УДК 528.71
DOI 10.33764/2618-981X-2024-6-240-247

В. С. Скориков[1], Г. Г. Паносян[1], В. В. Селифанов[1]*

Использование имитационного моделирования для оценки рисков

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: isaac.newton01@mail.ru

Аннотация. В настоящее время построение системы управления рисками является одной из приоритетных целей в области обеспечения информационной безопасности. Без должной оценки рисков системы могут быть неправильно выбраны соответствующие меры и средства защиты информации, что в последствии может негативно сказаться на бюджете и репутации организации. Так как вся процедура оценки доверия и качества работы системы управления рисками является масштабной и достаточно затратной, в статье продемонстрировано создание модели вышеописанной системы. При создании была использована модель типа «система массового обслуживания». В качестве метода исследования было использовано имитационное моделирование. Разработана имитационная модель системы управления рисками, а также описаны возможности ее применения. При построении модели было использовано прикладное программное обеспечение AnyLogic.

Ключевые слова: имитационное моделирование, оценка рисков, управление рисками

V. S. Skorikov[1], G. G. Panosyan[1], V. V. Selifanov[1]*

Using simulation to assess risks

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: isaac.newton01@mail.ru

Abstract. Currently, building a risk management system is one of the priority goals in the field of information security. Without a proper risk assessment of the system, appropriate measures and means of protecting information may be incorrectly selected, which can subsequently negatively affect the budget and reputation of the organization. Since the entire procedure for assessing the trust and quality of the risk management system is large-scale and quite expensive, the article demonstrates the creation of a model of the above-described system. When creating, a model of the “queuing system” type was used. Simulation modeling was used as a research method. The results of modeling the risk management system, as well as the possibilities of its application, are described. AnyLogic application software was used to build the model.

Keywords: simulation modeling, risk assessment, risk management

Введение

В наше время вопрос обеспечения информационной безопасности является одним из приоритетных для любой из существующих систем, использующих квантовое распределение ключей. Для обеспечения безопасности информации внутри системы необходимо понимать, какие риски существуют в рамках этой системы. Процесс управления рисками описан в соответствующем стандарте

ГОСТ Р ISO 27005, в котором рассмотрена и продемонстрированна работа по оценке рисков и дальнейшим действиям, которые необходимо предпринять, основываясь на результатах оценки [1-5, 8].

Создание системы для оценки рисков является необходимой задачей для любой из информационных систем. Такие системы должны проходить предварительную проверку на доверие, стоит ли доверять результатам оценки рисков, предоставленным решениям, которые предлагает данная система управления рисками и т.д. [6, 7]

Перед внедрением системы управления рисками в реальную информационную систему было бы хорошей практикой продемонстрировать работу такой системы в имитационной модели, так как процесс оценки рисков на реальном объекте является трудоемким и достаточно многозатратным. В связи с этим было принято решением воссоздать модель описанной системы и провести оценку при применении этой модели [10-12].

Обоснование применения имитационного моделирования

Для построения любой модели в начале необходимо определиться с типом моделирования. Изучив разные научные методы, было выбрано имитационное моделирование. Имитационное моделирование является методом исследования, при котором реальная система описывается с высокой точностью и при котором с построенной системой проводятся эксперименты, цель которых в получении информации об этой системе. Данная модель удобна в контексте исследования тем, что в ней существует возможности ввода изначальных данных и изменения параметров для получения разных результатов. Помимо этого, имитационное моделирование также позволяет качественно оценить эффективность системы, позволяя оценить надежность, производительность, пропускную способность и затраты ресурсов. Возможности такой детальной оценки системы позволяют принимать обоснованные решения, основываясь на полученных данных при минимальных рисках и затратах [12,14,15].

Построение модели

Построение модели реализовано с помощью программного обеспеченяи AnyLogic. Программа предназначена для построения моделей, а потому обладает графическим интерфейсом для удобства в процессе создания модели и позволяет использовать язык разработки Java для создания собственных моделей [9].

В качестве основы для построения модели использовался стандарт ГОСТ Р ISO 27005. Основываясь на данном стандарте была построена схема с описанием алгоритма процесса управления рисками (рис. 1).

Для управления рисками в алгоритме представлены следующие действия [13, 20, 21]:

– идентификация рисков, присутствующих в системе;

– процесс оценки неприемлемых рисков и рисков жизненного цикла информационной системы;

– управление неприемлемыми рисками и рисками жизненного цикла информационных систем;

– дальнейший мониторинг рисков.

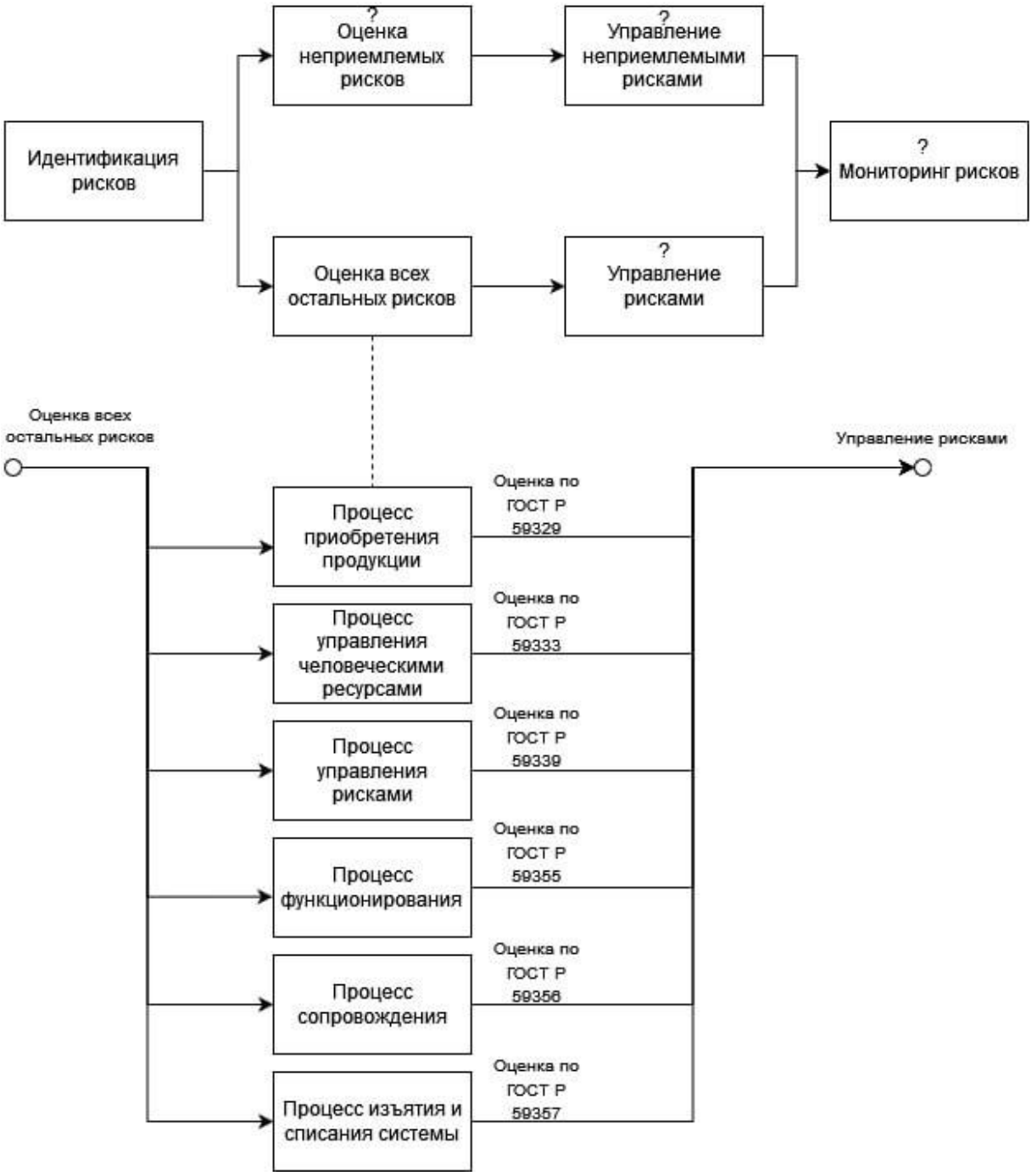

Рис. 1. Блок-схема алгоритма процесса управления рисками

Для более подробного описания работы построенной системы представлена блок-схема алгоритма работы этой системы (рис. 2).

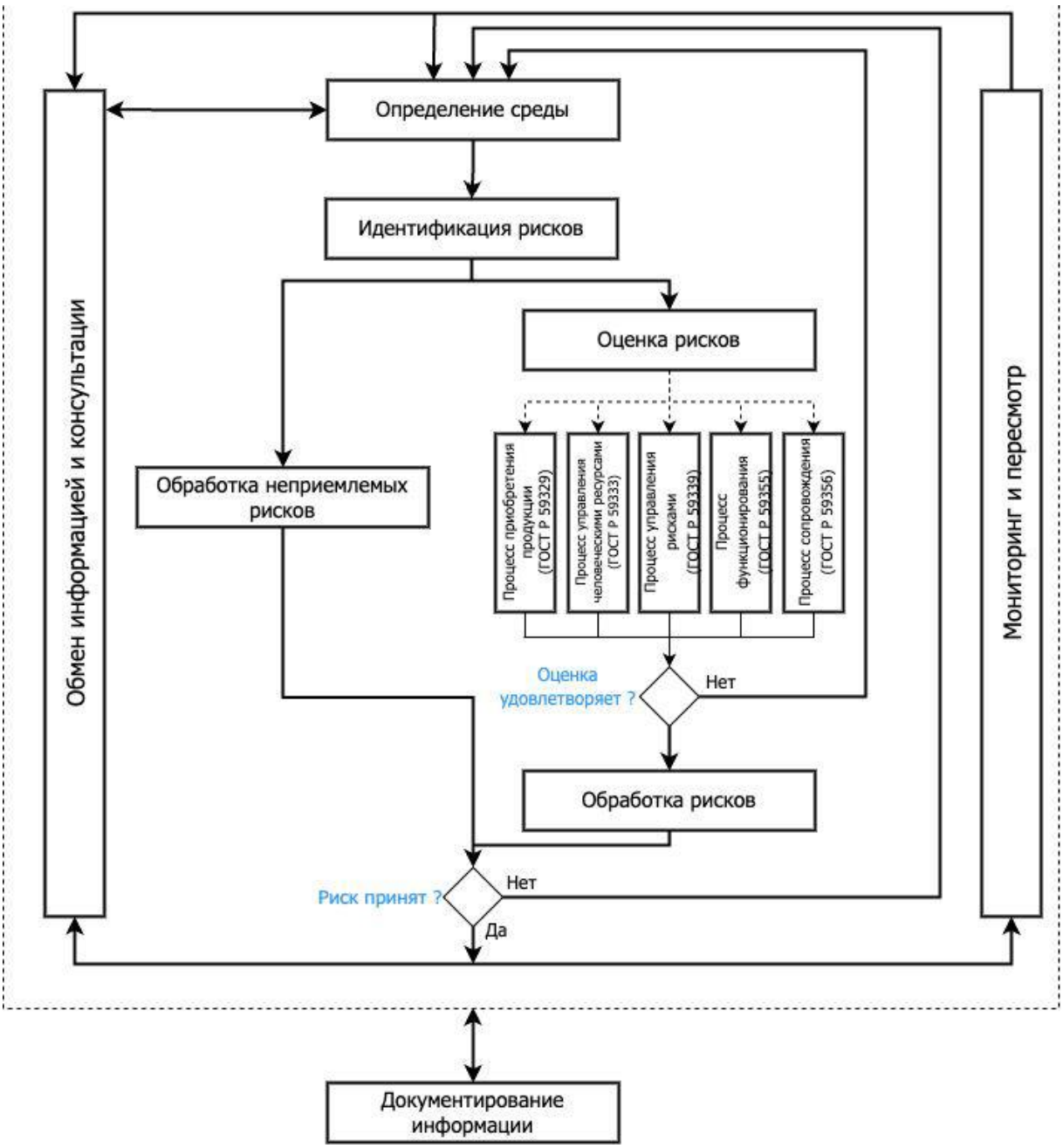

Рис. 2. Детальное описание алгоритма управления рисками

Как видно из схемы, представленной на рис. 2, обнаруженные риски также идентифицируются и обрабатываются в соответствии со стандартами. Если же риск удалось устранить, то систему продолжают анализировать на наличие новых рисков, не забывая документировать каждый случай управления рисками [16-19].

На основе вышеописанного алгоритма была построена компьютерная модель системы управления рискмаи информационной системы (рис. 3).

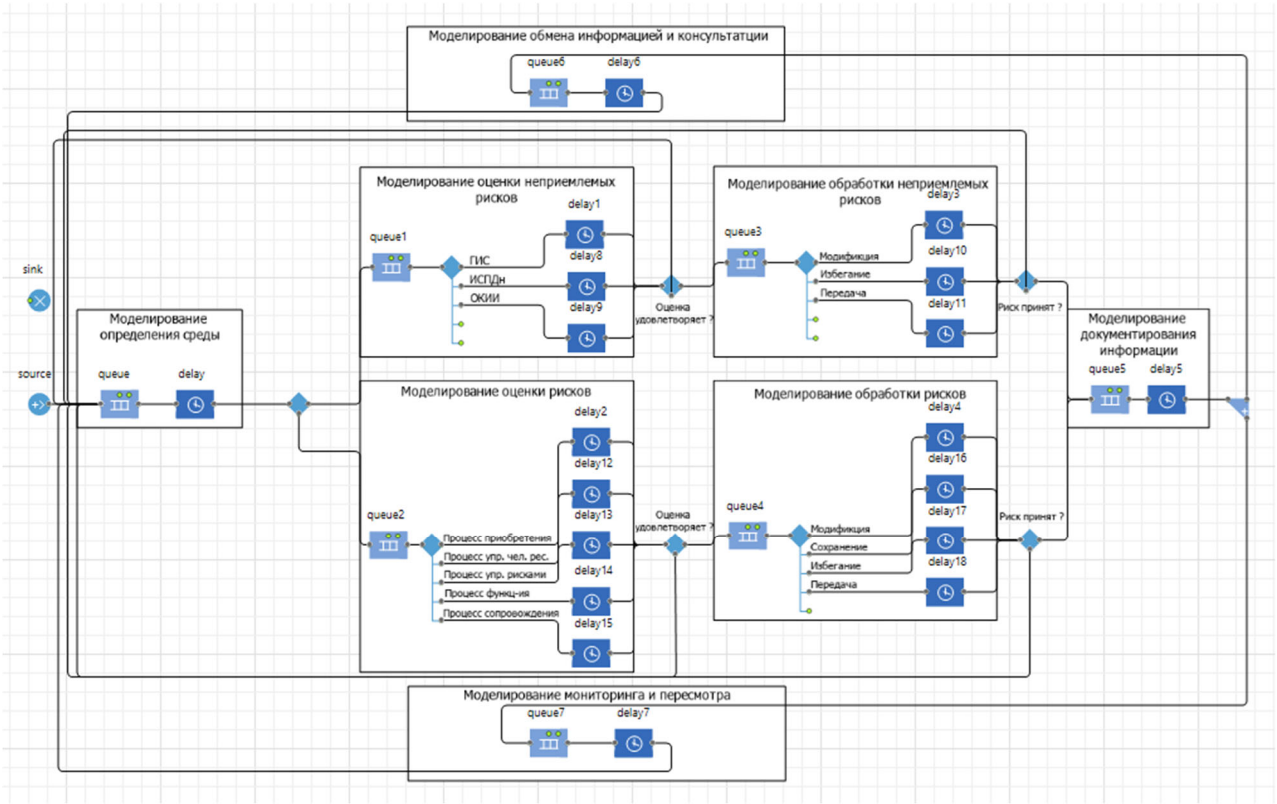

Рис. 3. Структура построенной модели

После запуска система начнет обрабатывать исходные данные, поступающие из блока «source». Прохождение агентов через каждый блок можно также пронаблюдать при необходимости (рис. 4).

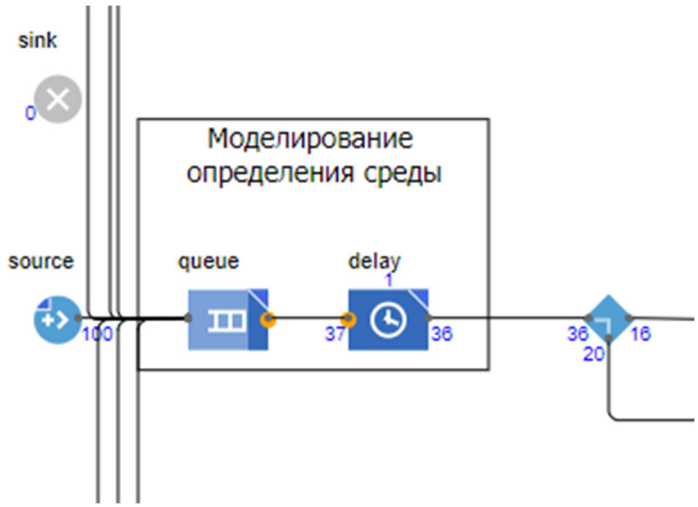

Рис. 4. Демонстрация поступления агентов

Из-за сложности процессов оценки рисков в процессе работы системы будут возникать очереди, которые также можно наблюдать (рис. 5).

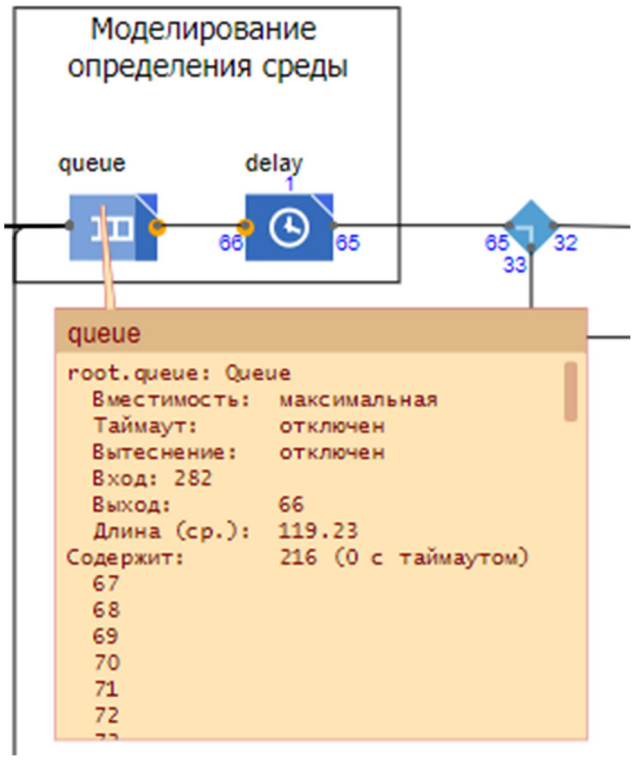

Рис. 5. Характеристики блока очереди

Система достаточно сильно детализирована, каждый из элементов можно настроить отдельно для обеспечения реалистичности и точности оценки рисков относительно оцениваемой информационной системы. Данная особенность положительно проявляется при предварительном просмотре работы оценки рисков, основываясь на результатах смоделированной системы.

Заключение

Разработанная модель системы управления рисками информационной системы позволит более детально рассмотреть процесс оценки рисков для системы с квантовым распределением ключей. Модель позволяет оценить перспективы и необходимость внедрения системы управления рисками, а также предварительно оценить работу системы перед внедрением в существующую инфраструктуру.

Возможность детальной настройки модели позволяет грамотно оценить необходимость внедрения системы оценки рисков в информационную систему с использованием квантового распределния ключей. Каждый из элементов системы может быть рассмотрен отдельно для лучшего понимания работы системы оценки рисков.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Begimbayeva YE., Quantum key distribution protocols based on Heisenberg's uncertainty / Begimbayeva YE., Zhaxalykov T. // Труды университета – 2023 г. – No. 1(90). – P. 423-429.

2. Kosari, A. Unilateral information reconciliation schemes FO quantum key distribution system / A. Kosari // Проблемы инфокоммуникаций. – 2021. – No. 2(14). – P. 44-50.

3. Suma M. R., An optimal swift key generation and distribution for QKD / M. R. Suma, P. Madhumathy // Scientific and technical journal of information technologies, mechanics and optics. – 2022. – No. 1. – P. 101-113.

4. Бобков Е. О. Применение технологии квантового распределения ключей в волоконно-оптических линиях связи / Е. О. Бобков, Е. А. Балашова, А. В. Крыжановский // Научный альманах Центрального Черноземья. – 2022. – № 1-4. – С. 29-36.

5. Габдулхаков И. М. Построение многоканальной системы квантового распределения ключей с частотным кодированием / И. М. Габдулхаков, О. Г. Морозов // Инженерный вестник Дона. – 2020. – № 5(65). – С. 53.

6. Габдулхаков И. М. Принципы построения универсальной системы квантового распределения ключей с частотным кодированиемна основе ампли-тудной модуляции и фазовой коммутации / И. М. Габдулхаков, О. Г. Морозов // Актуальные вопросы телекоммуникаций : Научно-техническая конференция Росинфоком-2017, Самара, 01 сентября 2017 года / Федеральное агентство свя-зи; Департамент информационных технологий и связи Самарской области; Поволжский государственный университет телекоммуникаций и информатики; Научно-исследовательский институт радио. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. – С. 81-82.

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

8. Жилин С. В. Квантовое распределение ключей по беспроводному оптическому каналу связи / С. В. Жилин, В. В. Архипенко, Е. С. Басан // Компьютерные и информационные технологии в науке, инженерии и управлении (КомТех-2022): Материалы Всероссийской научно-технической конференции с международным участием. В двух томах, Таганрог, 08–10 июня 2022 года. – Таганрог: Южный федеральный университет, 2022. – С. 194-200.

9. Луценко С. А. Способ квантового распределения ключей в облачных сетях / С. А. Луценко, П. В. Заика, С. Ю. Козлов // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 11–12 октября 2017 года. – Санкт-Петербург: Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации, 2017. – С. 218-220.

10. Методика оценки угроз безопасности информации. – Текст: электронный // Федеральная служба по техническому и экспортному контролю: [сайт]. – URL: https://fstec.ru/component/attachments/download/2919.

11. Задорин А. С., Принцип квантового распределения ключей по оптическому волокну на основе временных сдвигов ТВ-кубитов / А. С. Задорин, Д. А. Махорин // Известия вузов. Физика. – 2016. – № 3. – С. 24-29.

12. Жиляев А. Е. Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии // Доклады томского государственного университета систем и управления радиоэлектроники. – 2021. – Т. 24, № 4. – С. 33-39. – DOI 10.21293/1818-0442-2021-24-4-33-39.

13. Патент № 2621605 C Российская Федерация. Сеть квантового распределения ключей: № 2015141966: заявл. 02.10.2015: опубл. 06.06.2017 / К. С. Кравцов, С. П. Кулик, С. Н. Молотков [и др.]; заявитель Российская Федерация, от имени которой выступает ФОНД ПЕРСПЕКТИВНЫХ ИССЛЕДОВАНИЙ.

14. Патент № 2706175 C1 Российская Федерация. Способ квантового распределения ключей в однопроходной системе квантового распределения ключей: № 2018146854: заявл. 27.12.2018: опубл. 14.11.2019 / А. Г. Втюрина, К. А. Балыгин, В. И. Зайцев [и др.]; заявитель Открытое акционерное общество «Информационные технологии и коммуникационные системы».

15. Патент № 2741264 C1 Российская Федерация. Способ двухуровневого управления техническими средствами (варианты): № 2020122379: заявл. 07.07.2020: опубл. 22.01.2021 / В. А. Селифанов, В. В. Селифанов, А. В. Селифанов; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

16. Патент № 2741265 C1 Российская Федерация. Способ двухуровневого управления техническими системами (варианты): № 2020122382: заявл. 07.07.2020: опубл. 22.01.2021 / В. В. Селифанов, заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

17. Патент № 2747626 C1 Российская Федерация. Способ двухуровневого управления и система управления для его осуществления (варианты): № 2020114340: заявл. 22.04.2020: опубл. 11.05.2021 / В. А. Селифанов, В. В. Селифанов, А. В. Селифанов; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

18. Патент № 2752844 C1 Российская Федерация. Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты): № 2020140774: заявл. 10.12.2020: опубл. 11.08.2021 / А. Е. Жиляев; заявитель Акционерное общество «Информационные технологии и коммуникационные системы».

19. Румянцев, К. Е. Безопасность режима синхронизации системы квантового распределения ключей / К. Е. Румянцев, А. П. Пленкин // Известия ЮФУ. Технические науки. – 2015. – № 5(166). – С. 135-152.

20. Свидетельство о государственной регистрации программы для ЭВМ № 2022683792 Российская Федерация. ViPNet Модуль оптоэлектронный клиента квантового распределения ключей: № 2022683156: заявл. 28.11.2022: опубл. 08.12.2022; заявитель Акционерное общество «Информационные технологии и коммуникационные системы».

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