УДК 004.056.5
DOI10.33764/2618-981X-2025-6-165-171

Е. Ю. Солдатов[1], В. В. Селифанов[1]✉

Построение системы управления инцидентами в оптотехнических системах, созданных с использованием технологии квантового распределения ключей

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

Аннотация. В статье рассматривается проблема построения системы управления инцидентами информационной безопасности в оптотехнических системах, использующих технологию квантового распределения ключей (КРК). Проведен анализ патентов, определены два ключевых документа, пригодных для разработки системы управления инцидентами информационной безопасности. Изучены подходы обработки инцидентов, обоснована применимость приказов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности России, связанных с обработкой инцидентов. Описаны типичные атаки на КРК-системы, такие как атака с расщеплением по числу фотонов, атака «троянский конь» и ослепление детекторов с примерами их реализации. Подтверждена необходимость компьютерного моделирования для обработки данных инцидентов. Разработаны три модели: гибридная (включающая реагирование на атаки как на классический канал передачи информации, так и на оптотехнический канал КРК), и модель реагирования отдельно на классический и квантовые каналы. Сравнительный анализ моделей показал, что гибридная модель сравнима по времени цикла (34,17 мин, против классической 24,8 мин и квантовой 29,4 мин) и превосходит их по эффективности (Wэ = 0,79, против классической Wэ=0,38 и квантовой Wэ=0,34), что делает гибридную модель перспективной для повышения безопасности КРК-систем.

Ключевые слова: информационная безопасность, уязвимости, имитационное моделирование, обработка инцидентов

E. Yu. Soldatov[1], V. V. Selifanov[1]✉

Building an incident management system in optotechnical systems created using quantum key distribution technology

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

Annotation. The paper deals with the problem of building an information security incident management system in optotechnical systems using quantum key distribution (QKD) technology. Patents are analyzed, two key documents suitable for the development of information security incident management system are identified. Incident handling approaches are studied, applicability of orders of the Federal Service for Technical and Export Control and the Federal Security Service of Russia related to incident handling is substantiated. Typical attacks on AAC systems such as photon number splitting attack, Trojan horse attack and detector blinding are described with examples of their realization. The need for computer modeling to handle these incidents is confirmed. Three models were developed: a hybrid model (including response to attacks both on the classical channel of information transmission and on the optotechnical channel of the QKD), as well as separately response to the classical and quantum channels. Comparative analysis of the models showed that the hybrid model is comparable

in cycle time (34,17 min, against the classical 24,8 min and quantum 29,4 min) and exceeds them in efficiency (We = 0,79, against the classical We = 0,38 and quantum We = 0,34), which makes the hybrid model promising for improving the security of QKD-systems.

Keywords: information security, vulnerabilities, simulation modeling, incident handling

Введение

Технология квантового распределения ключей (КРК) предлагает принципиально новый уровень защиты информации, основанный на фундаментальных законах квантовой механики. Однако практическая реализация оптотехнических КРК-систем сталкивается с рядом аппаратных и программных уязвимостей, которые могут быть использованы злоумышленниками. Построение эффективной математической модели системы управления инцидентами позволит своевременно выявлять попытки несанкционированного доступа к каналу связи, оценивать потенциальные угрозы для различных сетевых топологий и обеспечивать должный уровень защиты передаваемой информации в соответствии с требованиями нормативных документов [1].

Анализ патентной документации

Для разработки системы управления инцидентами проанализированы патенты: RU 2747626 C1 (2021), RU 2022663610 (2022) и RU 2764458 C1 (2022). Они отражают развитие систем управления, применимых к информационной безопасности.

– RU 2747626 C1 предлагает расширение функциональных возможностей способа и системы управления [2];

– RU 2022663610 C1 интегрирует кибербезопасность, предлагая комплексное управление [3];

– RU 2764458 C1 расширяет функционал, включая защиту информации.

Патент RU 2022663610 C1 представляет ценность для исследования КРК-систем благодаря имитационному моделированию трехуровневого управления, позволяющему оценивать эффективность алгоритмов, загрузку элементов, время выполнения функций и вероятность корректных решений, что особенно важно при разработке систем управления инцидентами в оптотехнических комплексах [4].

Подходы к обработке инцидентов ИБ

На основании проведенных мер подготовлены следующие рекомендации для центра обеспечения безопасности (SOC):

– организовать непрерывный 24/7 контроль ключевых параметров — уровня квантовых ошибок (QBER) и скорости формирования ключей;

– включить в состав группы реагирования экспертов по квантовым технологиям;

– систематически проводить учения по противодействию атакам с применением симуляционного моделирования [5];

– своевременно обновлять информационную базу о новейших методах атак

на системы квантового распределения ключей [6].

Исследование демонстрирует, что существующие системы управления инцидентами информационной безопасности недостаточно приспособлены к особым требованиям оптико-технических комплексов КРК.

Угрозы на протокол КРК и техническую реализацию

Угрозы на канал КРК принято разделять как «атаки на техническую реализацию» и «атаки на протокол КРК». КРК-системы подвержены следующим угрозам:

– атака «троянский конь»: злоумышленник направляет свет через кодирующее устройство и анализирует отраженный сигнал в диапазоне 1000-2000 нм [7]. В 2022 году сотрудники Национального исследовательского технологического университета МИСИС, при проведении эксперимента извлекли ключ с помощью этой атаки;

– атака с лазерным повреждением: использование мощного лазерного излучения для снижения эффективности оптических аттенюаторов, что делает сигнал доступным для перехвата [8];

– атаки с использованием сверхъяркого света: запуск сверхъяркого света в оптоволокно для нарушения работы источника фотонов [8];

– PNS-атака (расщепление фотонного числа): перехват и измерение части фотонов без обнаружения [8]. В 2021 году Российский квантовый центр получил 15 % ключа на канале 50 км.

Необходимость разработки компьютерной модели для эталонной модели безопасности КРК-систем

Разработка компьютерной модели гибридной системы реагирования на атаки обусловлена следующими ключевыми факторами:

– интеграция защиты разнородных каналов: классические и квантовые каналы имеют принципиально разные уязвимости, требующие комплексного подхода и единой стратегии противодействия мультивекторным атакам;

– отсутствие адаптированных решений: современные системы управления инцидентами не учитывают специфику оптотехнических систем КРК, что создает потребность в создании эталонной модели при значительно меньших затратах по сравнению с экспериментами на реальной инфраструктуре;

– противодействие невыявленным угрозам: модель позволит разрабатывать превентивные механизмы защиты от атак, которые остаются незамеченными существующими системами обнаружения вторжений, объединяя преимущества различных типов моделирования для более эффективной защиты.

Построение моделей

Для реализации математических моделей системы управления инцидентами в оптотехнических системах с использованием технологии КРК было выбрано программное обеспечение AnyLogic. Это мощный инструмент для имитационного моделирования, поддерживающий дискретно-событийное, агентное и си-

стемно-динамическое моделирование, что делает его подходящим для моделирования сложных систем, таких как системы управления инцидентами в квантовых сетях [9].

В рамках разработки модели в AnyLogic реализован процесс управления инцидентами, включающий этапы обнаружения, анализа, реагирования и восстановления. Модели учитывают специфику КРК, включая мониторинг параметров, таких как уровень квантовых ошибок (QBER) и скорость генерации ключей, а также обработку атак на квантовые каналы. Использование AnyLogic позволило создать виртуальную среду для тестирования различных сценариев инцидентов, что минимизирует затраты на физические эксперименты [10].

Разработаны три модели в AnyLogic:

– гибридная: гибридная модель, включающая реагирование на атаки как на классический канал передачи информации, так и на оптотехнический канал КРК (рис. 1, 2, 3).

– классическая: реагирование на классический канал передачи информации;

– квантовая: реагирование на оптотехнический канал квантового распределения ключей;

Модели симулируют угрозы и оцениваются по эффективности.

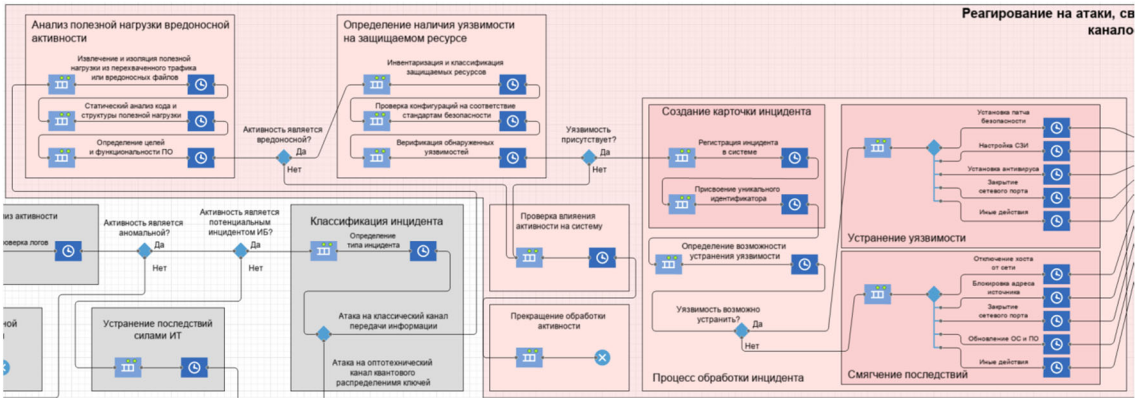

Рис. 1. Блок реагирования на атаки классического канала передачи информации

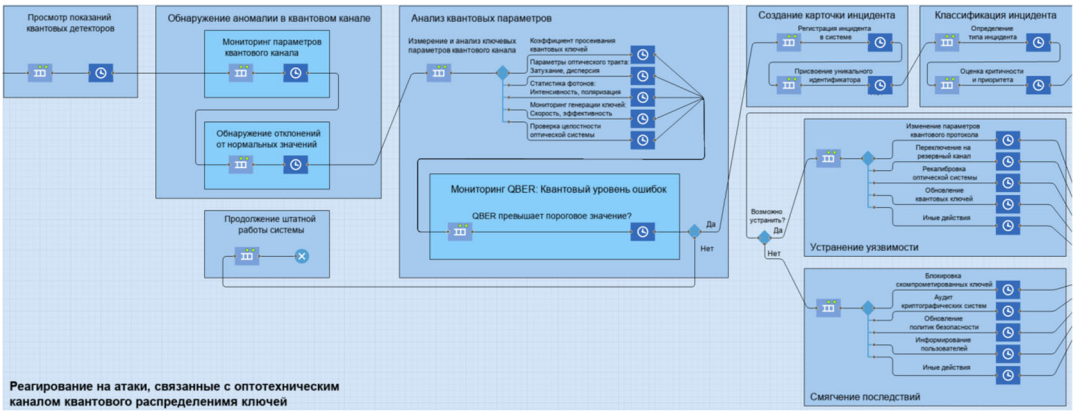

Рис. 2. Блок реагирования на атаки оптотехнического канала КРК

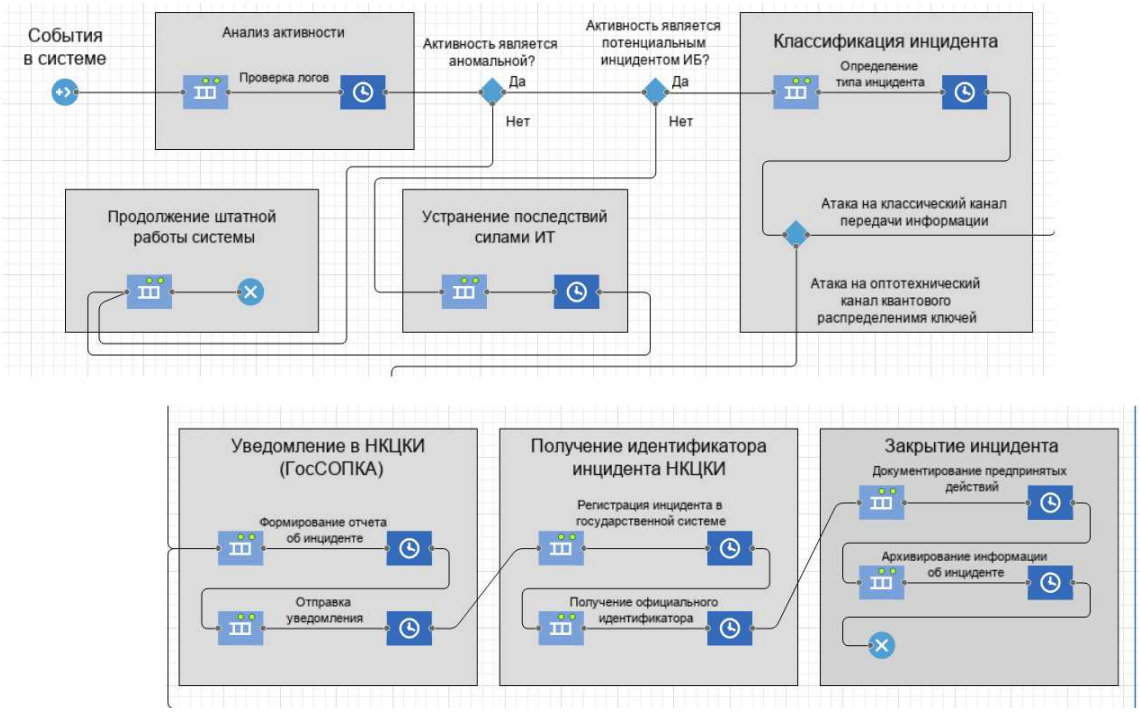

Рис. 3. Общий блок реагирования на атаки передачи информации

Оценка эффективности

Эффективность моделей оценивалась по формуле:

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

где $P_{св.сб}$ – вероятность своевременного сбора всей необходимой для принятия решений информации; $P_{пр}$ – вероятность правильного принятия решений; $P_{св.пр}$ – вероятность своевременного и правильного принятия решений; $P_р$ – вероятность своевременной реализации принятых решений.

Результаты моделирования после 19 126 прогонов представлены в табл.1.

Таблица 1

Сравнительный анализ моделей

Показатель	Гибридная модель	Классическая модель	Квантовая модель
Среднее время цикла, мин	34,17	24,80	29,40
Минимальное время, мин	1,31	4,10	15,20
Максимальное время, мин	132,25	144,40	112,50
Wэ	0,79	0,38	0,34

Гибридная модель демонстрирует меньшее время цикла (на 30 % по сравнению с классической и на 15% – с квантовой) и более высокую эффективность (Wэ = 0,79, против классической Wэ=0,38 и квантовой Wэ=0,34), что подтверждает ее преимущество.

Заключение

В результате исследования была разработана гибридная имитационная модель процесса обработки инцидентов информационной безопасности в оптотехнических системах с использованием технологии КРК, отличающаяся от рассмотренных подходов реагирования на классический и квантовый каналы передачи информации. Патент RU 2022663610 C1 важен для исследования систем КРК, так как предлагает имитационное моделирование трехуровневого управления, обеспечивающее комплексную метрологическую оценку производительности и надежности систем управления инцидентами в оптотехнической инфраструктуре. Определены ключевые решения, а также изучены подходы к процессу обработки инцидентов в разных каналах передачи информации. Оценка эффективности показала превосходство гибридной модели: Wэ = 0,79, против классической Wэ=0,38 и квантовой Wэ=0,34. Реализация предложенной модели обеспечит высокий уровень безопасности КРК-систем, позволяя эффективно реагировать на инциденты и оптимизировать проектирование защищенных оптотехнических решений для различных приложений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Голдобина А.С. Выбор имитационной модели процессов управления защитой информации для оценки эффективности государственных и муниципальных систем / А. С. Голдобина // Доклады ТУСУР. – Томск : ТУСУР, 2018. – Т. 21, №2. – С. 51-58.

2. Патент № 2747626 C1 Российская Федерация, МПК G05B 15/02. 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».

3. Свидетельство о государственной регистрации программы для ЭВМ № 2022663610 Российская Федерация. Имитационная модель процессов трехуровневого автоматизированного управления техническими средствами № 2461859-1 : № 2022660418 : заявл. 07.06.2022 : опубл. 18.07.2022 / В. А. Селифанов, А. В. Селифанов, В. В. Селифанов ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

4. Патент № 2764458 C1 Российская Федерация, МПК H04L 9/08. Способ распределения симметричных ключей между узлами вычислительной сети с системой квантового распределения ключей : № 2021113834 : заявл. 17.05.2021 : опубл. 17.01.2022 / М. А. Бородин, А. С. Рыбкин ; заявитель Акционерное общество «Информационные технологии и коммуникационные системы».

5. Об оценке эффективности защиты от оптических атак на волоконные квантовые криптографические системы выработки и распределения ключей / Дворецкий Д. А., Зазыкин А. П. // Научно-технический журнал «Фотон-Экспресс», 2023 г. : сборник материалов в 1 томе / МГУ им. М.В. Ломоносова. – Москва : МГУ им. М.В. Ломоносова, 2023 г. – С. 59-60.

6. Yuan Z. et al. Practical quantum key distribution with enhanced security // Phys. Rev. A. 2016. – P. 1-6.

7. Weier H. et al. Trojan-horse attacks on quantum key distribution systems // New J. Phys. 2011.– P. 8-12.

8. Исследование уязвимости систем квантового распределения ключей от атак с лазерным повреждением оптических компонентов на основе устройства с разрушающимся зеркалом / С.В. Алферов // Письма в Журнал технической физики. – Москва : Физико-технический институт им. А.Ф.Иоффе Российской академии наук, – 2023. – Т. 49, №5. – С. 43-46.

9. Моделирование 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.

10. AnyLogic. Справочное руководство по библиотеке моделирования процессов [Электронный ресурс]. – URL: https://anylogic.help/ru/library-reference-guides/process-modeling-library/index.html.

© Е. Ю. Солдатов, В. В. Селифанов, 2025