УДК 004.056.5
DOI 10.33764/2618-981X-2024-6-256-262

Е. Ю. Солдатов[1], М. А.Батурина[1], В. В. Селифанов[1]*

Вопросы построения модели системы управления инцидентами информационной безопасности

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: wilgieforz@mail.ru

Аннотация. В статье поднимается вопрос необходимости создания имитационной модели, которая позволит оценивать эффективность системы управления инцидентами информационной безопасности. Для осуществления системного анализа организационной деятельности различных объектов была создана контекстная диаграмма в нотации IDEF0. В ней описан весь жизненный цикл инцидента, начиная с получения событий в систему, заканчивая уведомлением в ГосСОПКА (НКЦКИ). В статье описана и обоснована необходимость создания и внедрения такой системы в информационную сеть, а также необходимость создания модели для оценки эффективности данной системы. Для достижения поставленной цели был проведен анализ рынка аналогичных систем, проблем при их сопровождении. Исходя из анализа, была разработана схема логики работы системы с последующей реализацией программного кода. Построенная имитационная модель позволяет наглядно рассмотреть и изучить процесс оценки эффективности системы контроля инцидентов информационной безопасности для последующего применения полученных знаний в построении системы защиты.

Ключевые слова: Инцидент, имитационная модель, оценка эффективности

E. Yu. Soldatov[1], M. A. Baturina[1], V. V. Selifanov[1]*

Issues of building a models of information security incident management systems

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: wilgieforz@mail.ru

Abstract. The article raises the question of the need to create a simulation model that will allow assessing the effectiveness of the information security incident management system. To carry out a systematic analysis of the organizational activities of various objects, a context diagram was created in IDEF0 notation. It describes the entire incident life cycle, starting with the receipt of events in the System and ending with the National Computer Incident Coordination Centre (NCCCI). The article describes and justifies the need to create and develop such a system in the information network, as well as the need to create a model for assessing the effectiveness of this system. To achieve this goal, an analysis of the market for similar systems and problems in their maintenance was carried out. As a result of the analysis, a diagram of the logic of the system operation with the implementation of the program code was developed. The constructed simulation model allows us to visually review and study the process of assessing the effectiveness of the information security incident control system for the subsequent application of the acquired knowledge in building a protection system.

Keywords. Incident, simulation model, performance assessment

Введение

В сегодняшней взаимосвязанной цифровой среде защита конфиденциальных данных, поддержание целостности и непрерывной работы информационных систем имеют первостепенное значение. Инциденты информационной безопасности представляют значительную угрозу как для организаций, правительств, так и для частных лиц. Будь то утечка данных, кибератака на инфраструктуру или случайное раскрытие информации – эти инциденты могут иметь довольно серьезные последствия.

В свете того, что атаки на информационные инфраструктуры организаций с каждым годом приобретают всё более серьезный и масштабный характер, Президентом и другими регуляторами РФ в последние года выдвигаются новые требования по обеспечению защиты критической информационной инфраструктуры, персональных данных и других областей цифровой среды нашей страны, при этом возникает потребность своевременно реагировать и регистрировать инциденты информационной безопасности, направленные на информационные системы.

Президентом Российской Федерации в 2022 году выпущены следующие правовые акты:

– Указ Президента РФ от 30.03.2022 №166, гласящий о том, что с 31 марта 2022 года введены ограничения на приобретение иностранного оборудования и программного обеспечения для субъектов КИИ, а также услуги по использованию такого ПО без согласования с уполномоченным органом [1];

– Указ Президента РФ от 01.05.2022 №250, гласящий о том, что с 1 января 2025 г. организациям запрещается использовать средства защиты информации, произведенные в недружественных государствах [2].

Также с 13 февраля 2023 года вступил в силу приказ ФСБ России №77, утверждающий порядок взаимодействия операторов с ГосСОПКА на информационные ресурсы РФ, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных [3].

В настоящий момент существует проблема: несмотря на то, что на рынке уже представлены коммерческие решения подобного класса систем, требования к программным и программно-техническим средствам, которые используются в целях обеспечения защиты информации (регистрация инцидентов в автоматизированной системе) регуляторами, никак не регламентированы. Таким образом, исследования по решению указанной проблемы представляются актуальными.

Обоснование применения имитационного моделирования

Для осуществления системного анализа организационной деятельности различных объектов предусмотрены специальные нотации моделирования бизнес-процессов. В свою очередь, специальные программные средства позволяют реализовать эти нотации и построить функциональные диаграммы потоков данных.

Функциональные диаграммы потоков данных позволяют детально рассмотреть существующие бизнес-процессы на предприятии и выявить слабые места в

его работе. Построение диаграмм необходимо для анализа работы предприятия в настоящее время («как есть») и построения диаграмм в дальнейшем, отображающих, что должно быть модернизировано («как должно быть»).

Моделирование бизнес-процессов, осуществляемых при проектировании и разработки системы, проводилось в нотациях IDEF0 и DFD [4].

Построение функциональных диаграмм осуществлялось с помощью программного средства «Microsoft Visio». Контекстная диаграмма «как есть», выполненная в нотации IDEF0 (рис. 1) [5, 6].

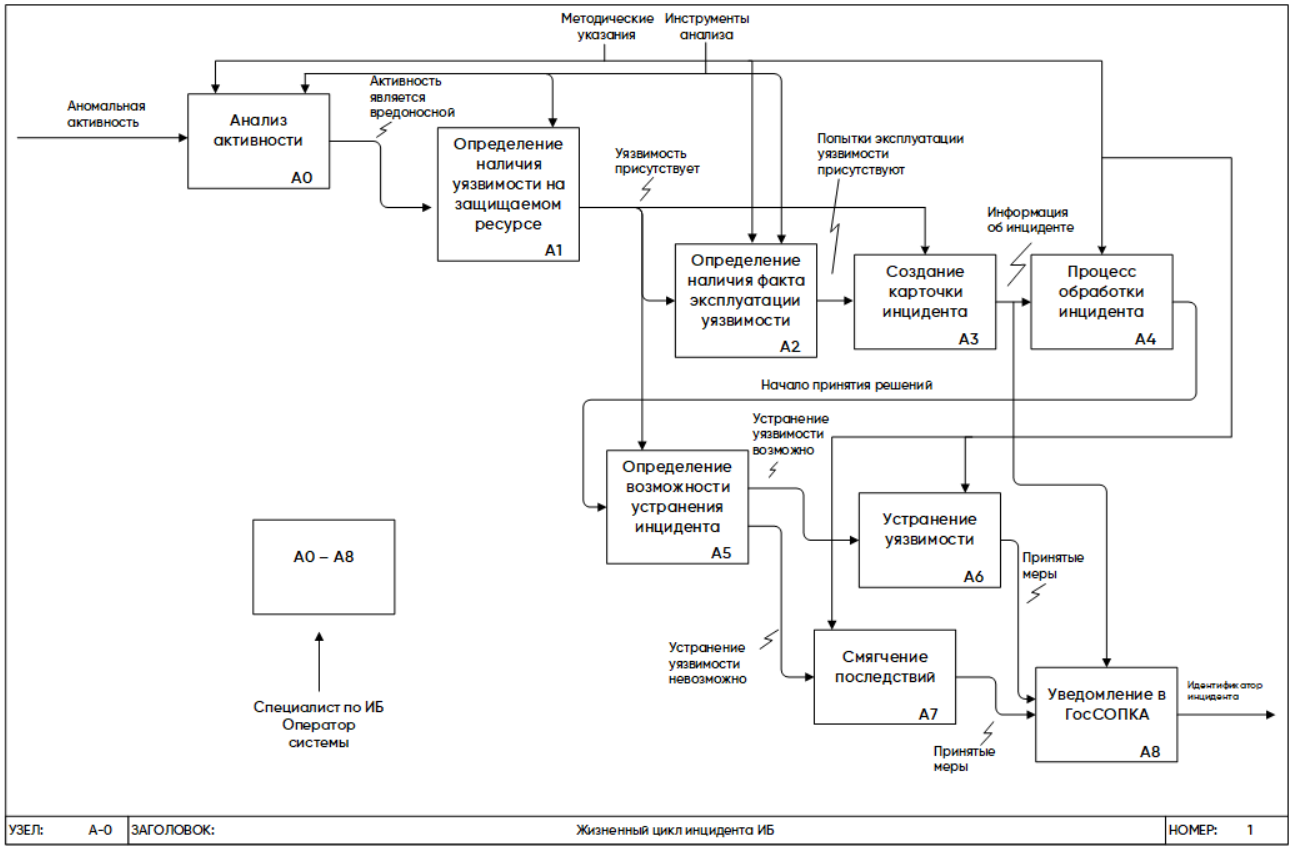

Рис. 1. Контекстная диаграмма системы управления инцидентами

Весь процесс создания системы управления инцидентами в области информационной безопасности начинается с изучения потребностей пользователей и анализа рынка. Необходимо изучить уже имеющиеся системы, оценить их конкурентоспособность и выявить проблемы, с которыми сталкиваются пользователи при выборе подобных продуктов. Полученная информация помогает определить требования к будущей системе, учитывая как опыт конкурентов, так и потребности конечных потребителей. Далее, опираясь на выходное техническое задание предыдущего процесса, а также на нормативно-правовую базу [7, 8], имеющую отношение к компьютерным инцидентам, можно приступать к проектированию системы (выбор метода и стратегии решения, выбор представления внутренних данных, разработка основного алгоритма, документирование программного обеспечения, тестирование и подбор тестов, выбор представления

входных данных). Итогом данного процесса является выбранная методология разработки и документация по архитектуре системы. Опираясь на требования в документации, можно приступать к непосредственной разработке самой системы и реализации программного кода. Инженер по тестированию получает программное обеспечение для проведения тестирования на корректность работы заявленных функций и выявления программных ошибок. После тестирования и успешной проверки работоспособности всех заявленных функций, а также нахождения программных ошибок в функциях (с последующим их исправлением разработчиком), системный администратор и инженер по эксплуатации выполняют внедрение системы в информационную сеть субъекта. Результатом данного процесса является полностью функционирующая система в информационной сети.

После разработки и внедрения системы в информационную сеть субъекта возникает необходимость оценить уровень доверия к ней, то есть быть уверенным, что при возникновении инцидента программное средство отработает корректно. Так как ни один регулятор не выдвигает свои требования к разработке, построению и функциональности систем подобного класса, а также, поскольку оценка эффективности в промышленной информационной сети во время всех рабочих процессов после внедрения является сложно реализуемым и затратным процессом, который может повлечь за собой сбои в работе, была разработана модель для оценки эффективности до ее ввода в промышленную эксплуатацию. В данном случае необходимо использовать метод имитационного моделирования.

Имитационное моделирование представляет собой метод исследования системы, при котором созданная виртуальная модель полностью повторяет функционал и структуру реальной системы с целью изучения данной системы при различных обстоятельствах. В такой модели можно изменять параметры, проводить эксперименты и анализировать результаты. Имитационное моделирование представляет собой инструмент, позволяющий анализировать различные параметры эффективности, включая производительность, надежность, использование ресурсов и пропускную способность. Данный подход позволяет принимать обоснованные решения на основе данных, полученных в контролируемой среде, минимизируя риски и затраты.

Методология имитационного моделирования применялась для решения ряда задач, включая оценку эффективности методов моделирования распределенной системы электронного документооборота, что способствовало решению задач реинжиниринга бизнес-процессов [9, 10].

Построение модели

Дискретно-событийное имитационное моделирование помогает провести анализ труднодопустимых ситуаций, определить слабые места в системе для последующего исключения их, спрогнозировать поведение системы при различных обстоятельствах. Преимуществом является возможность тестирования системы безопасности в различных сценариях, а также анализ последствий инцидентов без реального риска сбоя системы и потери ресурсов.

На основании построенной ранее контекстной диаграммы в нотации IDEF0, была разработана имитационная модель системы массового обслуживания системы управления инцидентами (рис. 2).

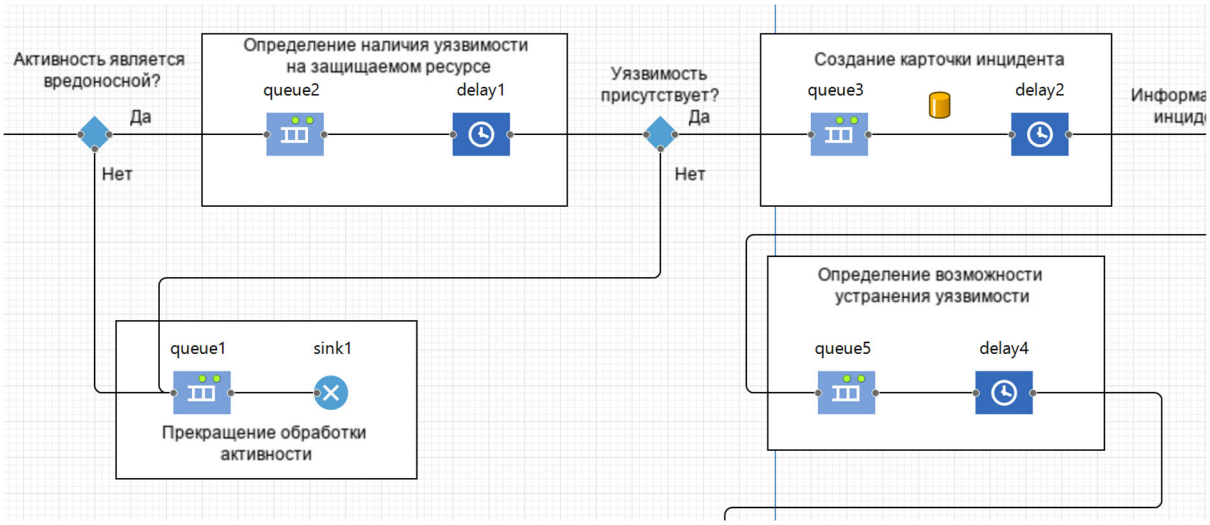

Рис. 2. Фрагмент построенной модели системы управления инцидентами

При работе системы можно видеть, как агенты поступают и проходят через каждый элемент (рис. 3).

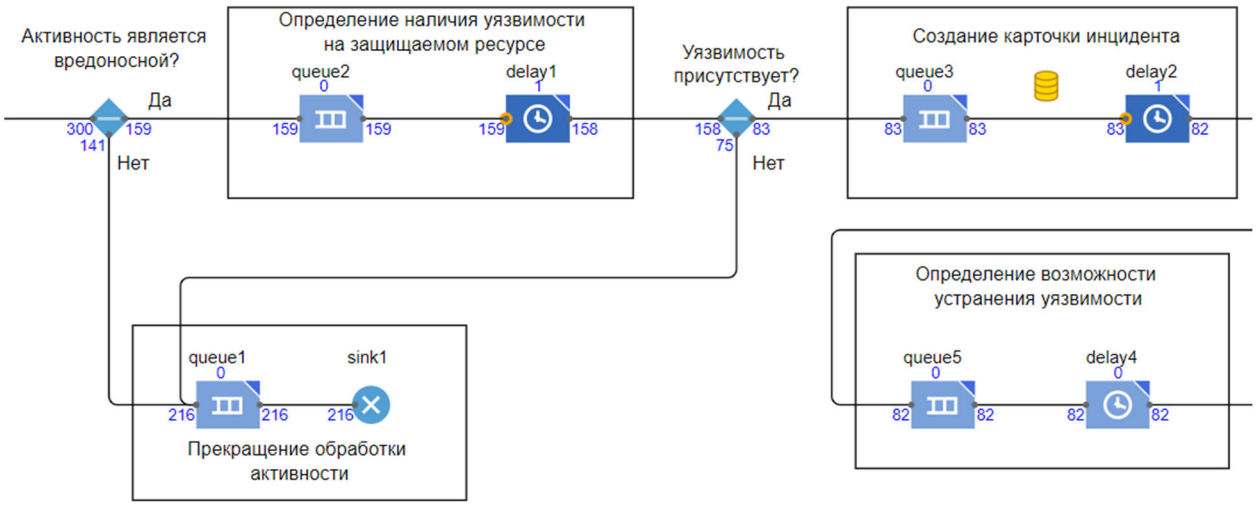

Рис. 3. Поступление агентов в блоки

Благодаря возможности проведения анализа каждого элемента модели в отдельности, становится осуществимым детальное изучение влияния изменений параметров на отдельные компоненты системы. Это способствует повышению точности настройки модели и улучшает её способность к адекватному отображению реальных процессов. Данный подход позволяет более эффективно осу-

ществлять оптимизацию процессов и принимать обоснованные решения на основе результатов моделирования.

Дискретно-событийное моделирование в AnyLogic предлагает гибкость в настройке параметров модели и их связи с реальными системами управления инцидентами. Параметры модели включают интенсивность прибытия событий, вместимость очереди и время задержки. Интенсивность прибытия определяет частоту поступления событий в систему, что в реальной системе управления инцидентами может соответствовать частоте создания карточек инцидентов. Вместимость очереди ограничивает количество инцидентов, которые могут находиться в очереди одновременно. Время задержки отражает время, которое инцидент проводит в системе до его обработки. Связь с реальными параметрами позволяет настроить модель на основе статистики поступления заявок в реальной системе. Можно установить ограничения на количество инцидентов в очереди и учесть среднее время обработки инцидентов. После настройки параметров модели проводятся эксперименты, в ходе которых изменяются параметры и анализируется влияние на производительность системы. Это помогает выявить слабые места и оптимизировать процессы управления инцидентами.

Заключение

Процесс обработки инцидентов кибербезопасности включает сбор и анализ данных, мониторинг событий безопасности, расследование инцидентов, принятие решений по защите информации и использование специализированных систем и технологий для реагирования на инциденты и управления рисками кибербезопасности.

Компьютерная модель системы контроля инцидентами информационной безопасности, интегрирующая такие параметры, как значимость информации об инцидентах, аномальную активность в оптико-электронных устройствах и системах, а также погрешность при обработке инцидентов, предоставляет возможность детально исследовать процесс управления инцидентами в системе, а также оценить его результативность. Визуализация модели системы контроля инцидентами информационной безопасности позволяет участникам процесса управления угрозами наглядно оценить динамические изменения потенциальных атак и аномальной активности, идентифицировать уязвимые места и отслеживать влияние различных факторов на общую картину безопасности системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Указ президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 30.03.2022. – № 14. – ст. 2242.

2. Указ президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 01.05.2022. – № 18. – ст. 3058.

3. Приказ ФСБ РФ от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с ГосСОПКА на информационные ресурсы, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (представление, распростра-

нение, доступ) персональных данных» // Официальный интернет-портал правовой информации (ФСБ России). – 20.02.2023. – №14.

4. Солдатов Е.Ю., Селифанов В.В., Кувшинов М.А. Разработка системы контроля инцидентов информационной безопасности // Безопасность цифровых технологий. – 2023. – № 3 (110). – С. 54-66.

5. 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.

6. Моделирование процессов и систем защиты информации AnyLogic : учебное пособие / А. В. Шабурова, В. А. Селифанов, В. В. Селифанов, П. А. Звягинцева, Ю. А. Исаева, А. С. Голбодина, А. В. Селифанов. – Новосибирск : СГУГиТ, 2020. – 70 с.

7. ГОСТ Р 59709-2022. Защита информации. Управление компьютерными инцидентами. Термины и определения : Национальный стандарт российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии 29 ноября 2022 г. № 1375-ст : введен впервые : дата введения 2023-02-01 / разработан Федеральным государственным казенным учреждением «Войсковая часть 43753» (в/ч 43753), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»). – М. : Российский институт стандартизации, 2022. – 20 с.

8. ГОСТ Р 59710-2022. Защита информации. Управление компьютерными инцидентами. Общие положения : Национальный стандарт российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии 29 ноября 2022 г. № 1376-ст : введен впервые : дата введения 2023-02-01 / разработан Федеральным государственным казенным учреждением «Войсковая часть 43753» (в/ч 43753), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»). – М. : Российский институт стандартизации, 2022. – 16 с.

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

10. Использование имитационного моделирования для решения задач реинжиниринга бизнес-процессов в среде моделирования Anylogic // Фялковский Е.Е. // Прикладная математика и фундаментальная информатика. 2021. – Т. 8. № 1. – С. 67-75.