УДК 004.056.5

К. А. Иванов[1], А. Ю. Солдатов[1], В. В. Селифанов[1]*

Моделирование процессов управления угрозами

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: 4ter2003@gmail.com

Аннотация. Создание системы управления угрозами – важная задача в современной информационной безопасности. Для обеспечения полноценной работы всей системы защиты необходимо обеспечить правильное функционирование подсистемы управления угрозами. Необходимо также понимать, что система отработает правильно и качественно. Поскольку оценка доверия и качества системы управления угрозами – масштабное и трудоемкое мероприятие на уже развернутых процессах в организации, в статье показано, как эффективнее создать модель такой системы. В качестве методов исследования разработанной системы использовались имитационное моделирование и модель системы массового обслуживания. Представлены результаты построения модели системы управления угрозами и параметры, изменяемые в ней. Для построения модели использовалось программное обеспечение AnyLogic.

Ключевые слова: угрозы безопасности информации, имитационная модель, управление угрозами

K. A. Ivanov[1], A. Yu. Soldatov[1], V. V. Selifanov[1]*

Modelling of threat management processes

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: 4ter2003@gmail.com

Abstract. Establishing of a threat management system is an important task for current information security. To ensure the full operation of the entire defense system, it is also necessary to provide the correct functioning of the threat management subsystem. It is also necessary to understand that the system will work correctly and qualitatively. Since the assessment of trust and quality of the threat management system is a large-scale and time-consuming activity with already deployed processes in the organization, the article shows how to create a model of such a system. Simulation modelling and a mass service system model were used as research methods. The results of building a model of the threat management system and the parameters to be changed in it are presented. AnyLogic software was used to build the model.

Keywords: information security threats, simulation model, threat management

Введение

В современном мире вопросы информационной безопасности стоят особенно остро, учитывая постоянное развитие технологий и возрастание уровня угроз. Безопасность – это динамичный процесс, который предполагает активное взаимодействие и непрерывное обновление данных, так как каждая новая уязвимость может привести к появлению новых угроз. Управление угрозами – это непрерывный, циклический процесс, который должен меняться в соответствии с воздействиями на систему (получением внешних данных) [1].

В соответствии с правовыми актами, информационные системы, подлежащие защите, должны иметь модель угроз. Разработка модели угроз закреплена приказами ФСТЭК №17 от 11.02.2013, №21 от 18.02.2013, №31 от 14.03.2014 и №239 от 25.12.2017 [2–6].

Также существует Методика оценки угроз безопасности информации ФСТЭК России от 5.02.2021, описывающая способы расчета актуальности угроз информационной безопасности, их тактики и техники реализации, а также определяющая потенциально возможных нарушителей, которые могут воспользоваться угрозами. Но построить модель угроз недостаточно, так как ее требуется регулярно (непрерывно и циклично) оценивать, определять являются ли угрозы, способы реализации, техники и тактики актуальными. При возникновении изменений в конфигурации информационной системы необходимо также переоценивать угрозы заново, для этого и нужна система управления угрозами, ведь чтобы противостоять атакам, необходимо своевременно реагировать на них [7].

Перед тем как строить и внедрять новые системы в активные процессы информационной безопасности, лучшим вариантом будет предварительно проверить их в виде математической модели. Важно понять, что система отработает качественно во времени. Эксперименты с моделями обходятся дешевле, безопаснее и менее трудоемки, чем реальные эксперименты и изменения в реальных системах. Построение математической модели системы управления угрозами является текущей задачей работы [8].

Далее в статье описывается обоснование применения метода имитационного моделирования.

Обоснование применения имитационного моделирования

Перед построением модели стояла задача выбора типа математического моделирования. Для оценки того, как отработает система управления угрозами во времени, подходит метод имитационного моделирования. Он позволяет исследовать и анализировать поведение систем благодаря созданию их компьютерных моделей и имитации изменения состояния системы в дискретные моменты времени в результате определенных событий, например, поступление различных входных данных [9, 10].

Этот метод позволяет задавать различные входные данные и гибко настраивать параметры для получения различных результатов. Имитационное моделирование позволяет оценить, как система будет справляться в различных условиях, а также изучить надежность и производительность каждого элемента системы в контексте конкретных нагрузок. Путем тестирования различных стратегий в виртуальной среде можно значительно снизить потенциальные затраты и риски, связанные с реализацией недостаточно проработанных решений в реальной операционной среде [11].

Сформированную модель системы управления угрозами можно рассматривать как систему массового обслуживания разомкнутого типа, где входящий поток данных – это не только угрозы, но и уязвимости, не ограниченные по коли-

честву, а шаги в системе описаны своей производительностью и временем обслуживания [12].

Построение модели

В качестве инструмента для создания такой модели был выбран AnyLogic. Данный инструмент поддерживает основные подходы к моделированию, имеет интуитивно понятный интерфейс и поддерживает Java-код, предоставляющий гибкость настройки модели [13].

В качестве основы для построения модели будет использоваться алгоритм определения угроз безопасности информации в соответствии с Методикой ФСТЭК и методический документ ФСТЭК, касающийся организации процесса управления уязвимостями. На основании данных методик была построена схема системы комплексного управления угрозами по нотации idef0 [14, 15]. (рис. 1)

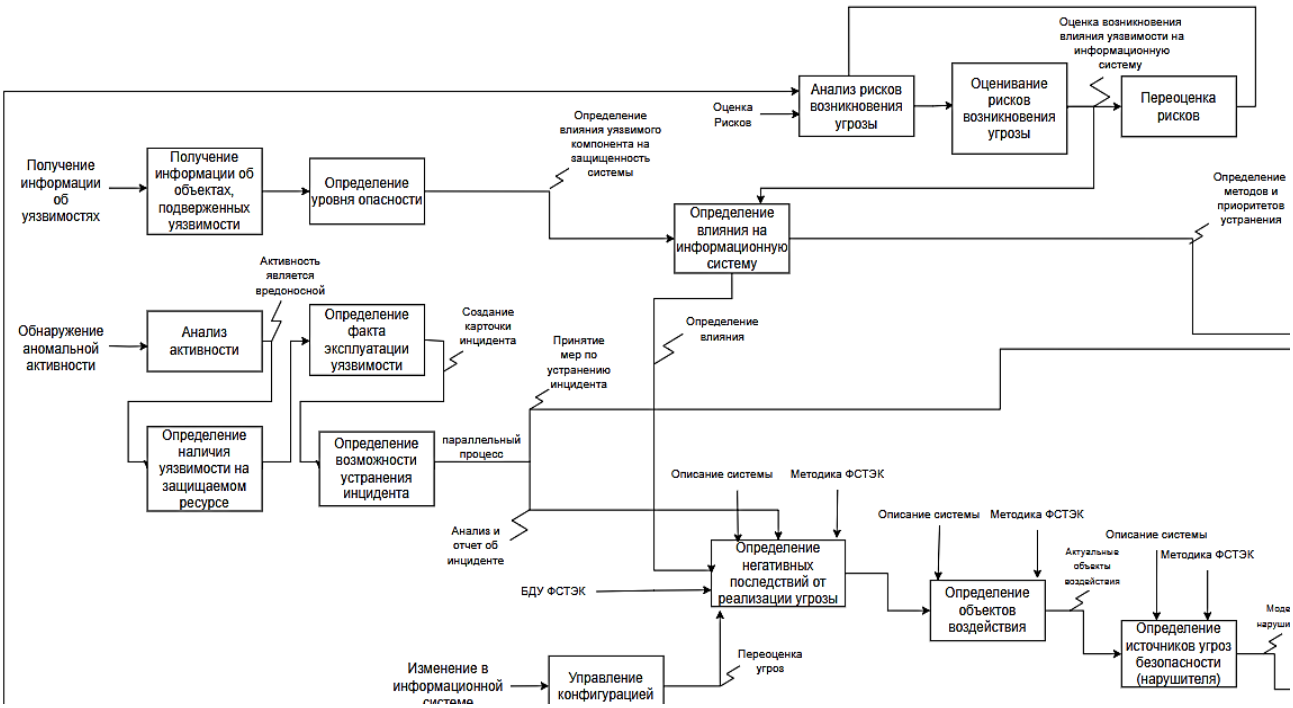

Рис. 1. Фрагмент схемы системы комплексного управления угрозами информационной безопасности по нотации idef0

Схема содержит несколько основных входных точек, каждая из которых оказывает свое влияние на основной блок оценки угроз и выходной результат, а именно:

– получение информации об уязвимостях;
– изменение в конфигурации информационной системы;
– оценка риска возникновения угрозы;
– меры реагирования на инциденты, создание отчета об инциденте.

Определены следующие процессы, как «Устранение уязвимостей», «Определение влияния», «Переоценка угроз» и «Определение влияния на информационную систему». Данные процессы проходят насквозь блока оценки угроз и подразумевают собой параллельно идущую с процессом оценки угроз активность, результат которой определяется актуальным списком угроз [16].

По мере продвижения от каждой входной точки взаимодействие элементов схемы приводит к постоянной итерации и обновлению процесса оценки угроз. Важно подчеркнуть, что схема системы построена таким образом, чтобы циклично перерабатывать полученную информацию, что позволяет ей адаптироваться к новым угрозам и изменениям в информационной среде [17].

Угроза считается актуальной, если для нее возможен хотя бы один сценарий реализации.

На основе графической схемы была построена математическая модель системы управления угроз, по дискретно-событийному методу моделирования (рис. 2).

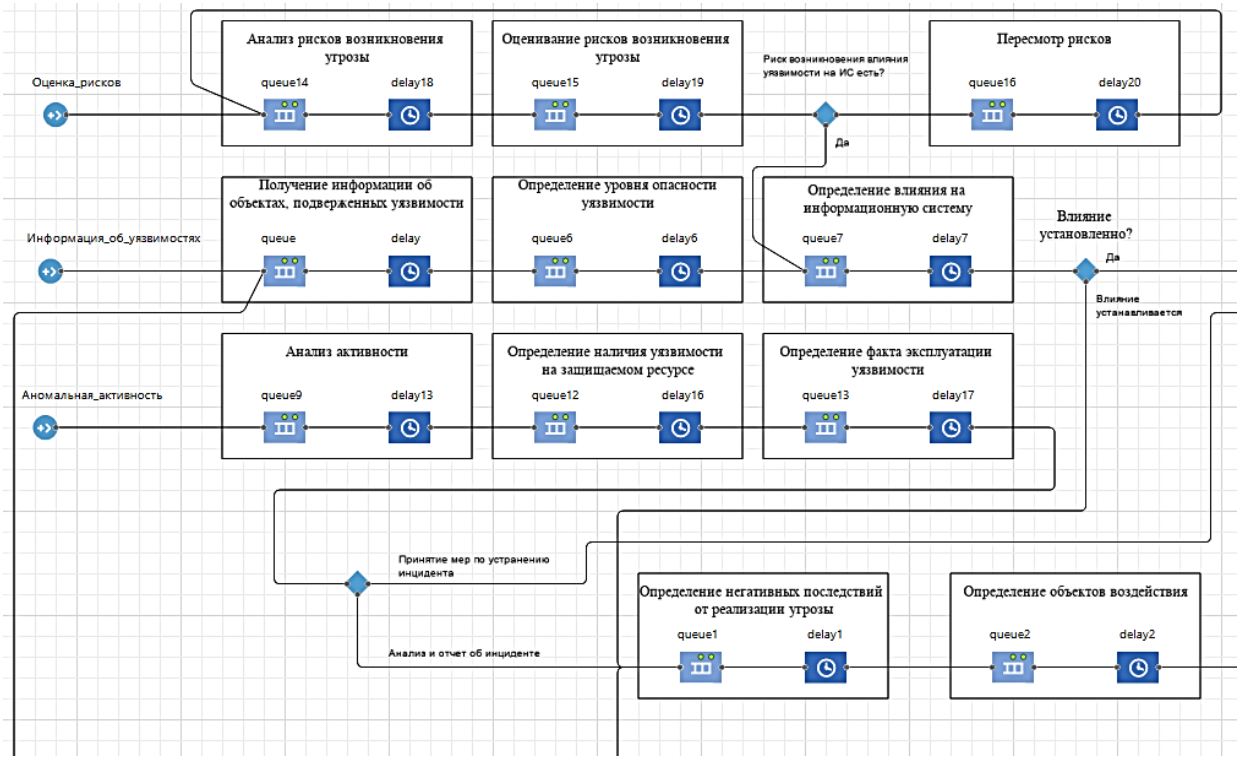

Рис. 2. Фрагмент структуры построенной модели

При запуске системы можно наблюдать поступление агентов и их прохождение через каждый блок (рис. 3).

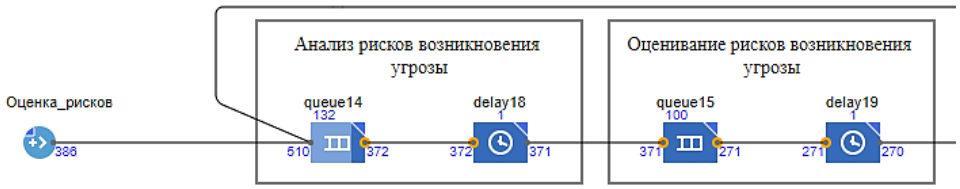

Рис. 3. Демонстрация поступления агентов

Также можно наблюдать наполняемость каждой очереди (рис. 4).

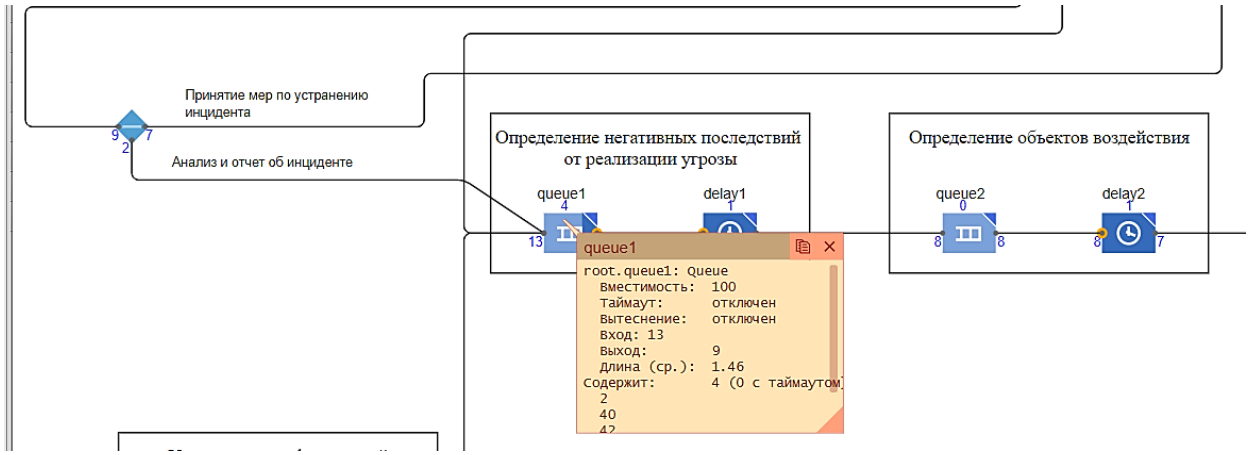

Рис. 4. Характеристики блока очереди

Заключение

Построена математическая модель системы управления угрозами безопасности информации. Данная модель может быть полезна перед вводом системы в эксплуатацию, и позволяет анализировать возможные сценарии развития событий в контексте угроз, оценивать риски и эффективность принимаемых мер защиты в динамике. В дальнейшем предполагается углубленное изучение и оценка эффективности работы данной модели [18–20].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Безопасность информации в организации / Р. С. Попов, И. П. Криволапов, И. Д. Чечевицын, С. Ю. Щербаков // Наука и Образование. – 2021. – Т. 4, № 2.

2. Российская Федерация. Законы. О персональных данных: Федеральный закон № 152-ФЗ: [принят Государственной думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. – СЗ РФ. – 2006. – № 31. – ст. 3451.

3. Российская Федерация. Приказы. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ Федеральной службы по техническому и экспортному контролю № 17 – СЗ РФ. – 2006 г. – №165. – ст. №3448.

4. Российская Федерация. Приказы. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при

их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю № 21 — СЗ РФ — 2006 г. — № 31. – ст. №3451.

5. Российская Федерация. Приказы. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: Приказ Федеральной службы по техническому и экспортному контролю № 31 – СЗ РФ – 2004 г. – № 34. – ст. №3541.

6. Российская Федерация. Приказы. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации: Приказ ФСТЭК России № 239 – СЗ РФ – 2017. – № 31. – ст. №4736.

7. Российская Федерация. Методические документы. Методика оценки угроз безопасности информации: Методический документ Федеральной службы по техническому и экспортному контролю – СЗ РФ – 2004 г. – № 34. – ст. №3541.

8. Исаева, Ю. А. Построение адаптивной двухуровневой имитационной модели управления системой защиты информации автоматизированной системы управления для оценки ее эффективности / Ю. А. Исаева // МНСК-2018: Информационные технологии : Материалы 56-й Международной научной студенческой конференции, Новосибирск, 22–27 апреля 2018 года. – Новосибирск: Новосибирский национальный исследовательский государственный университет, 2018. – С. 107.

9. Анализ эффективности методов моделирования распределенной системы электронного документооборота с использованием имитационного моделирования // Чернышева А.С., Литвинов В.Л. // Инновации. Наука. Образование. 2022. № 50. – С. 1929-1932.

10. Сабиров, Р. Р. Разработка дискретно-событийной имитационной модели на примере производственного процесса / Р. Р. Сабиров // Транспорт Азиатско-Тихоокеанского региона. – 2023. – № 2(35). – С. 28–35.

11. Байрамукова, Е. И. Использование методов имитационного моделирования при оценке рисков и оптимизации процессов управления на промышленных предприятиях / Е. И. Байрамукова // Известия Российского государственного педагогического университета им. А.И. Герцена. – 2008. – № 85. – С. 315–320.

12. Свидетельство о государственной регистрации программы для ЭВМ № 2022663610 Российская Федерация. Имитационная модель процессов трехуровневого автоматизированного управления техническими средствами № 2461859-1 : № 2022660418 : заявл. 07.06.2022 : опубл. 18.07.2022 / В. А. Селифанов, А. В. Селифанов, В. В. Селифанов.

13. Российская Федерация. Методические документы. Руководство по организации процесса управления уязвимостями в органе (организации): Методический документ Федеральной службы по техническому и экспортному контролю – СЗ РФ – 2004 г. – № 34. – ст. №3541.

14. Имитационная модель для управления защитой информации при оценке эффективности государственных и муниципальных системСелифанов В.В., Исаева Ю.А., Голдобина А.С., Звягинцева П.А.Интерэкспо Гео-Сибирь. 2018. № 7. С. 296-299.

15. Фялковский Е.Е. Использование имитационного моделирования для решения задач реинжиниринга бизнес-процессов в среде моделирования Anylogic // Прикладная математика и фундаментальная информатика – Омск, 2021. – Вып. 8 – С. 67-75.

16. Белова, Е. А. Имитационное моделирование угроз информационной безопасности / Е. А. Белова, В. О. Крылов, О. А. Мартиросова // Актуальные научные исследования в современном мире. – 2020. – № 11-2(67). – С. 32-36.

17. Мельников, А. В. Метод оценки и уменьшения опасности угроз информационной безопасности на основе анализа последовательностей эксплуатации уязвимостей / А. В. Мельников, В. Е. Чирков, А. В. Пузарин // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 39-47.

18. Монахов, А. Д. К вопросу об использовании имитационной среды Anylogic для оценки эффективности вычислительных систем / А. Д. Монахов // Интернет-журнал Науковедение. – 2011. – № 2(7). – С. 29.

19. Минаев, В. А. Имитационное моделирование функционирования центра мониторинга информационной безопасности / В. А. Минаев, А. А. Беликов // Информационная безопасность: вчера, сегодня, завтра : Сборник статей по материалам IV Международной научно-практической конференции, Москва, 22 апреля 2021 года / Под редакцией В.В. Арутюнова. – Москва: Российский государственный гуманитарный университет, 2021. – С. 48-55.

20. Краснов, А. Е. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности / А. Е. Краснов, А. С. Мосолов, Н. А. Феоктистова // Безопасность информационных технологий. – 2021. – Т. 28, № 1. – С. 106-120.