УДК 004.056.5

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

Моделирование процессов управления инцидентами информационной безопасности

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

Аннотация. В статье рассматривается вопрос проведения оценки эффективности системы управления инцидентами информационной безопасности с помощью имитационного моделирования. Обоснована необходимость и описан процесс ее создания и внедрения на объекте защиты, а также необходимость разработки имитационной модели для оценки эффективности. Разработана схема работы системы оценки эффективности системы управления инцидентами информационной безопасности, а также математическая модель с помощью программного средства AnyLogic, которая позволяет оценивать систему управления инцидентами информационной безопасности до ее ввода в промышленную эксплуатацию в информационную сеть, не требуя построения иных имитационных моделей, а также поможет выявить наиболее слабые места и оптимизировать процессы управления инцидентами.

Ключевые слова: Инцидент, имитационная модель, оценка эффективности

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

Modeling information security incident management processes

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

Abstract. The article considers the issue of evaluating the effectiveness of the information security incident management system using simulation modeling. The article substantiates the need and describes the process of its creation and implementation at the protection facility, as well as the need to develop a simulation model to assess effectiveness. A scheme of the logic of the system for evaluating the effectiveness of the information security incident management system was developed, as well as a mathematical model using the AnyLogic software tool, which allows the evaluating in the information security incident management system before it is put into commercial operation in the information network, without requiring the construction of other simulation models, and will also help identify the weakest points and optimize management processes incidents.

Keywords. Incident, simulation model, performance assessment

Введение

В современном цифровом мире наиважнейшими задачами являются: охрана конфиденциальных данных, обеспечение целостности и постоянного функционирования информационных систем. Инциденты в сфере информационной безопасности становятся ощутимой угрозой для организаций, государственных структур и отдельных лиц. Инциденты бывают разного характера: утечка данных, хакерские атаки на инфраструктуру, непреднамеренное разглашение данных, при этом все они чреваты серьезными последствиями.

Учитывая растущую серьезность и масштабность кибератак и потребность в соблюдении новых требований со стороны регулирующих органов к защите критической информационной инфраструктуры и персональных данных, становится важным своевременно выявлять и регистрировать инциденты информационной безопасности в целях защиты информационных систем. Примером этого являются следующие нормативно-правовые документы:

– Указ Президента РФ от 30.03.2022 №166 гласящий о том, что с 31 марта 2022 года были 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];

– 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].

На данный момент наблюдается пробел в регулировании, хотя на рынке существуют коммерческие системы управления инцидентами, нормативные акты не устанавливают конкретных требований к программному и техническому обеспечению, используемому для защиты информации в автоматизированных системах.

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»).

Построение функциональных диаграмм осуществлялось с помощью программного средства «Microsoft Visio». Контекстная диаграмма «как есть» представлена на рисунке 1 [4–6].

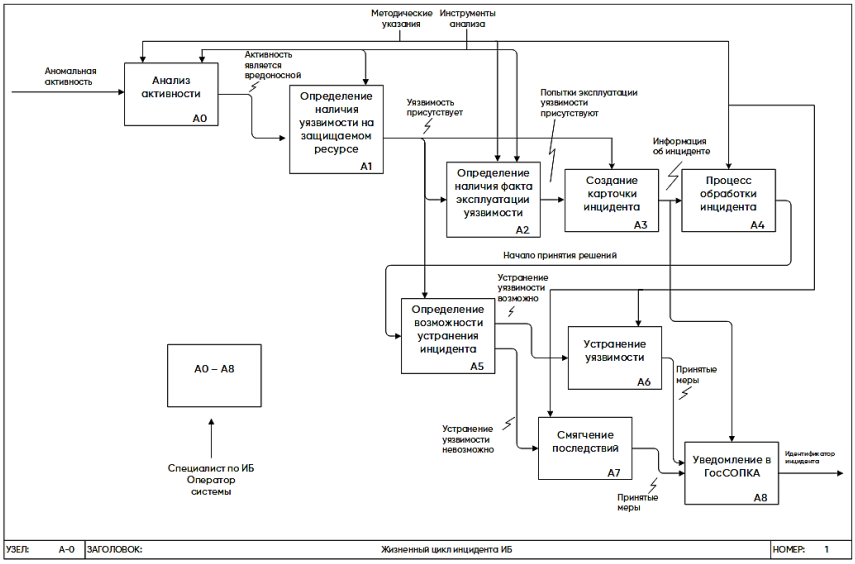

Рис. 1. Контекстная диаграмма системы управления инцидентами

Весь жизненный цикл системы управления инцидентами информационной безопасности начинается со спроса на аналогичные системы. Происходит исследование рынка, анализ уже существующих систем на рынке, оценка конкурентоспособности. Информация о ситуации на рынке и желании потребителя необходима для формирования требований будущей системы. Для успешного проектирования новой системы бизнес-аналитик собирает данные о существующих решениях конкурентов и потребностях целевых клиентов. Эта информация включает в себя:

– анализ предложений конкурентов и их соответствие требованиям рынка;

– идентификацию проблем и сложностей, испытываемых покупателями при использовании подобных систем;

– определение недостатков в функциональности существующих систем, таких как высокая стоимость, трудности во внедрении и поддержке.

Далее, опираясь на выходное техническое задание предыдущего процесса, а также на нормативно-правовую базу (приказы и некоторые ГОСТы [7, 8], связанные с компьютерными инцидентами) 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, а также известные последующие этапы. 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 возможных программных ошибок. После тестирования и успешной проверки работоспособности всех заявленных функций, а также нахождения каких-либо 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 предоставляет ценный инструмент для оценки эффективности систем в различных аспектах, включая производительность, надежность, потребление ресурсов и пропускную способность. Оно позволяет принимать обоснованные решения на основе данных, собранных в контролируемой среде, снижая риски и затраты. Метод имитационного моделирования успешно применяется в разнообразных областях, в том числе для анализа эффективности распределенных систем электронного документооборота и оптимизации бизнес-процессов через реинжиниринг [9, 10].

Построение модели

Дискретно-событийное имитационное моделирование помогает провести анализ трудно допустимых ситуаций, определить слабые места в системе для последующего исключения их, спрогнозировать поведение системы при различных обстоятельствах. Также преимуществом является возможность тестирования системы безопасности в различных сценариях и проведение анализа 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, схема которой приведена на рисунке 2.

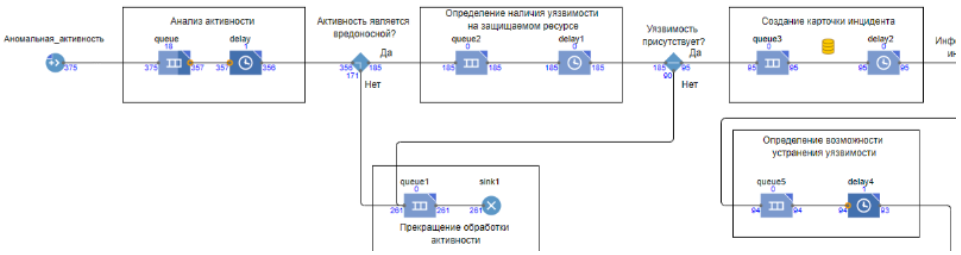

Рис. 2. Фрагмент имитационной модели системы управления инцидентами

Дискретно-событийное моделирование в AnyLogic предоставляет гибкие возможности для изменения параметров модели, а также их связи с реальными системами управления инцидентами [6]. Ниже приведены ключевые аспекты:

1. Детальная настройка параметров модели:

1.1. Скорость поступления – это параметр, определяющий интенсивность поступления событий (инцидентов) в систему. В реальной системе управления инцидентами это может быть, например, частота созданий карточек инцидентов;

1.2. Вместимость очереди – это параметр, определяющий количество инцидентов, находящихся в очереди одновременно. В моем случае, например, инциденты, которые ожидают устранения уязвимости;

1.3. Время ожидания – это параметр, определяющий время, которое инцидент проводит в системе до его обработки. В контексте реальной системы это может быть время, которое специалисты тратят на решение инцидента.

2. Сопоставление с реальными параметрами:

2.1. Скорость поступления: модель может быть сконфигурирована на основе статистики поступления запросов в реальной системе. Например, если в реальной системе инциденты поступают средним интервалом в 10 минут, то в модели можно установить соответствующую скорость поступления;

2.2. Сканирование зараженных систем на наличие факта возможной постэксплуатации, следов распространения вредоносного программного обеспечения;

2.3. Настройка средств защиты (например, блокировка IP-адресов злоумышленников);

2.4. Вместимость очереди: если в реальной системе есть ограничение на количество инцидентов в очереди, то в модели можно задать аналогичное ограничение;

2.5. Время ожидания: модель может учитывать среднее время обработки инцидентов в реальной системе. Это позволит оценить, сколько времени инцидент будет проводить в системе до его обработки.

3. Эксперименты и анализ: после настройки параметров модели можно проводить эксперименты, изменяя параметры и изучая, как это влияет на производительность системы. Это поможет выявить наиболее слабые места и оптимизировать процессы управления инцидентами.

Заключение

В рамках данной работы была построена имитационная модель, которая позволяет оценивать систему управления инцидентами информационной безопасности до ее ввода в промышленную эксплуатацию в информационную сеть, не требуя построения иных имитационных моделей.

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

4. Разработка системы контроля инцидентов информационной безопасности // Солдатов Е.Ю., Селифанов В.В., Кувшинов М.А. // 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 [Текст] : 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»). – Москва : Российский институт стандартизации, 2022, 20 с. – Текст : непосредственный.

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»). – Москва : Российский институт стандартизации, 2022, 16 с. – Текст : непосредственный.

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. 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.