безопасности, довольно ограничены. Владельцам защищаемой информации чаще всего необходимо не просто удовлетворить основным требованиям регуляторов, но и понимать какой конкретно объём инвестиций требуется для обеспечения того или иного уровня кибербезопасности. Таким образом, актуальной в настоящее время становится проблема разработки удобных и гибких количественных подходов для оценки эффективности защиты информации в автоматизированных системах. Не менее важной является и задача об оптимизации используемых защитных мер и механизмов, корректная формулировка которой возможна только при наличии именно количественных оценок эффективности систем кибербезопасности (систем защиты информации в автоматизированных системах).

Ясно, что любые количественные методы оценки эффективности систем защиты информации должны формулироваться в рамках строгих математических моделей, описывающих процессы, происходящие в защищённых информационных системах. В настоящее время подобных моделей известно довольно много, причём используемый при их описании математический аппарат весьма разнообразен. Особую роль среди них играют *стохастические* или *вероятностные* модели, основанные на подходах и моделях теории вероятностей и случайных процессов.

В [1–4] предложен и исследован некоторый класс моделей, формулируемых на языке теории марковских цепей и предназначенных для оценки эффективности систем защиты информации. В рамках данного класса моделей оказалось возможным корректно сформулировать несколько *метрик безопасности* – количественных показателей системы защиты, на основе которых можно сделать вывод об эффективности используемых мер кибербезопасности. В [6] удалось модифицировать данный класс моделей, добавив в них

ряд более реалистичных предположений. Цель настоящей статьи – показать, что данная модифицированная модель допускает формулировку нескольких оптимизационных задач, решение которых может быть чрезвычайно полезным в практических приложениях. Как будет показано ниже, эти оптимизационные задачи принадлежат классу задач нелинейного целочисленного математического программирования, поэтому актуальной также является проблема их эффективного решения. В этой связи в статье предложен один из возможных методов решения оптимизационных задач, основанный на концепции последовательного анализа вариантов, а также рассматривается пример задачи оптимизации.

1. Марковская модель кибератак

В [1–3] исследован класс марковских моделей кибератак с дискретным временем, в рамках которых авторам удалось корректно сформулировать и эффективно вычислить одну из возможных метрик безопасности – *среднее время до отказа безопасности*. В терминах указанных моделей также было сформулировано несколько довольно естественных оптимизационных задач, представляющих практический интерес, в частности, при разработке и проектировании систем защиты информации [4].

Напомним кратко основные положения моделей, рассмотренных в работах [1–3].

В указанных моделях рассматривается автоматизированная или информационная система, подверженная n различным кибератакам. Возникновение каждой из атак трактуется как случайное событие с заданной вероятностью. Далее, имеющиеся у автоматизированной системы средства защиты могут либо отразить возникшую атаку, либо, наоборот, атака успешно реализовывается. Эти исходы также рассматриваются как случайные взаимно исключающие друг друга случайные события. В зависимости от текущего статуса, в каждый дискретный момент времени $t = 1, 2, \dots$, автоматизированная система находится в одном из $n + 2$ возможных состояний: *безопасное* состояние, в котором нет никаких атак, n состояний, ассоциированных с каждой из атак, и состояние *отказа безопасности*, в которое система переходит, в случае успешной реализации любой из кибератак. Динамика переходов между состояниями трактуется как марковская цепь с дискретным временем с конечным числом состояний, одно из которых является *поглощающим*. В частности, в [2] удалось получить явные аналитические формулы для вероятностей состояний этой марковской цепи.

Важнейшим достоинством моделей кибератак, предложенных в работах [1–3], является возможность получения явных результатов в замкнутой аналитической форме. Это позволяет быстро и точно вычислять различные количественные характеристики безопасности защищённых автоматизированных систем, не прибегая к численным расчётам или имитационному моделированию. С другой стороны, описанный класс моделей имеет и ряд недостатков, два из которых представляются нам наиболее существенными. Во-первых, в этих моделях предполагается, что длительность каждой из кибератак одна и та же и равна одному временному шагу (напомним, что время в модели дискретно и измеряется целыми числами). Иными словами, делается предположение о том, что время пребывания системы в состоянии « i -ая кибератака» одно и то же для всех $i = 1, 2, \dots, n$. Данное допущение, конечно же, нереалистично, так как на практике длительности различных атак могут варьироваться в довольно широких пределах [5]. Во-вторых, в [1–3] предусматривалось лишь одно поглощающее состояние марковской цепи, которое символизировало успешную реализацию *любой* из кибератак. В то же время в ряде задач более уместным является введение *различных* поглощающих состояний для каждой из n возможных атак. Подобный подход, в частности, позволяет ввести ещё одну

метрику безопасности, точно рассчитываемую в терминах модели и учитывающую различный нанесённый системе ущерб, в зависимости от того, какая из атак была успешно реализована злоумышленником.

Указанные выше недостатки привели к необходимости существенной модификации марковских моделей, предложенных в [1–3]. Одна из возможных модификаций была предложена авторами настоящей статьи в [6]. В частности, в данной работе было введено предположение о том, что кибератаки могут осуществляться различное время, причём эти времена распределены случайно в соответствии с геометрическим законом распределения. Кроме того, в модифицированной версии модели также предусмотрено наличие n различных поглощающих состояний, ассоциированных с n различными кибератаками. В следующем разделе будет показано, что это приводит к возможности ввести ещё одну полезную метрику безопасности, называемую *средним риском* при реализации кибератаки.

С целью фиксации обозначений, а также для замкнутости изложения, приведём здесь основные положения и результаты из [6].

В отличие от исходной марковской модели атак, в модифицированном варианте автоматизированная система может находиться в $(2n + 1)$ возможных состояниях s_0, s_1, \dots, s_{2n} . Состояние s_0 – это *безопасное состояние*, т.е. состояние отсутствия кибератак. Состояние s_i ($i = 1, \dots, n$) показывает, что в данный момент система подвергается i -ой кибератаке. Наконец, состояние s_{n+i} ($i = 1, \dots, n$) ассоциируется с успешной реализацией i -ой кибератаки.

Переходы между состояниями свершаются в строго определенные промежутки времени: $t = 0, 1, 2, \dots$. При этом возможны только следующие переходы:

- 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 ($i = 1, \dots, n$); ясно, что с вероятностью $q_0 \equiv 1 - \sum_{i=1}^n q_i$ система останется в том же состоянии s_0 ;
- если в момент t система находится в состоянии s_i ($i = 1, \dots, n$), 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 -ое состояние отказа безопасности s_{n+i} с вероятностью $\tilde{r}_i = 1 - r_i - d_i$ (кибератака успешно осуществилась);
- оказавшись в момент t в одном из состояний отказа безопасности s_{n+i} ($i = 1, \dots, n$), система остаётся в нём навсегда, то есть это состояние марковской цепи – поглощающее.

Таким образом, входными количественными параметрами описываемой модели являются компоненты следующих трёх векторов:

- вектор вероятностей появления кибератак $q = (q_1, \dots, q_n)$;
- вектор вероятностей их отражений $r = (r_1, \dots, r_n)$;
- вектор вероятностей «задержек» кибератак $d = (d_1, \dots, d_n)$.

На рис. 1 приведён граф возможных переходов между состояниями соответствующей марковской цепи.

Динамика описанной модели описывается вектором вероятностей $p(t) = (p_0(t), p_1(t), \dots, p_{2n}(t))$ состояний марковской цепи в произвольный момент времени t . Как известно из общей теории марковских цепей, этот вектор находится в соответствии с формулой $p(t) = p(0) \cdot \Pi^t$, где Π – матрица переходных вероятностей марковской цепи (определяется в соответствии с графом на рис. 1), $p(0) = (1, 0, \dots, 0)$ –

вектор вероятностей состояний цепи в момент времени $t = 0$ (предполагается, что в этот момент времени система достоверно находится в безопасном состоянии).

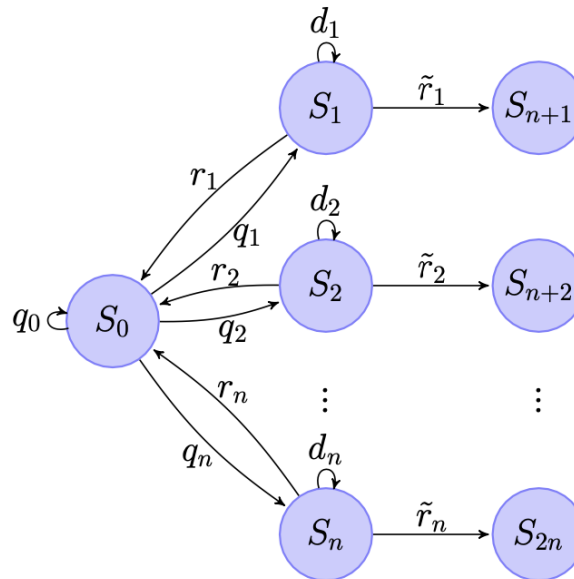


Рис. 1. Граф переходов марковской цепи в модифицированной модели
Fig. 1. Markov chain transition graph in the modified model

В отличие от более простых марковских моделей, рассмотренных в [1–3], данная модифицированная версия в общем случае не позволяет выписать в аналитическом виде вероятности состояний марковской цепи в произвольный момент времени. Это может быть сделано только в некоторых частных случаях (см. [6]), либо с помощью численных методов. С другой стороны, возможно получить явные аналитические формулы для некоторых метрик безопасности, формулируемых на основе представленной модели. Эти формулы будут приведены в следующем разделе.

2. Метрики безопасности, вычисляемые на основе марковской модели атак

Термин *метрика безопасности* применяется в тех случаях, когда речь идет об уровне защищенности или показателях безопасности той или иной информационной системы. Под этим термином обычно понимают некоторую оценку или систему оценок, основанную на имеющихся данных или полученную в результате измерений, которая позволяет выявлять недостатки в системе защиты информации и облегчает принятие решений [7].

Подробный обзор существующих метрик безопасности и условий их применимости дан в [8]. Некоторые вопросы, связанные с практическим применением метрик безопасности, отражены в ГОСТ Р ИСО/МЭК 27004-2021 «Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

Отметим, что в рамках стохастических подходов к моделированию процессов типа «атака-отражение», использующих марковские цепи, наиболее употребительными являются три типа метрик безопасности: среднее время до отказа безопасности (MTTSF), стационарная безопасность (steady-state security) и тип сбоя безопасности (the type of a security failure) [9]. Вторая из этих метрик для рассматриваемой модели не применима, так как требует, чтобы все состояния марковской цепи были переходными. Поэтому далее будет рассмотрена первая и третья из указанных метрик безопасности, для которых в

терминах модифицированной марковской модели были получены явные аналитические формулы [6].

По определению *временем до отказа безопасности* называется число T переходов между состояниями в марковской цепи до её первого попадания в любое из поглощающих состояний s_{n+i} . Так как определяемая таким образом величина является случайной, удобно пользоваться её математическим ожиданием – *средним временем до отказа безопасности* τ . Для описанной в предыдущем разделе марковской цепи была получена следующая формула для этой величины:

$$\tau = \frac{\prod_{j=1}^n (1 - d_j) + \sum_{i=1}^n q_i \prod_{j=1}^n [1 - (1 - \delta_{ij})d_j]}{\sum_{i=1}^n q_i \prod_{j=1}^n (1 - \delta_{ij}r_j - d_j)}, \quad (1)$$

где δ_{ij} – символ Кронекера, q_i , d_i , r_i – параметры модели (см. предыдущий раздел).

В качестве простого примера рассмотрим среднее время до отказа безопасности в случае, когда имеется всего одна актуальная кибератака. Полагая в (1) $n = 1$, получаем

$$\tau = \frac{1 - d + rd}{q(1 - d - r)}.$$

Видно, что при $q \rightarrow 0$ величина τ стремится к бесконечности (в отсутствие кибератак система функционирует бесконечно долго).

Отметим, что метрика безопасности τ – это характеристика, показывающая эффективность системы защиты от кибератак с функционально-временной точки зрения; именно такие метрики зачастую применяются в теории надёжности технических систем.

Для того, чтобы выписать вторую метрику безопасности, введём дополнительную нотацию. Допустим, что при реализации i -ой кибератаки *ущерб*, нанесенный системе, составляет U_i условных единиц. Если вероятность реализоваться данной атаке равна P_i , то мы можем оценить связанный с этим событием *риск* по формуле $R_i = P_i U_i$. Тогда *средний риск* R , связанный с отказом безопасности системы, это – математическое ожидание данной случайной величины:

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

Это и есть вторая метрика безопасности, вычисление которой возможно в терминах рассматриваемой марковской модели. В частности, в [6] была получена следующая формула для величины R :

$$R = \frac{\sum_{i=1}^n q_i U_i \prod_{j=1}^n (1 - \delta_{ij}r_j - d_j)}{\sum_{k=1}^n q_k \prod_{j=1}^n (1 - \delta_{kj}r_j - d_j)}.$$

Для одной атаки $n = 1$ данная формула приводит к тривиальному результату: $R = U_1$. В этом нет ничего удивительного, так как в случае одной атаки ущерб может принимать ровно одно возможное значение. В общем случае функция R линейна по величинам U_i ; соответствующий коэффициент перед U_i показывает долю вклада ущерба от i -ой кибератаки в средний суммарный ущерб.

С целью подробного исследования модифицированной марковской модели атак, изложенной в разделе 2, а также для детального изучения введённых выше метрик безопасности, нами был реализован пакет расширения MMInfoSec2 системы символьных вычислений Wolfram Mathematica [10]. В частности, в этом пакете реализованы и процедуры вычисления двух представленных метрик безопасности.

3. Оптимизация средств защиты на основе марковской модели атак

На основе ряда простых марковских моделей кибератак, исследованных в [1–3], были сформулированы несколько задач оптимизации, связанные с выбором оптимального в том или ином смысле набора средств защиты информации [4, 11]. При этом в качестве критериев оптимальности в данных работах выступали критерий максимизации среднего времени до отказа безопасности, либо критерий минимизации стоимости средств защиты. В рамках нашей модифицированной марковской модели также можно рассмотреть ряд подобных оптимизационных задач. Однако теперь метрик безопасности, формулируемых в терминах модели, стало две, и поэтому число возможных оптимизационных задач возрастает. Сформулируем их более подробно и обсудим один из эффективных алгоритмов решения этих задач, основанный на применении метода *последовательного анализа вариантов*.

Предположим, что для отражения кибератак, которые могут быть направлены на автоматизированную систему, имеется набор из m всевозможных средств защиты. Обозначим через z_a булеву переменную, сопоставленную a -ому средству защиты; эта переменная принимает значение 1, если данное средство задействовано, и 0 – в обратном случае. Тогда каждый возможный поднабор средств защиты из m возможных можно представить m -мерным булевым вектором $z = (z_1, z_2, \dots, z_m) \in \{0,1\}^m$.

Обозначим $r_{i,a}$ вероятность отражения i -ой атаки a -ым средством защиты. Так как в общем случае несколько различных средств защиты могут отражать одну и ту же кибератаку, вероятность отражения i -ой атаки *хотя бы одним* средством защиты в соответствии с формулой вероятности суммы нескольких совместных событий равна [12]:

$$r_i(z) = \sum_{k=1}^m (-1)^k \sum_{a_1 < a_2 < \dots < a_k} (r_{i,a_1} z_{a_1}) (r_{i,a_2} z_{a_2}) \dots (r_{i,a_k} z_{a_k}).$$

Данную вероятность можно проще вычислить:

$$r_i(z) = 1 - \prod_{k=1}^m (1 - r_{i,k} z_k),$$

так как произведение вероятностей вида $(1 - r_{i,k} z_k)$, где $k = 1, 2, \dots, m$, есть ничто иное как вероятность *не отразить i -ую атаку* ни одним из задействованных средств защиты.

В предыдущем разделе приведены две метрики безопасности, эффективное вычисление которых возможно в терминах рассматриваемой модифицированной марковской модели кибератак. Учтём теперь тот факт, что параметры модели r_i , представляющие собой вероятности отражения возможных кибератак, являются не заданными заранее постоянными, а функциями от m -мерного вектора z . Это влечёт тот факт, что рассмотренные выше метрики будут являться теперь *функциями* от вектора z . В качестве примера приведём здесь явное выражение такой функции для среднего времени до отказа безопасности:

$$\tau(z) = \frac{\prod_{j=1}^n (1 - d_j) + \sum_{i=1}^n q_i \prod_{j=1}^n [1 - (1 - \delta_{ij}) d_j]}{\sum_{i=1}^n q_i \prod_{j=1}^n (1 - \delta_{ij} (1 - \prod_{k=1}^m (1 - r_{i,k} z_k))) - d_j}.$$

Введём функцию *стоимости конфигурации системы защиты*. Для этого обозначим через c_a стоимость a -го средства защиты. Тогда стоимость всей данной конфигурации z может быть записана в виде следующей линейной по z функции:

$$C(z) = \sum_{a=1}^m c_a z_a.$$

Перечислим теперь некоторые возможные оптимизационные задачи, формулируемые в терминах модифицированной марковской модели атак.

1) Максимизация среднего время до отказа безопасности при ограниченных средствах на использование механизмов защиты:

$$\tau(z) \rightarrow \max, \quad C(z) \leq C_0.$$

2) Выбор конфигурации системы защиты, при которой затраты будут минимальные при ограничении на продолжительность функционирования автоматизированной системы:

$$\tau(z) \geq \tau_0, \quad C(z) \rightarrow \min. \quad (2)$$

3) Минимизация среднего риска при ограниченных средствах на применяемые средства защиты:

$$R(z) \rightarrow \min, \quad C(z) \leq C_0.$$

4) Минимизация затрат на использование механизмов защиты при ограничении сверху величины среднего риска:

$$C(z) \rightarrow \min, \quad R(z) \leq R_0.$$

5) Максимизация среднего времени до отказа безопасности при ограничении сверху величины среднего риска:

$$\tau(z) \rightarrow \max, \quad R(z) \leq R_0.$$

6) Минимизация среднего ущерба при ограничении снизу на величину среднего времени до отказа безопасности:

$$\tau(z) \geq \tau_0, \quad R(z) \rightarrow \min.$$

Здесь C_0 , R_0 и τ_0 – некоторые заданные параметры. Отметим, что могут быть сформулированы и более сложные многокритериальные оптимизационные задачи, в которых имеются две целевые функции или используются ограничения в виде двух неравенств. Рассмотрение таких задач в данной статье не рассматриваются.

Все перечисленные оптимизационные задачи принадлежат классу задач нелинейного целочисленного (булева) программирования. Как известно, решение таких задач довольно трудоёмко, причём универсального метода для этого не существует. Тем не менее, рассмотрим один из возможных подходов к решению этих задач, основанный на концепции последовательного анализа вариантов. Соответствующий метод решения задач дискретной нелинейной оптимизации был предложен В.С. Михалевичем [13, 14]. Изложим основные моменты этого метода применительно к оптимизационной задаче (2). Остальные задачи могут быть решены аналогично.

Главная идея метода последовательного анализа вариантов – пошаговое движение по дереву частичных решений и отсеив тех решений, которые не могут быть достроены ни до оптимальных, ни до допустимых. Отсев таких решений происходит с помощью набора *элиминирующих тестов* $\sigma = \{\xi_0, \xi_1, \dots, \xi_k\}$:

$$\sigma(h) = h^{(k+1)},$$

где $h^{(j)} = h^{(j-1)} \setminus \xi_{j-1}(h^{(j-1)})$, $j = 0, 1, \dots, k + 1$, $h^{(0)} = h$.

В данном случае h – некоторое множество *частичных решений* $z_{(p)} = (z_1, z_2, \dots, z_p)$ оптимизационной задачи, $\xi_i(h)$ обозначает множество частичных решений, исключаемых тестом ξ_i . В наборе σ всегда присутствуют два теста:

- ξ_0 – проверяет допустимость решения (удовлетворяет условию $\tau(z) \geq \tau_0$);

- ξ_1 – сравнивает допустимые решения по значению целевой функции $C(z)$.

Специфика оптимизационной задачи (2) позволяет определить еще два элиминирующих теста: ξ_2 и ξ_3 .

Тест ξ_2 использует свойство неубывания целевой функции $C(z)$ при вычислении оценки частичных решений вида:

$$\alpha(z_{(p)}) = C(z_1, \dots, z_p, 0, \dots, 0).$$

Пусть C^* – верхняя граница для минимума задачи представленной выше. Первоначально будем полагать, что $C^* = +\infty$. На каждом шаге метода будем менять значение C^* на наилучшее для целевой функции на множестве построенных допустимых решений. Элиминирующий тест ξ_2 для произвольного множества частичных решений задается соотношением:

$$\xi_2(h) = \{z_{(p)} \in h: \alpha(z_{(p)}) > C^*\}.$$

Ещё один элиминирующий тест ξ_3 осуществляет анализ допустимости частичных решений. Неравенство $\tau(z) \geq \tau_0$ можно представить в виде

$$g_1(z) - g_2(z) \leq 0,$$

где $g_1(z)$ и $g_2(z)$ – неубывающие функции. С учетом равенства

$$\beta(z_{(p)}) = g_1(z_1, \dots, z_p, 0, \dots, 0) - g_2(z_1, \dots, z_p, 1, \dots, 1),$$

элиминирующий тест ξ_3 можно записать в виде:

$$\xi_3(h) = \{z_{(p)} \in h: \beta(z_{(p)}) > 0\}.$$

Использование элиминирующих тестов ξ_2 и ξ_3 позволяет повысить эффективность алгоритма поиска оптимального решения. Это достигается за счёт того, что придвижении по дереву частичных решений некоторые из ветвей можно заведомо отбросить. Проведённые численные эксперименты показали увеличение скорости поиска оптимального решения по сравнению с методом прямого перебора.

4. Пример задачи оптимизации

В настоящем разделе рассмотрим пример формулировки и решения задачи оптимизации (2) в случае четырёх кибератак ($n = 4$), для отражения которых имеется пять возможных средств защиты ($m = 5$). Несмотря на довольно ограниченный характер, данный пример призван проиллюстрировать основные особенности сформулированных оптимизационных задач и процедуры их решения. Все вычисления проводились с помощью разработанного программного пакета расширения MMInfoSec2 [10].

В качестве значений входных параметров модели (векторов q , d и матрицы $\|r_{i,\alpha}\|$) выберем следующие значения:

$$q = (0.1, 0.25, 0.15, 0.1), \quad d = (0.005, 0.0, 0.08, 0.01),$$

$$c = (50\ 000, 100\ 000, 35\ 000, 150\ 000, 40\ 000).$$

$$\|r_{i,\alpha}\| = \begin{pmatrix} 0.90 & 0.00 & 0.00 & 0.78 & 0.00 \\ 0.00 & 0.92 & 0.75 & 0.98 & 0.00 \\ 0.84 & 0.50 & 0.00 & 0.00 & 0.85 \\ 0.0 & 0.00 & 0.89 & 0.90 & 0.62 \end{pmatrix}.$$

Отметим, что эти значения выбраны только лишь для демонстрации алгоритма решения оптимизационной задачи. В конкретных примерах при рассмотрении реальных систем данные значения могут быть получены либо экспертным путём, либо по имеющейся накопленной статистике. Это, однако, достаточно трудоёмкий и длительный процесс, который специфичен для каждой конкретной автоматизированной системы.

С помощью функции *GetMTTSF* из библиотеки *MInfoSec2* вычислим средние времена до отказа безопасности для всех возможных $2^5 = 32$ конфигураций средств защиты. Результаты вычислений приведены в табл. 1.

Таблица 1. Результаты вычислений с помощью функции *GetMTTSF*

Конфигурация СЗИ	00000	00001	00010	00011	00100	00101	00110	00111
Среднее время до отказа безопасности	1.67	2.44	5.36	19.31	3.09	5.32	5.75	22.40
Конфигурация СЗИ	01000	01001	01010	01011	01100	01101	01110	01111
Среднее время до отказа безопасности	3.40	5.95	9.41	27.90	5.25	8.39	10.30	31.10
Конфигурация СЗИ	10000	10001	10010	10011	10100	10101	10110	10111
Среднее время до отказа безопасности	2.61	3.33	25.25	77.93	9.44	12.73	37.11	175.56
Конфигурация СЗИ	11000	11001	11010	11011	11100	11101	11110	11111
Среднее время до отказа безопасности	7.12	14.68	43.66	155.83	27.51	51.98	73.01	366.07

Удобно изобразить полученные данные с помощью гистограммы приведенной на рис. 2. На горизонтальной оси указаны номера конфигураций, т.е. десятичные формы бинарных векторов z , а на вертикальной оси откладывается величина среднего времени до отказа безопасности.

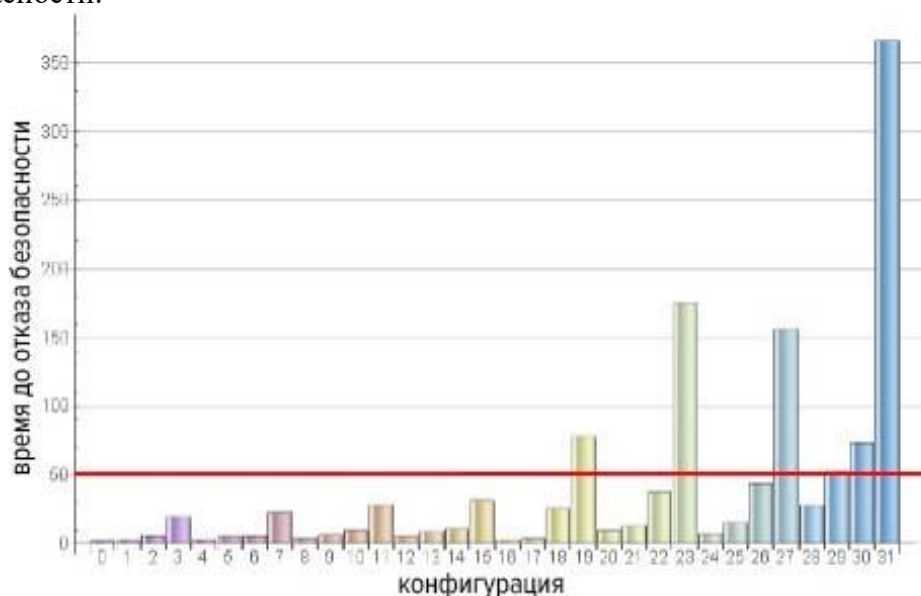


Рис. 2. Зависимость среднего времени до отказа безопасности от конфигурации средств защиты
 Fig. 2. Dependence of the mean time to safety failure on the configuration of protection means

Выберем нижний порог среднего времени до отказа безопасности: $\tau_0 = 50$. Как видно из рис. 2, условию $\tau(z) \geq \tau_0$ удовлетворяют шесть конфигураций: 19 = 10011, 23 = 10111, 27 = 11011, 29 = 11101, 30 = 11110 и 31 = 11111. Стоимости этих конфигураций приведены в табл. 2.

Таблица 2. Стоимости конфигураций средств защиты

Конфигурация	19=10011	23=10111	27=10111	29=11101	30=11110	31=11111
Стоимость	240 000	275 000	340 000	225 000	335 000	375 000

Из таблицы видно, что самой дешёвой конфигурацией является набор $z^* = 29 = 11101$. Это и есть решение оптимизационной задачи.

Конечно, данный пример является иллюстративным и может быть полностью проанализирован без привлечения методов решения оптимизационных задач. Это связано с малым числом m исходного набора средств защиты. С ростом m комбинаторные трудности возрастают и уже начиная с $m = 30$ метод прямого перебора нецелесообразен ввиду существенного увеличения времени поиска оптимального решения. При этом может быть использован описанный выше метод последовательного анализа вариантов. Эксперименты показали, что даже для m порядка 100 этот метод находит решение за приемлемое время.

Заключение

Разработанная марковская модель кибератак позволяет оценивать защищенность автоматизированной системы с учетом различного времени длительности кибератак. Данная модификация позволяет ввести две естественные метрики безопасности – среднее время до отказа безопасности и средний риск при реализации атаки. В работе показано, что, используя данные метрики, можно сформулировать несколько корректных оптимизационных задач, принадлежащих классу задач нелинейного дискретного программирования. Для решения последних предлагается метод последовательного анализа вариантов. Приведен пример решения одной из оптимизационных задач.

СПИСОК ЛИТЕРАТУРЫ:

1. 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. – EDN SWOGHT.
2. Магазев А.А., Цырульник В.Ф. Исследование одной марковской модели угроз безопасности компьютерных систем. Моделирование и анализ информационных систем. 2017;24(4):445-458. DOI: <https://doi.org/10.18255/1818-1015-2017-4-445-458>. – EDN ZDNQMZ.
3. Magazev A.A., Tsyrunlik V.F. 2021 J. Phys.: Conf. Ser. 1745 012111. DOI: <https://doi.org/1088/1742-6596/1745/1/012111>. – EDN HREXRT.
4. Магазев А.А., Цырульник В.Ф. Оптимизация выбора средств защиты информации в рамках одной марковской модели безопасности. Информационные технологии и нанотехнологии. 2018, с. 2050–2058. – EDN ХМХАВУ.
5. Белов А.С., Добрышин М.М., Шугуров Д.Е., Большебратский К.М. Подход к оценке защищенности компьютерной сети связи на основе количества уязвимостей. Приборы и системы. Управление, контроль, диагностика. 2022, № 11, с. 20–25. DOI: <https://doi.org/10.25791/pribor.11.2022.1371>. – EDN VSKPWO.
6. Касенов А.А., Магазев А.А., Трапезников Е.В. Применение одной марковской модели кибератак для оценки метрик безопасности. Математические структуры и моделирование. 2020, № 2(54), с. 129–144. DOI: <https://doi.org/10.24147/2222-8772.2020.2.129-144>. – EDN VHGBSC.
7. Purboyo T.W., Rahardjo B. and Kuspriyanto. Security metrics: A brief survey. 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering, Bandung, Indonesia. 2011, p. 79–82. DOI: <https://doi.org/10.1109/ICICI-BME.2011.6108598>.
8. Jaquith, A. Security Merics: Replacing Fear Uncertainty and Doubt. AddisonWesley. Reading. 2007. URL: <https://api.semanticscholar.org/CorpusID:72855989> (дата обращения: 01.09.2023).

9. 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, vol. 57, no. 10, p. 2159–2180. DOI: <https://doi.org/10.1016/j.comnet.2013.03.011>.
10. Свидетельство о гос. регистрации программы для ЭВМ. Пакет расширения системы символьных вычислений Mathematica для исследования марковских моделей безопасности с учетом задержек компьютерной атаки. Е.В. Трапезников, А.А. Магазев; Омск. гос. техн. ун-т. – RU № 2023663326; заявл. 13.06.2023; опублик. 21.06.2023.
11. Касенов А.А., Магазев А.А., Цырульник В.Ф. Марковская модель совместных киберугроз и ее применение для выбора оптимального набора средств защиты информации. Моделирование и анализ информационных систем. 2020;27(1):108-123. DOI: <https://doi.org/10.18255/1818-1015-2020-1-108-123>.
12. Feller W. An Introduction to Probability Theory and Its Applications. Vol. 1. W. Feller, V. Feller. 3rd ed. New York: John Wiley & Sons, 1968. – 528 p.
13. Михалеви́ч В.С., Ку́кса А.И. Методы последовательной оптимизации в дискретных сетевых задачах оптимального распределения ресурсов. М.: Наука, 1983. – 208 с.
14. Ковалев М. М. Дискретная оптимизация. Целочисленное программирование. М.: УРСС, 2003. – 190 с.

REFERENCES:

- [1] Rosenko A.P., Bordak I.V. A mathematical model for determining the probability of consequences from the implementation of the attacker threats to information security limited distribution. Izvestiya Yufu. Tekhnicheskkiye Nauki. 2015, no. 7(168), p. 6–19 (in Russian). – EDN SWOGHT.
- [2] Magazev A.A., Tsyruulik V.F. Investigation of a Markov Model for Computer System Security Threats. Modeling and Analysis of Information Systems. 2017;24(4):445-458. DOI: <https://doi.org/10.18255/1818-1015-2017-4-445-458> (in Russian). – EDN ZDNQMZ.
- [3] Magazev A.A., Tsyruulik V.F. 2021 J. Phys.: Conf. Ser. 1745 012111. DOI: <https://doi.org/1088/1742-6596/1745/1/012111>. – EDN HREXRT.
- [4] Magazev A.A., Tsyruulik V.F. Optimizing the selection of information security remedies in terms of a Markov security model. Informacionnye tekhnologii i nanotekhnologii. 2018, s. 2050–2058 9 (in Russian). – EDN XMXABV.
- [5] Belov A.S., Dobryshin M.M., Shugurov D.E., Bolshebratsky K.M. An approach to assessing the security of a computer communication network based on the number of vulnerabilities. Pribory i sistemy. Upravleniye, kontrol, diagnostika. 2022, no. 11, p. 20–25. DOI: <https://doi.org/10.25791/pribor.11.2022.1371> (in Russian). – EDN VSKPWO.
- [6] Kassenov A.A., Magazev A.A., Trapeznikov E.V. Using a markov cyberattack model for evaluation of security metrics. Matematicheskiye struktury i modelirovaniye. 2020, no. 2(54), p. 129–144. DOI: <https://doi.org/10.24147/2222-8772.2020.2.129-144> (in Russian). – EDN VHGBSC.
- [7] Purboyo T.W., Rahardjo B. and Kuspriyanto. Security metrics: A brief survey. 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering, Bandung, Indonesia. 2011, p. 79–82. DOI: <https://doi.org/10.1109/ICICI-BME.2011.6108598>.
- [8] Jaquith, A. Security Merics: Replacing Fear Uncertainty and Doubt. AddisonWesley. Reading. 2007. URL: <https://api.semanticscholar.org/CorpusID:72855989> (дата обращения: 01.09.2023).
- [9] 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, vol. 57, no. 10, p. 2159–2180. DOI: <https://doi.org/10.1016/j.comnet.2013.03.011>.
- [10] Certificate of state registration of a computer program. Extension package for the Mathematica symbolic computation system for the study of Markov security models taking into account the delays of a computer attack. E.V. Trapeznikov, A.A. Magazev; O. gos. tech. un-t. – RU № 2023663326; dec. 13.06.2023; publ. 21.06.2023 (in Russian).
- [11] Kassenov A.A., Magazev A.A., Tsyruulik V.F. A Markov Model of Non-Mutually Exclusive Cyber Threats and its Applications for Selecting an Optimal Set of Information Security Remedies. Modeling and Analysis of Information Systems. 2020;27(1):108-123. DOI: <https://doi.org/10.18255/1818-1015-2020-1-108-123> (in Russian).
- [12] Feller W. An Introduction to Probability Theory and Its Applications. Vol. 1. W. Feller, V. Feller. 3rd ed. New York: John Wiley & Sons, 1968. – 528 p.
- [13] Mikhalevich V.S., Kuksa A.I. Sequential optimization methods in discrete network problems of optimal resource allocation. М.: Наука, 1983. – 208 p. (in Russian).
- [14] Kovalev M. M. Discrete optimization. Integer programming. М.: URSS, 2003. – 190 p. (in Russian).

*Поступила в редакцию – 23 июля 2023 г. Окончательный вариант – 20 октября 2023 г.
Received – July 23, 2023. The final version – October 20, 2023.*