Научная статья
УДК 004.56
DOI: 10.26583/bit.2025.2.02

ПРИМЕНЕНИЕ СРЕДЫ ANYLOGIC ДЛЯ МОДЕЛИРОВАНИЯ И АНАЛИЗА ПРОЦЕССА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Камилла М. Хуранова[1], Игорь Д. Кологоров[2], Сергей А. Резниченко[3], Леонид Н. Кессаринский[4]
[1,2,3]Финансовый университет при правительстве Российской Федерации, Ленинградский пр-кт, 49, Москва, 125993, Россия
[3,4]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[3]Российский государственный гуманитарный университет, Миусская площадь, 6, Москва, 125047, Россия
[1]222393@edu.fa.ru, https://orcid.org/0009-0002-3650-8415
[2]224044@edu.fa.ru, https://orcid.org/0009-0001-8285-7600
[3]rsa_5@bk.ru, https://orcid.org/0000-0002-1539-0457
[4]LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166

Аннотация. В статье приводятся результаты комплексного анализа процесса аудита информационной безопасности (ИБ) с использованием методов имитационного моделирования в среде AnyLogic. Актуальность исследования обусловлена возрастающей сложностью киберугроз и необходимостью оптимизации ресурсов, затрачиваемых на обеспечение безопасности информационных систем. Цель работы – разработка и исследование динамической модели, позволяющей оценивать временные и логические параметры аудита ИБ, а также выявлять критические точки процесса. Методологическую основу исследования составляет агентно-ориентированный подход, реализованный в AnyLogic. Данный инструмент выбран благодаря возможности интеграции дискретных событийных и системно-динамических методов, что обеспечивает многомерный анализ взаимодействия этапов аудита. Модель включает пять ключевых этапов: планирование, сбор данных, анализ рисков, формирование отчёта и корректирующие действия. Входные данные, предоставленные RTM Group, содержат статистику временных интервалов выполнения этапов, также найдены частоты возникновения инцидентов. Результаты моделирования выявили нелинейную зависимость между длительностью этапов и количеством обнаруживаемых уязвимостей. Визуализация процесса в AnyLogic позволила идентифицировать узкие места. Разработанная модель обладает свойством адаптивности: параметры быть скорректированы с учётом организационной специфики. Для валидации проведено сравнение с реальными данными RTM Group, показавшее погрешность прогноза длительности аудита в пределах нескольких процентов. Выводы исследования свидетельствуют о результативности внедрения имитационного моделирования как инструмента обеспечения прозрачности аудиторских процедур в области информационной безопасности. В отличие от традиционных, подход на базе AnyLogic обеспечивает количественную оценку сценариев. Исследование вносит вклад в развитие методологии управления информационной безопасностью, предлагая инструмент для балансировки между операционной эффективностью и требованиями киберзащиты. Полученные результаты могут быть применены как в коммерческих организациях, так и в государственных структурах, работающих с критически важными данными.

Ключевые слова: *аудит информационной безопасности, имитационное моделирование, AnyLogic, агентно-ориентированный подход, временные затраты.*

Для цитирования: *Хуранова, Камилла М. и др. Применение среды ANYLOGIC для моделирования и анализа процесса аудита информационной безопасности. Безопасность информационных технологий, [S.l.], т. 32, № 2, с. 21–31, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1781. DOI: 10.26583/bit.2025.2.02.*

Scientific article

USING THE ANYLOGIC ENVIRONMENT FOR MODELING AND ANALYSIS OF THE INFORMATION SECURITY AUDIT PROCESS

Kamilla M. Khuranova[1], Igor D. Kologorov[2], Sergey A. Reznichenko[3], Leonid N. Kessarinskiy[4]
[1,2,3]*Financial University under the Government of the Russian Federation, Leningradsky Ave., 49, Moscow, 125993, Russia*
[3,4]*National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia*
[3]*Russian State University for the Humanities, Miusskaya Square, 6, Moscow, 125047, Russia*
[1]*222393@edu.fa.ru, https://orcid.org/0009-0002-3650-8415*
[2]*224044@edu.fa.ru, https://orcid.org/0009-0001-8285-7600*
[3]*rsa_5@bk.ru, https://orcid.org/0000-0002-1539-0457*
[4]*LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166*

Abstract. The article presents the results of a comprehensive analysis of the information security audit process using simulation methods in the AnyLogic environment. The relevance of the study is due to the increasing complexity of cyber threats and the need to optimize the resources spent on ensuring the security of information systems. The research aims to develop a dynamic model for evaluating temporal and logical parameters of security audits while identifying critical process bottlenecks. Methodologically, the study employs an agent-based approach implemented in AnyLogic. This environment platform was selected for its ability to integrate discrete event and system dynamics methods, enabling a multidimensional analysis of audit stage interactions. The model incorporates five key phases: planning, data collection, risk analysis, report generation, and corrective actions. Input data from RTM Group includes statistical timelines for audit stages and incident frequency patterns. Simulation results revealed a non-linear relationship between phase durations and detected vulnerabilities. AnyLogic's visualization tools helped pinpoint process bottlenecks. The developed model features adaptability, allowing parameter adjustments to align with organizational specifics. Validation against RTM Group's real-world data showed an audit duration prediction error margin within a few percentage points. Conclusions confirm the effectiveness of simulation modeling for enhancing audit transparency. Unlike traditional methods, the AnyLogic-based approach enables quantitative scenario evaluation. The study contributes to information security management methodology by providing a tool to balance operational efficiency and cybersecurity requirements. Results are applicable to both commercial entities and government institutions handling mission-critical data.

Keywords: *information security audit, simulation modeling, AnyLogic, agent-based approach, time costs.*

For citation: *Khuranova, Kamilla M. et al. Using the AnyLogic environment for modeling and analysis of the information security audit process. IT Security (Russia), [S.l.], v. 32, no. 2, p. 21–31, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1781. DOI: 10.26583/bit.2025.2.02.*

Введение

Рост количества использований информационных технологий пропорционально их применению отображается на увеличении количества угроз безопасности организации, конфиденциальности сведений, которые в ней обрабатываются [1].

Эволюция социально-экономических систем от постиндустриальной фазы к информационной парадигме детерминирует экспоненциальный рост значимости информации как стратегического актива. Данная трансформация требует приоритезации разработки комплексных механизмов обеспечения информационной безопасности, что обусловлено необходимостью защиты критически важных данных в условиях цифровизации глобальных коммуникационных процессов [2].

Компания Positive Technologies, являющаяся ключевым игроком на рынке разработки решений в сфере информационной безопасности[1], на основании анализа статистических данных, полученных в результате мониторинга более 2300 российских организаций, констатирует устойчивую динамику роста кибератак.

Согласно аналитике Positive Technologies общее количество инцидентов в 2023 г. увеличилось на 17,7%, рис. 1.

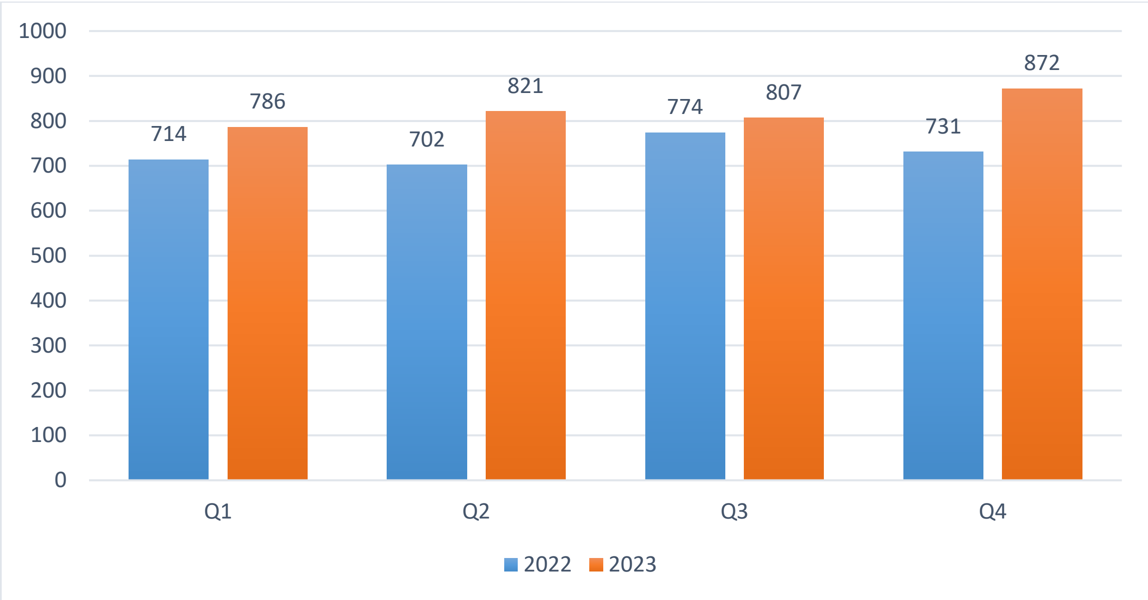


Рис. 1. Количество инцидентов в 2022 и 2023 годах (по кварталам)[2]

На фоне нарастающего количества инцидентов предприятиям стоит на регулярной основе проводить проверку правильного функционирования всех информационных систем, средств защиты информации и т. д. Данный тип проверки именуется аудитом информационной безопасности. Так, аудит информационной безопасности (аудит ИБ) – это независимая проверка системы защиты данных, которая соответствует заданным критериям (требованиям закона или принятым корпоративным стандартам). Наличие аудита безопасности информационных систем повышает вероятность принятия адекватных мер безопасности и предотвращения различных видов атак или снижения негативных последствий. [3]

Посредством экспертного аудита осуществляется вычисление вероятности атаки, а уровень ущерба – собственником информации [4].

Целью работы является рассмотрение проведения аудита информационной безопасности, его этапов и методов в целом, а также моделирование процесса с использованием инструмента имитационного моделирования AnyLogic.

[1]О компании. Positive Technologies. 2022. URL: https://www.ptsecurity.com/ru-ru/about/ (дата обращения: 22.03.2025).
[2]Актуальные киберугрозы: IV квартал 2023 года. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ (дата обращения: 03.03.2025).

1. Этапы проведения аудита информационной безопасности

Аудит информационной безопасности представляет собой систематический процесс, включающий последовательность пяти взаимосвязанных этапов, каждый из которых вносит вклад в достижение целостного понимания состояния защищённости информационных активов организации.

1. Планирование является фундаментальным этапом, на котором формируется методологическая основа аудита. На данном этапе определяются цели, границы и критерии оценки, соответствующие международным стандартам или внутренним регламентам организации. Разрабатывается детальный план, включающий перечень проверяемых объектов, методы сбора данных, временные рамки и распределение ресурсов. Особое внимание уделяется идентификации критически важных активов и потенциальных рисков, что позволяет сфокусировать усилия на наиболее уязвимых компонентах инфраструктуры.

2. Сбор данных предполагает комплексное применение автоматизированных и ручных методов для получения релевантной информации о состоянии системы защиты. Автоматизированный сбор логов и метрик осуществляется с использованием специализированных инструментов, что обеспечивает объективность и масштабируемость процесса. Параллельно проводится опрос сотрудников посредством анкетирования или структурированных интервью, направленный на выявление субъективных факторов, таких как уровень осведомлённости в области ИБ. Дополнением служит анализ документов: политик, регламентов, отчётов об инцидентах и результатов предыдущих проверок, что позволяет оценить соответствие декларируемых мер реальной практике.

3. Анализ полученных данных осуществляется с применением качественных и количественных методов. На данном этапе выявляются отклонения от нормативных требований, оценивается эффективность внедрённых контрмер и моделируются потенциальные угрозы. Используются методы сравнительного анализа, например, сопоставление текущих показателей с базовыми уровнями безопасности или эталонными сценариями.

4. Формирование отчёта представляет собой структурированное изложение результатов аудита, включающее описание обнаруженных несоответствий, оценку их критичности и рекомендации по устранению. Отчёт должен быть адаптирован для различных стейкхолдеров: технические специалисты получают детализированные данные об уязвимостях, а руководство – сводные выводы с акцентом на стратегические риски и экономические аспекты. Документ служит основой для разработки корректирующих действий и интеграции выводов аудита в общую систему управления информационной безопасностью организации.

5. Исправление завершает цикл аудита и предполагает практическую реализацию рекомендаций, изложенных в отчёте. На данной стадии формируются рабочие группы, ответственные за устранение недостатков, устанавливаются сроки выполнения и критерии приемки. Этот этап обеспечивает замкнутость процесса, трансформируя выводы аудита в конкретные меры по повышению устойчивости информационной системы.

2. Основания применения AnyLogic для моделирования процесса аудита информационной безопасности

Имитационное моделирование представляет собой методологию анализа систем, осуществляемую посредством создания их виртуального аналога и последующего тестирования генерируемых моделью прогнозных сценариев. Данная модель формализует структурно-функциональные зависимости между компонентами системы, отражая алгоритмизированные принципы их взаимодействия в рамках заданных параметров [5].

Современная научная парадигма определяет моделирование как базисный исследовательский инструментарий, обладающий кросс-дисциплинарной применимостью и обеспечивающий верифицируемую оценку системных характеристик высокоуровневых комплексов. Методологическая валидность данного подхода подтверждается его способностью формализовать структурно-функциональные взаимосвязи объектов исследования посредством математически обоснованных репрезентаций [6].

Место имитационного моделирования (ИМ) среди иных способов исследования системы представлено на рис. 2.

Имитационное моделирование основывается на принципе замещения прямого расчёта влияния отдельных элементов на результат анализом их динамических взаимодействий, с последующей симуляцией системного поведения в заданном временном интервале. В ходе итеративного процесса отслеживается эволюция моделируемого объекта, идентифицируются его ключевые параметры, что формирует базу для выработки рекомендаций по повышению эффективности системы.

Техническая реализация метода предполагает модульную архитектуру, обеспечивающую декомпозицию сложных систем на иерархические компоненты с ограниченными интерфейсными связями. Каждый модуль допускает автономную параметризацию с использованием специализированных математических методов, а возможность замены структурных элементов обеспечивает гибкость при проектировании новых моделей [7].

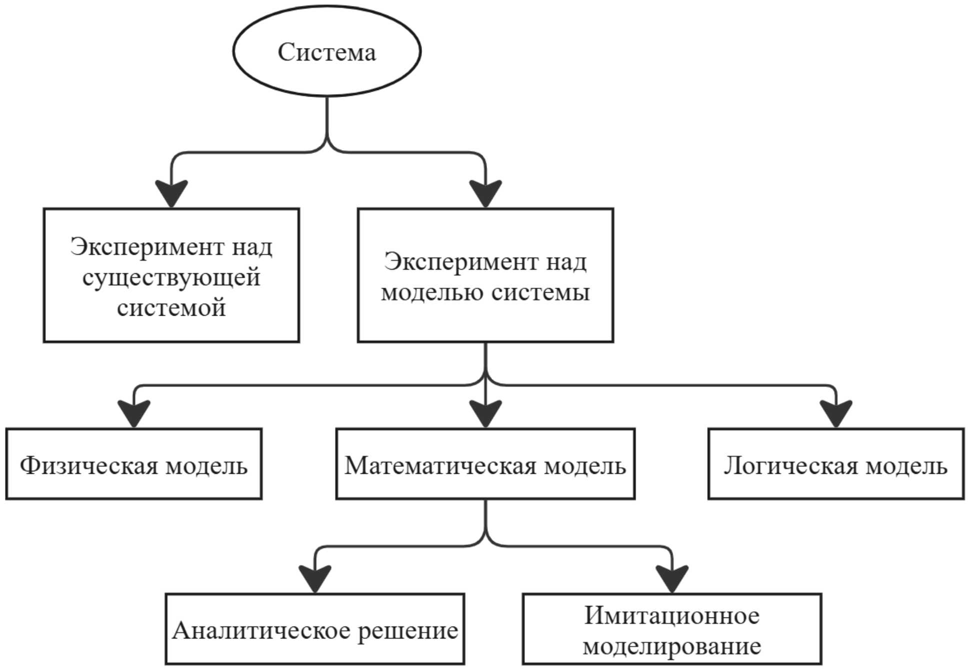


Рис. 2. Место ИМ среди других методов исследования

ИМ представляет собой метод разработки логико-математической модели, которая описывает функционирование сложной системы. Такая модель позволяет на основе исходных данных прогнозировать и оценивать состояние системы при различных внешних и внутренних воздействиях. Моделирование процесса дает возможность провести однозначную оценку эффективности построенной системы и предложить пути ее оптимизации.

AnyLogic отвечает всем нуждам, необходимым при моделировании различных процессов, а также позволяет рассматривать различные бизнес-процессы и оценивать возможности по их оптимизации [8]. AnyLogic поддерживает моделирование с использованием системной динамики, дискретных событий и агентных моделей, а также гибридных моделей, содержащих любую комбинацию этих различных подходов к моделированию в одном и том же симуляторе [9].

AnyLogic одна из немногих российских разработок в области имитационного моделирования, получивших признание за рубежом. По сравнению с традиционными инструментами AnyLogic обеспечивает более существенные возможности при меньших трудозатратах [10].

Использование ИМ позволяет наглядно и доступно представить систему в виде процесса, состоящего из последовательности взаимосвязанных событий, что особенно полезно при проектировании процесса проведения аудита информационной безопасности, так как позволяет визуализировать все этапы и взаимодействия между ними.

Процедуры аудита могут быть рассмотрены как система массового обслуживания замкнутого типа. В такой системе источники заявок (в данном случае – процедуры аудита) являются внутренними элементами системы и имеют фиксированное количество. Заявки в этой системе представляют собой непосредственно сами процедуры аудита, которые обрабатываются в соответствии с заданными правилами и параметрами.

Для обеспечения оперативного и наглядного анализа на основе разработанной схемы проведения аудита информационной безопасности была создана имитационная модель с использованием российской платформы AnyLogic.

Целью данного моделирования выступает идентификация корреляционных зависимостей между локальными параметрами агентов и их модификациями, детерминирующими глобальную динамику системы, с последующей генерацией прогностических сценариев или ретроспективной интерпретацией наблюдаемых феноменов.

3. Моделирование процесса проведения аудита ИБ

Приоритетным требованием выступает формирование массива верифицированных экспериментальных данных, поскольку корректная параметризация имитационных моделей информационных систем требует наличия репрезентативных исходных параметров, обеспечивающих адекватность моделирования. В качестве исходных данных принимается в счёт время, затраченное на проведение того или иного этапа. Вся первоначальная информация была получена на основании данных, взятых от компании, предоставляющая услуги по проведению аудита информационной безопасности RTM Group[3]. Согласно полученным данным, составим табл. 1 с описанием затраченного времени на выполнение каждого этапа.

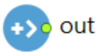
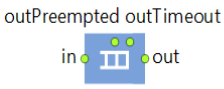
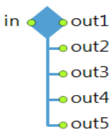
Таблица 1. Время выполнения каждого этапа

Наименование этапа		Затраченное время на выполнение этапа (в сутках)
Планирование		2 – 5
Сбор данных	Автоматизированный сбор логов	14 – 19
	Опрос сотрудников	14 – 19
	Анализ документов	14 – 19
Анализ	Анализ	19 – 28
	Срочное реагирование (по необходимости)	От 1 часа до суток
Формирование отчёта		5 – 9
Исправление		0,5 – 3

[3]Аудит ИБ в рамках отдельных бизнес-процессов. RTM Group. 2024. URL: https://rtmtech.ru/services/audit-ib-biznes-protsessov/ (дата обращения: 22.03.2025).

В табл. 2 представлены все блоки, которые используются при разработке модели, а также описание их функций.

Таблица 2. Описание использованных блоков

Обозначение блока	Название блока	Описание
	Source	Осуществляет генерацию агентов в контексте агент-ориентированного моделирования, выступая исходным элементом для инициализации их последующего перемещения в рамках заданной процессуальной логики.
	Sink	Обеспечивает терминацию агентных сущностей, поступающих в систему, выполняя роль финального узла в структуре их процессуального перемещения в рамках агент-ориентированной модели.
	Delay	Реализует временную приостановку обработки агентных сущностей на заданный интервал, длительность которого определяется динамически с учетом параметров стохастического распределения, индивидуальных атрибутов текущего агента или внешних условий системы в рамках агент-ориентированной модели.
	Queue	Реализует функционал упорядоченного хранения агентных сущностей в условиях ожидания их обработки последующими модулями в процессуальной цепочке или выступает в качестве универсального контейнера для временного размещения агентов.
	Batch	Осуществляет агрегацию определенного количества поступающих агентных сущностей в единый составной агент, функционирующий как логическая группа. Режим работы блока допускает два сценария: формирование статической партии или динамической партии.
	TimeMeasureStart	Функционирует как стартовая точка инструментального комплекса, предназначенного для фиксации временных метрик, связанных с перемещением агентных сущностей между узлами процессуальной диаграммы в рамках агент-ориентированного моделирования.
	TimeMeasureEnd	Выступает финальным элементом измерительного контура, инициируемого блоком TimeMeasureStart, и обеспечивает завершение процедуры хронометража временных интервалов, ассоциированных с перемещением агентных сущностей между узлами процессуальной диаграммы в контексте агент-ориентированного моделирования. Его функциональность заключается в регистрации момента завершения пребывания агента в заданном сегменте системы
	SelectOutput	Реализует условную маршрутизацию агентных сущностей через один из двух выходных интерфейсов процессуальной диаграммы, основанную на оценке заданного логического условия детерминированного или вероятностного характера.
	SelectOutput5	Реализует условную маршрутизацию агентных сущностей через один из пяти выходных интерфейсов процессуальной диаграммы на основе анализа заданных критериев, которые могут носить детерминированный или вероятностный характер.

Первым делом при запуске модели формируется агент, представляющий из себя момент, в котором находится процесс аудита прямо сейчас. Агент попадает на первый этап (планирование), где обрабатывается определённое время, указанное в табл. 1. При входе на следующий этап (сбор данных), агент разделяется на три субагента, обрабатывающихся в соответствующих подэтапах (автоматизированный сбор логов, опрос сотрудников и анализ документов), а затем обратно соединяются в исходного агента. На этапе анализирования агент находится в блоке delay (Анализ), заданное табл. 1 время, а затем с вероятностью 0,66[4] обнаруживаются критические уязвимости и проводится срочное реагирование, которое перезапускает процесс анализа.

Следующим этапом является формирование отчёта, после которого исправляются все несоответствия в предприятии, а затем проводится проверка изменений в соответствии с вероятностью 0,986. Данная вероятность была выбрана в соответствии с исследованием[5], в котором отмечено, что человек совершает 500 ошибок в день, а также согласно другому исследованию[6] человек принимает около 35000 решений в день. На этом процесс проведения аудита ИБ завершается.

На основании имеющихся данных была составлена имитационная модель проведения аудита ИБ, представленная на рис. 3.

Проведя несколько экспериментов с составленной моделью, а именно обработки десяти заявок на проведение аудита, выведем итоговый график среднего затраченного времени на выполнение каждого этапа, приведённого на рис. 4.

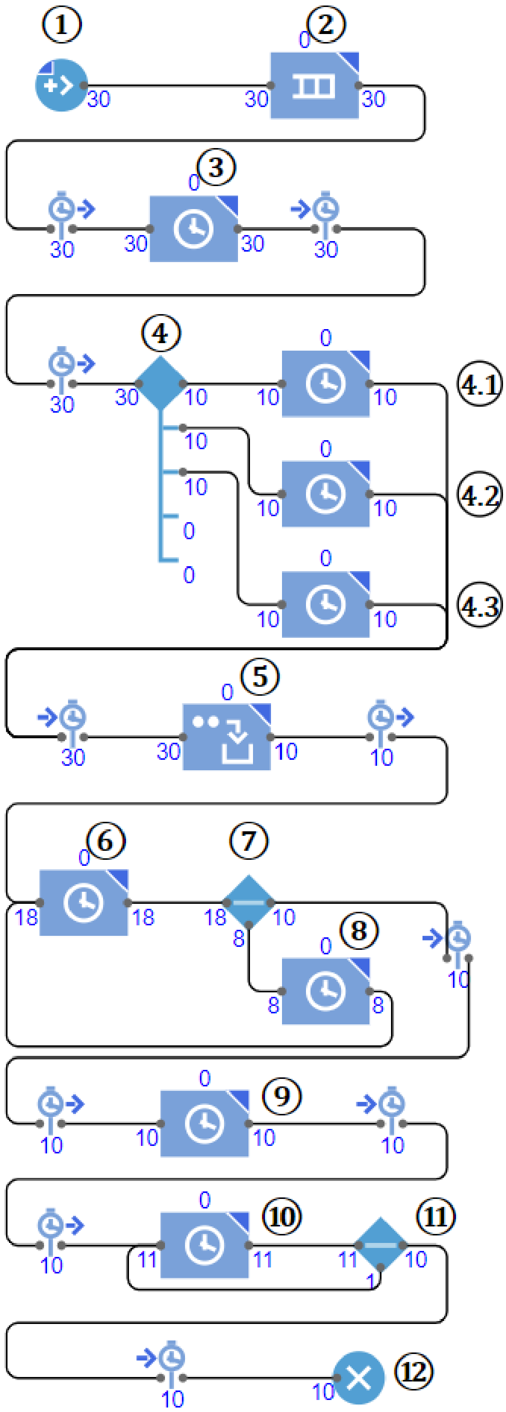


Рис. 3. Имитационная модель аудита ИБ

[4]Positive Technologies: треть выявленных в российских компаниях уязвимостей имели критическую и высокую степень риска. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-tret-vyyavlennyh-v-rossijskih-kompaniyah-uyazvimostej-imeli-kriticheskuyu-i-vysokuyu-stepen-riska/ (дата обращения: 24.03.2025).
[5]Louise Carroll: Mistakes just another form of learning. URL: https://clck.ru/3JSRp6 (дата обращения: 24.03.2025).
[6]Усталость от принятия решений становится объектом внимания. URL: https://goo.su/sMGT (дата обращения: 24.03.2025).

При всей простоте разработанной модели она является достаточно показательной и информативной как минимум для измерения времени, потраченного на проведение внутреннего аудита.

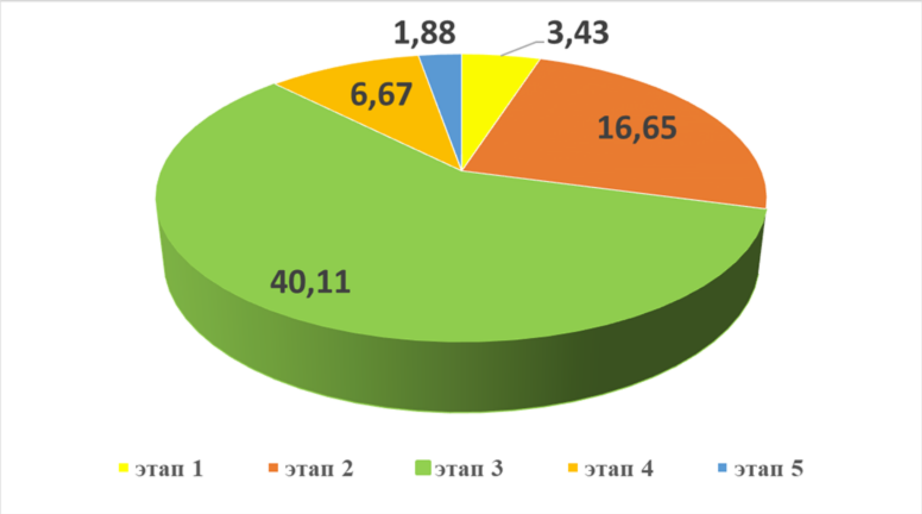


Рис. 4. Результат проведения аудита ИБ

Стоит отметить, что разработанная модель является примерной и для всех организаций она не будет являться релевантной. Поэтому компаниям следует видоизменять её в соответствии со своим положением о внутреннем аудите. В качестве видоизменений могут выступать не только временные рамки, но и коэффициент загруженности аудиторов, потраченных финансовых средств на проведение аудита и другое.

Заключение

Результаты комплексного анализа процесса аудита информационной безопасности с использованием методов имитационного моделирования в среде AnyLogic показали, что проведение аудита обусловлено увеличивающейся сложностью угроз в области информационной безопасности и необходимостью оптимизации ресурсов, затрачиваемых на обеспечение безопасности информационных систем. В ходе работы была разработана и исследована динамическая модель, которая позволила оценивать временные и логические параметры аудита ИБ, а также выявить критические точки процесса. Агентно-ориентированный подход реализован в AnyLogic. Данный инструмент выбран благодаря возможности интеграции дискретных событийных и системно-динамических методов, что обеспечивает многомерный анализ взаимодействия этапов аудита.

Разработанная модель включает пять ключевых стадий. На основе входных данных, предоставленных компанией RTM Group, была собрана статистика временных интервалов выполнения этапов, а также найдены частоты возникновения инцидентов. Результаты моделирования выявили нелинейную зависимость между длительностью этапов и количеством обнаруживаемых уязвимостей. Визуализация процесса в AnyLogic позволила выявить узкие места. Разработанная модель обладает свойством адаптивности – параметры могут быть скорректированы с учётом организационной специфики.

Для валидации проведено сравнение с реальными данными RTM Group, показавшее погрешность прогноза длительности аудита в пределах пяти процентов. Выводы подтверждают эффективность применения имитационного моделирования для повышения прозрачности аудита ИБ. В отличие от традиционных методов, подход на базе AnyLogic обеспечивает количественную оценку сценариев.

Исследование вносит вклад в развитие методологии управления информационной безопасностью, предлагая инструмент для уравновешивания между операционной эффективностью и требованиями информационной безопасности. Полученные результаты могут быть применены как в коммерческих организациях, так и в государственных структурах. Данный подход на базе AnyLogic, который обеспечивает количественную оценку сценариев проведения аудита, используется в учебном процессе Финансового университета при Правительстве РФ при изучении дисциплины аудит информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. Путято М.М., Макарян А.С., Черкасов А.Н., Кучер В.А. Разработка имитационной модели в области защиты информации с использованием программного обеспечения AnyLogic. Вестник Адыгейского государственного университета: Естественно-математические и технические науки. 2024, вып. 1(336), с. 60–69. DOI: 10.53598/2410-3225-2024-1-336-60-69.
2. Филяк П.Ю., Золотарев В.В. AnyLogic как инструмент агентного моделирования информационной безопасности //Вестник Московского финансово-юридического университета. 2015, № 4, с. 30–34. URL: https://cyberleninka.ru/article/n/anylogic-kak-instrument-agentnogo-modelirovaniya-informatsionnoy-bezopasnosti (дата обращения: 19.03.2025).
3. Филяк П.Ю., Потехин Н.А. Моделирование в целях обеспечений безопасности. В сборнике: Десятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2021). Труды конференции (электронное издание). Редакторы Плотников А.М., Долматов М.А., Смирнова Е.П., Санкт-Петербург. 2021, с. 432–443. – EDN: GGPIWR.
4. Белова Е.А., Крылов В.О., Мартиросова О.А. Имитационное моделирование угроз информационной безопасности. Актуальные научные исследования в современном мире. 2020, № 11-2, с. 32–36. – EDN: PRXRCH.
5. Крючков А.В., Прус Ю.В., Бутузов С.Ю. Технологические основы информационной безопасности. Технологии техносферной безопасности. 2017, с. 205–208. – EDN: YWYDOS.
6. Мальцев В.Н., Прус Ю.В., Резниченко С.А., Аспекты информационной безопасности на начальном этапе создания инновационных продуктов. Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2021, с. 173–183. – EDN: TIWWEK.
7. Беляева О.В., Грицык В.А. Имитационное моделирование систем защиты информации. Международный журнал экспериментального образования. 2010, № 5, с. 67. – EDN: RAJQGL.
8. Хроль Е.В., Уварова А.Г., Кужильный А.В. Разработка имитационных моделей с по мощью AnyLogic. Современные инновации, системы и технологии. 2023, т. 3, № 4, с. 119–130. DOI: 10.47813/2782-2818-2023-3-4-0119-01310. – EDN: UYVFEM.
9. Сиротский, Алексей А.; Резниченко, Сергей А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 103–117, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.09.
10. Груздева Л.М. Применение системы имитационного моделирования AnyLogic при обучении студентов направления «Информационная безопасность». Современные научные исследования и инновации. 2014, № 10, ч. 1. URL: https://web.snauka.ru/issues/2014/10/39768 (дата обращения: 19.03.2025).
11. Ashiku L., Dagli C. Agent based cybersecurity model for business entity risk assessment. IEEE International Symposium on Systems Engineering (ISSE). 2020, p. 1–6. DOI: 10.1109/ISSE49799.2020.9272234.
12. Lerums J.E., La'Reshia D.P., Dietz J.E. Simulation modeling cyber threats, risks, and prevention costs. IEEE International Conference on Electro/Information Technology (EIT). 2018, p. 0096–0101. DOI: 10.1109/EIT.2018.8500240.
13. Микула А.А., Подлегаев А.И., Селифанов В.В. Вопросы моделирования системы управления аудитом. Сборники материалов Международной научной конференции «Интерэкспо ГЕО-Сибирь 2024». 2024, 7(3), с. 146–152. DOI: 10.33764/2618-981X-2024-6-210-217.
14. Резниченко С.А., Дмитриева Т.В., Подкосов С.В., Евдокимов О.Г., Семухин С.Д. Проблемы управления информационной безопасностью в кредитно-банковской системе передачи данных. Московский экономический журнал. 2022, № 2. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/.

15. Хуранова К.М. Преимущества и недостатки искусственного интеллекта в обеспечении информационной безопасности. Hi-Hume Journal. 2023, № 3(3), с. 72–79. – EDN: QZXBBZ.

REFERENCES:
[1] Putyato M.M., Makaryan A.S., Cherkasov A.N., Kucher V.A. Development of a simulation model in the field of information protection using AnyLogic software. 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 (in Russian).
[2] Filyak P.Yu., Zolotarev V.V. AnyLogic as an agent-based information security modeling tool. Bulletin of the Moscow University of Finance and Law. 2015, no. 4, p. 30–34. URL: https://cyberleninka.ru/article/n/anylogic-kak-instrument-agentnogo-modelirovaniya-informatsionnoy-bezopasnosti (accessed: 19.03.2025) (in Russian).
[3] Filyak P.Yu., Potekhin N.A. Modeling for security provisions. In the collection: The Tenth All-Russian Scientific and Practical Conference on Simulation Modeling and its Application in Science and Industry "Simulation Modeling. Theory and Practice" (IMMOD-2021). Conference Proceedings (electronic publication). Editors Plotnikov A.M., Dolmatov M.A., Smirnova E.P., St. Petersburg. 2021, p. 432–443. – EDN: GGPIWR (in Russian).
[4] Belova E.A., Krylov V.O., Martirosova O.A. Simulation modeling of information security threats. Current scientific research in the modern world. 2020, no. 11-2, p. 32–36. – EDN: PRXRCH (in Russian).
[5] Kryuchkov A.V., Prus Yu.V., Butuzov S.Y. Technological foundations of information security. Technosphere security technologies. 2017, c. 205–208. – EDN: YWYDOS (in Russian).
[6] Maltsev N.V., Prus, Yu.V., Reznichenko S.A. The aspects of information security the initial stage of creation of innovative products. Collection of articles of International scientific-practical conference of the Russian state University for the Humanities. 2021, p. 173–183. – EDN: TIWWEK (in Russian).
[7] Belyaeva O.V., Gritsyk V.A. Simulation modeling of information security systems. International Journal of Experimental Education. 2010, no. 5, p. 67. – EDN: RAJQGL (in Russian).
[8] Krol E.V., Uvarova A.G., Kuzhilny A.V. Development of simulation models using the AnyLogic package. Modern innovations, technologies and systems. 2023, v. 3, no. 4, p. 119–130. DOI: 10.47813/2782-2818-2023-3-4-0119-01310. – EDN: UYVFEM (in Russian).
[9] Sirotskiy, Alexei A.; Reznichenko, Sergei A. A formalized model of an organization information security audit for compliance with the requirements of standards. IT Security (Russia), [S.l.], v. 28, no. 3, p. 103–117, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.09 (in Russian).
[10] Gruzdeva L.M. Application of the AnyLogic simulation modeling system in teaching students in the field of "Information security". Modern scientific research and innovations. 2014, no. 10, part 1. URL: https://web.snauka.ru/issues/2014/10/39768 (accessed: 19.03.2025) (in Russian).
[11] Ashiku L., Dagli C. Agent based cybersecurity model for business entity risk assessment. IEEE International Symposium on Systems Engineering (ISSE). 2020, p. 1–6. DOI: 10.1109/ISSE49799.2020.9272234.
[12] Lerums J.E., La'Reshia D.P., Dietz J.E. Simulation modeling cyber threats, risks, and prevention costs. IEEE International Conference on Electro/Information Technology (EIT). 2018, p. 0096–0101. DOI: 10.1109/EIT.2018.8500240.
[13] Mikula A.A., Podlegaev A.I., Selifanov V.V. Issues of modeling the audit management system. Proceedings of the International Scientific Conference "Interexpo GEO-Siberia 2024".2024, 7(3), p. 146–152. DOI: 10.33764/2618-981X-2024-6-210-217 (in Russian).
[14] Reznicenko S.A., Dmitrieva T.V., Podkosov S.V., Evdokimov O.G., Semukhin S.D. Problems of information security management in the credit and banking data transmission system. Moscow Economic Journal. 2022, no. 2. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/ (in Russian).
[15] Khuranova K.M. Advantages and disadvantages of artificial intelligence in ensuring information security. Hi-Hume Journal. 2023, no. 3(3), p. 72–79. – EDN: QZXBBZ (in Russian).

Статья поступила в редакцию 03.03.2025; одобрена после рецензирования 29.04.2025; принята к публикации 14.05.2025
The article was submitted 03.03.2025; approved after reviewing 29.04.2025; accepted for publication 14.05.2025