УДК 004.056
DOI: 10.26102/2310-6018/2024.45.2.011

Марковская модель кибератак и ее применение к анализу защищенности информации в автоматизированных системах

Е.В. Трапезников✉, А.А. Магазев, А.А. Касенов

Омский государственный технический университет, Омск, Российская Федерация

Резюме. В работе представлено описание марковской модели кибератак как метода анализа защищенности информации в автоматизированных системах. На основе представленной модели в работе дается описание двух метрик безопасности – среднего времени до отказа безопасности (среднее число переходов между состояниями в соответствующей марковской цепи до ее первого попадания в одно из поглощающих состояний) и среднего риска при отказе безопасности (сумма произведений ущербов при реализации каждой из кибератак на соответствующие вероятности реализации этих кибератак). Дается алгоритм оценки входных параметров на основе взаимосвязи баз данных угроз и уязвимостей CVE, CWE и CAPEC. Описанные в работе взаимосвязи позволяют вычислить вектор вероятностей возникновения кибератак и вектор ущербов от кибератак, которые формируются как входные данные для модели оценки защищенности. Также в работе рассматривается проблема численной оценки параметров через метрики CVSS. В исследовании демонстрируется, что вектор вероятностей отражения кибератак и вектор вероятностей «задержек» кибератак возможно получить только с помощью метода экспертных оценок, либо статистики. В работе также дается описание разработанного программного продукта, который позволяет выполнить оценку защищенности автоматизированной системы на заданном промежутке времени.

Ключевые слова: метрики безопасности, метрика CVSS, CVE, CWE, CAPEC, модель кибератак, алгоритм сбора данных, автоматизированная система, марковская цепь, метод экспертных оценок.

Благодарности: Исследование частично выполнено за счет гранта Российского научного фонда № 24-21-20025, https://rscf.ru/project/24-21-20025/

Для цитирования: Трапезников Е.В., Магазев А.А., Касенов А.А. Марковская модель кибератак и ее применение к анализу защищенности информации в автоматизированных системах. *Моделирование, оптимизация и информационные технологии.* 2024;12(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1554 DOI: 10.26102/2310-6018/2024.45.2.011

The Markov model of cyber attacks and its application to the analysis of information security in automated systems

E.V. Trapeznikov✉, A.A. Magazev, A.A. Kasenov

Omsk State Technical University, Omsk, the Russian Federation

Abstract. The paper presents a description of the Markov model of cyber attacks as a method for analyzing information security in automated systems. Based on the presented model, the work provides a description of two safety metrics - the average time to safety failure (the average number of transitions between states in the corresponding Markov chain before it first enters one of the absorbing states) and the average risk in case of safety failure (the sum of the products of damages during the implementation of each from cyber attacks to the corresponding probabilities of these cyber attacks). An algorithm for estimating input parameters is given based on the relationship between the threat and vulnerability databases CVE, CWE and CAPEC. The relationships described in the work allow us to calculate the vector of probabilities of the occurrence of cyber attacks and the vector of damage from cyber attacks, which are formed as input data for the security assessment model. The paper also addresses the problem

of numerical estimation of parameters through CVSS metrics. The study demonstrates that the vector of probabilities of repelling cyber attacks and the vector of probabilities of “delays” of cyber attacks can only be obtained using the method of expert assessments or statistics. The work also provides a description of the developed software product, which allows one to assess the security of an automated system over a given period of time.

Keywords: security metrics, CVSS metric, CVE, CWE, CAPEC, cyberattack model, data collection algorithm, automated system, Markov chain, expert assessment method.

Acknowledgements: The research was partially supported by a grant from the Russian Science Foundation № 24-21-20025, https://rscf.ru/project/24-21-20025/

For citation: Trapeznikov E.V., Magazev A.A., Kasenov A.A. The Markov model of cyber attacks and its application to the analysis of information security in automated systems. *Modeling, Optimization and Information Technology*. 2024;12(2). URL: https://moitvivt.ru/ru/journal/pdf?id=1554 DOI: 10.26102/2310-6018/2024.45.2.011 (In Russ.).

Введение

Опыт использования автоматизированных систем (АС) показал, что в большинстве случаев нарушение надежности их функционирования связано с попытками несанкционированного доступа (НСД) к информационным ресурсам [1]. При формировании требований к средствам защиты в АС руководствуются международными стандартами по информационной безопасности, отраслевыми стандартами и ГОСТами, а также руководящими документами ФСТЭК России (ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»). Анализ этих и других нормативных актов выявил, что наиболее важным моментом при эксплуатации автоматизированных систем является оценка эффективности используемых систем защиты информации (СЗИ) и их оптимальное конфигурирование. С другой стороны, требования к применяемым средствам защиты информации в автоматизированных системах определяются руководящими документами ФСТЭК России и задаются классами защищенности этих систем. К сожалению, данная методика не пригодна для получения точных количественных оценок эффективности СЗИ от НСД, которые часто необходимы пользователям АС, особенно в коммерческом секторе экономики. Также следует отметить недостаточно разработанное математическое обеспечение для оценки эффективности функционирования СЗИ от НСД в АС, которое учитывало бы различные аспекты их эксплуатации. Таким образом, проблема создания универсальной системы показателей, а также разработки новых моделей и алгоритмов оценки эффективности СЗИ от НСД, остается все еще актуальной.

Ясно, что любые подходы к количественной оценке эффективности СЗИ в АС должны базироваться на строгих математических моделях. На настоящий момент таких математических моделей разработано довольно много, например, [2], причем выбор конкретной из них зависит от тех характеристик функционирования СЗИ, которые необходимо принять во внимание в конкретной задаче. При этом желательно, чтобы используемая модель предоставляла возможность точно и эффективно вычислять эти характеристики в как можно более широком диапазоне входных параметров моделируемой системы.

В контексте оценки эффективности СЗИ, все большую популярность среди математических моделей кибербезопасности приобретают теоретико-вероятностные или стохастические модели, формулированные на языке теории марковских цепей [3–5]. Данная группа моделей дает возможность количественного описания процессов

взаимодействия между «злоумышленником» и «защитником» информационной системы, рассматривая такие процессы, как случайные переходы между ее различными состояниями. При этом принимаются во внимание такие важные аспекты эксплуатации СЗИ, как время функционирования системы до момента отказа безопасности, а также величина среднего ущерба от реализации той или иной кибератаки. Применительно к оценке эффективности СЗИ от НСД в АС возможность применения таких моделей была отмечена некоторыми из отечественных авторов [6, 7]. Отметим, что в работе [7] авторы преимущественно используют численные и имитационные методы моделирования, в то время как в статье [6] доминирует именно аналитическая точка зрения.

В дальнейшем класс марковских моделей, предложенных в работе [6], был тщательно исследован и расширен [8–10]. Важной особенностью именно этих моделей является возможность получения на их основе преимущественно аналитических оценок эффективности СЗИ (метрик безопасности), что избавляет от использования трудоемких имитационных или численных методов моделирования. Кроме того, аналитические оценки легко масштабируются и могут быть применены к системам с любым числом актуальных кибератак, в то время как трудоемкость применения имитационного моделирования, как правило, возрастает с их ростом, замедляя расчеты. Однако, рассмотренные в [6, 8–10] модели обладают рядом недостатков, среди которых наиболее важными мы считаем два. Во-первых, в этих моделях длительности кибератак считаются одинаковыми, что, конечно же, не реалистично. Во-вторых, рассматриваемые в данных моделях марковские цепи обладают лишь одним поглощающим состоянием, символизирующим отказ безопасности при успешной реализации любой из атак. Эта особенность не позволяет дифференцировать между собой различные типы отказов, произошедшие в результате реализации различных кибератак.

Указанные недостатки были исправлены авторами настоящей статьи в работе [11] путем модификации марковских моделей, рассмотренных ранее в работах [8–10]. Данная модификация, однако, имела и свою цену: ввиду усложнений не удалось получить явные аналитические формулы для вероятностей состояний соответствующей марковской цепи. С другой стороны, аналитические результаты все же были получены для двух метрик безопасности: среднего времени до отказа безопасности и среднего ущерба от реализации атаки.

Основная цель настоящей статьи – применение модифицированной марковской модели атак, изложенной в [11], к задаче оценки эффективности СЗИ от НСД в АС. В частности, мы излагаем методику формирования основных входных данных модели с привлечением известных систем каталогизации уязвимостей CVE и CWE, а также с использованием системы оценки уязвимостей CVSS. Мы также приводим описание разработанного нами для этих целей программного обеспечения.

Описание марковской модели атак и вычисление метрик безопасности

В работе [11] была представлена марковская модель кибератак, представляющая собой очередной этап модификации моделей, рассмотренных в работах [6, 8–10]. Изложим здесь основные положения этой модели.

Информационная (автоматизированная) система рассматривается как система с конечным числом $2n + 1$ различных состояний: $S_0, \dots, S_{2n}$. Состояние S_0 характеризуется отсутствием кибератак и называется *безопасным.* Состояния $S_1, \dots, S_n$ ассоциируются с n возможными кибератаками, а состояния $S_{n+1}, \dots, S_{2n}$ – с отказами *безопасности*, возникающими в результате реализации соответствующих кибератак. Между данными состояниями АС возможны следующие переходы (Рисунок 1).

1. Если в момент времени t система находится в состоянии S_0, то в момент времени $t+1$ система с вероятностью q_i может оказаться в состоянии S_i, либо с вероятностью $q_0 \equiv 1 - \sum_{i=1}^{n} q_i$ останется в прежнем состоянии S_0.

2. Если в момент t система находится в одном из состояний S_i, где $i = 1, \dots, n$, 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 i-ое состояние отказа безопасности S_{n+i} с вероятностью $\tilde{r}_i = 1 - r_i - d_i$ (кибератака успешно осуществилась).

3. Оказавшись в момент t в одном из состояний отказа безопасности S_{n+i}, система останется в нем навсегда, то есть состояния $S_{n+1}, \dots, S_{2n}$ – поглощающие.

Согласно изложенным выше положениям, модель АС эволюционирует следующим образом: в начальный момент времени $t = 0$ система находится в состоянии S_0, а затем случайным образом блуждает между различными состояниями в соответствии со свойством марковости. Эта эволюция позволяет рассматривать динамику модели как марковскую цепь с дискретным временем и конечным числом состояний.

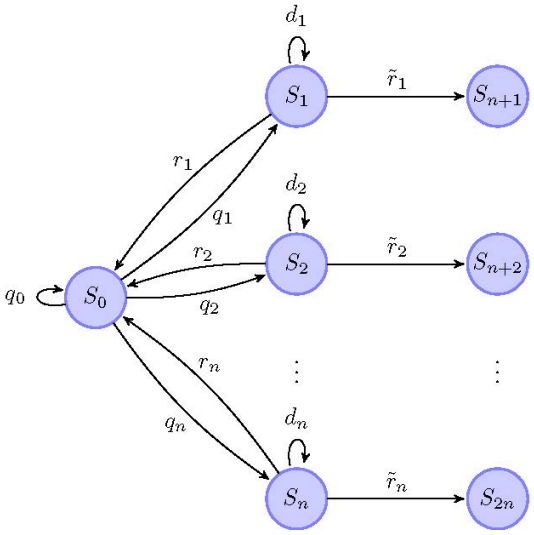

Рисунок 1 – Граф переходов марковской цепи, ассоциированной с АС
Figure 1 – Transition graph of the Markov chain associated with the AS

Обозначим через $p_i(t)$ вероятность состояния S_i в момент времени t. Согласно общей теории марковских цепей, вероятности $p_i(t)$ могут быть вычислены в соответствии с векторно-матричной формулой

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

где $\mathbf{p}(t) = \big(p_0(t), \dots, p_{2n}(t)\big)$ – вектор вероятностей состояний цепи в момент t; Π – *матрица переходных вероятностей* марковской цепи (определяется в соответствии с графом переходов, изображенном на Рисунке 1; $\mathbf{p}(0) = (1,0, \dots, 0)$ – вектор вероятностей состояний цепи в момент времени $t = 0$ (предполагается, что в этот момент времени система достоверно находится в безопасном состоянии). Следует отметить, что в общем виде получить явные аналитические формулы для вычисления вероятностей $p_i(t)$ не удается, хотя для некоторых частных случаев это возможно [11].

Итак, описанная модель кибератак на АС задается набором $3n$ входных параметров:

– n-мерным вектором вероятностей возникновения кибератак $q = (q_1, \dots, q_n)$;
– n-мерным вектором вероятностей их отражения $r = (r_1, \dots, r_n)$;

– n-мерным вектором вероятностей «задержек» кибератак $d = (d_1, \dots, d_n)$.

Несмотря на то, что явные аналитические выражения для вероятностей состояний $p_i(t)$ выписать не удается, описанная марковская модель позволяет это сделать для двух важнейших метрик безопасности – *среднего времени до отказа безопасности* τ и величины *среднего ущерба* R от реализации кибератаки. Данные метрики могут быть использованы для количественной оценки эффективности СЗИ от НСД в АС как по отдельности, так и в составе некоторой общей интегральной оценки. Кроме того, данные метрики могут быть рассмотрены в качестве целевых функций в различных задачах оптимизации СЗИ [9, 10].

Напомним определение этих двух метрик и приведем явные формулы для их вычисления в рамках рассматриваемой модели атак на АС.

Среднее время до отказа безопасности – это среднее число переходов между состояниями в соответствующей марковской цепи до ее первого попадания в одно из поглощающих состояний. В работе [11] было показано, что эта величина вычисляется в соответствии с формулой

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

Здесь δ_{ij} – символ Кронекера, равный единице, если $i = j$, и нулю – в обратном случае.

Средний ущерб (риск) при отказе безопасности – это сумма произведений ущербов при реализации каждой из кибератак на соответствующие вероятности реализации этих кибератак. 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 ущерб (риск) по формуле $R_i = P_i U_i$. Тогда *средний ущерб* R, связанный с любым из отказов безопасности системы, это – математическое ожидание случайной величины R_i. В работе [11] была получена формула расчета среднего ущерба для рассмотренной марковской модели:

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

Таким образом, для использования данной формулы, помимо перечисленных выше параметров модели, требуется ввести еще n дополнительных параметров $U_1, U_2, \dots, U_n$.

Оценка параметров модели

Основная трудность применения многих моделей информационной безопасности – проблема получения входных параметров модели. На сегодняшний день эта проблема, в основном, решается двумя способами: накопление статистики об инцидентах или экспертный метод. Оба эти подхода, однако, не свободны от недостатков; накопление статистики – это трудоемкий и затратный процесс, в то время как экспертные подходы во многом субъективны.

Как было указано выше, входные параметры нашей модели АС – это четыре вектора:

1) вектор вероятностей возникновения кибератак q;
2) вектор вероятностей отражения кибератак r;
3) вектор вероятностей «задержек» кибератак d;
4) вектор ущербов от кибератак U.

Каждый из представленных параметров требует своей оценки для получения достоверных результатов в результате оценки защищенности.

Как известно, сама возможность осуществления кибератаки на информационную систему тесно связана с наличием в последней различных *уязвимостей*. На сегодняшний день существует некоторое количество систем каталогизации уязвимостей ПО, в которых, помимо информации о самих уязвимостях и методах их смягчения, приводится также информация об их опасности, эксплуатируемости и вероятности использования. В частности, самая известная общемировая база данных уязвимостей CVE (Common Vulnerabilities and Exposures) на регулярной основе обновляет свои каталоги как самостоятельно, так и с помощью партнеров, которые сотрудничают с программой CVE. Российское решение в виде банка данных угроз безопасности информации (БДУ ФСТЭК) агрегирует в себе угрозы и уязвимости, в том числе российского программного обеспечения, некоторые из которых нельзя встретить в базе данных CVE. В свою очередь БДУ ФСТЭК содержит в себе ссылки на базу данных CVE.

Стоит отметить, что многие уязвимости можно классифицировать на основе ряда присущих им общих признаков. Такая классификация была выработана мировым сообществом и объединена в единую базу данных недостатков («слабостей») программного и аппаратного обеспечения (Common Weakness Enumeration или сокращенно CWE). «Слабость» – это состояние в программном обеспечении, микропрограммном обеспечении, аппаратном обеспечении или сервисном компоненте, которое при определенных обстоятельствах может способствовать внедрению уязвимостей. Данная база обновляется в среднем раз в три-четыре года. «Слабости», в свою очередь, приводят уже к возможным сценариям кибератак, которые каталогизированы и описаны в реестре шаблонов атак (Common Attack Pattern Enumerations and Classifications (CAPEC)).

Указанные выше системы каталогизации взаимосвязаны; на Рисунке 2 схематически представлены имеющиеся зависимости.

Рисунок 2 – Взаимосвязи систем
Figure 2 – System interconnections

Эти зависимости позволяют (по крайней мере, в принципе) на основе имеющегося списка выявленных уязвимостей АС сформировать актуальный перечень кибератак и оценить вероятность реализации каждой из них. Опишем, как это может быть сделано.

Допустим, что на основе данных, полученных при сканировании программного обеспечения АС, обнаружен список уязвимостей $V = \{CVE_k : k = 1, \dots, N\}$. Каждой уязвимости CVE_k из этого списка отвечает определенная «слабость» $CWE(CVE_k)$, которой, в свою очередь, отвечает некоторый список возможных сценариев атак: $CAPEC(CVE_k)$. В каждом таком списке атаки могут дублироваться. Более того, один и тот же сценарий атаки может встречаться в различных списках атак, ассоциированных с разными уязвимостями. Объединив между собой все списки $CAPEC(CVE_k)$ и подсчитав кратность вхождения в этот объединенный список каждой из атак, мы получаем следующие данные: множество актуальных для нашей системы сценариев атак $CAPEC_i$ и соответствующих им частот встречаемости m_i: $A = \{(CAPEC_i, m_i) : i = 1, \dots, n\}$. Логично предположить, что вероятность q_i реализации i-ого сценария атаки является пропорциональной кратности m_i вхождения этого сценария в наш объединенный список: $q_i \sim m_i$. Далее, в описании каждого из сценариев атак в каталоге CAPEC имеется

поле «Likelihood Of Attack», характеризующее абсолютную частоту встречаемости данного сценария. Это поле принимает три возможных символьных значения («low», «medium» и «high»), в связи с чем введем еще один числовой параметр k_i, характеризующий данный сценарий атаки $CAPEC_i$:

$$k_i = \begin{cases} 1, & \text{if "Likelihood of Attack "= "low",} \\ 2, & \text{if "Likelihood of Attack" = "medium",} \\ 3, & \text{if "Likelihood of Attack" = "high".} \end{cases}$$

Предполагая, что $q_i \sim k_i$, отсюда получаем

$$q_i = \lambda\, k_i m_i,$$

где нормирующий множитель λ можно определить из равенства

$$\lambda = \frac{1}{T^*_{\mathrm{AT}} \sum_i k_i m_i}.$$

Здесь T^*_{AT} – средний интервал времени между атаками. Оценка величины T^*_{AT} задается либо экспертами, либо определяется по имеющейся статистике об инцидентах для данной АС.

Для оценки вектора ущербов от кибератак U можно использовать систему оценок уязвимостей CVSS (англ. Common Vulnerability Scoring System) – открытый стандарт, используемый для расчета количественных оценок уязвимостей. Напомним, что интегральной оценкой каждой из известных уязвимостей является ее *рейтинг* – число от 0 до 10.

Выше мы уже отмечали зависимость между системами каталогизации CVE, CWE и CAPEC (Рисунок 2). Для оценки ущерба от каждого из сценариев атак $CAPEC_i$ сформируем множество $CVE(CAPEC_i) = \{v_{i,1}, v_{i,2}, \dots, v_{i,l}\}$ – набор тех уязвимостей из множества V, которые делают возможным использование данного сценария $CAPEC_i$. Тогда в качестве ущерба от i-го сценария атаки U_i можно выбрать средний рейтинг уязвимостей из множества $CVE(CAPEC_i)$:

$$U_i = \frac{1}{l} \sum_{j=1}^{l} CVSS(v_{i,j}).$$

Здесь $CVSS(v_{i,j})$ – рейтинг уязвимости $v_{i,j}$ из списка $CVE(CAPEC_i)$.

К сожалению, входные параметры как вектор вероятности отражения (r) и задержек кибератак (d) получить представленным выше методом затруднительно, поэтому в рамках нашего подхода данные параметры оцениваются с помощью экспертов.

Программная реализация модели

Представленная модель была реализована нами в виде программного обеспечения для анализа защищенности в автоматизированной системе (Рисунок 3).

Программное обеспечение реализуется на языке программирования C#, база данных используется PostgreSQL.

В общем виде программное обеспечение реализует следующий алгоритм:

Пользователю предоставляется возможность провести аудит автоматизированной системы на основе анкетирования.

1. После аудита необходимо загрузить данные об актуальных уязвимостях для автоматизированной системы.

2. Перечень уязвимостей позволяет в автоматическом режиме сформировать зависимость CVE (БДУ ФСТЭК) – CWE – CAPEC, что в дальнейшем позволит произвести расчет.

3. Метрики CVSS также будут рассчитаны автоматически.

4. Наша модель не предполагает расчет векторов вероятностей отражения и задержек кибератак, поэтому пользователю необходимо произвести оценку с помощью экспертов через соответствующий модуль внутри программного обеспечения.

5. Подготовленные оценки позволяют выполнить расчет и предоставить пользователю соответствующий отчет.

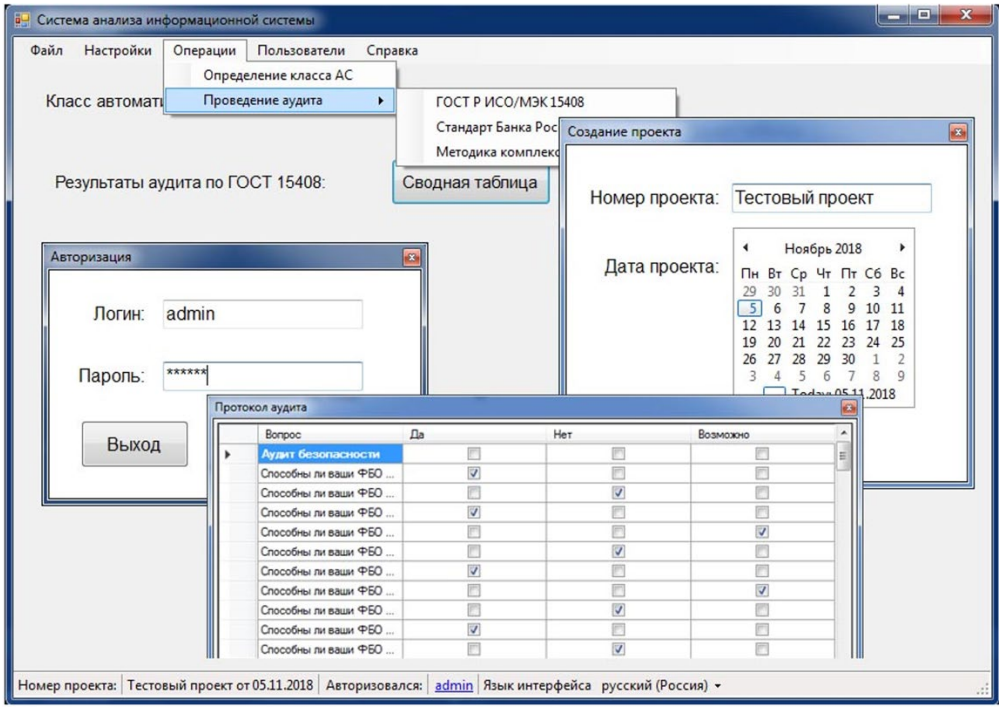

Рисунок 3 – Пример интерфейса
Figure 3 – Interface example

Вся необходимая информация в процессе деятельности сохраняется внутри базы данных и позволяет пользователю анализировать историю изменения оценки защищенности для выработки соответствующих решений. Наличие программного обеспечения позволяет производить необходимые расчеты в достаточно короткие сроки.

Обсуждение и заключение

Обеспечение защиты информации в настоящее время ставится одной из основных целей любой организации. Как было представлено в исследовании, существует множество подходов к решению данной проблемы. В настоящей работе была представлена марковская модель кибератак как метод анализа и оценки защищенности информации в автоматизированной системе. На основе модели было описано две метрики безопасности, которые призваны оценить стойкость системы защиты информации и ее возможности по отражению атак. В работе было продемонстрировано, что вектор вероятностей возникновения кибератак возможно получить через взаимосвязь известных баз данных, таких как CVE, CWE и CAPEC. В работе также показано, что с помощью применения общей системы уязвимостей CVSSv3 вектор ущерба от кибератак может быть оценен на основе малого числа эмпирических данных,

что является несомненным преимуществом по сравнению, например, с методом экспертных оценок. Однако, метод экспертных оценок также используется для формирования входных данных, таких как вектор отражения и задержек кибератак. Стоит отметить, что описанная нами модель кибератак имеет ряд допущений, связанных, в частности, с невозможностью одновременного появления нескольких кибератак, а также с их независимостью друг от друга. Представленные допущения представляются нам перспективными для дальнейшего исследования и улучшения нашей модели, что в будущем позволит нам получить более обобщенную модель. Представленное программное обеспечение было апробировано на действующих организациях и показало свою эффективность как один из элементов по оценке защищенности информации.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Бокова О.И., Дровникова И.Г., Етепнев А.С., Рогозин Е.А., Хвостов В.А. Методики оценивания надежности систем защиты информации от несанкционированного доступа в автоматизированных системах. *Труды СПИИРАН*. 2019;18(6):1301–1332. https://doi.org/10.15622/sp.2019.18.6.1301-1332.
   Bokova O.I., Drovnikova I.G., Etepnev A.S., Rogozin E.A., Khvostov V.A. Methods of estimating reliability of information security systems which protect from unauthorized access in automated systems. *Trudy SPIIRAN = SPIIRAS Proceedings.* 2019;18(6):1301–1332. (In Russ.). https://doi.org/10.15622/sp.2019.18.6.1301-1332.
2. Девянин П.Н. *Модели безопасности компьютерных систем.* Москва: Издательский центр «Академия»; 2005. 144 с.
   Devyanin P.N. *Modeli bezopasnosti komp'yuternykh sistem.* Moscow: Publishing House Academia; 2005. 144 p. (In Russ.).
3. Abraham S., Nair S. Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains. *Journal of Communications*. 2014;9(12):899–907. https://doi.org/10.12720/jcm.9.12.899-907.
4. Almasizadeh J., Mohammad A.A. A stochastic model of attack process for the evaluation of security metrics. *Computer Networks*. 2013;57(10):2159–2180. https://doi.org/10.1016/j.comnet.2013.03.011.
5. Zhang Y., Malacaria P. Optimization-Time Analysis for Cybersecurity. *IEEE Transactions on Dependable and Secure Computing*. 2021;19(4):2365–2383. https://doi.org/10.1109/TDSC.2021.3055981.
6. Росенко А.П. Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе. *Известия ЮФУ. Технические науки.* 2008;(8):71–81.
   Rosenko A.P. Mathematical modelling of internal threats on safety of the confidential information circulating in automated information system availability. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences.* 2008;(8):71–81. (In Russ.).
7. Дровникова И.Г., Мещерякова Т.В., Попов А.Д., Рогозин Е.А., Ситник С.М. Математическая модель оценки эффективности систем защиты информации с использованием преобразования Лапласа и численного метода Гивенса. *Труды СПИИРАН*. 2017;(3):234–258. https://doi.org/10.15622/sp.52.11.
   Drovnikova I.G., Meshcheryakova T.V., Popov A.D., Rogozin E.A., Sitnik S.M. Mathematical model for estimating the efficiency of information security systems by means of Laplace transformation and Givens method. *Trudy SPIIRAN = SPIIRAS Proceedings.* 2017;(3):234–258. (In Russ.). https://doi.org/10.15622/sp.52.11.

8. Магазев А.А., Цырульник В.Ф. Исследование одной марковской модели угроз безопасности компьютерных систем. *Моделирование и анализ информационных систем*. 2017;24(4):445–458. https://doi.org/10.18255/1818-1015-2017-4-445-458.
Magazev A.A., Tsyrulnik V.F. Investigation of a Markov model for computer system security threats. *Modelirovanie i analiz informatsionnykh sistem = Automatic Control and Computer Sciences*. 2018;52(7):615–624. https://doi.org/10.3103/S0146411618070180.
9. Magazev A.A., Tsyrulnik V.F. Optimizing the selection of information security remedies in terms of a Markov security model. *Journal of Physics: Conference Series*. 2018;1096. https://doi.org/10.1088/1742-6596/1096/1/012160.
10. 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. https://doi.org/10.18255/1818-1015-2020-1-108-123.
Kassenov A.A., Magazev A.A., Tsyrulnik V.F. A Markov Model of Non-Mutually Exclusive Cyber Threats and its Applications for Selecting an Optimal Set of Information Security Remedies. *Modelirovanie i analiz informatsionnykh sistem = Automatic Control and Computer Sciences*. 2020;27(1):108–123. (In Russ.). https://doi.org/10.18255/1818-1015-2020-1-108-123.
11. Касенов А.А., Магазев А.А., Трапезников Е.В. Применение одной марковской модели кибератак для оценки метрик безопасности. *Математические структуры и моделирование*. 2020;(2):129–144. https://doi.org/10.24147/2222-8772.2020.2.129-144.
Kassenov A.A., Magazev A.A., Trapeznikov E.V. Using a Markov cyberattack model for evaluation of security metrics. *Matematicheskie struktury i modelirovanie = Mathematical Structures and Modeling*. 2020;(2):129–144. (In Russ.). https://doi.org/10.24147/2222-8772.2020.2.129-144.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Трапезников Евгений Валерьевич, старший преподаватель кафедры «Комплексная защита информации», Омский государственный технический университет, Омск, Российская Федерация.
e-mail: evtrapeznikov@yandex.ru
ORCID: http://orcid.org/0000-0003-3205-193X

Evgeny V. Trapeznikov, senior Lecturer of the Department of "Integrated Information Protection", Omsk State Technical University, Omsk, the Russian Federation.

Магазев Алексей Анатольевич, доктор физико-математических наук, профессор кафедры «Комплексная защита информации», Омский государственный технический университет, Омск, Российская Федерация.
e-mail: magazev@mail.ru
ORCID: http://orcid.org/0000-0002-8725-9183

Aleksey A. Magazev, Doctor of Physical and Mathematical Sciences, Professor of the Department of "Integrated Information Security", Omsk State Technical University, Omsk, the Russian Federation.

Касенов Адиль Аскарович, ассистент кафедры «Комплексная защита информации», Омский государственный технический университет, Омск, Российская Федерация.
ORCID: http://orcid.org/0000-0002-2770-1144

Adil A. Kasenov, Assistant of the Department of "Integrated Information Protection", Omsk State Technical University, Omsk, the Russian Federation.

Статья поступила в редакцию 15.04.2024; одобрена после рецензирования 22.04.2024; принята к публикации 28.04.2024.

The article was submitted 15.04.2024; approved after reviewing 22.04.2024; accepted for publication 28.04.2024.