Научная статья
УДК 004.94:004.4.056
ББК 16.84
Р 17
DOI: 10.53598/2410-3225-2024-1-336-60-69

Разработка имитационной модели в области защиты информации с использованием программного обеспечения AnyLogic

(*Рецензирована*)

Михаил Михайлович Путято[1], Александр Самвелович Макарян[2], Александр Николаевич Черкасов[3], Виктор Алексеевич Кучер[4]

[1–4] *Кубанский государственный технологический университет, Краснодар, Россия*
[1] *putyato.m@gmail.com*
[2] *msanya@yandex.ru*
[3] *cherk@mail.ru*
[4] *vakucher@bk.ru*

Аннотация. *Применение имитационных моделей для задач информационной безопасности представляет собой сложный многоэтапный процесс. Результат функционирования имитационной модели даст возможность определить необходимые данные и рекомендации по усилению системы информационной безопасности. Данная статья рассматривает основные понятия и способы моделирования, отмечает важность анализа угроз и определения уязвимостей. Для определения общих принципов работы был произведен сравнительный анализ систем имитационного моделирования. Кроме того, показана реализация имитационных моделей в области безопасности информации с использованием программного обеспечения AnyLogic и определены общие принципы разработки имитационных моделей в области защиты информации, которые могут быть использованы для анализа и оценки защищенности информационных систем. Результаты данного исследования могут быть применены для повышения уровня защищенности информационных систем организаций и эффективного управления угрозами информационной безопасности.*

Ключевые слова: *имитационная модель, процесс моделирования, AnyLogic, информационная безопасность, актуальные угрозы, средства защиты*

Для цитирования: *Разработка имитационной модели в области защиты информации с использованием программного обеспечения AnyLogic / М. М. Путято, А. С. Макарян, А. Н. Черкасов, В. А. Кучер // Вестник Адыгейского государственного университета. Сер. : Естественно-математические и технические науки. 2024. Вып. 1* (*336*)*. С. 60–69. DOI: 10.53598/2410-3225-2024-1-336-60-69*

Original Research Paper

Development of a simulation model in the information protection in the field of using AnyLogic software

Mikhail M. Putyato[1], Aleksandr S. Makaryan[2], Aleksandr N. Cherkasov[3], Viktor A. Kucher[4]

[1–4] *Kuban State Technological University, Krasnodar, Russia*
[1] *putyato.m@gmail.com*
[2] *msanya@yandex.ru*
[3] *cherk@mail.ru*
[4] *vakucher@bk.ru*

Abstract*. The application of simulation models for information security problems is a complex multi-step process. The result of the simulation model operation will make it possible to determine the necessary data and recommendations for strengthening the information security system. This article examines the basic concepts and methods of modeling, notes the importance of threat analysis and vulnerability identification. To determine the general principles of operation, a comparative analysis of simulation modeling systems is carried out. In addition, the implementation of simulation models in the field of information security using AnyLogic software is shown and the general principles of the development of simulation models in the field of information security that can be used to analyze and evaluate the security of information systems are defined. The results of this study can be applied to increase the level of security of information systems of organizations and effective management of threats to information security.*

Keywords: *simulation model, simulation process, AnyLogic, information security, current threats, means of protection*

For citation: *Development of a simulation model in the field of information protection using AnyLogic software / M. M. Putyato, A. S. Makaryan, A. N. Cherkasov, V. A. Kucher // The Bulletin of the Adyghe State University. Ser. : Natural-Mathematical and Technical Sciences. 2024. Iss. 1 (336). P. 60–69. DOI: 10.53598/2410-3225-2024-1-336-60-69*

Введение. Во время современной повсеместной цифровизации информационные технологии актуализируются не только в применении государственными и властными структурами, но и крупными и средними коммерческими структурами. В приведенном аспекте подчеркнута выраженная ключевая роль информации в деятельности организаций, данная информация применяется для обработки, хранения и передачи по разнообразным каналам. При этом стоит подчеркнуть, что рост количества использований информационных технологий пропорционально их применению отображается на увеличении количества угроз безопасности организации, конфиденциальности сведений, которые в ней обрабатываются. В связи с вышеизложенным необходимо выделить важнейший аспект деятельности в организации – это разработка и реализация мер по защите информации. Для профилактики кибербезопасности, собственно, и применяются превентивные методы борьбы с такими угрозами, а именно создаются центры информационной безопасности, которые направлены на контроль, организацию средств защиты, проверку уязвимостей автоматизированных систем. Таким образом, используя передовые средства в центрах информационной безопасности, в том числе имитационные модели, повышается степень защищенности информации и автоматизированных систем [1].

Цель данной статьи – определение общих принципов разработки имитационных моделей в области информационной безопасности. Моделирование позволяет создать модель системы, которая может быть использована для определения возможных сценариев атак и оценки эффективности системы защиты информации [2].

Более подробно в данной статье будут рассмотрены актуальные угрозы безопасности информации, далее будут смоделированы информационные системы, которые в дальнейшем будут применяться в различных сегментах организации, начиная от бухгалтерии до технического отдела. Первоначально необходимы данные, которые будут использованы в данном эксперименте, а именно для построения имитационных моделей различных информационных систем необходимо наличие первоначальных данных [3].

Моделирование угроз информационной безопасности будем производить в сфере ЛВС (локальной вычислительной сети). Так как именно в приведенных департаментах и осуществляется обработка персональных данных сотрудников, клиентов, заказчиков и поставщиков организации. Определим часть актуальных для выделенного сегмента угроз безопасности информации (УБИ), которые будут применены при моделировании [4]:

УБИ 31. Угроза использования механизмов авторизации для повышения привилегий.

УБИ 67. Угроза неправомерного ознакомления с защищаемой информацией. Данная угроза обусловлена уязвимостями средств контроля доступа.

УБИ 179. Угроза несанкционированной модификации защищаемой информации.

УБИ 6. Угроза внедрения кода или данных.

УБИ 30. Угроза использования информации идентификации / аутентификации, заданной по умолчанию.

УБИ 86. Угроза несанкционированного изменения аутентификационной информации.

УБИ 140. Угроза приведения системы в состояние «отказ в обслуживании».

УБИ 144. Угроза программного сброса пароля BIOS.

УБИ 18. Угроза загрузки нештатной операционной системы.

УБИ 167. Угроза заражения компьютера при посещении неблагонадежных сайтов.

УБИ 186. Угроза внедрения вредоносного кода через рекламу, сервисы и контент.

УБИ 191. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения.

В качестве исходных данных для прогнозируемой информационной системы можно использовать вероятность реализации угроз. Так, выделяют две основные группы угроз: угрозы, реализация которых прерывает движение запроса, и угрозы, реализация которых не влияет на продвижение запроса [5].

Материалы и методы. Формирование новых моделей безопасности на основе систем моделирования и экспертного мнения. При рассмотрении многоаспектных проблем и развития ситуации активно могут применять системы имитационного, агентного и дискретно-событийного моделирования. Включение процедур экспертной поддержки позволит получить дополнительную информацию по проблемам безопасности [6].

На рисунке 1 нами произведено посторенние имитационной модели для департаментов ЛВС, на диаграмме подробно показан процесс работы сервера и компьютера в AnyLogic.

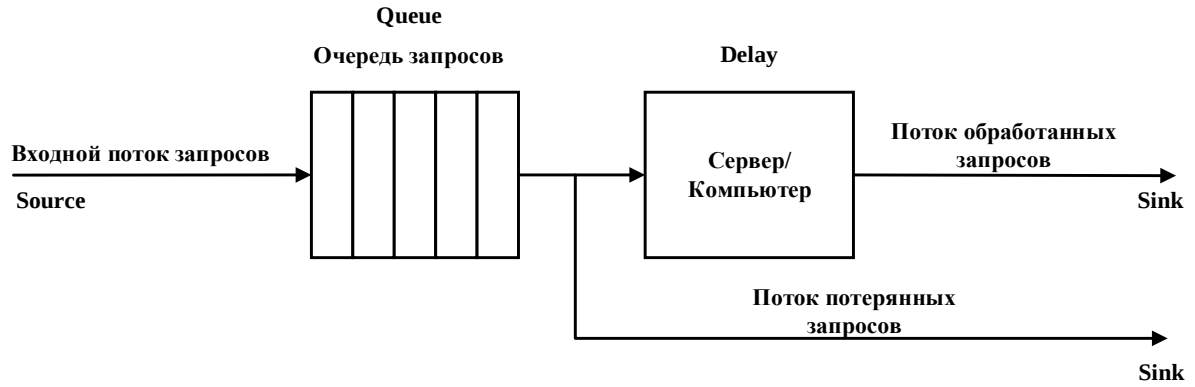

Рис. 1. Диаграмма процесса работы сервера и компьютера в AnyLogic [7]
Fig. 1. Diagram of server and computer operation process in AnyLogic [7]

Дадим краткую характеристику объектов рисунка 1.

1. Объект Source генерирует заявки.

2. Объект Queue моделирует очередь заявок, ожидающих приема объектами, следующими за данным в диаграмме процесса. В нашем случае он будет моделировать очередь запросов, ожидающих освобождения сервера или компьютера.

3. Объект Delay задерживает заявки на заданный период времени.

4. Объект Sink уничтожает поступившие заявки [3].

Теперь распишем обобщенную схему действия имитационной модели, которая учитывает процесс работы информационной системы «сервер-компьютер» в AnyLogic.

В первую очередь стоит указать, что и запросы, и угрозы проходят по каналу связи, соответственно там и генерируются. Затем они объединяются в соединительные линии, которые проходят через информационные системы «сервер-компьютер», расположенные в департаментах ЛВС. Когда угроза от сервера попадает на компьютер, то происходит точка возможности угрозы. Если угроза не наступила, то запрос продолжает продвижение, а в счетчике, привязанном к данной угрозе, фиксируется факт того, что угроза не наступила; если же угроза наступила, то запрос попадает на альтернативный путь продвижения и в счетчике фиксируется факт того, что угроза наступила. На основании этого выделяется два основных типа угроз: влияющих на продвижение запроса, когда запрос прекращает движение, и угрозы, не влияющие на дальнейшее продвижение, после реализации которых запрос продолжает движение [8].

Для получения результатов, достоверность которых будет достаточной для изучения поведения системы, в ходе проведения экспериментов было принято решение использовать 175200 единиц модельного времени (условных единиц времени, используемых в среде моделирования), что равносильно 1 году. За данный промежуток модельного времени, то есть за время проведения одного эксперимента, генерируется в среднем 4900 угроз и 43700 запросов.

Далее рассмотрим две имитационных модели с разными заданными условиями.

1. Первым рассмотрим процесс моделирования угроз до применения средств защиты.

В качестве исходных данных для данной модели применяются вероятности реализации угроз. В таблице 1 показаны вероятности реализации угроз до применения средств защиты информации (СЗИ) [9]. Наименования УБИ в таблице не приведены, они описаны выше в статье.

Таблица 1

Вероятности реализации угроз

Table 1. Probabilities of threat realization

Идентификатор УБИ	Объект воздействия	Вероятность реализации
31	Сервер	0,25
67	Сервер	0,25
179	Сервер	0,1
6	Сервер	0,1
30	Сервер	0,25
86	Сервер	0,1
140	Сервер	0,25
144	Компьютер	0,1
18	Компьютер	0,25
167	Компьютер	0,25
186	Компьютер	0,25
191	Компьютер	0,25

Имитационная модель реализации угроз безопасности информации до применения СЗИ представлена на рисунке 2.

Результаты работы данной модели приведены на рисунке 3.

Изучив результаты проведенных экспериментов с моделью, вычислено, что лишь 79,04 % запросов завершают движение, то есть 20,96 % сгенерированных запросов прекращают движение вследствие реализации угроз.

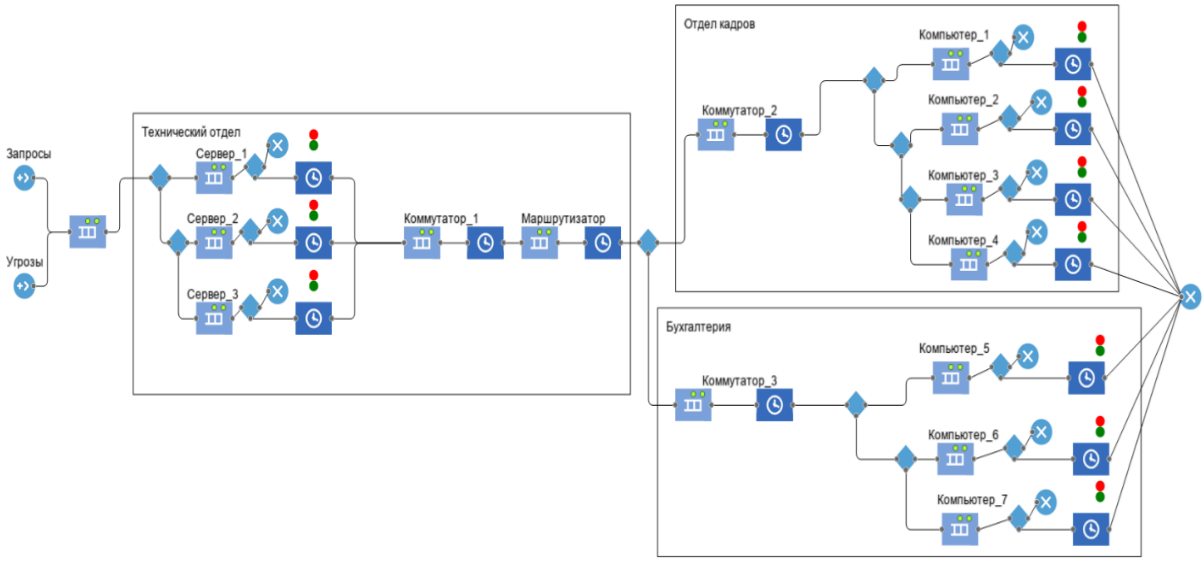

Рис. 2. Имитационная модель реализации угроз безопасности информации до применения СЗИ [5]

Fig. 2. Simulation model of realization of information security threats before application of protection systems [5]

Рис. 3. Результат работы модели до применения СЗИ

Fig. 3. The result of the model before the application of the protection system

В целях выявления угроз, которые наиболее значимо влияют на конечный результат, в таблице 2 показан процент от общего количества реализованных угроз [3].

Таблица 2

Количество реализованных угроз

Table 2. Number of threats realized

Идентификатор УБИ	Количество реализованных угроз	% от общего количества реализованных угроз
31	113	12,612
67	92	10,268
179	44	4,911
6	43	4,799
30	42	4,688
86	45	5,022
140	93	10,379
144	47	5,246
18	96	10,714
167	83	9,263
186	106	11,830
191	92	10,268
ИТОГО	**896**	**100%**

Проведенные эксперименты с имитационной моделью показали, что к наиболее вероятным угрозам относятся следующие:

– угроза использования механизмов авторизации для повышения привилегий – 12,612 % от общего количества реализовавшихся угроз;

– угроза неправомерного ознакомления с защищаемой информацией – 10,268 % от общего количества реализовавшихся угроз;

– угроза приведения системы в состояние «отказ в обслуживании» – 10,379 % от общего количества реализовавшихся угроз;

– угроза загрузки нештатной операционной системы – 10,714 % от общего количества реализовавшихся угроз;

– угроза внедрения вредоносного кода через рекламу, сервисы и контент – 11,83 % от общего количества реализовавшихся угроз;

– угроза внедрения вредоносного кода в дистрибутив программного обеспечения – 10,268 % от общего количества реализовавшихся угроз.

2. Вторым рассмотрим процесс моделирования угроз с применением средств защиты.

Для перекрытия наиболее вероятных угроз необходимо использовать средства межсетевого экранирования, антивирусное программное обеспечение и средства защиты от несанкционированного доступа (СЗИ от НСД) [3].

На данном этапе в имитационной модели учтены дополнительные меры защиты от реализации угроз, применяемые в информационной системе. В качестве исходных данных применяются вероятности реализации угроз с применением средств защиты информации. Имитационная модель реализации угроз безопасности информации с применением СЗИ представлена на рисунке 4 [3].

Результаты работы данной модели показаны на рисунке 5.

Изучив результаты проведенных экспериментов с моделью, вычислено, что 98,57 % запросов завершают движение, то есть 1,43 % сгенерированных запросов прекращает движение вследствие реализации угроз.

В таблице 3 показан процент от количества реализованных угроз.

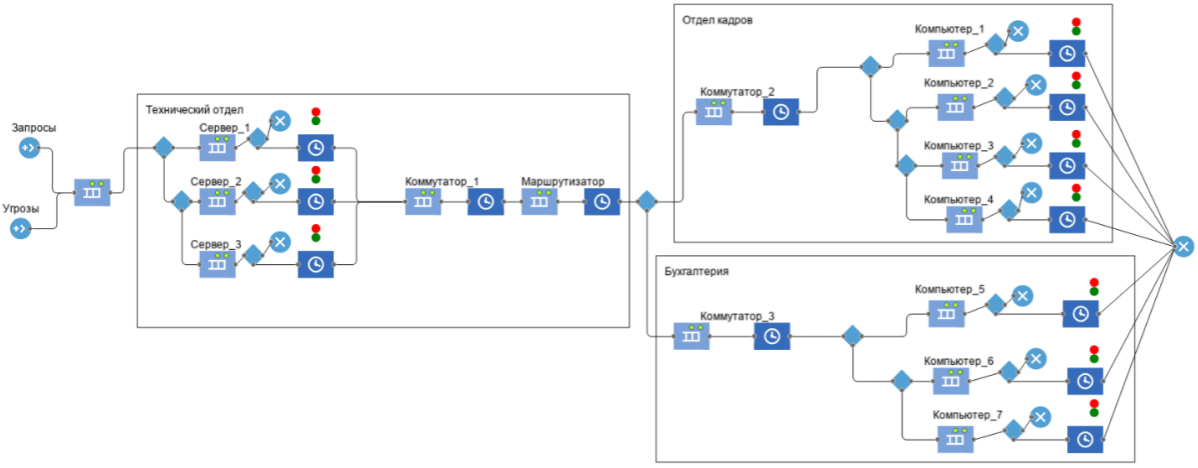

Рис. 4. Имитационная модель реализации угроз безопасности информации с применением СЗИ

Fig. 4. Simulation model of realization of threats to information security with the use of information protection systems

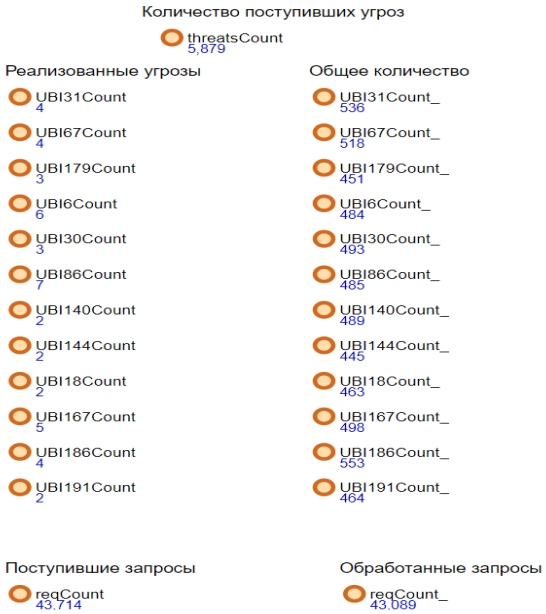

Рис. 5. Результат работы модели с применением СЗИ

Fig. 5. Result of the model with the application of a protection system

Таблица 3

Процент от количества реализованных угроз

Table 3. Percentage of the number of realized threats

Идентификатор УБИ	Количество реализованных угроз	Общее количество угроз	% от количества реализованных угроз
31	4	536	0,746
67	4	518	0,772
179	3	451	0,665
6	6	484	1,240
30	3	493	0,609
86	7	485	1,443
140	2	489	0,409
144	2	445	0,449
18	2	463	0,432
167	5	498	1,004
186	4	553	0,723
191	2	464	0,431
Итого	**44**	**5879**	**8,923**

Эффективность средств защиты можно оценить, сравнив процент реализации конкретной угрозы от общего количества реализованных угроз с процентом количества реализованных угроз, защита от которых не учитывалась во время проведения эксперимента, от общего количества реализованных угроз. Данные измерения приведены в таблице 4 [3].

Таблица 4

Сравнение процентов реализации угроз

Table 4. Comparison of percentages of threat realization

Идентификатор УБИ	% реализации угрозы с защитой от количества реализованных угроз	% реализации угрозы без защиты от количества реализованных угроз
31	0,746	28,827
67	0,772	22,115
179	0,665	10,185
6	1,240	10,238
30	0,609	10,396
86	1,443	10,949
140	0,409	22,906
144	0,449	12,082
18	0,432	25,532
167	1,004	23,315
186	0,723	24,824
191	0,431	23,291

Таким образом, анализируя результаты, представленные в таблице 6, можно сделать вывод, что при построении имитационной модели актуальных угроз безопасности информации представленная система защиты информации является эффективной. Например, сравнивая показатели по УБИ 31 с применением защиты и без применения защиты в сторону первого показателя можно наблюдать уменьшение вероятности угрозы в 28 раз.

Заключение. В данной статье был проведен анализ способов моделирования, основывающихся на программном обеспечении AnyLogic (версия Personal Learning Edition), далее проведен анализ систем имитационного моделирования AnyLogic до применения СЗИ и после применения СЗИ, рассмотрена реализация имитационных моделей в сфере информационной безопасности, а также приведены и применены принципы разработки имитационных моделей.

В результате исследования можно отметить, что имитационное моделирование является эффективным инструментом, например, после проведенной оценки процент реализации угроз с СЗИ от общего количества реализованных угроз без применения СЗИ показывает рост от 10 до 28 раз в зависимости от рассматриваемой угрозы. Проведенный сравнительный анализ систем имитационного моделирования позволил выбрать наиболее подходящую систему для создания имитационных моделей в области защиты информации.

Тем самым, применяя имитационные модели в сфере информационной безопасности, необходимо использовать возможности описанного подхода для планирования и анализа надежности различных элементов информационных систем, а также для проверки наличия угроз безопасности персональных данных в организации. Для этого необходимо проводить постоянные оценки эффективности мер защиты информационных систем, в том числе и с использованием имитационных моделей. В настоящее время в области защиты информации определены принципы разработки имитационных моделей, что определяет необходимые возможности наиболее эффективно

применять моделирование в организациях, в том числе и в департаментах, занимающихся ЛВС, в дальнейшем это повысит уровень безопасности информационных систем в организации.

Резюмируя вышеизложенное, отметим, что оценка защищенности организации от актуальных угроз информационной безопасности позволяет своевременно применять современные подходы для повышения безопасности информационных систем в различных организациях, для этого в том числе и создаются имитационные модели для анализа угроз информационной безопасности.

Примечания

1. Разработка методов обнаружения вредоносного воздействия на основе корреляционного анализа событий информационной безопасности в SIEM-системах / С. А. Шишков, М. М. Путято, А. С. Макарян, В. О. Немчинова // Прикаспийский журнал: управление и высокие технологии. 2022. № 3 (59). С. 103–111.

2. Моделирование процессов и систем : учебник и практикум для вузов / Е. В. Стельмашонок, В. Л. Стельмашонок, Л. А. Еникеева, С. А. Соколовская; под редакцией Е. В. Стельмашонок. Москва : Изд-во Юрайт, 2023. 289 с. URL: https://urait.ru/bcode/511904

3. Пожигайло Р. А. Анализ защищенности организации на основе моделирования угроз информационной безопасности : дипломная работа по специальности 10.05.03 «Информационная безопасность автоматизированных систем» / Пожигайло Роман Александрович ; Кубанский государственный технический университет. Краснодар, 2023. 94 с.

4. Методический документ. Методика оценки угроз безопасности информации : утв. ФСТЭК России 05.02.2021. URL: https://www.consultant.ru/document/cons_doc_LAW_378330 (дата обращения: 21.12.2023).

5. Акопов А. С. Имитационное моделирование : учебник и практикум для вузов. Москва : Изд-во Юрайт, 2023. 389 с. URL: https://urait.ru/bcode/511425

6. Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра / М. М. Путято, А. С. Макарян, А. Н. Черкасов, И. Г. Горин // Прикаспийский журнал: управление и высокие технологии. 2020. № 4 (52). С. 75–84. URL: https://cyberleninka.ru/article/n/adaptivnaya-sistema-kompleksnogo-obespecheniya-bezopasnosti-kak-element-infrastruktury-situatsionnogo-tsentra (дата обращения: 21.12.2023).

7. Возможности AnyLogic. URL: https://www.anylogic.ru, свободный (дата обращения: 21.12.2023).

8. Касымов А. А. Разработки интегрального показателя сравнительной оценки систем имитационного моделирования // Управление рисками в АПК. 2020. № 2. С. 73–83. URL: http://www.agrorisk.ru/ (дата обращения: 21.12.2023).

9. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat (дата обращения: 21.12.2023).

References

1. Development of methods for detecting malicious effects based on correlation analysis of information security events in SIEM systems / S. A. Shishkov, M. M. Putyato, A. S. Makaryan, V. O. Nemchinova // Caspian Journal: Management and High Technologies. 2022. No. 3 (59). P. 103–111.

2. Modeling of processes and systems : textbook and workshop for universities / E. V. Stelmashonok, V. L. Stelmashonok, L. A. Enikeeva, S. A. Sokolovskaya; edited by E. V. Stelmashonok. Moscow : Yurayt Publishing House, 2023. 289 p. URL: https://urait.ru/bcode/511904

3. Pozhigaylo R. A. Analysis of the security of an organization based on modeling threats to information security : thesis on specialty 10/05/03 “Information security of automated systems” / Pozhigaylo Roman Aleksandrovich; Kuban State Technological University. Krasnodar, 2023. 94 p.

4. Methodical document. Methodology for assessing threats to information security : approved by FSTEC of Russia 05/02/2021. URL: https://www.consultant.ru/document/cons_doc_LAW_378330 (access date: 21/12/2023).

5. Akopov A. S. Simulation modeling : textbook and workshop for universities. Moscow : Yurayt Publishing House, 2023. 389 p. URL: https://urait.ru/bcode/511425

6. Adaptive integrated security system as an element of the situational center infrastructure /

M. M. Putyato, A. S. Makaryan, A. N. Cherkasov, I. G. Gorin // Caspian Journal: Management and High Technologies. 2020. No. 4 (52). P. 75–84. URL: https://cyberleninka.ru/article/n/adaptivnaya-sistema-kompleksnogo-obespecheniya-bezopasnosti-kak-element-infrastruktury-situatsionnogo-tsentra (access date: 21/12/2023).

7. Features AnyLogic. URL: https://www.anylogic.ru (access date: 21/12/2023).

8. Kasymov A. A. Development of an integral indicator of comparative evaluation of simulation modeling systems // Risk Management in the Agroindustrial Complex. 2020. No. 2. P. 73–83. URL: http://www.agrorisk.ru (access date: 21/12/2023).

9. Data bank of information security threats. URL: https://bdu.fstec.ru/threat (access date: 21/12/2023).

Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 05.02.2024; *одобрена после рецензирования 25.02.2024*; *принята к публикации 26.02.2024.*

The authors declare no conflicts of interests.

The article was submitted 05.02.2024; *approved after reviewing 25.02.2024*; *accepted for publication 26.02.2024.*