УДК 004.056.5
DOI 10.33764/2618-981X-2025-6-205-212

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

Оценка угроз и уязвимостей информационной безопасности в оптотехнических системах с использованием технологии квантового распределения ключей

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

Аннотация. В статье рассматривается проблема оценки угроз и уязвимостей информационной безопасности в оптотехнических системах, использующих технологию квантового распределения ключей (КРК). Проведён анализ патентов, определены два ключевых документа, пригодных для разработки системы управления угроз. Изучены подходы к оценке угроз, среди которых обоснована применимость методики ФСТЭК России 2021 года. Описаны типичные угрозы КРК-систем, такие как атака с расщеплением по числу фотонов, атака «троянский конь» и ослепление детекторов, с примерами их реализации. Подтверждена необходимость компьютерного моделирования для анализа угроз. Разработаны три модели: эталонная (дискретно-событийная), с топологией «Звезда» и «Точка-Точка». Сравнительная оценка показала, что эталонная модель превосходит модели, построенные по другим топологиям, по времени цикла на 40 % и на 59 % соответственно, по показателю эффективности – на 15 % и 28 % соответственно, что делает её перспективной для повышения безопасности КРК-систем.

Ключевые слова: информационная безопасность, уязвимости, имитационное моделирование, оценка угроз

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

Assessment of threats and vulnerabilities of information security in optotechnical systems using quantum key distribution technology

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

Abstract. The paper deals with the problem of assessing threats and vulnerabilities of information security in optotechnical systems using quantum key distribution (QKD) technology. Patents are analyzed, two key documents suitable for the development of threat management system are identified. Approaches to threat assessment are studied, applicability of the FSTEC of Russia 2021 methodology is substantiated. Typical threats to 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 for threat analysis is confirmed. Three models were developed: a reference model (discrete-event), with Star topology and Point-to-Point topology. Comparative evaluation showed that the reference model outperforms the alternatives in terms of cycle time (1.665 min) and efficiency (We = 0.23), which makes it promising for improving the security of AAC systems.

Keywords: information security, vulnerabilities, simulation modeling, threat assessment

Введение

Оптотехнические системы с технологией квантового распределения ключей (КРК) обеспечивают высокий уровень защиты данных. Однако практическая ре-

ализация таких систем сталкивается с угрозами и уязвимостями, обусловленными аппаратными и программными ограничениями. Рост числа квантовых атак и требования нормативных документов, таких как методика ФСТЭК России, подчёркивают актуальность исследования [1-3].

Цель статьи — разработка и оценка имитационной модели для анализа угроз и уязвимостей в КРК-системах. Для достижения данной цели необходимо выполнить ряд задач, которые включают в себя анализ патентов, изучение подходов к оценке угроз, описание типичных атак, создание трёх моделей и их сравнение по эффективности.

Анализ патентной документации

Для разработки модели угроз проанализированы патенты: RU 2326442 C1 (2008) [4], RU 2503985 C2 (2014) [5], RU 2665096 C1 (2018) [6] и RU 2747626 C1 (2021) [7]. Они отражают развитие систем управления, применимых к информационной безопасности.

– RU 2326442 C1 предлагает метод оценки эффективности через частные показатели, полезный для анализа мер защиты.

– RU 2503985 C2 вводит двухуровневую архитектуру управления, повышая гибкость.

– RU 2665096 C1 расширяет функционал, включая защиту информации.

– RU 2747626 C1 интегрирует кибербезопасность, предлагая комплексное управление.

Патенты RU 2665096 C1 и RU 2747626 C1 выделены как наиболее релевантные для КРК благодаря двухуровневой архитектуре и возможностям анализа данных, что позволяет адаптировать их для мониторинга квантовых каналов и управления ключами.

Подходы к оценке угроз безопасности информации

Среди подходов к оценке угроз (методика ФСТЭК 2008 г., 2021 г., модели угроз CAPEC и ATT&CK) методика ФСТЭК России 2021 года выбрана как основная благодаря соответствию российским стандартам и структурированности. Данная методика включает следующие этапы:

– определение класса защищённости;
– анализ негативных последствий;
– выявление объектов воздействия;
– определение источников угроз;
– оценка способов реализации;
– оценка актуальности угроз.

Для КРК-систем методика может быть также адаптирована с учётом квантовых атак (например, PNS-атака, атаки на детекторы), что делает её оптимальной при условии расширения возможных объектов воздействия и списка возможных угроз.

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:

• PNS-атака: использование многофотонных импульсов для перехвата ключей. Для примера можно привести ситуацию, когда в 2021 году команда Российского квантового центра продемонстрировала PNS-атаку на систему с длиной канала 50 км, получив 15 % ключевой информации [8]. Также другой эксперимент Diamanti, E et al. (2016) [9] подтвердил эффективность PNS-атак в системах с ослабленными лазерными импульсами. При длине канала 50 км атакующий получал до 30 % ключевой информации, используя квантовую память для хранения перехваченных фотонов;

• атака «троянский конь»: зондирование импульсами для раскрытия состояния системы. Для примера актуальности данной атаки можно привести работу автора Henning Weier и его коллег (2011) [10], в которой было показано, что атака «троянский конь» позволяет восстановить до 60 % ключа в системах без оптических изоляторов. Импульсы мощностью 0,5 мВт вызывали измеримые отражения, раскрывающие состояние фазовых модуляторов;

• ослепление детекторов: подавление детекторов для навязывания ключей. В 2010 году международная группа исследователей (Lydersen et al.) продемонстрировала успешную атаку на коммерческую систему QKD (ID Quantique), используя ослепление детекторов. Злоумышленники подавали импульсы мощностью 1 мВт, что привело к полному контролю над генерацией ключа без генерации ошибок [11].

Все вышеперечисленные примеры подтверждают необходимость анализа угроз через моделирование.

Необходимость разработки компьютерной модели

Разработка компьютерной модели для оценки угроз и уязвимостей в оптотехнических системах с использованием технологии КРК обусловлена следующими причинами.

1. Любая обработка данных требует защиты: в любых системах, где осуществляется обработка информации, включая КРК, необходимо строить систему защиты для предотвращения утечек и атак, что подтверждается нормативными требованиями, такими как приказы ФСТЭК России № 21 [12] и № 31.

2. Снижение затрат: проведение экспериментов на реальных системах дорого и трудозатратно, что делает моделирование экономически выгодной альтернативой.

3. Оптимизация проектирования: моделирование позволяет заранее симулировать атаки и разрабатывать эффективные контрмеры, упрощая проектирование защищённых систем передачи данных.

Модель обеспечивает анализ специфических угроз и повышает надёжность КРК-систем, что особенно важно в условиях роста квантовых атак.

Построение моделей

Разработаны три модели в программной среде AnyLogic [13]. Это российская платформа для имитационного моделирования, поддерживающая три известных моделирования:

– системная динамика;

– дискретно-событийное моделирование;

– агентное моделирование

– Эталонная модель: основана на дискретно-событийном подходе, включает сбор данных, принятие решений и реализацию мер защиты (рис. 1–3).

– Топология «Звезда»: централизованная система с единым аналитическим ядром.

– Топология «Точка-Точка»: децентрализованная система с автономным анализом узлов [14].

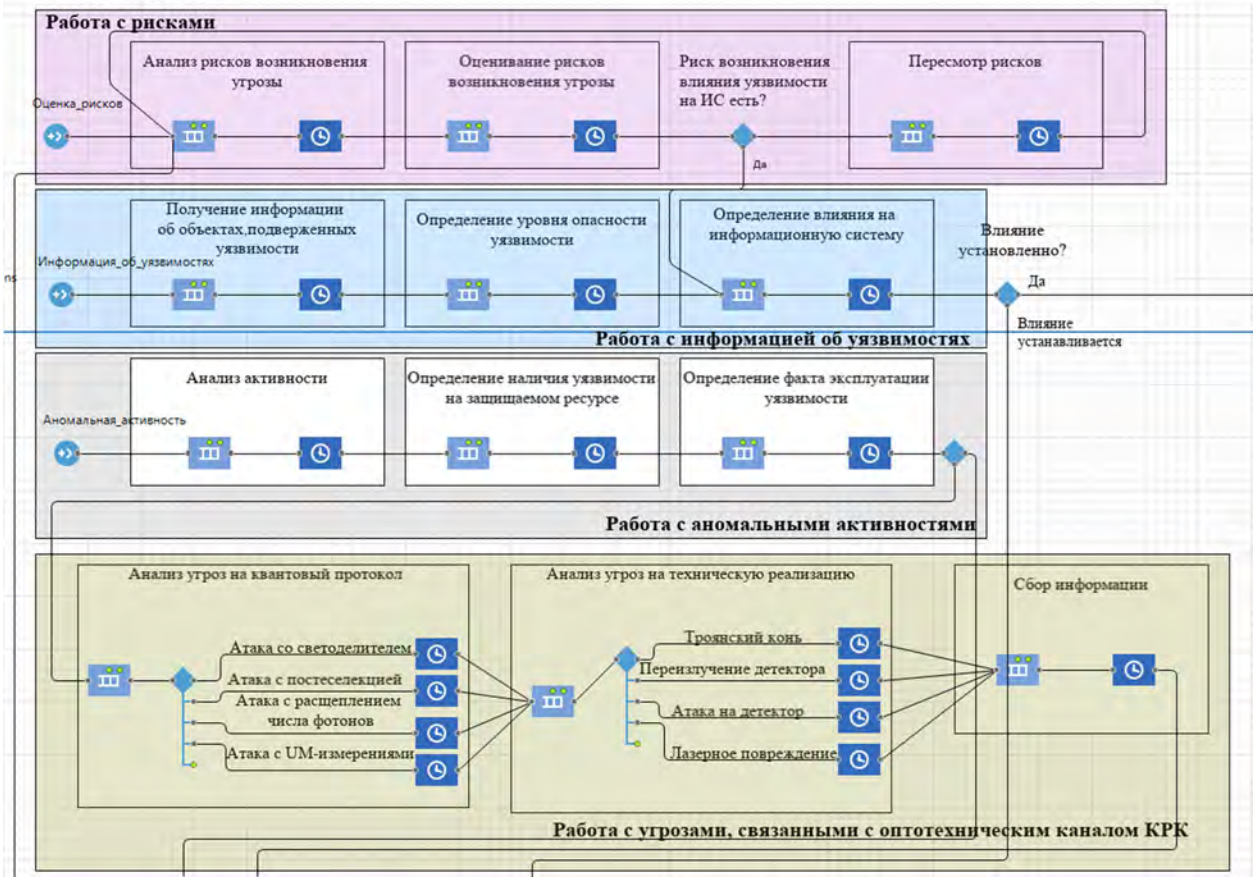

Рис. 1. Фрагмент модели системы управления угрозами – блоки с анализом поступающей информации

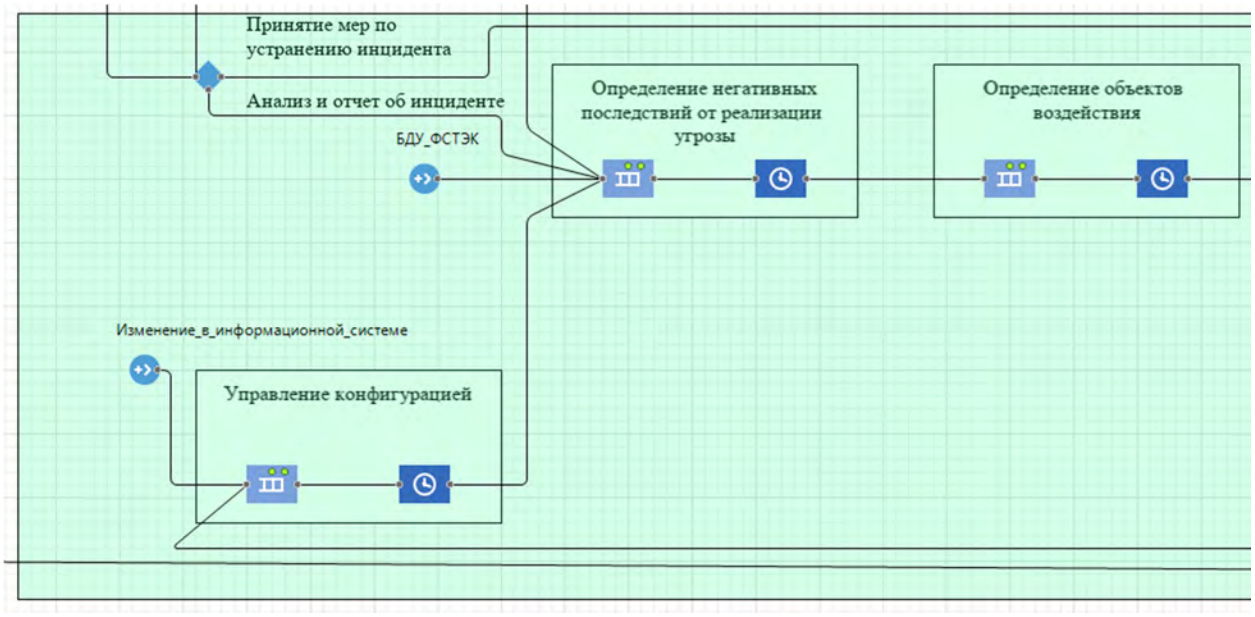

Рис. 2. Фрагмент модели системы управления угрозами – блок с выявлением актуальных угроз

Рис. 3. Фрагмент модели системы управления угрозами – блок работы с устранением выявленных уязвимостей

Разработанная модель имеет основные изменяемые параметры, а именно [14]:

– интенсивность прибытия агентов, определяющая как часто будут поступать события в систему;

– вместимость очереди событий, поступающих в систему;

– время задержки события, поступающего в систему, до его обработки. Данные параметры имеют своё отражение в реальной системе управления угрозами. Интенсивность прибытия может быть настроена на основе статистики поступления событий в реальной системе. Вместимость очереди подразумевает очередь обработки поступивших событий в реальной системе. Время задержки учитывает среднее время жизни события до полной его обработки в реальной системе.

Далее для построенных моделей была проведена оценка эффективности для выявления того варианта, который по конкретным показателям окажется более эффективным в работе.

Оценка эффективности

Эффективность моделей измерялась формулой [15]:

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

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 после 17211 запусков моделей представлены в табл. 1.

Таблица 1

Сравнительный анализ моделей

Показатель	Эталонная модель	Топология «Звезда»	Топология «Точка-Точка»
Среднее время цикла, мин	1,665	2,8 ± 0,3	4,1 ± 0,5
Минимальное время, мин	0,104	0,3	0,7
Максимальное время, мин	9,030	12,4	8,9
Wэ	0,23	0,2	0,18

Эталонная модель демонстрирует меньшее время цикла (на 40 % по сравнению с «Звездой» и на 59 % с «Точка-Точка») и более высокую эффективность (15 % и 28 % соответственно), что подтверждает её преимущество.

Заключение

В результате исследования была разработана эталонная имитационная модель оценки угроз и уязвимостей в оптотехнических системах с использованием технологии КРК, отличающаяся от рассмотренных топологий «Звезда» и «Точка-Точка». Проведён анализ патентной документации, определены ключевые реше-

ния, а также изучены подходы к оценке угроз, среди которых методика ФСТЭК 2021 года выбрана как оптимальная. Оценка эффективности показала превосходство дискретно-событийной модели (на 15 % и 28 % соответственно) над альтернативными вариантами. Реализация предложенной модели обеспечит высокий уровень безопасности КРК-систем, позволяя эффективно противодействовать специфическим угрозам и оптимизировать проектирование защищённых оптотехнических решений для различных приложений [16-20].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аверьянов В. С. О некоторых вопросах, идеях и технологических решениях в области квантового распределения ключей безопасности // Информационная безопасность : сб. докл. Всерос. Школы молодых ученых, Новосибирск, 14–18 нояб. 2022 г. – Новосибирск : СибГУТИ, 2022. – С. 34–39. – DOI 10.55648/978-5-91434-080-0-2022-34-39.

2. Алексеев А. Л., Егоров В. И., Щербаков А. Ю. Об одном способе защиты интерфейса взаимодействия квантовой аппаратуры распределения ключей и средств криптографической защиты информации // Вестник современных цифровых технологий. – 2021. – № 9. – С. 15–18.

3. 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.

4. Патент № 2326442 Российская Федерация, МПК G07C 3/00, G06F 17/00. Способ оценки эффективности управления и устройство для его осуществления : № 2007102742/09 : заявл. 24.01.2007 : опубл. 10.06.2008 / В. А. Селифанов, В. В. Селифанов ; заявитель Федеральное государственное военное образовательное учреждение высшего профессионального образования "Военный авиационный инженерный университет" (г. Воронеж) Министерства обороны Российской Федерации.

5. Патент № 2503985 Российская Федерация, МПК G05B 15/00. Способ двухуровневого управления техническими средствами и система для его осуществления : № 2012105841/08 : заявл. 17.02.2012 : опубл. 10.01.2014 / В. А. Селифанов ; заявитель Федеральное государственное военное образовательное учреждение высшего профессионального образования "Военный авиационный инженерный университет" (г. Воронеж) Министерства обороны Российской Федерации.

6. Патент № 2665096 Российская Федерация, МПК G05B 15/00. Способ двухуровневого управления и система для его осуществления (варианты) : № 2018113685 : заявл. 13.04.2018 : опубл. 28.08.2018 / В. А. Селифанов ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет».

7. Патент № 2747626 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».

8. Молотков С. Н. Побочные каналы утечки информации в квантовой криптографии: не строго однофотонные состояния, разные квантовые эффективности детекторов, конечные передаваемые последовательности // Журнал экспериментальной и теоретической физики. – 2021. – Т. 160, вып. 3 (9). – С. 327–365. – URL: http://www.jetp.ras.ru/cgi-bin/dn/r_160_0327.pdf (дата обращения: 24.04.2025).

9. Diamanti E. Practical challenges in quantum key distribution / E. Diamanti, H.-K. Lo, B. Qi [et al.]. – Текст : электронный // npj Quantum Information. – 2016. – Vol. 2. – Article 16025. – DOI:

10.1038/npjqi.2016.25. – URL: https://www.nature.com/articles/npjqi201625 (дата обращения: 24.04.2025).

10. Weier H. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors / H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, H. Weinfurter. – Текст : электронный // New Journal of Physics. – 2011. – Vol. 13, № 7. – P. 073024. – DOI: 10.1088/1367-2630/13/7/073024. – URL: https://ui.adsabs.harvard.edu/abs/2011NJPh...13g3024W (дата обращения: 24.04.2025).

11. Lydersen L. Hacking commercial quantum cryptography systems by tailored bright illumination / L. Lydersen, C. Wiechers, C. Wittmann [et al.]. – Текст : электронный // Nature Photonics. – 2010. – Vol. 4. – P. 686–689. – DOI: 10.1038/nphoton.2010.214. – URL: https://www.nature.com/articles/nphoton.2010.214 (дата обращения: 24.04.2025).

12. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. — 2013. — № 107.

13. Справочное руководство по библиотеке моделирования процессов. AnyLogic, 2024.

14. Методика оценки угроз безопасности информации. ФСТЭК России, 2021.

15. Шабурова А. В., 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 : учебное пособие. – Новосибирск : СГУГиТ, 2020. – 70 с.

16. Хабр. Топология физических связей [Электронный ресурс]. – URL: https://habr.com/ru/articles/850834/ (дата обращения: 20.04.2025).

17. 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.

18. 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 го-да. – 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.

19. 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.

20. Габдулхаков И. М. Принципы построения универсальной системы квантового распределения ключей с частотным кодированием на основе амплитудной модуляции и фазовой коммутации / И. М. Габдулхаков, О. Г. Моро-зов // Актуальные вопросы телекоммуникаций : Научно-техническая конференция Росинфоком-2017, Самара, 01 сентября 2017 года / Федеральное агентство связи; 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.