УДК 004.056.5

А. А. Микула[1], А. И. Подлегаев[1], В. В. Селифанов[1]*

Вопросы моделирования процедур аудита информационной безопасности

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

Аннотация. В статье рассмотрены проведение процедур аудита и процесс оценки процедур аудита информационной безопасности с применением имитационного моделирования. Составлена имитационная модель аудита информационной безопасности, способная наглядно продемонстрировать и данный процесс, и выполнить оценку его эффективности. В рамках оценивания эффективности выполнен обзор блоков, включенных в состав данной модели. В итоге получена функциональная модель, позволяющая произвести оценку эффективности проведения процедур аудита информационной безопасности.

Ключевые слова: аудит информационной безопасности, оценка защищенности, имитационное моделирование

A. A. Mikula[1], A. I. Podlegaev[1], V. V. Selifanov[1]*

Issues of modeling information security audit procedures

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

Abstract. The article discusses the implementation of audit procedures and the process of assessing information security audit procedures using simulation modeling. An information security audit simulation model was compiled that could clearly demonstrate this process and evaluate its effectiveness. As part of the efficiency assessment, a review of the blocks included in this model was performed. As a result, a functional model was obtained that allows evaluating the effectiveness of information security audit procedures.

Keywords: information security audit, security assessment, simulation modeling

Введение

С развитием информационных технологий стало очевидно, что одной из важнейших проблем является обеспечение информационной безопасности. И для грамотного построения системы информационной безопасности существенное значение имеет качественная и своевременная оценка ее защищенности.

Оценка защищенности, а именно аудит информационной безопасности – неотъемлемая часть работы любой организации, заинтересованной в обеспечении защиты информации от несанкционированного доступа, утечек конфиденциальных данных или других угроз. В настоящее время информационная безопасность является одним из ключевых аспектов организации качественной защиты деятельности компаний, в особенности в условиях столь быстрого развития цифровых технологий и увеличения количества киберугроз. Аудит позволяет

выявить уязвимости в системе защиты данных, оценить уровень рисков и разработать эффективные меры по их минимизации [1, 2].

Однако на данный момент не существует достаточно объективной оценки уровня доверия к процедурам аудита информационной безопасности, позволившей бы иметь представление, насколько реальна оценка защищенности и ее результаты. Для этого в статье будет рассмотрен вопрос моделирования процедур аудита информационной безопасности, представлена имитационная модель этих процедур и рассмотрено проведение оценки эффективности на ее основе [1, 3].

Методы и материалы

Важность аудита информационной безопасности заключается в следующем.

1. Идентификация уязвимостей: проведение аудита помогает выявить слабые места в системах безопасности и идентифицировать потенциальные угрозы для информации.

2. Соблюдение требований законодательства: многие отраслевые стандарты и законы обязывают компании проводить аудиты информационной безопасности, чтобы защитить персональные данные клиентов и соблюдать конфиденциальность.

3. Повышение доверия клиентов: клиенты все более обращают внимание на защиту своей личной информации. Проведение аудита информационной безопасности позволяет демонстрировать клиентам, что их данные защищены.

4. Улучшение внутреннего управления рисками: результаты аудита помогают управляющим и руководству организации лучше понять уровень информационных рисков и принять меры по их снижению.

5. Повышение эффективности и эффективности работы IT-инфраструктуры: аудит информационной безопасности позволяет выявить узкие места в работе информационных систем и процессов, что в свою очередь способствует повышению эффективности и надежности IT-инфраструктуры [4, 5].

Процедуры аудита информационной безопасности включают три основных блока (рис.1):

1. Планирование аудита;

2. Проведение аудита;

3. Завершение аудита [5, 6].

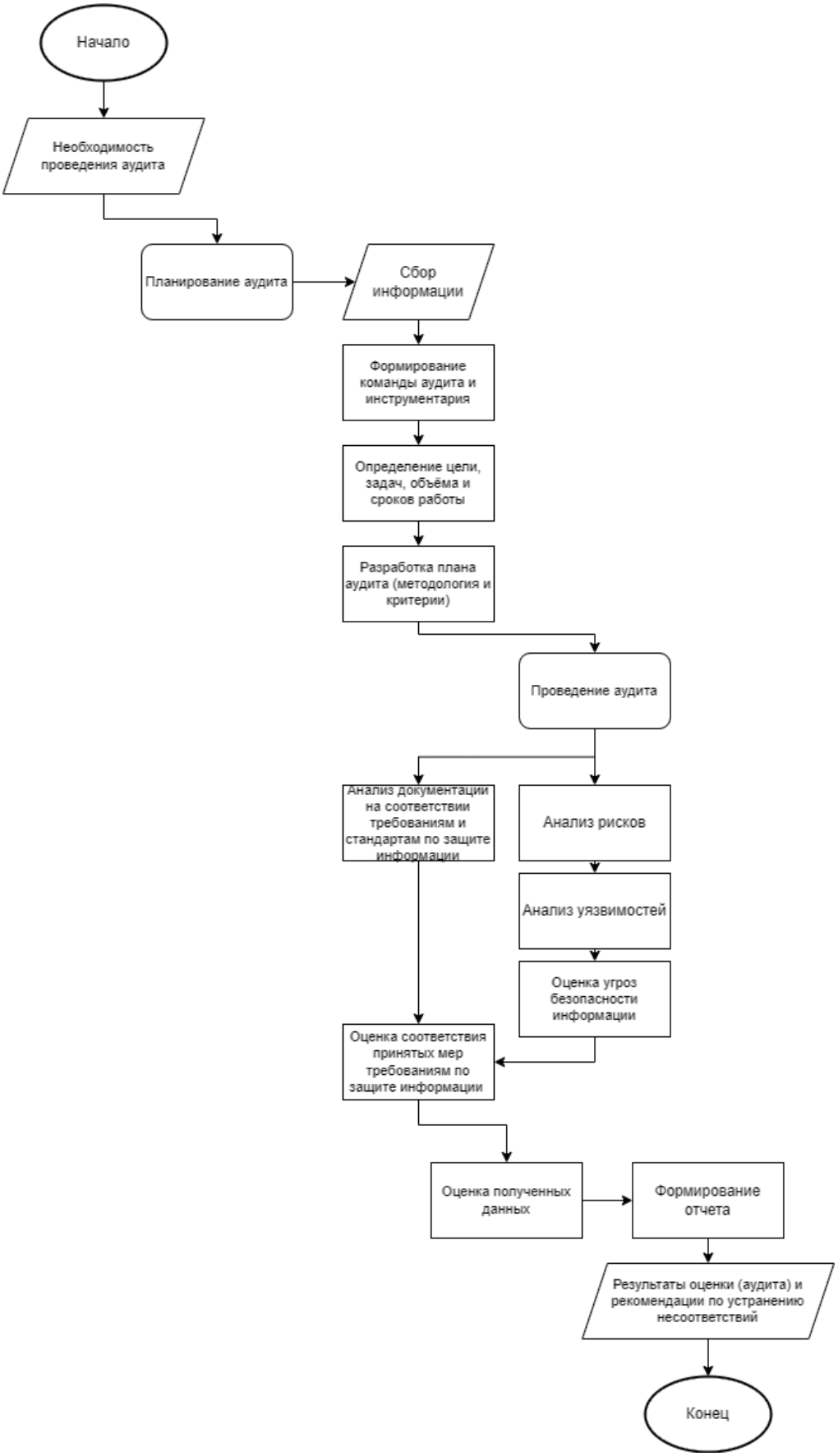

Рис. 1. Блок-схема процесса аудита информационной безопасности

Аудит информационной безопасности позволяет определить, насколько эффективно защищены данные от несанкционированного доступа, взломов и кражи. Для заказчика, заинтересованного в оценке защищенности своей информационной системы, критически важно быть уверенным в компетентности выбранного исполнителя, поскольку результаты аудита могут иметь серьезное влияние на безопасность информационных ресурсов компании. И сейчас действует множество организаций, способных выполнить данную задачу. Однако возникает вопрос – как оценить, насколько можно доверять выполненным процедурам аудита? Этот вопрос рассмотрим, проведя имитационное моделирование процедур аудита [6, 7].

При имитационном моделировании разрабатывается логико-математическая модель функционирования сложной системы, позволяющая на основе исходных данных спрогнозировать и оценить состояние этой системы при каких-либо возможных воздействиях на нее. При этом модель процесса дает возможность провести однозначную оценку построенной системы и повысить ее эффективность. Так имитационное моделирование позволит заменить практические исследования [8].

Подходящим методом оценки эффективности системы в этом случае будет динамическая оценка, предполагающая использование имитационного моделирования.

Благодаря имитационному моделированию можно наглядно и доходчиво представить систему в виде процесса, а именно совокупность следующих друг за другом событий, и отобразить структуру проведения процедур аудита информационной безопасности. После чего уже станет возможным осуществление оценки доверия к процедурам аудита на примере конкретной модели [9, 10].

Процедуры аудита в данном случае будут рассматриваться как система массового обслуживания замкнутого типа, в которой источники заявок включены в систему и имеют фиксированное количество внутри системы, а в качестве заявок выступают непосредственно сами процедуры аудита.

Для того, чтобы обеспечить быстрый и показательный анализ, на основе составленной схемы проведения аудита информационной безопасности была создана модель в AnyLogic, российском программном обеспечении для имитационного моделирования, которое позволяет рассматривать различные бизнес-процессы и оценивать возможности по их оптимизации [11].

Результаты

Критерии оценки уровня доверия к аудиту информационной безопасности будут содержать в себе несколько ключевых аспектов – полнота, качество, своевременность и доверие к поставщику услуг (исполнителю).

Проведение процедуры аудита может быть неполной, что может привести к ошибочным выводам и недостаточной защищенности системы.

Своевременность проведения процедуры аудита является одним из ключевых аспектов, который необходимо учитывать при ее планировании и реализации. Ведь, если проведение процедуры затянется, то время, в течение которого

система может быть уязвимой, увеличится. С другой стороны, слишком частая проведение оценки защищенности может привести к перегрузке персонала и затратам на процедуру [5, 6].

Оценка качества проведения процедуры аудита помогает убедиться, что все этапы процесса проводятся правильно, полностью и своевременно. Оценка качества проведения процедуры аудита может быть выполнена различными способами, включая оценку точности, полноты и своевременности. Оценка точности может помочь выявить ошибки, допущенные в процессе оценки, и предложить рекомендации по их исправлению. Оценка полноты может выявить пропущенные уязвимости или проблемы в системе безопасности, которые не были учтены в процессе оценки. Оценка своевременности может показать, была ли процедура проведена в соответствии с заданным графиком и вовремя [9, 10].

При выборе поставщика услуг проведения процедуры аудита, если такой поставщик есть, необходимо убедиться, что он обладает достаточным уровнем компетенции и опыта, чтобы грамотно оценить уровень защищенности системы. Также важным аспектом является репутация поставщика услуг. Необходимо изучить их историю и опыт работы в данной сфере. Провести исследование и узнать, какие компании уже пользовались услугами данного поставщика и как они оценивают качество их работы. Наконец, необходимо убедиться, что поставщик услуг имеет необходимые лицензии и сертификаты на выполнение соответствующих работ. Что рассмотрено на модели (рис. 2).

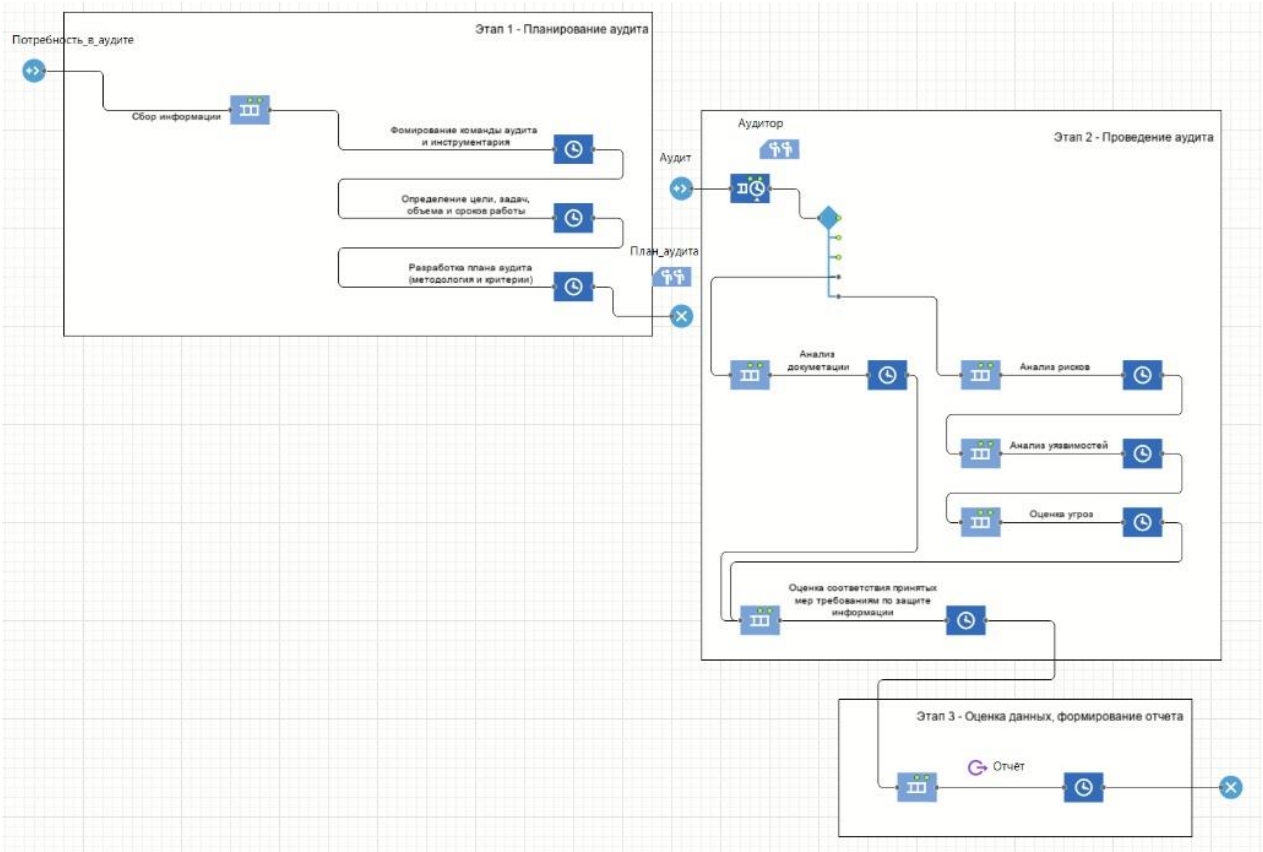

Рис. 2. Имитационная модель процесса аудита информационной безопасности

Обсуждение

Имитационная модель процесса аудита информационной безопасности позволяет оценить уровень доверия к данному процессу, используя перечисленные критерии оценки. При изменении параметров задержки и максимальной вместимости агентов на каждом блоке модели можно оценить своевременность проведения аудита. Полноту проведения аудита можно отследить по движению агента по процессу и сформированному плану аудита. Оценить качество аудита можно изменив поведение агента на этапе проведения. Оценка доверия к поставщику услуг будет влиять от частоты прихода заявок (потребность в аудите), компетенций формирующейся команды на этапе планирования аудита [8].

Имитационная модель процесса аудита информационной безопасности позволяет оценить уровень доверия к данному процессу, используя перечисленные критерии оценки. При изменении параметров задержки и максимальной вместимости агентов на каждом блоке модели можно оценить своевременность проведения аудита. Полноту проведения аудита можно отследить по движению агента по процессу и сформированному плану аудита. Оценить качество аудита можно изменив поведение агента на этапе проведения. Оценка доверия к поставщику услуг будет влиять от колличества заявок (потребность в аудите), компетенций формирующейся команды на этапе планирования аудита [10–12].

Заключение

Аудит информационной безопасности важным процессом для любой организации, особенно в наше время, когда цифровая безопасность становится все более приоритетной. Аудит позволяет оценить уровень защиты информации и выявить уязвимости в информационных системах и процессах.

Проводя систематический аудит информационной безопасности, организация сможет оперативно реагировать на обнаруженные уязвимости и предотвращать инциденты, которые могли бы привести к крупным потерям и утрате доверия со стороны клиентов.

Имитационное моделирование процесса аудита информационной безопасности – эффективный метод, позволяющий в реальном времени оценить работоспособность системы защиты информации, выявить ее уязвимости и оценить уровень доверия к процедурам аудита информационной безопасности.

Оценка качества проведения процедуры аудита помогает убедиться, что все этапы процесса проводятся правильно, полностью и своевременно. Правильно оцененное доверие к субъектам информационного обмена данного процесса позволяет защитить ценные данные и ресурсы компании. Благодаря этому происходит повышение уровня защиты информации и минимизируются рисков, что помогает соблюдать нормативы и стандарты безопасности [9, 12].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Многоуровневая концепция безопасности систем управления большими данными // Зегжда Д.П., Калинин М.О. // Вопросы кибербезопасности. Статья в журнале – научная статья. – 2023 г. – № 5 (57) – С. 25-36.

2. Влияние проведения аудита на информационную безопасность предприятий // Клочкова Т.В. // Внедрение современных конструкций и передовых технологий в путевое хозяйство. Статья в журнале – научная статья. – 2019 г. – № 14. – С. 64-66.

3. Объекты аудита информационной безопасности и направления их проверки // Каширская Л.В. // Аудитор. Статья в журнале – научная статья. – 2022 г. – № 1. – С. 21-31.

4. Роль аудита информационных технологий в Информационной безопасности // Клочкова Т.В. // Вопросы науки и образования. Статья в журнале – научная статья. – 2019 г. – № 56. – С. 4-12.

5. Автоматизация аудита информационной безопасности выделенного помещения с заданными параметрами с использованием имитационного моделирования // Иванова М.Е., Напалкова Н.В., Щербаков В.А. Статья в сборнике трудов конференции // РЭУС-2019. – 2019 г. – С. 303-308.

6. Роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной безопасности объектов критической информационной инфраструктуры // Гильманова Э.А. // Форум молодых ученых. Статья в журнале – научная статья. – 2022 г. – № 66. – С. 34-37.

7. Формализованная риск-ориентированная модель системы информационных технологий // Аносов Р.С. // Вопросы кибербезопасности. Статья в журнале – научная статья. – 2020 г. – № 5 (39) – С. 69-76.

8. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Сиротский А.А. // Безопасность информационных технологий. Статья в журнале – научная статья. – 2021 г. – № 3 – С. 103-117.

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. 1Моделирование 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.

11. Построение модели угроз информационной безопасности информационной системы с использованием методологии объектно-ориентированного проектирования // Грибанова-Подкина М. Ю. // Вопросы безопасности. – 2017 г. № 2. С. 25-34.

12. Оценка доверия к безопасности информационных технологий // Грищенко Л.А. // Вопросы науки и образования. Статья в журнале – научная статья. – 2018 г. – № 19. – С. 62-66.