УДК 004.056.5
DOI 10.33764/2618-981X-2024-6-210-217

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

Вопросы моделирования системы управления аудитом

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

Аннотация. В условиях стремительно развивающихся информационных технологий и технологий информатизации стал очевидным факт, что одной из важнейших проблем, требующей особого подхода к решению, является обеспечение информационной безопасности. Для построения системы информационной безопасности существенное значение имеет качественная оценка ее защищенности. В статье рассмотрен процесс оценки процедур аудита информационной безопасности с помощью имитационного моделирования. Составлена модель аудита информационной безопасности, позволяющая рассмотреть данный процесс и выполнить оценку его эффективности. Выполнен обзор блоков, включённых в состав данной модели. Для построения модели используется прикладное программное обеспечение AnyLogic. Получена функциональная модель, позволяющая произвести оценку результативности проведения аудита.

Ключевые слова: аудит, оценка защищенности, имитационное моделирование

A. I. Podlegaev[1], A. A. Mikula[1], V. V. Selifanov[2]*

Issues of modeling the audit management system

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

Abstract. In the context of rapidly developing information technologies and informatization technologies, it has become obvious that one of the most important problems requiring a special approach to solving is ensuring information security. For building an information security system, a qualitative assessment of its security is essential. The article discusses the process of evaluating information security audit procedures using simulation modeling. An information security audit model has been compiled that allows us to review this process and evaluate its effectiveness. An overview of the blocks included in this model has been performed. AnyLogic application software is used to build the model. A functional model has been obtained that allows evaluating the effectiveness of the audit.

Keywords: audit, security assessment, simulation modeling

Введение

Аудит информационной безопасности – важная составляющая работы любой организации, стремящейся обеспечить защиту своей информации от несанкционированного доступа, утечек данных или других угроз. В настоящее время информационная безопасность становится ключевым аспектом деятельности компаний в условиях быстрого развития цифровых технологий и увеличения числа киберугроз. Аудит позволяет выявить уязвимости в системе защиты данных, оценить уровень рисков и разработать эффективные меры по их минимизации [1-3].

Важность аудита информационной безопасности заключается в следующем:

– идентификация уязвимостей: проведение аудита помогает выявить слабые места в системах безопасности и идентифицировать потенциальные угрозы для информации;

– соблюдение требований законодательства: многие отраслевые стандарты и законы обязывают компании проводить аудиты информационной безопасности, чтобы защитить персональные данные клиентов и соблюдать конфиденциальность;

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

– улучшение внутреннего управления рисками: результаты аудита помогают руководству организации лучше понять уровень информационных рисков и принять меры по их снижению;

– 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.

Однако на данный момент не существует достаточно объективной оценки уровня доверия к процедурам аудита информационной безопасности, позволяющий иметь представление, насколько реальна оценка защищенности и ее результаты. Именно поэтому в данной статье рассмотрен процесс оценки процедур аудита информационной безопасности и представлена имитационная модель этих процедур [4-10].

Процедуры аудита информационной безопасности

Аудит информационной безопасности — это процесс оценки и проверки системы защиты информации в организации с целью выявления уязвимостей, недостатков и рисков, которые могут привести к утечке или несанкционированному доступу к конфиденциальным данным. Процедуры аудита информационной безопасности включают в три основных блока (рис.1):

– планирование аудита;

– проведение аудита;

– завершение аудита.

В первом блоке определяются цели и задачи аудита, формируется аудиторский состав, проводится предобследование системы, выбираются методы и инструменты аудита, составляется программа проведения аудита.

Второй блок – проведение аудита – здесь аудиторы собирают данные о текущем состоянии системы защиты информации, проводят анализ организационно-распорядительной, проектной и эксплуатационной документации, интервьюируют сотрудников, осматривают технические средства. На основе собранной информации проводится анализ уязвимостей и рисков, определяются потенци-

альные угрозы и возможные последствия нарушения безопасности. Далее проходит оценка эффективности реализованных мер системы защиты информации с использованием специализированных инструментов.

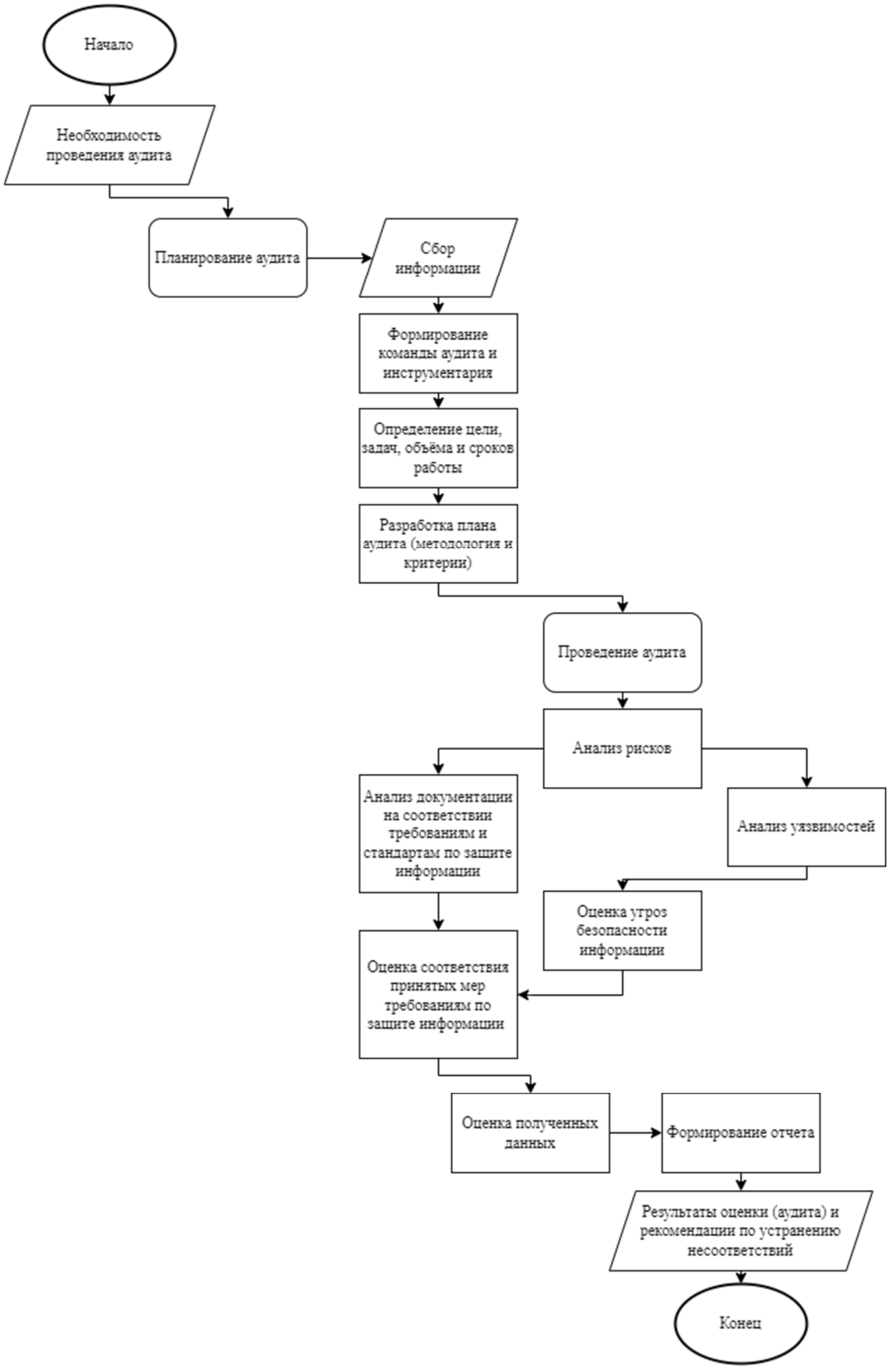

Рис. 1. Блок-схема процесса аудита информационной безопасности

В третьем блоке проводится анализ полученных результатов, выявляются проблемные места и разрабатываются рекомендации по улучшению системы безопасности. На основе проведенного аудита составляется отчет, в котором содержатся описание проведенных процедур, выявленные уязвимости, предложения по улучшению безопасности и рекомендации по дальнейшим действиям.

Аудит информационной безопасности является критически важной задачей для любой организации, которая хранит и обрабатывает конфиденциальную информацию. Он позволяет определить, насколько эффективно защищены данные от несанкционированного доступа, взломов и кражи [11]. Для заказчика очень важно убедиться в компетентности и надежности выбранного исполнителя, поскольку результаты аудита могут иметь серьезное влияние на безопасность информационных ресурсов компании. Существует множество фирм и специалистов, способных выполнить данную задачу, но как оценить и довериться выполненным процедурам аудита?

Обоснование применения имитационного моделирования

При имитационном моделировании разрабатывается логико-математическая модель функционирования сложной системы, позволяющая на основе исходных данных спрогнозировать и оценить состояние этой системы при каких-любо возможных воздействиях на нее. При этом модель процесса позволяет провести однозначную оценку построенной системы и повысить ее эффективность. Так имитационное моделирование в определенных случаях может заменить практические исследования [12-13].

Применение имитационного моделирования позволяет наглядно и доступно представить систему в виде процесса, представляемого как совокупность следующих друг за другом событий, спроецировать процесс проведения аудита информационной безопасности. После чего возможно проведение оценки уровня доверия к процедурам аудита на примере конкретной модели.

Процедуры аудита рассматриваются 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 [14-16].

Для того, чтобы обеспечить быстрый и показательный анализ на основе составленной схемы проведения аудита информационной безопасности была создана модель на российской платформе AnyLogic для выполнения имитационного моделирования [17-18].

Анализ процедур аудита информационной безопасности с использованием имитационного моделирования

Критерии оценки уровня доверия к аудиту информационной безопасности будут содержать в себе несколько ключевых аспектов – полнота, качество, своевременность и доверие к поставщику услуг (исполнителю) [19-20].

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

Своевременность проведения процедуры аудита является одним из ключевых аспектов, который необходимо учитывать при её планировании и реализа-

ции. Если проведение процедуры затянется, то время, в течение которого система может быть уязвимой, увеличится. С другой стороны, слишком частое проведение оценки защищённости может привести к перегрузке персонала и затратам на процедуру.

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.

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

Имитационная модель процесса аудита информационной безопасности позволяет оценить уровень доверия к данному процессу, используя перечисленные критерии оценки (рис. 2).

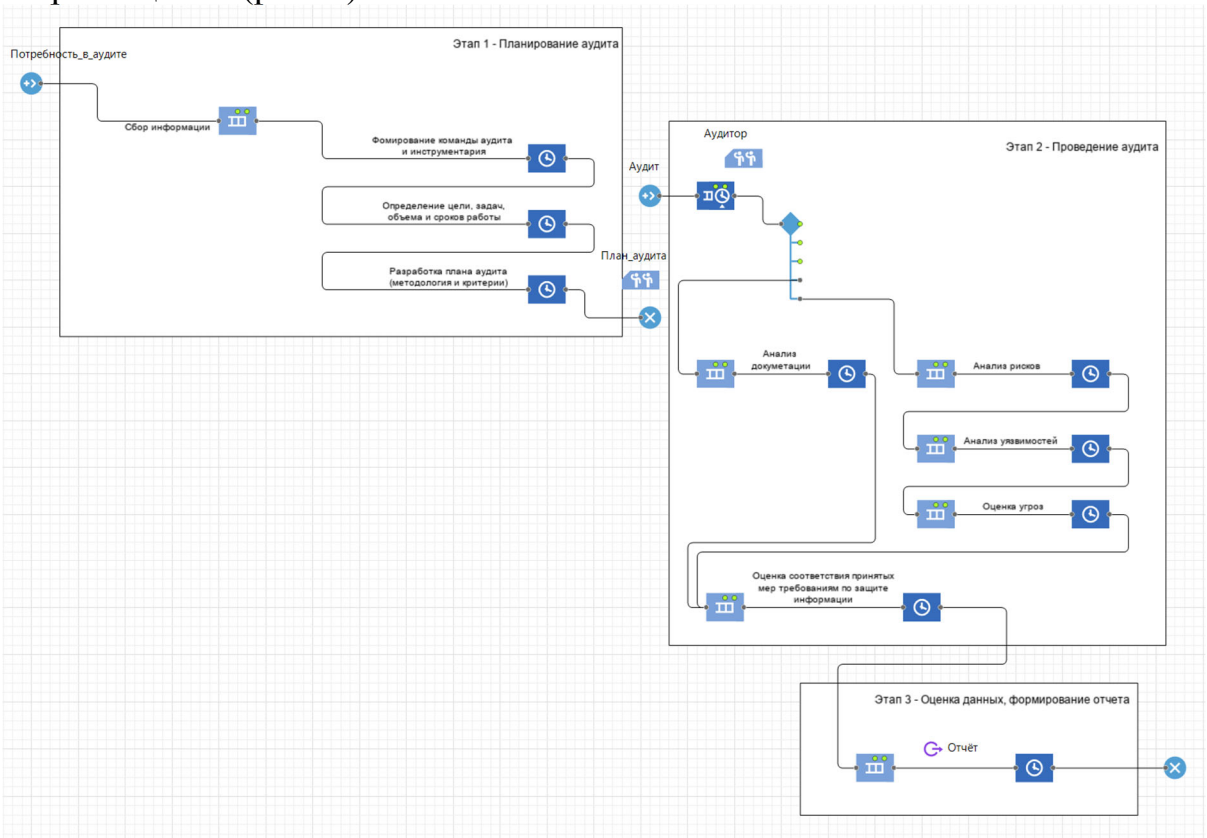

Рис. 2. Имитационная модель процесса аудита информационной безопасности

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 команды на этапе планирования аудита.

Прохождение агентов через блоки системы с расставленными вероятностями и временем задержки изображено на рис. 3.

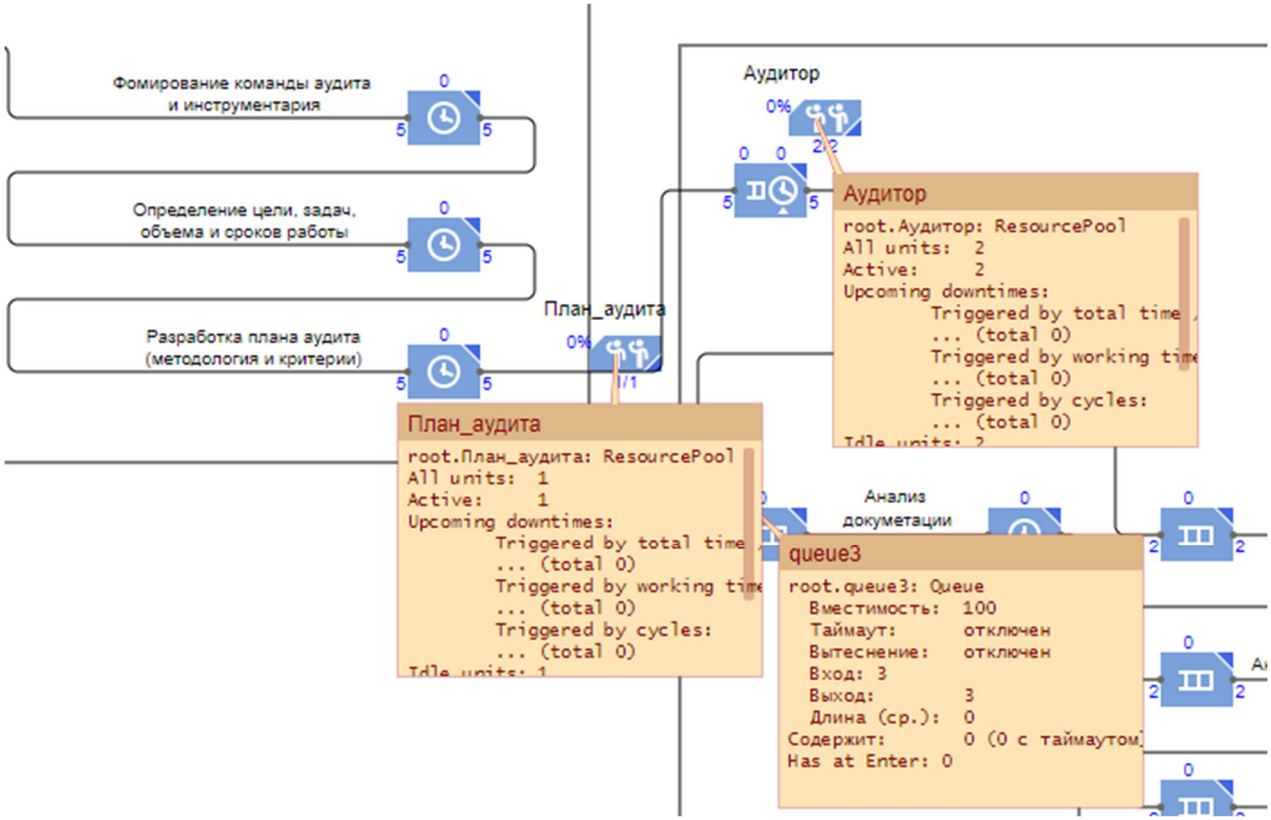

Рис. 3. Демонстрация работы модели

Заключение

Аудит информационной безопасности является 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.

Благодаря проведению систематического аудита информационной безопасности, компания может оперативно реагировать на обнаруженные уязвимости и предотвращать возможные инциденты, которые могут привести к серьезным убыткам и утрате доверия со стороны клиентов.

Имитационное моделирование процесса аудита информационной безопасности — это эффективный метод, который позволяет оценить работоспособность

системы защиты информации, выявить ее уязвимости, а также оценить уровень доверия к процедурам аудита информационной безопасности.

Оценка доверия к процедурам аудита информационной безопасности является критически важным аспектом для любой организации. Правильно оцененное доверие к субъектам информационного обмена данного процесса позволяет защитить ценные данные и ресурсы компании. Это способствует повышению уровня защиты информации, минимизации рисков и обеспечению соблюдения нормативов и стандартов безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аверьянов В. С. О некоторых вопросах, идеях и технологических решениях в области квантового распределения ключей безопасности / В. С. Аверьянов // Информационная безопасность : Сборник докладов Всероссийской Школы молодых ученых, Новосибирск, 14–18 ноября 2022 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. – С. 34-39.
2. Ашуров Х. М. Оценка защищенности информационной системы при помощи рисков / Х. М. Ашуров, А. Зокиров // Вестник Таджикского технического университета. – 2012. – № 3(19). – С. 40-44.
3. Баранкова И. И. Сложности, возникающие при проведении аудита информационной безопасности на предприятии / И. И. Баранкова, У. В. Михайлова, Т. В. Быкова // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 1(31). – С. 53-56.
4. Егоров М. А. Методика аудита информационной безопасности в современных условиях / М. А. Егоров // Вестник науки и образования. – 2019. – № 11-2(65). – С. 34-37.
5. Ефремов А. В. Анализ существующих методик оценки средств аудита информационной безопасности / А. В. Ефремов, Г. Е. Панамарев // Вестник Военного инновационного технополиса «Эра». – 2021. – Т. 2, № 4. – С. 38-45.
6. Зелинская Е. Л. Аудит безопасности информационных систем: виды и этапы работ / Е. Л. Зелинская, А. Г. Зелинский // Морская стратегия и политика России в контексте обеспечения национальной безопасности и устойчивого развития в XXI веке : Сборник научных трудов. ч. 2 . – Севастополь : Черноморское высшее военно-морское ордена Красной Звезды училище им. П.С. Нахимова, 2019. – С. 165-169.
7. Иванова М. Е. Автоматизация аудита информационной безопасности выделенного помещения с заданными параметрами с использованием имитационного моделирования / М. Е. Иванова, Н. В. Напалкова, В. А. Щербаков // Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-2019 : Доклады Всероссийской конференции (с международным участием), М. : Московское НТО радиотехники, электроники и связи им. А.С. Попова, 2019. 29–31 мая 2019 года.– С. 303-308.
8. Комарова А. В. Основные угрозы безопасности и устранение их методом аудита информационной безопасности / А. В. Комарова, К. В. Толокольникова // Взаимодействие науки и общества: проблемы и перспективы : сборник статей Международной научно-практической конференции: в 4 частях, Казань, 08 июня 2017 года. Т.4. – Казань: Общество с ограниченной ответственностью «ОМЕГА САЙНС», 2017. – С. 63-66.
9. Метод оценивания рисков в системах принятия решений с учетом защиты информации / В. В. Селифанов, А. Ю. Солдатов, Е. Ю. Солдатов [и др.] // Вестник СибГУТИ. – 2023. – Т. 17, № 2. – С. 84-92.
10. Палканов И. С. Внутренний аудит информационной безопасности как инструмент получения объективных оценок состояния информационной безопасности организации / И. С. Палканов, В. Е. Рачков // Студенческая наука для развития информационного общества : Сборник материалов X Всероссийской научно-технической конференции с международным уча-

стием, Ставрополь, 07–08 ноября 2019 года. Ч. 1. – Ставрополь: Северо-Кавказский федеральный университет, 2019. – С. 153-161.

11. Гильманова Э. А. Роль аудита информационной безопасности в жизненном цикле системы обеспечения информационной безопасности объектов критической информационной инфраструктуры / Э. А. Гильманова, Р. И. Ахметшина // Форум молодых ученых. – 2022. – № 2(66). – С. 34-37.

12. Панченко В. М. Системный анализ. Метод имитационного моделирования : Учеб. пособие : Для студентов специальности «Автоматизир. системы обраб. информ. и упр.» направления подгот. дипломир. специалиста «Информатика и вычислит. Техника» / В. М. Панченко ; В.М. Панченко; М-во образования Рос. Федерации, Моск. гос. ин-т радиотехники, электроники и автоматики (техн. ун-т). М:–Моск. гос. ин-т радиотехники, электроники и автоматики (техн. ин-т), 2003. – 131 с

13. Филяк П. Ю. Системы моделирования в обеспечении информационной безопасности организации / П. Ю. Филяк // Современные проблемы безопасности жизнедеятельности: интеллектуальные транспортные системы : Материалы IV международной научно-практической конференции, Казань, 25–26 февраля 2016 года. – Казань: Научный центр безопасности жизнедеятельности, 2016. – С. 529-538.

14. 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.

15. Галиуллин Н. Имитационное моделирование в обеспечении информационной безопасности предприятия / Н. Галиуллин // Collegium linguisticum - 2019 : тезисы докладов Ежегодной конференции Студенческого научного общества МГЛУ, Москва, 17–19 октября 2019 года. – Москва: Московский государственный лингвистический университет, 2019. – С. 286.

16. Гречихин П. А. Моделирование рисков информационной безопасности с использованием имитационной модели / П. А. Гречихин // Радиоэлектроника, электротехника и энергетика : Тезисы докладов, Москва, 15–16 марта 2018 года. – М.: Общество с ограниченной ответственностью «Центр полиграфических услуг» «РАДУГА», 2018. – С. 592.

17. Грицкевич Е. В. Компьютерный анализ систем оптотехники и информационной безопасности : учеб. пособие / Е. В. Грицкевич, П. А. Звягинцева. – Новосибирск : СГУГиТ, 2017. – 70 с.

18. Способ оценки эффективности управления и устройство для его осуществления: пат. № 2326442 Российская Федерация, № 2007102742/09 ; заявл. 24.01.2007 : опубл. 10.06.2008 / В. А. Селифанов, В. В. Селифанов.

19. Современный менеджмент и управление: тенденции и перспективы развития : Сборник научных трудов. – Симферополь : Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2023. – 723 с.

20. Хубиева М. Д. Анализ методов проведения аудита информационной безопасности предприятия / М. Д. Хубиева, Ф. Б. Тебуева // Новые технологии и проблемы технических наук : Сборник научных трудов по итогам международной научно-практической конференции, Красноярск, 11 ноября 2016 года. Ч. 3. – Красноярск: Инновационный центр развития образования и наук, 2016. – С. 33-37.