ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 519.711.3

DOI: 10.21822/2073-6185-2023-50-4-109-114 Оригинальная статья /Original article

Динамическое моделирование при функционировании систем защиты в области обеспечения информационной безопасности

А.М. Конаков, А.Г. Певнева
Национальный исследовательский университет ИТМО,
197101, г.Санкт-Петербург, Кронверкский пр., д. 49, Россия

Резюме. Цель. Целью исследования являются определение функциональных возможностей проектирования, построения и внедрения систем защиты с учётом временного фактора. **Метод.** Проведён анализ функционального взаимодействия построения трёх последовательно взаимосвязанных динамических моделей и передачи данных между ними. **Результат.** Разработана и предложена к внедрению общая модель системы защиты и прогнозирования возможных угроз при обеспечении безопасности информации и инфраструктуры с учётом временного фактора. **Вывод.** Рассматриваемая в статье область информационной безопасности является необходимым составляющим элементом обеспечения защиты информационных ресурсов и сопутствующих систем от различных угроз. Применение основ динамического моделирования данных, процессов и структур с точки зрения времени, позволяет оценить риски и угрозы, выявить определённые существенные недостатки и устранить их, тем самым оптимизировать затраты, повысить эффективность обеспечения безопасности и уровень защиты информационной инфраструктуры в целом.

Ключевые слова: моделирование, моделирование времени, математическая модель, аудит информационной безопасности, нечёткая логика, анализ данных, анализ безопасности систем

Для цитирования: А.М. Конаков, А.Г. Певнева. Динамическое моделирование при функционировании систем защиты в области обеспечения информационной безопасности. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(4):109-114. DOI:10.21822/2073-6185-2023-50-4-109-114

Dynamic modeling in the functioning of security systems in the field of information security

A.M. Konakov, A.G. Pevneva
National Research University ITMO,
49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. **Objective**. The purpose of the study is the functionality of designing, building and implementing protection systems taking into account the time factor. **Method.** The analysis of the functional interaction of the construction of three sequentially interconnected dynamic models and data transfer between them is carried out. **Result.** A general model of the system of protection and forecasting of possible threats in ensuring the security of information and infrastructure, taking into account the time factor, has been developed and proposed for implementation. **Conclusion.** The field of information security considered in the article is a necessary component of ensuring the protection of information resources and related systems from various threats. The application of the basics of dynamic modeling of data, processes and structures in terms of time, allows you to assess risks and threats, identify certain significant shortcomings and eliminate them, thereby optimizing costs, increasing the efficiency of ensuring security

Keywords: modeling, time modeling, mathematical model, information security audit, fuzzy logic, data analysis, system security analysis

For citation: A.M. Konakov, A.G. Pevneva. Dynamic modeling in the functioning of security

systems in the field of information security. Herald of Daghestan State Technical University. Technical Sciences. 2023; 50(4):109-114. DOI:10.21822/2073-6185-2023-50-4-109-114

Введение. Информационные технологии и сопутствующая инфраструктура является неотъемлемой составляющей современного общества и государства. Она затрагивает жизненно важные функции для общества и государства такие как экономическое и социальное развитие, а также реализация политики и мероприятий по достижению технологического суверенитета [1,2].

Постановка задачи. С учётом своей важности при ускоренной цифровизации, ростом влияния и объёмов создаваемой, обрабатываемой и циркулирующей информации, информационная инфраструктура постоянно подвергается рискам и угрозам от внутренних и внешних факторов, которые в случае реализации, могут приводить к негативным последствиям различной степени значимости [3,4].

В связи с этим, возникает необходимость в разработке методов и моделей анализа временного фактора, которые можно использовать при обеспечении безопасности функционирующих систем.

Разработанная модель, своими функциональными возможностями позволит повысить эффективность и «действенность» реализуемых мер защиты, оптимизировать риски и затраты на их минимизацию, а также проводить анализ полученные результатов, в целях дальнейшего улучшения систем управления информационной безопасности в целом.

Методы исследования. Динамическое моделирование - процесс, представляющий собой, создание таких математических моделей, которые позволяют описать изменения объектов и явлений во времени. С точки зрения информационной безопасности (и других сфер деятельности в целом) это важный инструмент для проведения анализа и прогнозирования различных протекающих процессов, таких как технические, экономические, организационные и др [5].

Моделирование динамических процессов позволяет проводить анализ обеспечения информационной безопасности систем и инфраструктур, которые непрерывно могут изменятся во времени и в хаотичном порядке [6].

Например, если рассмотреть систему безопасности использующую такие методологии моделирования обеспечения процессов информационной безопасности как

1. «Теория игр с природой»;
2. Теоретико - множественные и матричные модели;
3. «Марковские цепи».

И расставить их в поэтапном порядке функционирования, где конечные данные одного процесса моделирования, являются исходными данными другого, то получатся следующие схемы выстроенного взаимодействия данных методологий, представленные на рис. 1,2.

Рис. 1 Общая схема стратегий системы
Fig. 1 General scheme of system strategies

Первым этапом моделирования процессов идёт методология «Теория игр», а точнее «Теория игр с природой», где в данном случае, природа - это функционирующая система безопасности информационной инфраструктуры, которую злоумышленнику необходимо обойти, учитывая хаотичность и неопределённый порядок изменений установок в структуре безопасности [7].

Рис. 2. Методологии моделирования процессов обеспечения информационной безопасности
Fig. 2. Methodologies for modeling information security processes

Варианты развития стратегий «Теории игр с природой» рассматриваемой системы безопасности, формируются в виде матрицы (А), где строки соответствуют известным исходным данным о функционирующей информационной инфраструктуре ($I_{исх.}$), а столбцы - вероятности успеха реализации определённой последовательности действий злоумышленника ($P_{р.усп.}$).

Пример такой матрица представлен ниже.

$$A = \begin{matrix} 15 \\ 55 \\ 45 \\ 25 \end{matrix}$$

В табл. 1 представлена матрица доступа субъектов к объектам в информационной системе для следующего этапа (матричные и теоретико - множественные модели), основанная на модели безопасности «Харрисона - Руззо - Ульмана», где каждый субъект по отношению к объектам, наделен определёнными правами, а именно:

1. Ч - чтение;
2. М - модификация;
3. С - создание;
4. У - удаление;

Таблица 1. Матрица доступа субъектов к объектам системы с определёнными правами
Table 1. Matrix of access of subjects to system objects with certain rights

Субъект (S)/Объект доступа (О) Subject, access object	O_1	O_2	O_3	O_4	…	$O_м$
S_1	-	ЧМС	ЧМ	-	...	-
S_2	ЧМСУ	ЧМСУ	ЧМСУ	ЧМСУ	...	ЧМСУ
S_3	-	ЧМСУ	-	ЧМ	...	ЧМ
S_4	ЧМ	-	ЧМ	-	...	-
	...	...	...	...	...	...
S_N	-	ЧМС	-	ЧМСУ	...	ЧМ

Поведение в матрице доступа формируется и моделируется во времени на основе понятия «состояния». То есть, осуществляется переход между различными состояниями (В определённый момент времени меняются права субъекта над объектом) [8]. Изначально неизвестно, в какой момент времени у определённого субъекта изменятся права над объектом и какова вероятность наступления этого события [9, 10].

На графике (рис. 3), указана точка возможного входа злоумышленника в функционирующую информационную систему в зависимости от накопления критических ошибок (R) во времени (t), благодаря которой возникает благоприятный для злоумышленника

инцидент безопасности ($R_{инц}$; $t_{инц}$), после которого возможно исполнение одного из нескольких вариантов развития событий (X_1,X_2,X_3). Так как, предполагаемая точка входа злоумышленника заранее неизвестна, для её выявления, берётся определённый промежуток времени ([t_1 ; t_2]) для проведения анализа данных событий безопасности информационной системы.

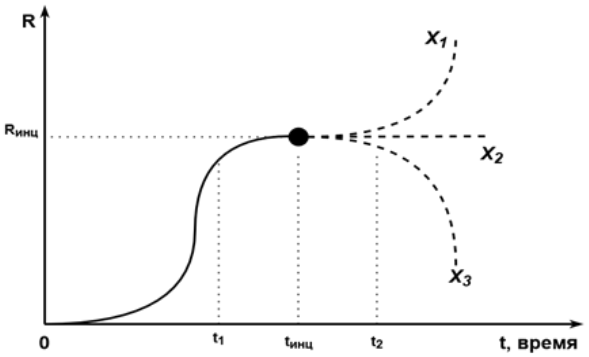

Рис. 3. График точки входа злоумышленника в систему в зависимости от накопления критических ошибок во времени
Fig. 3. Graph of an attacker's entry point into the system depending on the accumulation of critical errors over time

Исходя из того, что злоумышленник на каждом этапе будет реализовывать различные варианты стратегий проникновения, отличающиеся от предыдущих, на каждом соответствующе выстроенном этапе системы используется определённые инструменты безопасности (табл. 2), позволяющие в выбранном промежутке времени, провести сканирование и дальнейший анализ полученных данных на предмет «признаков» компрометации.

Таблица 2. Инструменты безопасности для поиска точек входа злоумышленника
Table 2. Security tools for finding attacker entry points

№	Используемая методология/ Methodology used	Используемый инструмент безопасности с учётом временного фактора/Security tool used, taking into account the time factor
1	«Теория игр» "Game theory"	Анализ сканирования портов Анализ сканирования на различные уязвимости/ Port Scan Analysis Analysis of scans for various vulnerabilities
2	Теоретико - множественные и матричные модели/ Set-theoretic and matrix models	Анализ журнала безопасности ОС Анализ «логов» системного журнала/ OS security log analysis Analysis of system logs
3	«Марковские цепи»/ "Markov chains"	Анализ журнала средства Антивирусной защиты (САВЗ)/ Analysis of the Anti-Virus Protection Tool (AVZ) log

И в конечном итоге, исходя из проанализированных данных и сформированных процессов взаимодействия описанных методологий и их функциональных возможностей, можно сформулировать вероятность момента времени ($Pt_{инц}$), когда проникновение злоумышленника в систему наиболее возможно в зависимости от вероятностей выбранной стратегии игр с природой ($P_{и.с.п}$), изменения матрицы доступа ($P_{и.м.д}$) и использования средств анализа безопасности ($P_{и.с.а}$) (табл. 3).

Ее можно численно вычислить по формуле, представленной ниже:

$$Pt_{инц} = P_{и.с.п} * P_{и.м.д} * P_{и.с.а}$$

Таблица 3. Вероятности использования инструментов безопасности
Table 3. Probabilities of using security tools

Процесс/ Вероятность этого процесса Process/Probability of this process	1 раз в неделю*	Чётные дни недели*	Нечётные дни недели*	1 раз в день	1-я половина дня	2-я половина дня	Не используется
Сканирование портов и поиск уязвимостей Scanning ports and searching for vulnerabilities	1	0,4	0,6	0,2	0,1	0,1	0
Анализ безопасности журнала ОС OS log security analysis	1	0,4	0,6	0,2	0,1	0,1	0
Анализ журнала Антивируса Anti-Virus log analysis	1	0,4	0,6	0,2	0,1	0,1	0
Анализ «логов» системного журнала Analysis of system logs	1	0,4	0,6	0,2	0,1	0,1	0

Вывод. В статье представлен структурный анализ существующих динамических моделей с точки зрения динамического распределения, архитектуры случайных процессов и существующих систем безопасности.

Рассмотренные модели своими функциональными возможностями, предназначены для проведения анализа и оценки рисков и угроз во времени при непрерывном функционировании систем и реализации защитных мер обеспечения безопасности на всех этапах жизненного цикла [11].

В конечном итоге, динамическое моделирование является важным инструментом в информационной безопасности критических информационных инфраструктур, который позволяет эффективно осуществлять планирование изменений, прогнозировать угрозы и атаки на информационные ресурсы, а также определять оптимальные стратегии защиты [12].

Разработка и внедрение новых методов и технологий в данной области будет способствовать улучшению безопасности информационной инфраструктуры и сокращению рисков для организаций. Это позволяет работать в условиях возможных ограничений по ресурсам, при этом эффективно реализуя функционал и возможности защитных механизмов.

Библиографический список:

1. Окольнишников В. В. Представление времени в имитационном моделировании //Вычислительные технологии. – 2005. – Т. 10. – №. 5. – С. 57-80.
2. Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // URL: http://www.kremlin.ru/acts/bank/47796 (Дата обращение 15.05.2023);
3. Карпухин И. Н., Кораблин Ю. П., Незнанов А. А. Модели времени в имитационном моделировании //Научно-техническая информация. Серия 2: Информационные процессы и системы. – 2012. – №. 5. – С. 16-21.
4. Клочко О. С., Федорова В. А. Использование аппарата скрытых моделей Маркова при разработке системы прогнозирования функциональной безопасности информационной системы //Вопросы радиоэлектроники. – 2015. – №. 10. – С. 54-57.;
5. Щеглов К. А., Щеглов А. Ю. Марковские модели угрозы безопасности информационной системы // Известия высших учебных заведений. Приборостроение. – 2015. – Т. 58. – №. 12. – С. 957-965;
6. Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. Учебное пособие.– СПб: Университет ИТМО, 2015 – 93с.;
7. Прокушев Я. Е., Пономаренко С. В., Шишов Н. В. Моделирование процессов проектирования систем защиты информации в критических информационных инфраструктурах //Computational

nanotechnology. – 2022. – Т. 9. – №. 2. – С. 45-55.
8. Пономаренко С. В., Пономаренко С. А., Прокушев Я. Е. Информационная безопасность критических систем информационной инфраструктуры. – 2021.
9. Фоменко К. Э., Кущёв А. В. Модель обеспечения информационной безопасности элементов критической информационной инфраструктуры на основе онтологического подхода в условиях деструктивных воздействий. – 2022.
10. Малых А. В., Юркин Д. В. Вероятностно-временные методы оценки соответствия автоматизированных систем требованиям информационной безопасности //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). – 2017. – С. 496-500.
11. Котеленко С. А. Формальное описание онтологий на основе нечёткой гиперграфовой модели данных // Известия Южного федерального университета. Технические науки. – 2005. – Т. 50. – №. 6. – С. 138-145.
12. Максименко В. Н., Ясюк Е. В. Основные подходы к анализу и оценке рисков информационной безопасности //Экономика и качество систем связи. – 2017. – №. 2 (4). – С. 42-48.

References

1. Okolnishnikov V.V. Representation of time in simulation modeling. *Computing technologies*. 2005; 10(5): 57-80. (In Russ)
2. Decree of the President of the Russian Federation No. 250 dated 01.05.2022 “On additional measures to ensure information security of the Russian Federation” // URL: http://www.kremlin.ru/acts/bank/47796 (Date of appeal 15.05.2023); (In Russ)
3. Karpukhin I. N., Korablin Yu. P., Neznanov A. A. Time models in simulation modeling. *Scientific and technical information. Series 2: Information processes and systems.* 2012; 5: 16-21. (In Russ)
4. Klochko O. S., Fedorova V. A. The use of hidden Markov models in the development of a system for predicting the functional security of an information system. *Radio electronics issues.* 2015;10:54-57; (In Russ)
5. Shcheglov K. A., Shcheglov A. Yu. Markov models of the threat to the security of an information system. *Izvestia of higher educational institutions. Instrumentation*. 2015; 58 (12):957-965. (In Russ)
6. Shcheglov A.Yu., Shcheglov K.A. Mathematical models and methods of formal design of information systems protection systems. Textbook.– St. Petersburg: ITMO University, 2015 – 93 p.; (In Russ)
7. Prokushev Ya. E., Ponomarenko S. V., Shishov N. V. Modeling of information security system design processes in critical information infrastructures. *Computational nanotechnology*. 2022; 9(2):45-55. (In Russ)
8. Ponomarenko S. V., Ponomarenko S. A., Prokushev Ya. E. Information security of critical information infrastructure systems. 2021. (In Russ)
9. Fomenko K. E., Kushchev A.V. A model for ensuring information security of critical information infrastructure elements based on an ontological approach in conditions of destructive influences. 2022. (In Russ)
10. Malykh A.V., Yurkin D. V. Probabilistic-temporal methods for assessing the compliance of automated systems with information security requirements. *Actual problems of infotelecommunications in science and education (APINO 2017)*. 2017; 496-500. (In Russ)
11. Kotelenko S. A. Formal description of ontologies based on a fuzzy hypergraphic data model. *Izvestia of the Southern Federal University. Technical sciences.* 2005; 50(6):138-145. (In Russ)
12. Maksimenko V. N., Yasyuk E. V. Basic approaches to the analysis and assessment of information security risks. *Economics and quality of communication systems*. 2017;2 (4): 42-48. (In Russ)

Сведения об авторах:
Конаков Александр Михайлович, магистрант, Helium1937@yandex.ru.
Певнева Анна Геннадьевна, кандидат технических наук, доцент; pevnevaa@inbox.ru.
Information about authors:
Alexander M. Konakov, Master’s student, Helium1937@yandex.ru.
Anna G. Pevneva, Cand. Sci. (Eng), Assoc. Prof.; pevnevaa@inbox.ru
Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/ Received 10.09.2023.
Одобрена после рецензирования/ Reviced 11.10.2023.
Принята в печать/ Accepted for publication 11.10.2023.