УДК 528.71
DOI 10.33764/2618-981X-2025-6-156-164

В. С. Скориков[1]✉, *В. В. Селифанов*[1]

Разработка оценки эффективности для моделей систем оценки рисков оптических и оптико-электронных систем

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

Аннотация. Активная разработка моделей систем для оценки рисков в оптических и оптико-электронных системах позволяет организациям контролировать и демонстрировать работу подобных систем, оценивать потенциальные затраты ее внедрения и поддержки, а также анализировать, насколько удачным решением является внедрение этой системы для оценки рисков в организацию. Однако для полного доверия к модели и объективного оценивания ее работы необходимо проводить оценку эффективности. Разработанная оценка эффективности позволяет качественно и без лишних затрат производить вычисления для дальнейшего объективного сравнения и выбора оптимальной модели системы оценки рисков. Расчеты проводились на модели типа «система массового обслуживания», построенной в прикладном программном обеспечении AnyLogic. В качестве метода исследования было использовано имитационное моделирование.

Ключевые слова: оценка эффективности, имитационное моделирование, оценка рисков, управление рисками

V. S. Skorikov[1]✉, *V. V. Selifanov*[1]

Development of an effectiveness evaluation for risk assessment models of optical and optoelectronic systems

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

Abstract. The active development of system models for risk assessment in optical and optoelectronic systems enables organizations to monitor and demonstrate the operation of such systems, evaluate the potential costs of their implementation and maintenance, and analyze how successful the adoption of these risk assessment systems will be within the organization. However, to fully trust the model and objectively evaluate its performance, it is necessary to conduct an effectiveness evaluation. The developed effectiveness evaluation allows for high-quality calculations without excessive costs, facilitating objective comparison and selection of the optimal risk assessment system model. Calculations were performed on a queueing system model built using the applied software AnyLogic. Simulation modeling was used as the research method.

Keywords: effectiveness evaluation, simulation modeling, risk assessment, risk management

Введение

Обеспечение безопасности оптических и оптико-электронных систем является ключевым условием их надежного функционирования и устойчивого развития. На сегодняшний день существуют модели оценки рисков, оценки угроз, ре-

агирования на инциденты, а также модель аудита информационной безопасности в этих системах. К сожалению, невозможно полностью доверять результатам таких моделей без соответствующей оценки эффективности [1, 2].

Оценка эффективности позволяет детально изучить работу модели и сравнить ее с другими, измененными моделями той же категории. Например, модификация стандартной модели оценки рисков позволяет внедрить ее для систем с КРК. Добавление этапов оценки рисков, характерных для этой технологии, может продемонстрировать небольшое снижение результатов оценки эффективности. В таком случае, если результаты оценки будут удовлетворительными, модифицированная модель будет считаться оптимальной для внедрения в системы с технологией КРК [3, 4, 5].

В случаях, если модифицированная система покажет результаты оценки ниже требуемых, то это позволит организации избежать нежелательных трат ресурсов на внедрение новой системы [6, 7].

Обоснование применения имитационного моделирования

При разработке оценки эффективности было принято решение использовать имитационное моделирование. Это решение обосновано несколькими факторами: использование языка программирования Java, установка соответствующих системе характеристик для работы модели, возможность модифицирования модели. Использование языка программирования Java позволило встроить оценку эффективностии напрмяую в модель. В совокупности с возможностями регулирования характеристик и модифицирования модели, использование языка программирования Java позволило внедрить оценку эффективности в модель. Это означает, что для измерения оценки эффективности новой системы достаточно изменить свойства необходимых блоков, а не внедрять всю оценку эффективности в новую модель [8, 9].

Разработка оценки эффективности

Оценка эффективности моделей систем для оценки рисков играет ключевую роль в обеспечении надежной защиты данных в организации. Этот процесс необходим на всех этапах жизненного цикла системы, требуя тщательного анализа и определения подходящих критериев оценки, особенно в условиях быстро меняющейся технологической среды и новых угроз. При выборе показателя эффективности важно учитывать, что оценка систем управления рисками (СУР) определяется через показатель эффективности управления. Этот показатель отражает, насколько система соответствует своему назначению и определяется как вероятность своевременного принятия и реализации правильного решения, обеспечивающего оптимальное использование технических ресурсов. Для расчета этого показателя используется следующая мультипликативная формула [10, 11, 12]:

$$W_э = P_{св.сб} \times P_{пр} \times P_{св.пр} \times P_{св.р}, \quad (1)$$

где $P_{св.сб}$ – вероятность того, что вся требуемая для принятия решений информация будет собрана вовремя; $P_{пр}$ – вероятность корректного выбора решения; $P_{св.пр}$ – вероятность одновременного своевременного и правильного принятия решений; $P_{св.р}$ – вероятность своевременного выполнения уже принятых решений.

Формула (1) позволяет количественно оценить эффективность управления и принимать обоснованные решения по обеспечению информационной безопасности. Порядок оценки показателя эффективности принятия решений включает следующие этапы [13, 14, 15, 16]:

– ввод исходных данных;

– измерение продолжительности, затраченной конекретным лицом на принятие решения в заданной ситуации;

– оценка времени, которое понадобилось на реализацию принятого решения;

– оценка времени, затраченного на сбор всей необходимой информации для принятия решения;

– подсчет количества решений, которые были приняты и реализованы вовремя;

– подсчет случаев, когда требуемая информация была собрана своевременно;

– подсчет количества решений, принятых правильно;

– вычисление вероятности, что принятые решения оказались верными, $P_{пр}$ по формуле:

$$P_{пр} = \frac{1}{M} \sum \frac{S_{пр}}{L}, \quad (2)$$

где M – общее число анализируемых ситуаций; L – количество участников, принимающих решения, задействованных в конкретной ситуации; $S_{пр}$ – число решений, принятых корректно в рамках данной ситуации.

– вычисление вроятности того, что вся требуемая для принятия решений информация будет собрана вовремя $P_{св.сб}$;

– расчет вероятности одновременного своевременного и правильного принятия решений $P_{св.пр}$ по формуле:

$$P_{св.пр} = \frac{1}{M} \sum \frac{R}{S_{пр}}, \quad (3)$$

где R – количество решений, которые были приняты вовремя и с правильным содержанием для конкретной ситуации;

– определение вероятности своевременного выполнения уже принятых решений $P_{св.р}$ по формуле:

$$P_{св.р} = \frac{1}{Q \times M} \sum \frac{C}{R}, \quad (4)$$

где C – количество решений, которые были реализованы своевременно и приняты корректно в каждой конкретной ситуации; Q – количество каналов связи, соответствующее числу исполнителей.

На основании собранной информации рассчитываются статистические параметры исследуемых показателей, включая текущие, минимальные, максимальные и средние значения. Кроме того, для наглядного представления результатов создаются графики и гистограммы. Это позволяет лучше понять функционирование системы и выявить особенности её работы. Основная цель оценки эффективности СУР заключается в своевременной перестройке систем защиты информации. При работе с Anylogic выполняются эксперименты, в ходе которых параметры модели изменяются в заданных пределах. Это позволяет не только проанализировать, как отдельные параметры влияют на поведение системы, но и выявить оптимальные значения для повышения эффективности СУР. Такой подход автоматизирует многократные запуски модели с разными параметрами и помогает визуализировать результаты с помощью графиков, что облегчает поиск наилучших настроек модели для эффективного управления рисками [17, 18, 19, 20,21].

В качестве примера для оценки эффективности была использована модель системы оценки рисков для оптических и оптико-электронных систем (рис. 1). В рамках простого эксперимента установлено, что заявки на обслуживание поступают в систему моделирования группами по 35 штук с интервалом в 30 минут. Время обслуживания рассчитывается согласно экспоненциальному распределению и зависит от параметров, связанных с алгоритмом управления. В процессе эксперимента параметры изменялись, что позволило оценить, как эффективность управления зависит от количества заявок, поступающих одновременно на обслуживание (рис. 2). Итогами моделирования являются следующие результаты:

– статистические параметры исследуемых показателей, включая текущие, минимальные, максимальные и средние значения;

– графические представления, показывающие текущие и средние значения анализируемых показателей;

– гистограммы и функции распределения, иллюстрирующие распределение значений оцениваемых параметров.

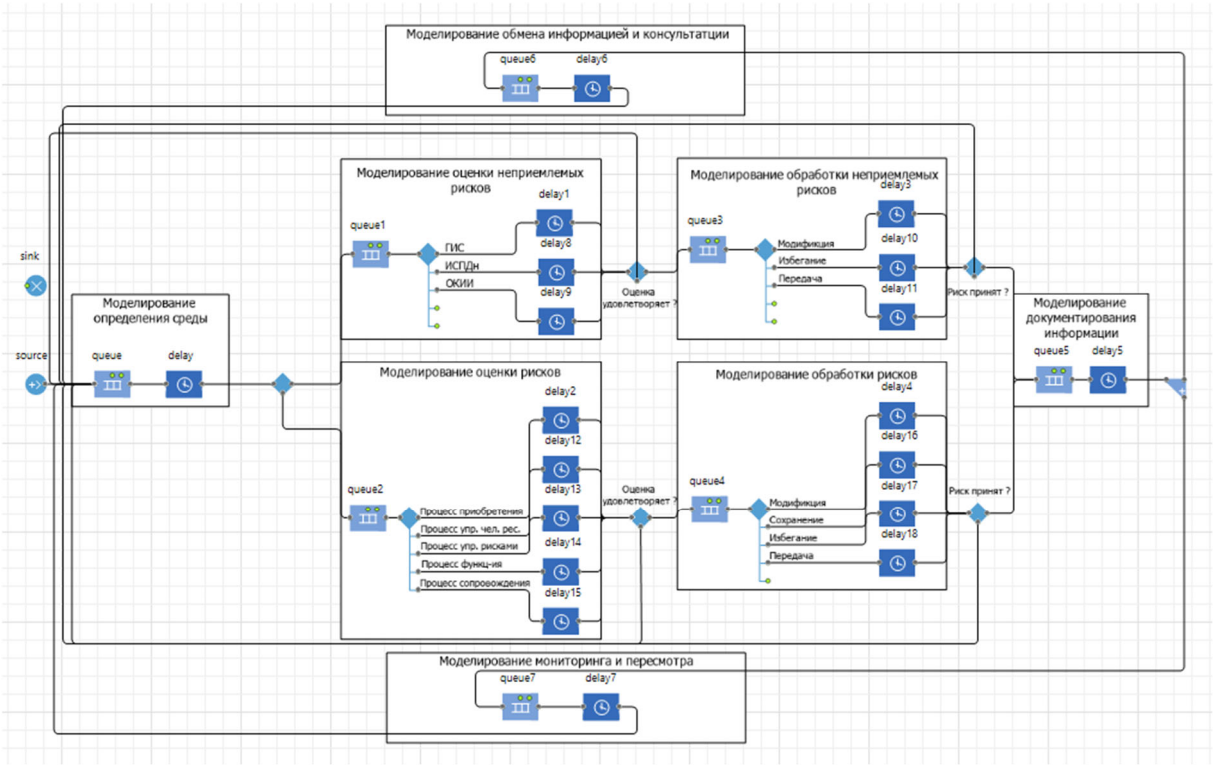

Рис. 1. Модель системы оценки рисков

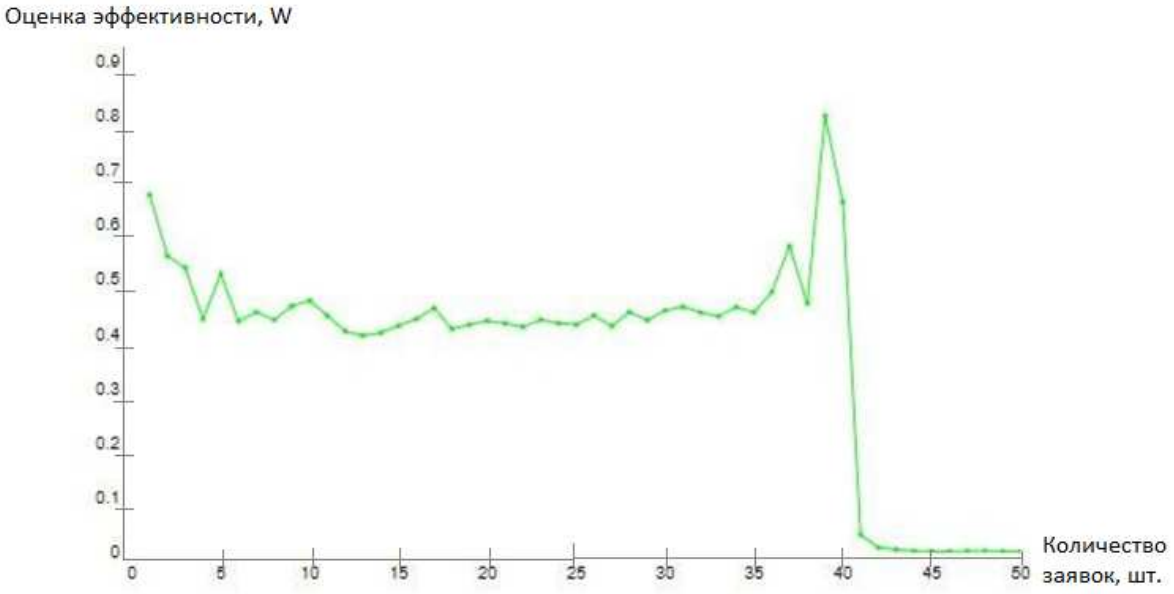

Рис. 2. Зависимость оценок эффективности

Расчеты по формулам (1) – (4) проводятся в соответствии с этапами работы модели системы оценки рисков. Данные для вычисления оценки эффективности собираются на различных этапах моделирования: моделирование определения среды, моделирование оценки неприемлемых рисков, моделирование обработки неприемлемых рисков, моделирование оценки рисков, моделирование обра-

ботки рисков, а также моделирование документации информации. Моделирование документации информации является ключевым этапом, так как к этому моменту модель собирает все необходимые для расчета вероятностей данные и вычисляет оценку эффективности. Когда все агенты проходят полный путь, модель фиксирует время работы и количество прошедших через систему агентов, демонстрируя статистику через диаграммы.

По итогам работы модели было выведено распределение времени цикла управления в виде гистограммы (рис.3), диаграмма времени ожидания обработки (рис. 4), а также получены следующие результаты оценки: при 17 498 прогонах минимальное время цикла управления техническими средствами составило $t_{\min}$ = 2,526 мин, максимальное время цикла управления составило $t_{\max}$ = 9,999 мин, среднее время цикла управления составило $t_{ср}$ = 5,002 мин. Показатель эффективности управления рисками при проведения простого эксперимента $W_э$ = 0,44 (рис. 5).

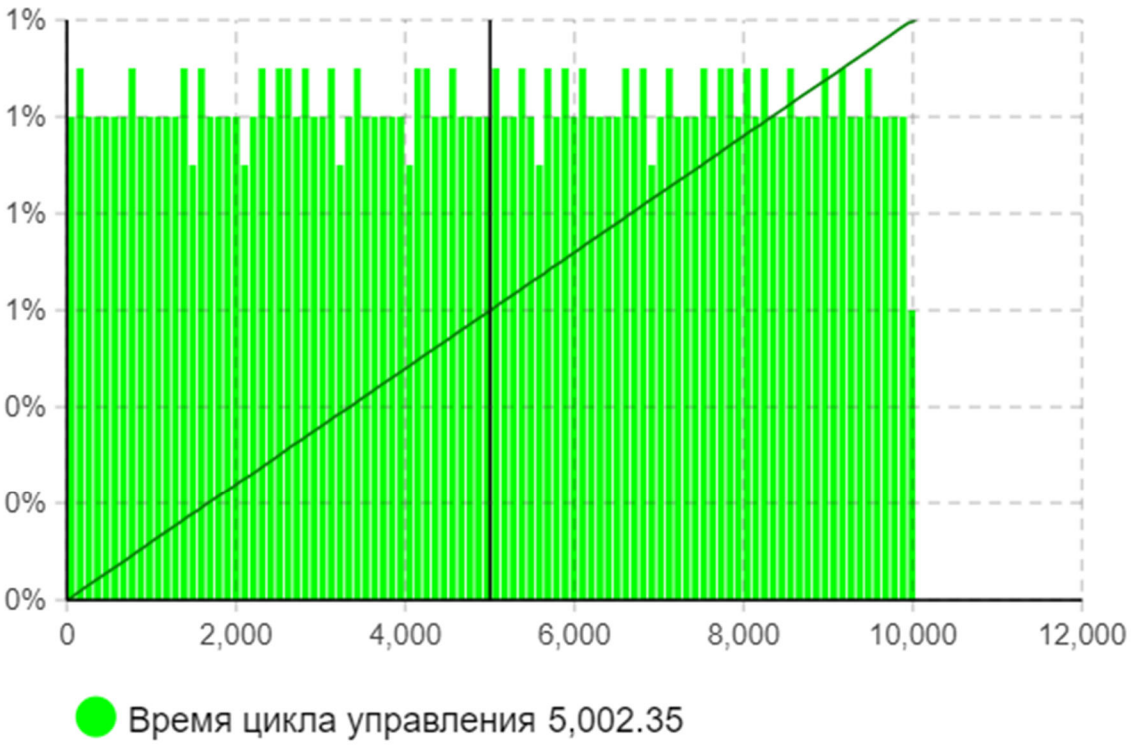

Рис. 3. Гистограмма распределения времени цикла управления

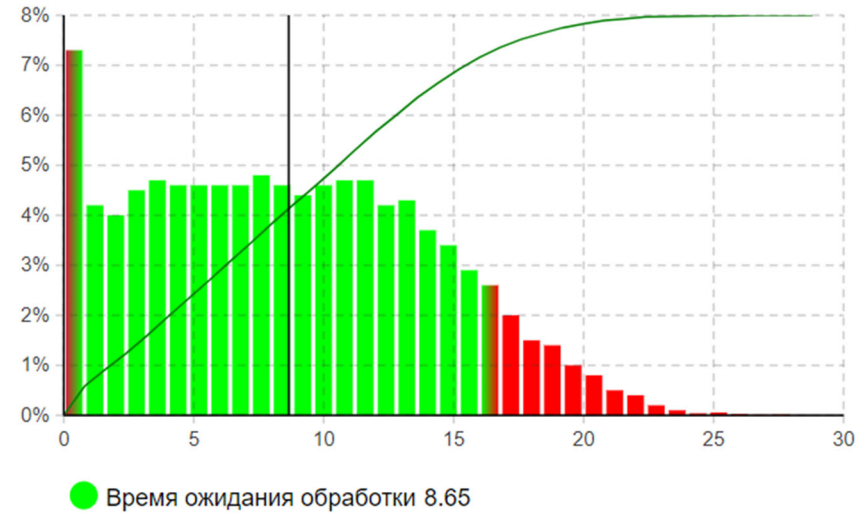

Рис. 4. Диаграмма времени ожидания обработки

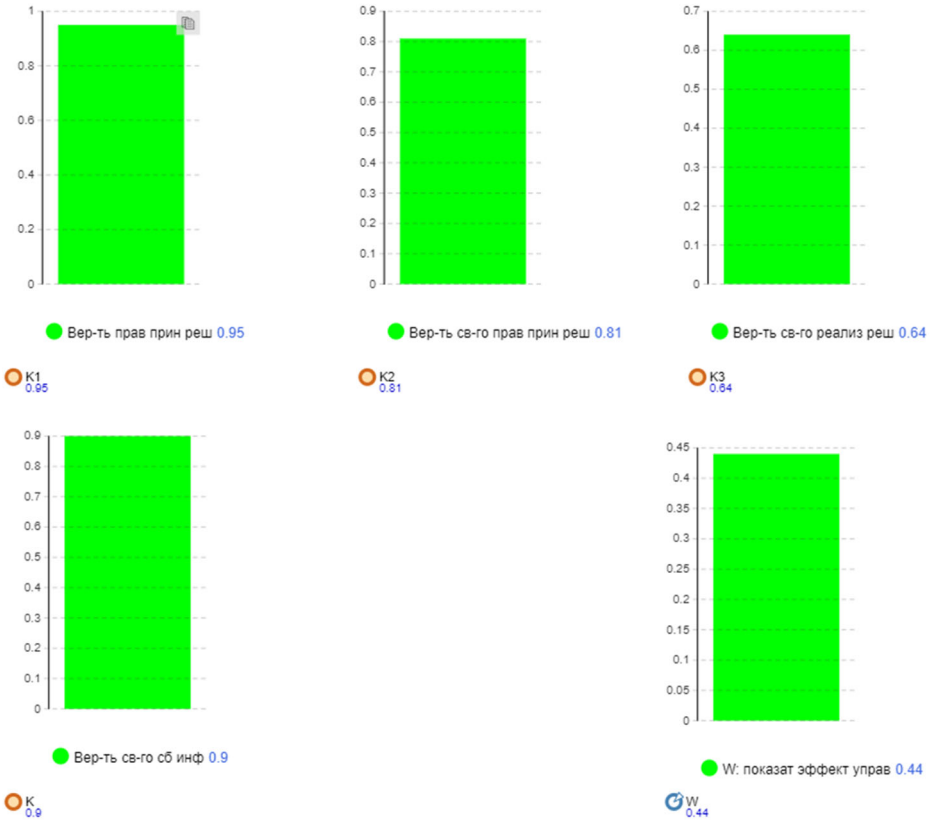

Рис. 5. Показатели эффективности управления

По итогу работы модели выводятся диаграммы, показывающие скорость работы и ожидания обработки в минутах. Основываясь на показателях диаграмм, специалисты могут решить, является ли время работы достаточно эффективным. Также приведены значения всех вероятностей, которые были использованы для

оценки эффективности: вероятность правильного принятия решения, вероятность своевременного и правильного принятия решения, вероятность своевременной реализации решения, а также вероятность своевременного сбора информации.

Заключение

Результативность созданной модели управления рисками оценивалась с учётом показателей, характеризующих своевременность и корректность принимаемых решений, что способствует максимально эффективному использованию технических ресурсов. Такой подход позволяет организации не только обеспечить высокий уровень информационной безопасности, но и адаптироваться к изменяющимся угрозам и требованиям.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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

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

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

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

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

6. Габдулхаков И. М., Морозов О. Г. Принципы построения универсальной системы квантового распределения ключей с частотным кодированием на основе амплитудной модуляции и фазовой коммутации // Актуальные вопросы телекоммуникаций: научно-техническая конференция Росинфоком-2017, Самара, 01 сентября 2017 года. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. – С. 81–82.

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

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

9 . Луценко С. А., Заика П. В., Козлов С. Ю. Способ квантового распределения ключей в облачных сетях // Инновационная деятельность в Вооруженных Силах Российской Федерации: труды всеармейской научно-практической конференции, Санкт-Петербург, 11–12 октября 2017 года. – Санкт-Петербург: Военная академия связи имени Маршала Советского Союза С. М. Буденного, 2017. – С. 218–220.

10. Методика оценки угроз безопасности информации [Электронный ресурс]. – Федеральная служба по техническому и экспортному контролю. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 04.05.2025).

11. Задорин А. С., Махорин Д. А. Принцип квантового распределения ключей по оптическому волокну на основе временных сдвигов ТВ-кубитов // 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 РФ № 2621605 С. Сеть квантового распределения ключей: заявл. 02.10.2015; опубл. 06.06.2017. Заявитель: Фонд перспективных исследований. МПК H04L 9/08, H04B 10/00, G06F 21/60.

14. Патент РФ № 2706175 С1. Способ квантового распределения ключей в однопроходной системе квантового распределения ключей: заявл. 27.12.2018; опубл. 14.11.2019. – Заявитель: ОАО «Информационные технологии и коммуникационные системы». – МПК H04L 9/08, G06F 21/72.

15. Патент РФ № 2741264 С1. Способ двухуровневого управления техническими средствами (варианты): заявл. 07.07.2020; опубл. 22.01.2021. – Заявитель: Новосибирский государственный технический университет. – МПК G05B 15/00.

16. Патент РФ № 2741265 С1. Способ двухуровневого управления техническими системами (варианты): заявл. 07.07.2020; опубл. 22.01.2021. – Заявитель: Новосибирский государственный технический университет. – МПК G05B 15/00.

17. Патент РФ № 2747626 С1. Способ двухуровневого управления и система управления для его осуществления (варианты): заявл. 22.04.2020; опубл. 11.05.2021. – Заявитель: Новосибирский государственный технический университет. – МПК G05B 15/02.

18. Патент РФ № 2752844 С1. Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты): заявл. 10.12.2020; опубл. 11.08.2021. – Заявитель: АО «Информационные технологии и коммуникационные системы». – МПК H04L 9/08.

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

20. Селифанов В. В., Исаева Ю. А., Голдобина А. С., Звягинцева П. А. Имитационная модель для управления защитой информации при оценке эффективности государственных и муниципальных систем // Интерэкспо Гео-Сибирь. – 2018. – № 7. – С. 296–299.

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