05.13.18

ОЦЕНКА УРОВНЯ ЗАЩИЩЁННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА ОСНОВЕ МАРКОВСКОЙ МОДЕЛИ КИБЕРУГРОЗ

Е.В. Трапезников[1], А.А. Магазев[1]

[1] *ФГБОУ ВО «Омский государственный технический университет» (ОмГТУ), г. Омск*

В настоящей работе исследуется вопрос оценки защищенности автоматизированной системы обработки информации различного класса. Предлагается алгоритм проведения такой оценки с помощью одно стохастической марковской модели защиты информации. Алгоритм также включает в себя сбор и анализ исходных данных, использующий известную базу данных угроз и уязвимостей ФСТЭК РФ, а также последующую их экспертную оценку. Предлагаемый алгоритм реализован в виде программного средства.

Ключевые слова: автоматизированная система, марковская цепь, киберугрозы, экспертная оценка, уровень защищенности.

ВВЕДЕНИЕ

Современные автоматизированные системы обработки и хранения информации имеют дело с большими массивами данных различного рода. Для обеспечения их целостности и доступности используются различные наборы средств защиты, необходимые и достаточные для определенного класса автоматизированных систем. Одной из наиболее важных проблем в области информационной безопасности является определение и обоснование количественных оценок защищенности данных в автоматизированных системах, а также гарантирование соответствующего уровня их безопасности в критически важных объектах.

В настоящее время существуют различные методы и подходы к оценке защищенности информации. Наиболее распространенные из них – это *метод натурных испытаний* (достаточно дорогостоящий и длительный процесс), а также *метод математического моделирования*, который вследствие своей доступности и дешевизны получил широкое распространение, как в нашей стране, так и за рубежом. Как следствие, число научных исследований, посвященных разработке и анализу моделей защиты информации, неуклонно растет из года в год, а используемый в них математический арсенал постоянно расширяется.

Наиболее распространённый способ моделирования систем защиты информации состоит в использовании *стохастических марковских процессов*. При этом число задач, решаемых с применением подобных моделей, оказывается неожиданно большим: обнаружение кибератак и вопросы стратегического управления информационной безопасностью [1-4], системы обнаружения уязвимостей [5], определение показателей надежности для VoIP [6], а также определение количественных метрик, определяющих уровень безопасности защищаемой системы [7]. Среди отечественных работ следует выделить статью [8], в которой авторы оценивают ряд характеристик надежности и безопасности информационных систем, основываясь на некотором классе марковских моделей. В данной работе авторы делают важное заключение о том, что в качестве основного элемента безопасности должны выступать не угрозы атаки, а угрозы уязвимости. Это позволило интерпретировать киберугрозы соответствующими схемами резервирования, заимствованными из теории надежности. Отметим здесь также работу [9], в которой авторы использовали динамические марковские модели для обнаружения аномалий в различных данных, в том числе и с позиций защиты информации.

В цикле статей А. П. Росенко [10-13] был предложен класс стохастических марковских моделей, в которых защищаемая система рассматривалась как система с отказами и восстановлениями. Дальнейшее развитие эти модели получили в работах [14, 15], в которых авторы провели детальное аналитическое исследование соответствующих марковских цепей, ввели важные функционально-временные характеристики системы, а также сформулировали задачу о выборе оптимальной конфигурации средств защиты информации. Основной целью настоящей статьи является применение указанной модели для задачи оценки уровня информации защищенности в автоматизированных системах. В частности, мы приводим поэтапный алгоритм решения данной задачи с кратким описанием самой модели, а также реализовываем его в виде специализированного программного обеспечения, функционирующего в связке с базой данных угроз и уязвимостей ФСЭК РФ.

МАРКОВСКАЯ МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Марковская модель системы защиты информации представляет собой марковскую цепь с $n + 2$ состояниями, где n – число различных киберугроз, действующих на систему [14]. Состояние s_0 соответствует

отсутствию воздействия какой-либо киберугрозы; назовем его *безопасным*. Состояния s_1, …, s_n символизируют появление соответствующей киберугрозы, для отражения которой система защиты привлекает имеющиеся механизмы и средства защиты. В случае отражения угрозы, цепь возвращается в состояние s_0. В обратном случае угроза считается реализованной, что приводит к возникновению инцидента нарушения информационной безопасности. В этой ситуации цепь переходит в финальное состояние s_f, которое является поглощающим. Граф состояний марковской цепи приведен на рис. 1.

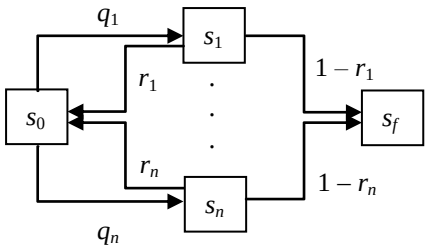

Рис. 1. Граф состояний марковской цепи

Динамика марковской цепи представляет собой последовательность переходов между состояниями s_1, …, s_n, s_f. Входными параметрами модели являются:

– вероятности q_i переходов из s_0 в s_i ; эти вероятности интерпретируются как вероятности появления угроз за выбранный интервал времени;

– вероятности r_i отражения возникших угроз имеющимися средствами и механизмами защиты.

В рамках рассматриваемой модели принимаются также следующие допущения:

– все переходы происходят только в фиксированные моменты времени (дискретное время);

– очередная киберугроза появляется, только если успешно ликвидирована предыдущая.

В работе [14] были получены явные аналитические выражения для вероятностей состояний описываемой марковской цепи:

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

$$p_i(t) = p_0(t-1)q_i, \quad i = \overline{1,n}; \qquad (2)$$

$$p_f(t) = 1 - p_0(t) - (1-q_0)\,p_0(t-1). \qquad (3)$$

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

Из формулы для $p_0(t)$ в частности следует, что марковская цепь будет периодически возвращаться в состояние s_0, однако со временем вероятность этого события будет экспоненциально стремится к нулю. Иными словами, рано или поздно система окажется в финальном состоянии s_f. Принимая неизбежность подобного исхода, мы, тем не менее, можем быть заинтересованы в как можно более продолжительном функционировании системы. Для проведения соответствующей оценки введем следующую временную характеристику марковской цепи. *Временем жизни* марковской цепи назовем момент времени T, в котором марковская цепь впервые оказалась в финальном состоянии s_f. Очевидно, что время жизни – случайная величина, зависящая от входных параметров модели q_i и r_i. Далее для оценки уровня защищенности мы будем использовать математическое ожидание данной случайной величины:

$$\mathbf{M}_T(q,r) = \sum_{t=0}^{\infty} P(T)T\,, \qquad (4)$$

где $P(T)$ – распределение вероятностей случайной величины T. Данное распределение нетрудно получить, если известны выражения (1)–(3) для вероятностей состояний марковской цепи (рис. 1):

$$P(T) = p_0(T-2)\sum_{i=1}^{n} q_i(1-r_i)\,. \qquad (5)$$

Подставляя (5) в (4) и суммируя возникающий после этого бесконечный ряд, получаем итоговое выражение для среднего времени жизни марковской цепи:

$$\mathbf{M}_T(q,r) = \frac{1 + \sum_{i=1}^{n} q_i}{\sum_{i=1}^{n} (1-r_i)q_i}\,. \qquad (6)$$

АЛГОРИТМ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ И ЕГО РЕАЛИЗАЦИЯ

Как указывалось во введении, основным результатом настоящей работы является разработка поэтапного алгоритма оценки уровня защищенности автоматизированной системы хранения и обработки информации. Следует отметить, что, несмотря на высокую частоту кибератак на современные автоматизированные системы, последние проводят гораздо больше времени в безопасном состоянии, которое, однако, постоянно чередуется с состояниями сбоя. На наш взгляд, оценка уровня безопасности таких систем с точки зрения статических свойств, таких как обнаружение уязвимостей или эффективность служб безопасности, не дает реалистичного представления об истинном уровне безопасности. Безопасность автоматизированной системы лучше всего оценивать с учетом ее функционально-временных параметров, характеризующих длительность ее успешного функционирования в течении заданного периода времени. Для этих целей может быть привлечена марковская модель, описанная нами в предыдущем разделе.

В обобщенном виде алгоритм оценки уровня защищенности автоматизированной системы изображен на рис. 2.

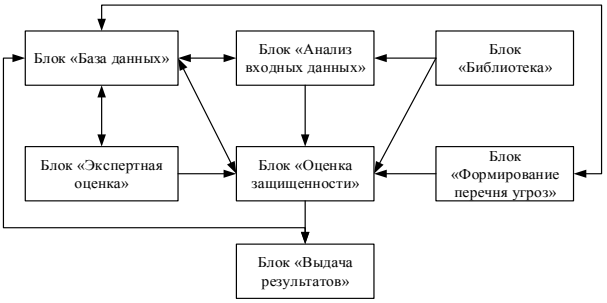

Рис. 2. Схема модели

Как видно из рисунка, алгоритм состоит из семи основных взаимосвязанных блоков:

- блок «Библиотека»;
- блок «База данных»;
- блок «Анализ входных данных»;
- блок «Оценка защищённости»;
- блок «Формирования перечня угроз»;
- блок «Экспертная оценка»;
- блок «Выдача результатов».

Блок «База данных» содержит базы данных угроз и уязвимостей ФСТЭК РФ, потенциально опасных для автоматизированных систем обработки и хранения информации (особенно, для критически важных объектов). Блок «Библиотека» представляет собой совокупность актуальной нормативно-правовой документации, требуемой для организации защиты информации в автоматизированных системах. Данные из этих двух блоков существенно используются в блоке «Анализ входных данных», в котором для каждой конкретной автоматизированной системы определяется ее класс защищенности, а также проводится сбор и оценка дополнительных данных, требуемых для работы блока «Оценка защищенности». Детальное описание этого блока см. в работах [16,17].

Отметим, что для определения текущего состояния системы сформирован набор анкет, которые составлены с использованием нормативных документов [18]. Сопоставление анкетных данных с набор уязвимостей и угроз определяет возможный перечень атак на систему защиты информации. При этом во время сбора исходных данных определяется текущий набор средств защиты.

Далее все собранные данные передаются в блок «Экспертная оценка». Оценка полученной информации осуществляется группой экспертов (5–10 чел.), итоговая цель которых – оценить вероятности возникновения угроз q_i, выбранных из сформированного ранее списка, а также вероятности r_i отражения этих угроз имеющимися средствами защиты. Предоставленные экспертами оценки проходят последующую стадию статистической обработки в соответствие со стандартными методиками обработки экспертной информации. В частности, определяются коэффициенты компетентности экспертов, которые учитываются при получении конечных взвешенных оценок.

Подготовленные данные переходят в блок «Оценка защищенности». Основа блока – стохастическая марковская модель киберугроз, описанная в предыдущем разделе. Для формирования оценки задается еще один дополнительный параметр системы – критическое время ее безопасного функционирования T_{cr}. После того, как в блок «Оценка защищенности» поступили входные данные модели – вероятности q_i и r_i – производится расчет средного времени жизни системы в соответствие с формулой (6) и после этого полученный результат сравнивается с параметром T_{cr} . Если среднее время жизни оказывается меньшим, чем T_{cr}, делается вывод о неудовлетворительном уровне защиты (блок «Выдача результатов»). После этого экспертами пересматриваются имеющиеся средства и механизмы кибербезопасности, принимается решение о дополнительных мерах защиты, и все этапы алгоритма осуществляются заново уже с новыми входными данными.

Представленные результаты реализованы как программное обеспечение [19]. Программное обеспечение обеспечивает оценку уровня защищенности на основе представленного алгоритма и модели оценки уровня защищенности на основе стохастической марковской модели киберугроз.

ЗАКЛЮЧЕНИЕ

В работе была рассмотрена стохастическая марковская модель защиты информации, на основе которой предложен новый подход к оцениванию уровня защищенности информации в автоматизированных системах. Для этих целей также был разработан алгоритм сбора и анализа входных данных, основанных на использовании базы данных угроз и уязвимостей ФСТЭК РФ. Приведенный алгоритм оценки был реализован в виде соответствующего программного обеспечения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. J. Tan. Optimal strategy selection approach to moving target defense based on Markov robust game/ J. Tan, C. Lei, H. Zhang, and Y. Cheng // Computers & Security. 2019. Vol. 85. P. 63-76.

2. Lalropuia K.C. Modeling cyber-physical attacks based on stochastic game and Markov processes / K.C. Lalropuia, V. Gupta // Reliability Engineering & System Safety. 2019. Vol. 181. P. 28-37.

3. C. Lei. Incomplete information Markov game theoretic approach to strategy generation for moving target defense / C. Lei, H.-Q. Zhang, L.-M. Wan, L. Liu, and D. Ma // Computer Communications. 2018. Vol. 116. P. 184-199.

4. S. Shin. Advanced probabilistic approach for network intrusion forecasting and detection / S. Shin, S. Lee, H. Kim, and S. Kim // Expert Systems with Applications. 2013. Vol. 40 (1). P. 315-322.

5. T. Kudo. Stochastic modeling of self-evolving botnets with vulnerability discovery / T. Kudo, T. Kimura, Y. Inoue, H. Aman, and K. Hirata // Computer Communications. 2018. Vol. 124. P. 101-110.

6. Gupta V. Semi-Markov modeling of dependability of VoIP network in the presence of resource degradation and security attacks / V. Gupta, S. Dharmaraja // Reliability Engineering & System Safety. 2011. Vol. 96 (12). P. 1627-1636.

7. Almasizadeh J. A stochastic model of attack process for the evaluation of security metrics : Towards a Science of Cyber Security / J. Almasizadeh, M.A. Azgomi // Computer Networks. 2013. Vol. 57 (10) P. 2159-2180.

8. Щеглов К.А. Марковские модели угрозы безопасности информационной системы / К.А. Щеглов, А.Ю. Щеглов // Известия Высших Учебных Заведений. Приборостроение. 2015. Т. 58. № 12. С. 957-965.

9. Ren H. Anomaly detection based on a dynamic Markov model / H. Ren, Z. Ye, Z. Li // Information Sciences. 2017. Vol. 411. P. 52-65.

10. Росенко А.П. Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения / А.П. Росенко, И.В. Бордак // Известия Юфу. Технические Науки. 2015. № 7 (168). С. 6-19.

11. Росенко А.П. Математическое моделирование вероятного ущерба от утечки конфиденциальной информации в автоматизированной информационной системе / А.П. Росенко, Р.С. Аветисов // Вестник Ставропольского Государственного Университета. 2009. № 4. С. 51-61.

12. Росенко А.П. Применение марковских случайных процессов с дискретным параметром для оценки уровня информационной безопасности / А.П. Росенко // Известия Юфу. Технические Науки. 2009. № 11 (100). С. 169-172.

13. 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. № 8 (85). С. 71-81.

14. 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.

15. Magazev A.A. Optimizing the selection of information security remedies in terms of a Markov security model / A.A. Magazev, V.F. Tsyrulnik // Journal of Physics: Conference Series. 2018. Vol. 1096. P. 012160.

16. Трапезников Е.В. Реализация системы оценки уровня защищенности информации в информационной системе / Е.В. Трапезников // Метрология, стандартизация, качество: теория и практика. – Омск: Омский государственный технический университет. 2017. С. 334-339.

17. Трапезников Е.В. Разработка программного обеспечения для реализации процесса аудита состояния защищённости информации / Е.В. Трапезников // Южно-Сибирский научный вестник. 2019. № 2 (26). С. 12-17.

18. ГОСТ Р ИСО/МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. М.: Стандартинформ, 2013.

19. Программа для ЭВМ «Оценка защищенности АРМ»: Свидетельство о государственной регистрации программы для ЭВМ № 2018617812/Е.В. Трапезников. заявл. 18.05.2018 ; опубл. 02.07.2018, RU ОБПБТ № 7

Трапезников Евгений Валерьевич – старший преподаватель кафедры «Комплексная защита информации», ФГБОУ ВО ОмГТУ, тел. +7-913-673-94-76, e-mail: evtrapeznikov@yandex.ru.

Магазёв Алексей Анатольевич – д.ф.-м.н. профессор кафедры «Комплексная защита информации», ФГБОУ ВО ОмГТУ, тел. +7-913-979-15-15, e-mail: magazev@mail.ru.

EVALUATING THE SECURITY LEVEL OF THE AUTOMATED SYSTEM BASED ON A STOCHASTIC MARKOV MODEL OF CYBER THREATS

E.V. Trapeznikov, A.A. Magazev
Omsk State Technical University (OmSTU), Omsk

Abstract – In this paper, we study the issue of evaluating the security of an automated information processing system of a various class. For obtaining of such evaluation, an algorithm based a stochastic Markov model of information security is suggested. The algorithm also includes the collection and analysis of initial data using the threat and vulnerability data base of FSTEC Russia, and their subsequent expert evaluating. The algorithm proposed is realized as a software program.

Keywords: automated system, Markov chain, cyber threats, expert evaluation, security level.

REFERENCES

1. J. Tan, C. Lei, H. Zhang, and Y. Cheng. *Optimal strategy selection approach to moving target defense based on Markov robust game*, In *Computers & Security*, vol. 85. pp. 63-76, 2019.

2. K.C. Lalropuia, V. Gupta. *Modeling cyber-physical attacks based on stochastic game and Markov processes,* In *Reliability Engineering & System Safety*, vol. 181. pp. 28-37, 2019.

3. C. Lei, H.-Q. Zhang, L.-M. Wan, L. Liu, and D. Ma. *Incomplete information Markov game theoretic approach to strategy generation for moving target defense*, In *Computer Communications*, 2018. Vol. 116. P. 184-199.

4. S. Shin, S. Lee, H. Kim, and S. Kim. *Advanced probabilistic approach for network intrusion forecasting and detection*, In *Expert Systems with Applications*, vol. 40 (1). pp. 315-322, 2013.

5. T. Kudo, T. Kimura, Y. Inoue, H. Aman, and K. Hirata. *Stochastic modeling of self-evolving botnets with vulnerability discovery,* In *Computer Communications*, vol. 124. pp. 101-110, 2018.

6. V. Gupta and S. Dharmaraja. *Semi-Markov modeling of dependability of VoIP network in the presence of resource degradation and security attacks*, In *Reliability Engineering & System Safety*, vol. 96 (12). pp. 1627-1636, 2011.

7. J. Almasizadeh and M.A. Azgomi. *Astochastic model of attack process for the evaluation of security metrics : Towards a Science of Cyber Security*, In *Computer Networks*, vol. 57 (10). pp. 2159-2180, 2013.

8. K.A. Scheglov and A.Yu. Scheglov. *Markov models of information system security threat,* In *Proceedings of Higher Educational Institutions. Instrumentation*, vol. 58. no 12. pp. 957-965, 2015

9. H. Ren, Z. Ye, Z. Li. *Anomaly detection based on a dynamic Markov model,* In *Information Sciences*, vol. 411. pp. 52-65, 2017.

10. A.P. Rosenko and I.V. Bordak. *A mathematical model for determining the likelihood of consequences from the implementation by an attacker of threats to the security of information of limited distribution*, In *Izvestia Yufu. Technical science*, no. 7 (168). pp. 6-19, 2015.

11. A.P. Rosenko and R.S. Avetisov. *Mathematical modeling of probable damage from confidential information leakage in an automated information system* In *Bulletin of the Stavropol State University*, no. 4. pp. 51-61, 2009.

12. A.P. Rosenko. *Application of Markov random processes with a discrete parameter to assess the level of information security.* In *Izvestia Yufu. Technical science*, no. 11 (100). pp. 169-172, 2009.

13. A.P. Rosenko. *Mathematical modeling of the influence of internal threats on the security of confidential information circulating in an automated information system*. In *Izvestia Yufu. Technical science*, no. 8 (85). pp. 71-81, 2008

14. A.A. Magazev and V.F. *Investigation of a Markov model of threats to the security of computer systems.* In *Modeling and analysis of information systems*, Vol. 24. no. 4. pp. 445-458, 2017.

15. A.A. Magazev and V.F. Tsyrulnik. *Optimizing the selection of information security remedies in terms of a Markov security model,* In *Journal of Physics: Conference Series*, vol. 1096. pp. 012160, 2018.

16. E.V. Trapeznikov. *The implementation of the system for assessing the level of information security in the information system,* In *Metrology, standardization, quality: theory and practice*, pp. 334-339, 2017.

17. E.V. Trapeznikov. *Software development for the implementation of the process of auditing the state of information security / E.V. Trapeznikov,* In *Yuzhno-Sibirskiy nauchnyy* , no. 2 (26). pp. 12-17, 2019.

18. *Information technology. Security methods and tools. Information Technology Security Assessment Criteria*, Federal standard R ISO/IEC 15408, Moscow, Standatrinform, 2013.

19. E.V. Trapeznikov. *Computer program "ARM security assessment":* Certificate on state registration of a computer program No. 2018617812. declared 05/18/2018; publ. 07/02/2018, RU OBPBT No. 7

Trapeznikov Evgeny Valerievich – Senior Lecturer, Complex Information Security Department, Omsk State Technical University., +7-913-673-94-76, e-mail:evtrapeznikov@yandex.ru.

Magazev Alexey Anatol'evich – doctor of physical and mathematical sciences, professor, Complex Information Security Department, Omsk State Technical University, +7-913-979-15-15, e-mail: magazev@mail.ru.