Федеральное агентство воздушного транспорта
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет гражданской авиации» (МГТУ ГА)
Факультет прикладной математики и вычислительной техники
Кафедра основ радиотехники и защиты информации

Разработка рекомендаций по обеспечению мер защиты информации и минимизации рисков использования технологий квантовой криптографии и квантовых сетей при использовании SMART-технологий

Колесникова Дарья Сергеевна
Очная форма обучения
Информационная безопасность телекоммуникационных систем
4 курс, группа БИ 4-1

Романчева Нина Ивановна
кандидат технических наук
доцент

Москва 2021

Содержание

Введение

Эффективность деятельности предприятий в значительной степени зависят от наличия систем информационных и связных технологий (ICT), а также от точности и конфиденциальности данных. В условиях рыночной экономики у авиапредприятий все больше проявляется необходимость в защите разного рода информации — базы данных сотрудников, клиентов и поставщиков, собственных разработок, бизнес-информации и др. Технологические достижения в IT-сфере позволяют создать системы безопасности, которые постоянно совершенствуются, эволюционируют, адаптируются и сами ищут новые способы предотвратить прежде неизвестные виды атак. Однако, активное внедрение систем искусственного интеллекта (ИИ), SMART-технологий заставляет пересмотреть подходы к обеспечению информационной безопасности авиапредприятия. Кроме того, в соответствии с ФЗ № 187 "О безопасности критической информационной инфраструктуры Российской Федерации", необходимо предусмотреть меры информационной безопасности при передаче данных на предприятиях гражданской авиации в связи со стремительно возрастающим потенциалом использования SMART-технологий для проведения кибератак. Все это делает данное исследование актуальным.

Данная работа связана с исследованием перспективного направления криптографии - квантовой криптографии, в обеспечении безопасности информационных систем транспортных предприятий, представляющего собой качественно новое решение в условиях растущей тенденции к применению ультрасовременных технологий для получения несанкционированного доступа к конфиденциальной информации. Высокая надежность квантовой криптографии является её неоспоримым преимуществом, однако для полноценного практического внедрения необходимо провести анализ уязвимостей данной технологии и разработать рекомендации по обеспечению мер защиты информации и минимизации рисков её использования в условиях развития SMART-технологий.

Раздел 1. Анализ технологий квантовой криптографии и квантовых сетей в гражданской авиации
Перспективные SMART-технологии

Технологические достижения в IT-сфере позволяют создать системы безопасности, которые постоянно совершенствуются, эволюционируют, адаптируются и сами ищут новые способы предотвратить прежде неизвестные виды атак. Именно это и является основным прорывом - их способность не допустить кибер-атаки. Однако следует отметить ряд технологий, которые меняют взгляды на информационную безопасность:

1. Биометрическая идентификация пассажиров. Биометрическая идентификация пассажиров занимает ведущее место в списке SMART технологий и является наиболее динамично развивающейся из внедряемых в аэропортах мира. К ней относятся идентификация по лицу и различные биометрические методы, например, идентификация по отпечаткам пальцев. Так же развитию этой технологии активно способствует бесконтактный способ получения сведений и широкий выбор источников распознавания пользователей, такие как видеоряды, фотографии, данные видеонаблюдения.

2. ИИ как средство аналитики. ИИ на сегодняшний день находит все больших применений в самых различных сферах деятельности человека, в том числе и в аэропортах. По данным SITA, 61% аэропортов рассмотрят проекты внедрения ИИ в течение следующих трех лет с целью оптимизирования системы прогнозной аналитики и повышения пропускной способности аэропорта. В этом случае, ИИ поможет проводить мониторинг процессов аэропорта и улучшит понимание того, что в нем происходит сейчас и что будет происходить.

3. Использование роботов в аэропортовой деятельности. Роботы уже давно перестали быть новинкой и все более широко применяются в сфере обслуживания. Например, в аэропорту Женевы разработанный SITA робот Лео помогает пассажирам с регистрацией и перемещением багажа.

4. Блокчейн. Технология блокчейн также весьма перспективна для использования в аэропорте. Сфера применений очень обширна — от распространения билетов до идентификации пассажиров и ускорения обслуживания часто летающих клиентов. Всё это позволяет значительно увеличить пропускную способность аэропорта.

В таких условиях сложность задачи построения системы защиты информации обусловлена рядом факторов:

- разнообразием типов задач, которые могут решаться;

- разнообразием типов и моделей бизнес-процессов;
- разнообразием технических средств;
- наличием неопределенностей, увеличивающимся противодействием со стороны киберпреступников, и динамично изменяющейся в процессе выполнения задания обстановкой;
- при использовании классических методов защиты информации планирования требуются затраты времени, что снижает степень оперативности при принятии решений.

С развитием «умных технологий» и переходом на программно-определяемые сети (Software Defined Networking, SDN) подмена программного кода становится практически незаметной для широкого круга специалистов по информационной безопасности [1].

Анализ современных направлений в криптографии

Современные криптографические системы для получения шифрованных сообщений чаще всего используют методы сложения (по неким правилам) передаваемой информации со специальным секретным ключом, известным отправителю и получателю [2]. Теоретически доказано, что при выполнении определенных условий (ключ должен быть не короче сообщения, абсолютно случаен, и использован только один раз) можно получить так называемый «абсолютно стойкий ключ» (АСК), то есть такой, не обладая которым невозможно разгадать шифротекст, полученный с его помощью [3].

Таким образом, проблема поиска «идеального» ключа была теоретически решена, но на практике возникла ещё одна не менее важная: необходимость обеспечения секретности во время обмена ключами между легитимными пользователями. Эту проблему называют проблемой распространения ключа.

Квантовая криптография — направление в криптографии, решающее проблему распространения ключа с позиций квантовой физики. Процесс отправки, передачи и приема информации выполняется физическими средствами, в частности, при помощи фотонов в линиях волоконно-оптической связи, а подслушивание может рассматриваться как измерение физических объектов — носителей информации. Технология квантовой криптографии опирается на принципиальную неопределенность поведения квантовой системы — невозможно измерить один её параметр, не исказив

другой, и дублировать неизмеренное квантовое состояние. Таким образом, любая попытка измерения взаимосвязанных параметров в квантовой системе вносит в нее нарушения, и полученная в результате такого измерения информация определяется принимающей стороной как дезинформация [2].

Квантовая криптография решает несколько задач, среди которых разработка физических алгоритмов получения АСК, проектировка и создание практических систем, использующих эти алгоритмы, обнаружение присутствия нелегитимных пользователей канала связи, а также проверка полученного ключа на наличие ошибок и их устранение.

В предложенных к настоящему времени методах квантового кодирования информации чаще всего используются поляризация излучения или его фаза [3], при кодировании может быть использовано различное число квантовых состояний. В зависимости от этого применяются различные алгоритмы формирования АСК, называемые протоколами, хотя общая идея всегда остается неизменной. Обмен сообщениями между легитимными пользователями происходит по двум каналам связи: квантовый является защищенным и используется для передачи информации с использованием квантовых частиц; открытый – свободно прослушиваемым.

На практике же возникает целый ряд проблем. Во-первых, существующие высокочувствительные приёмники излучения неизбежно характеризуются некоторым уровнем шумов, который в экспериментальных системах может быть достаточно низким для наличия возможности эффективной работы устройства, но весьма высоким для того, чтобы перехватчик мог маскировать свои действия под шумы. Во-вторых, низкая квантовая эффективность приёмника и поглощение в волоконных линиях связи, использующихся в качестве квантового канала, также усиливают реальные возможности перехватчика остаться незамеченным. Проблема, связанная с возможностью злоумышленника маскироваться под шумы, была частично решена разработкой специальных алгоритмов анализа количества ошибок в ключе и их устранения [4]. В-третьих, нельзя забывать о том, что обладание даже малой частью ключа не исключает возможности расшифровки всего сообщения. Кроме того, на сегодняшний день не были созданы источники света, имеющие возможность испускать одиночные фотоны, а используемые приёмы ослабления не дают абсолютной гарантии наличия в импульсе не более чем одного фотона.

Таким образом, квантовая криптография рассматривается как один из самых перспективных методов защиты информации вследствие того, что теоретические выкладки указывают на возможность создания системы с единичной вероятностью обнаружения нелегитимного пользователя при

осуществлении им неправомерного перехвата информации [3, 5, 6]. Использование таких технологий в аэропортовой деятельности с одной стороны, значительно повысит уровень информационной безопасности, с другой стороны, ограничение на передачу данных не позволит соединить несколько аэропортов квантовыми системами.

Раздел 2. Исследование уязвимостей и разработка модели оценки рисков информационных систем, построенных на технологиях квантовой криптографии и квантовых сетей в системах управления гражданской авиации при использовании SMART-технологий

В результате проведенного в первом разделе исследования было установлено, что рассматриваемые технологии квантовой криптографии и квантовых сетей на текущий момент являются одними из самых перспективных направлений в обеспечении информационной безопасности объектов гражданской авиации. Выявление специфических особенностей проведения оценки защищенности является тем основанием, на котором строятся все остальные аспекты исследования, проводимые во втором разделе.

Информационные системы предприятий гражданской авиации стремительно усложняются вследствие увеличения числа потоков обмена данными (рис. 1), включающих передачу конфиденциальной информации [7].

Рисунок 1 - Схема информационных потоков авиапредприятия

В соответствии с классификацией Банка данных угроз безопасности информации ФСТЭК следует упомянуть соответствующие УБИ.069 и

УБИ.111 [8]. В таком случае в качестве методов защиты применяются различные аппаратные средства, основанные на физической природе информационных сигналов. Внедрение криптографических средств являлось оправданно распространенным методом защиты до тех пор, пока активно развивающиеся технологии ИИ и квантовых компьютеров не смогли справиться с невозможностью эффективного вычислительного решения математических задач, которые определяли надежность данных средств. В сентябре 2019 года на сайте NASA был размещен доклад специалистов Google о возможностях разработанного ими квантового компьютера произвести за считанные минуты вычисления, на которые самому мощному в мире суперкомпьютеру Summit (IBM) потребовалось бы 10 тыс. лет [9]. Еще одним фактом, на который стоит обратить внимания, является постоянный рост «безопасного размера» ключей ассиметричного шифрования. За последние 20 лет он увеличился в 10 раз, когда как для систем симметричного шифрования длина ключа увеличилась немного менее чем в два раза. К усложнению информационных систем КИИ также приводит стремительный поток технологических инноваций, который «вынуждает оцифрованное человечество приспосабливаться к жизни в VUCA-мире» [10].

Проведенный в первом разделе анализ литературы показал, что вышеперечисленные недостатки существующих каналов связи и асимметричной криптографии отсутствуют в системах квантовой коммуникации в связи с их фундаментальными особенностями, однако проведенный анализ литературы [11-15] выявил и позволил классифицировать другие предположительные атаки на квантовые криптосистемы (рис. 2).

Атака с помощью светоделителя [11]	Данная атака заключается в сканировании и расщеплении импульсов на две части и анализе каждой из частей в одном из двух базисов.
Атака «Троянский конь» [12]	Данная атака заключается в сканировании импульса через оптический мультиплексор по направлению к стороне-отправителю или стороне-получателю. Импульс делится на две части для синхронности детектирования и поступает на схему декодирования, при этом искажение передающихся фотонов не происходит.
Когерентная атака для случая однофотонных сигналов [13]	Когерентные атаки основаны на тактике ретрансляции кубитов и заключаются в перехвате фотонов от стороны-отправителя, измерении их состояний, замене пересылаемых фотонов на псевдофотоны в измеренных состояниях и отправке измененных данных стороне-получателю.
Некогерентная атака для случая однофотонных сигналов [13]	Некогерентные атаки заключаются в перехвате фотонов от стороны-отправителя, перепутывании пробы с целой группой передаваемых одиночных фотонов, измерении ее состояния и отправке измененных данных стороне-получателю.
Атака с «ослеплением» лавинных фотодетекторов [14]	Перехватывающей стороне становится доступен секретный ключ, при этом наблюдаемые статистики фотоотчетов остаются неизменны у стороны-получателя.
Атака путем разделения числа фотонов [15]	Данная атака заключается в обнаружении в импульсе более одного фотона, отведении его, перепутывании с пробой и отправке оставшейся неизмененной части информации стороне-получателю, при этом перехватывающая сторона получает точное значение переданного бита без внесения ошибок в просеянный ключ.

Рисунок 2 - Примеры атак на квантовые криптосистемы

Одним из важных шагов в обеспечении ИБ является грамотная оценка рисков существующих систем, происходящая по определенным алгоритмам. Основные методологии оценки рисков приведены в работах [16, 17].

На практике широко применяется метод качественной оценки рисков, заключающийся в присвоении определенным параметрам риска значения, соответствующего одной из заранее оговоренных качественных категорий, представленный на рисунке 3 и соответствующий действующим международным стандартами ISO/IEC 27005:2011 и ISO 31000:2009. Данный метод позволяет лишь поверхностно расставить приоритеты для рационализации способов защиты и не дает четких результатов, способных однозначно установить размер инвестиций в информационную безопасность.

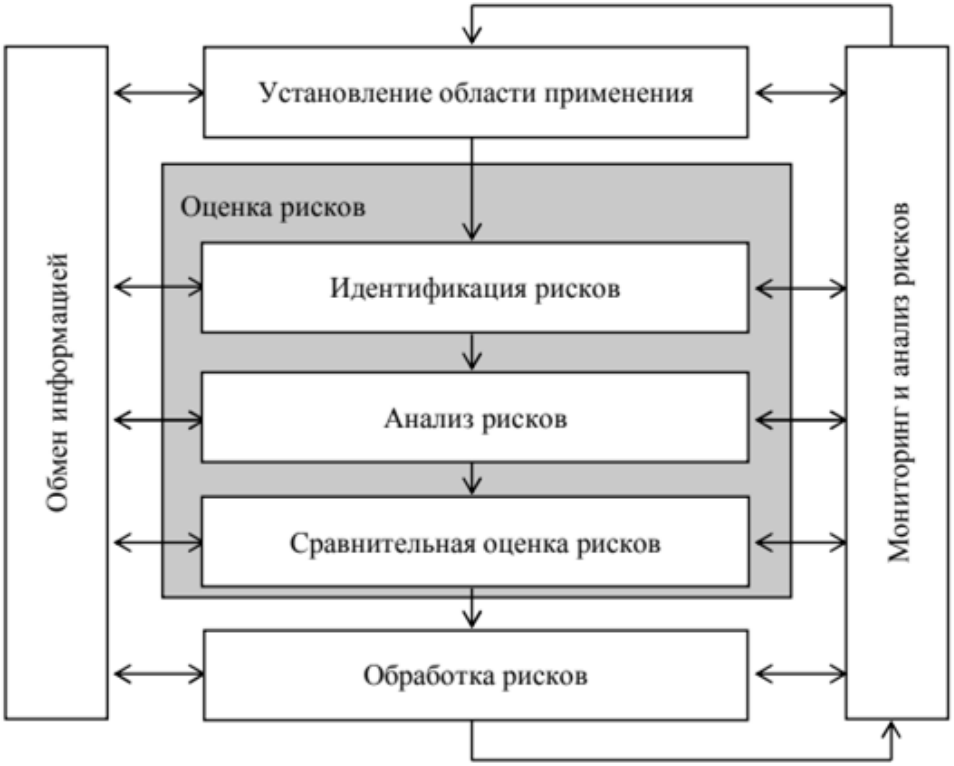

Рисунок 3 – Алгоритм качественного метода оценки рисков информационной безопасности

В работе [18] приведены уязвимости и рассчитаны риски степени потенциального ущерба при реализации угроз на активы и вероятности реализации угроз для типовой информационной системы телекоммуникационного предприятия. В [11] описывается атака с помощью светоделителя, но устойчивость квантовой криптосистемы очень высокая. В литературе [12] сказано, что для совершения атаки «Троянский конь» необходимо использовать мультиплексор, чтобы дублировать информацию, не искажая её, но в литературе [19] показано, что при одновременном использовании изоляторов и детекторов-стражей злоумышленнику будет гораздо сложнее бороться сразу с двумя контрмерами и пытаться выйти сразу

за два спектральных диапазона. Атаки, описанные в [13] и [14], ввиду несовершенства оборудования, практически неосуществимы, отмечается в [20]. Самой серьезной уязвимостью является атака разделения числа фотонов [15], от которой можно защититься, лишь если уровень ошибок при передаче не превышает ~14%, но в таком случае очень сильно снизится скорость передачи ключа [20].

Большой недостаток таких методологий заключается в том, что они не учитывают стремительное развитие SMART-технологий. В [21] приводится пример ИИ, способного обеспечивать каналы не только для крайне быстрых атак, но и маломощных и медленных. ИИ сможет выступать в качестве инструмента, анализирующего скорость передачи данных, и прогнозировать, как на эту активность будут реагировать решения безопасности. Такие ИИ и другие SMART-технологии в руках злоумышленников значительно увеличивают вероятности реализации уязвимостей существующих каналов связи, а вместе с ними растет потребность в проведении более точной и гибкой оценки, качества которой позволят специалистам в области ИБ адаптироваться в условиях стремительной цифровизации.

Модернизация телекоммуникационной отрасли меняет модель угроз, в связи с этим существующую классическую модель оценки рисков необходимо улучшать. Вариант изменения существующей модели оценки рисков представлен на рисунке 4, при этом каждый из этапов требует большей корректировки с каждым днем.

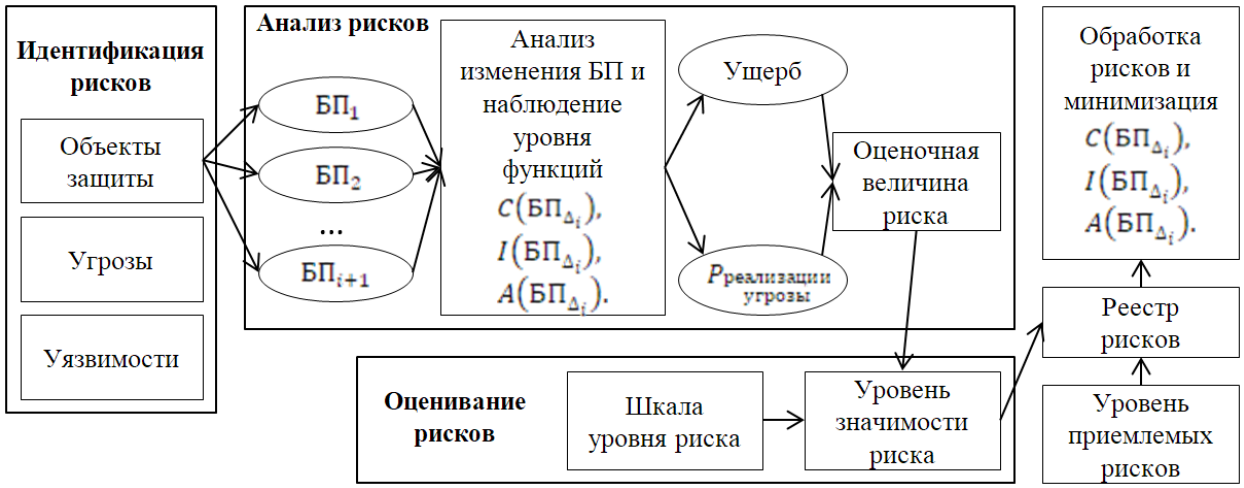

Рисунок 4 – Вариант улучшенной модели оценки рисков

В качестве дополнительных показателей оценки предлагаются функции: $C(\text{БП}_{\Delta_i})$ – нарушение конфиденциальности, $I(\text{БП}_{\Delta_i})$ – нарушение целостности, $A(\text{БП}_{\Delta_i})$ – нарушение доступности, вызванные динамическими изменениями бизнес-процессами, обусловленные постоянным ростом развития ИТ-сферы и отражающие влияние нарушений конфиденциальности, целостности и доступности соответственно на бизнес-процессы.

Математически функции $C(\text{БП}_{\Delta_i})$, $I(\text{БП}_{\Delta_i}), A(\text{БП}_{\Delta_i})$ представляют собой степень деструктивизации состояний БП и являются ключевыми параметрами, определяющими результат оценивания рисков ИБ.

Для предприятий гражданской авиации на рисунке 5 представлены БП системного уровня модели деятельности в соответствии с их классификацией и исследованные в первом разделе SMART-технологии, которые при внедрении окажут на них наибольшее влияние.

Классификация БП	БП
Процессы управления	Стратегическое управление (планирование и контроль деятельности всех департаментов АК)
	SMART-технологии: искусственный интеллект
Основные процессы	Обслуживание службами аэропортов
	SMART-технологии: биометрическая идентификация пассажиров, искусственный интеллект, роботы, блокчейн
	Маркетинг и продажи услуг авиакомпании
	SMART-технологии: искусственный интеллект, блокчейн
Обеспечивающие процессы	Управление финансами
	SMART-технологии: искусственный интеллект
	Управление человеческими ресурсами
	SMART-технологии: искусственный интеллект

Рисунок 5 - Процессы системного уровня авиакомпании

Самому большому изменению будет подвергнуто обслуживание службами аэропорта (в основном регистрация пассажиров и багажа). Увеличится пропускная способность аэропорта, качество скорость обслуживания, но при этом высока вероятность возникновения уязвимостей, приводящих к утечке конфиденциальной информации или к созданию условий для преднамеренного отказа информационных систем, что приведет к появлению финансовых и репутационных негативных последствий. То же самое относится к применению технологий ИИ в качестве инструмента аналитики для совершенствования процессов стратегического управления, маркетинга и продажи услуг, управления финансами и человеческими ресурсами.

Таким образом, становится очевидным необходимость усовершенствования существующей модели оценки рисков путем внедрения дополнительных этапов, учитывающих значительное влияние развивающихся SMART-технологий на БП и прогнозирующих изменение существующих на данный момент рисков, вызванное таким глобальной научной разработкой, как квантовые вычисления. Возникает потребность в поиске более эффективных методов защиты от возрастающих угроз и корректированию уже используемых.

Раздел 3. Разработка рекомендаций по обеспечению мер защиты информации и минимизации рисков использования технологий квантовой криптографии и квантовых сетей при использовании SMART-технологий

В третьем разделе поставлена задача разработки рекомендаций по обеспечению мер защиты информации и минимизации рисков квантовой криптографии и квантовых сетей при использовании SMART-технологий, что подразумевает более подробный разбор явлений, описанных во втором разделе, а также функций, предложенных для использования в усовершенствованной модели оценки рисков. Для рассмотрения были выбраны БП верхнего уровня авиакомпании, для которых существуют или разрабатываются инновационные решения, основанные на самых перспективных на данный момент SMART-технологиях: биометрическая идентификация, ИИ, роботы и блокчейн. Кратко они были освещены в первом разделе в качестве подтверждения наблюдаемой тенденции к разнообразному и ускоренному обновлению многих процессов авиакомпании, однако для поставленной в третьем разделе задачи необходимо конкретизировать каждое внедрение в БП (рис. 6).

SMART-технологии / Бизнес-процессы		Блокчейн		Искусственный интеллект		Биометрическая идентификация	Робототехника	
Процессы управления	Стратегическое управление	*I*	*C*	*A*	*C*			
	Оперативно-тактическое управление	*I*	*C*	*A*	*C*			
	Организационное управление	*I*	*C*	*A*	*C*			
	Управление качеством	*I*	*C*	*A*	*C*		*A*	*C*
	Управление персоналом	*I*	*C*	*A*	*C*	*C*	*A*	*C*
Основные процессы	Сервис на борту ВС	*I*	*C*	*A*	*C*			
	Обеспечение безопасности полетов	*I*	*C*			*C*		
	Обслуживание службами аэропорта	*I*	*C*	*A*	*C*	*C*	*A*	*C*
Вспомогательные процессы	Учет и отчетность	*I*	*C*					
	Правовое обеспечение	*I*	*C*					
	Документационное обеспечение	*I*	*C*					

- увеличение функции; - уменьшение функции;
- неоднозначное изменение; - невозможность внедрения.

Рисунок 6 - Изменения функций деструктивизации состояний БП в зависимости от внедряемых SMART-технологий

Влияние SMART-технологий на функции деструктивизации основных БП

Следует начать с процессов управления, нацеленных на обеспечение согласованности основных и вспомогательных бизнес-процессов. Они подразумевают постановку и достижение целей долгосрочного и краткосрочного планирования, преобразование и детального управления ресурсами. В данные процессы могут быть вовлечены технологии ИИ с целью проведения анализа деятельности аэропорта в режиме реального времени и прогнозирования результатов неоднозначных экономических решений. Технология может взять на себя некоторые функции управления персоналом, принимая участие в обучении работников и своевременном уведомлении о решенных ситуационных задачах. Также ИИ может консультировать клиентов, анализировать их потребности и составлять портреты разных типов клиентов, чтобы предложить им соответствующие услуги, оценить качество выполнения и предполагать результаты проведения различных мероприятий [22]. С одной стороны, ИИ повысит доступность разнообразной актуальной информации (уменьшит функцию *A*) на территории аэропорта и обеспечит согласованность процессов управления, с другой стороны, появятся новые задачи по обеспечению конфиденциальности потоков персональной информации о пассажирах, сотрудниках и внутренней информации авиакомпании, представляющей интерес для злоумышленников (увеличение функции *C*). Значительно уменьшить угрозу конфиденциальности, возникающей из-за специфики каналов связи, может внедрение технологии квантовой криптографии, сводя вероятность реализации угрозы к минимуму. Для достижения эффективной деятельности авиакомпании также может быть внедрена технология блокчейна, которая обеспечит единый достоверный (снижение функции *I*) источник данных для использования не только внутри одной авиакомпании, но и во множестве связанных компаний одновременно, в связи с чем технология может оперировать самой различной информацией о множестве самых различных процессов. Для совершения транзакций и защиты проводных каналов связи так же, как и при внедрении предыдущей SMART-технологии, рекомендуется внедрить технологию квантовой криптографии. Следующая технология, роботы, влияют на такие БП, как управление качеством и управление персоналом. Во-первых, их использование подразумевает расширение штата обученных для их настройки и ремонта сотрудников и восполняет потребность компании увеличении скорости обслуживания клиентов и переноса грузов. Во-вторых, роботы могут быстро

собирать информацию о качестве оказанных услуг и, таким образом, помогать устранять причины неудовлетворенности клиентов. Явным плюсом данной технологии является значительное увеличение доступности информации (уменьшение функции *A*) по отношению к клиентам и сотрудникам компании, но минусом становится обеспечение конфиденциальности данных, передаваемых по проводным и беспроводным сетям. Стоит отметить, что в пределах одного аэропорта роботы могут передавать и принимать как не требующую серьезной защиты информацию, например, о состоянии или местонахождении устройства, так и персональные данные клиентов, в связи с чем определение требуемого уровня конфиденциальности и его обеспечение может быть совершенно различным. Намного более высокие требования у следующей технологии – биометрической идентификации. В процессах управления она затрагивает управление персоналом и вызывает необходимость подбора и обучения сотрудников для контроля нормальной работоспособности основанных на ней систем доступа в различные зоны аэропорта (уменьшение *C* – функции). Скорость и объемы передаваемых внутри систем по проводным каналам связи персональных данных, в свою очередь, приводят к потребности в организации их надежной защиты, которую в области передачи данных от серверов к терминалам может обеспечить внедрение технологии квантовой криптографии.

Следующими в базовой классификации описания бизнес-процессов верхнего уровня являются основные процессы. Наибольшее применение SMART-технологии нашли в БП, связанных с обслуживанием клиентов аэропорта, то есть в прямой взаимосвязи с процессами управления маркетингом, качеством и персоналом, что подробно было описано выше. Развитие проектов в данной области привело к значительному увеличению доступности необходимой для оказания услуг информации, а их персональный подбор, осуществленный при помощи ИИ, во многих случаях достаточная консультация виртуальных агентов и чат-ботов, актуальная информация о рейсах и услугах, предоставляемая авиакомпанией при помощи технологии блокчейн, уменьшение очередей и удобство прохождения обязательных процедур, обеспеченные биометрическими пропускными пунктами и роботами-помощниками, положительно влияют на комфортное пребывание клиента на территории аэропорта. Однако персонализация обслуживания и разнообразие точек доступа к персональным и коммерческим данным предоставляют злоумышленнику больше возможностей для нанесения атак.

Обслуживание клиентов продолжается на борту ВС и заключается, в первую очередь, в обеспечении безопасности полета. Одним из лучших

решений является биометрическая идентификация личности экипажа, а в случае внедрения технологии блокчейн для повышения целостности (уменьшение функции *I*) передаваемой и хранимой информации о рейсе. То же самое касается сервиса на борту ВС, но в таком случае речь идет о предпочтениях и пожеланиях конкретного пассажира, которые когда-либо были учтены авиакомпанией или были предложены системой ИИ (уменьшение функции *A*) в результате анализа имеющейся информации о клиенте. Таким образом, увеличение доступности и целостности, позволяющее повысить эффективность основных процессов авиакомпании, снова приводит к вынужденной модернизации систем информационной безопасности аэропорта.

Вспомогательные процессы в своей совокупности могут быть приведены в цифровой вид при помощи технологии блокчейн, что приведет к более прозрачному и эффективному документообороту, уменьшит долю ручных процессов заполнения и увеличит целостность информации (уменьшение функции *I*) [23]. Стоит учесть, что большая ее часть представляет собой коммерческую информацию, передаваемую по проводным каналам связи, для повышения конфиденциальности которой возможно применение технологии квантовой криптографии.

Таким образом, значительная часть атак, осуществимых в связи с внедрением SMART-технологий, невозможна в квантовых сетях, что представляет собой один из самых эффективных методов защиты информации. Предотвращаются атаки вида “adversarial examples” и подмены данных на этапе обучения ИИ, которые приводят к принятию неверных решений и выполнению неучтенных команд и основаны на возможности передачи специфических данных от злоумышленника к системе [24]. В случае с технологией биометрической идентификации сводится к минимуму возможность совершения атак на межсоединения системных модулей: троянов, атаки «человек посередине» и атаки воспроизведения [25]. При использовании технологии блокчейн защита системных модулей и каналов связи, хранящих и передающих цепочки связанных блоков транзакций, определяет вероятность совершения практически всех возможных атак: атаки 51%, на отказ в обслуживании, атаки Сибиллы, “гибкости транзакций” и др. [26]. Всё вышеперечисленное обеспечивает конфиденциальность передаваемой по проводным каналам связи информации. Однако следует обратить внимание на методы и принципы, позволяющие учесть прочие уязвимости SMART-технологий.

Рекомендации по обеспечению мер защиты информации и минимизации рисков квантовой криптографии и квантовых сетей при использовании SMART-технологий

Огромным недостатком внедрения еще развивающихся и совершенствующихся технологий является ориентирование, в первую очередь, на мгновенное практическое их применение, причем зачастую не уделяется должное внимания потенциально реализуемым угрозам информационной безопасности, в связи с чем возникает общая рекомендация, относящаяся к использованию любых SMART-технологий: пользоваться услугами, программным обеспечением и устройствами, предоставляемыми ответственными производителями и интеграторами, способными обеспечить диагностику и устранение проблем, обнаруженных как на стадии тестирования, так и в процессе эксплуатации. Особенно сильно это касается связанных друг с другом технологий, в совокупности способных нанести большой ущерб компании: ИИ и робототехники. Отслеживать защищенность первой следует еще на стадии обучения. Предоставляемая для этого информация должна быть получена из надежных источников, например в результате реального функционирования аэропорта или на основе отчетов, составленных сотрудниками авиакомпании, однако и она требует предварительной обработки для предотвращения атак и ошибок, связанных с нестандартными или заведомо некорректными данными. Также необходимо гарантировать устойчивость системы ИИ посредством обеспечения надежной технической основы, например использованием методологии drop out, позволяющей поддерживать работоспособность нейронной сети при отключении или повреждении определенного количества “нейронов” [27]. При внедрении “умных” роботов, предназначенных для физического взаимодействия с людьми в совместной рабочей среде, ошибки, вызванные недостатками системы ИИ, могут привести к причинению серьезного вреда здоровью человека, нанесению материального ущерба и шпионажу посредством разнообразных устройств считывания информации. В таких случаях дополнительные меры защиты определяются особенностями области применения робота и заключаются в утверждении дополнительных ограничивающих условий, выполнение которых отслеживается при помощи дополнительных систем контроля или логических цепочек, установленных и настраиваемых специалистами, обеспечивающими его постоянную поддержку.

Несмотря на высокую надежность и дополнительный функционал технологии биометрической идентификации в качестве механизма контроля доступа, кроме описанных выше и сведенных к минимуму уязвимостей каналов связи, существуют скрытые атаки, которые сложно обнаружить. Распространенное явление утечки персональных данных из базы биометрических шаблонов клиентов приводит к возникновению угрозы использования подделки злоумышленником. Система идентификации должна использовать один из многочисленных существующих методов идентификации живого человека и отличия его от подделки, например путем фиксирования непроизвольных факторов, таких как моргание. Для обеспечения безопасности базы шаблонов предложены методы, заключающиеся в хранении лишь части информации, полученной из биометрического шаблона, называемой защищенным эскизом. Имея только защищенный эскиз, злоумышленник не сможет восстановить шаблон для создания подделки, так как это возможно только при наличии другого биометрического образца, принадлежащего одному человеку.

Заключение

Таким образом, возникает потребность в поиске более эффективных методов защиты информационных систем от возрастающих угроз и корректировании уже используемых методов.

Проведенное в данной работе исследование показало возможность использования квантовых криптографических систем как основного метода передачи информации на предприятиях гражданской авиации в условиях развития SMART-технологий и необходимость модернизации существующей модели оценки рисков информационной безопасности систем предприятий ГА, используемых при эксплуатации аэропортов и наземном обеспечении полетов воздушных судов.

Теоретическая модель системы связи, спроектированная на основе квантовых явлений, гарантирует практически стопроцентное обнаружение попытки подслушивания канала злоумышленниками, однако невозможность реального ее конструирования в полном соответствии с теорией создает трудности при оценке защищенности построенных систем от перехвата информации.

Для решения проблемы в работе предложено внедрить дополнительные этапы оценки рисков, как учитывающие влияние развивающихся SMART-технологий на бизнес-процессы, так и прогнозирующие изменения существующих рисков, вызванные использованием квантовых вычислений и квантовых сетей, в связи с чем были разработаны рекомендации по обеспечению мер защиты информации и минимизации рисков для данных информационных систем.

Предложенный подход, в условиях перехода к цифровой экономике, позволит не только повысить эффективность применения SMART-технологий, но и выявить их воздействия на бизнес-процессы для создания устойчивой и безопасной информационно-телекоммуникационной инфраструктуры предприятий гражданской авиации.

Список использованных источников

1. Романчева Н.И. Индикаторы достижения информационной безопасности в условиях перехода на SMART-технологии. – Пятигорск, Пятигорский госуниверситет, 2019.
2. C. Bennett, G. Brassard. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. – 1984. - pp. 175-179.
3. Молотков С.Н. «Квантовая криптография и теоремы В. А. Котельникова об одноразовых ключах и об отсчетах» // Успехи физических наук. – 2006. Т.176. №7. – С. 777-788.
4. C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography // J. Cryptology. – 1992. Vol.5. - pp. 3-28.
5. К.Е. Румянцев, И.Е. Хайров. Эффективность волоконно-оптической системы передачи информации // Информационное противодействие угрозам терроризма. – 2004.
6. N. Lütkenhaus. Quantum key distribution: How Do We Know It’s Secure? // Optics & Photonics News. – 2004. – pp.24-28.
7. Колесникова Д.С., Ганичев А.А. Квалиметрия информационных рисков безопасности полетов // Труды Международного симпозиума «Надежность и качество». – 2018. Т.1 С. 114-116.

8. Банк данных угроз безопасности информации ФСТЭК Режим доступа: https://bdu.fstec.ru/

9. Google достигла квантового превосходства Режим доступа: https://habr.com/ru/news/t/468361/

10. Кибербезопасность в эпоху стратегической неопределенности Режим доступа: https://bis-expert.ru/news/vulnerabiliti/59071

11. Молотков С.Н., Тимофеев А.В. Явная атака на ключ в квантовой криатографии (протокол BB84), достигающая теоретического предела ошибки Qc ≈11% / Письма в ЖЭТФ, №10(85), 2007. – 6.

12. Плохова М.А. Квантовая механика, творчество и внутренний опыт/ Эпистемология и философия науки, №4(6), 2005. – 9 с.

13. Пономарева В.В., Розова Я.С. Протоколы квантового распределения ключей/ Прикладная информатика, №6(18), 2008. – 11 с.

14. Серикова Ю.И., Качалин С.В., Серикова Н.И. Квантовая статистическая регуляризация вычислений спектрального представления данных малых выборок/ Научные исследования и открытия XXI века: сборник статей по материалам международной –практической конференции (г. Челябинск, 25 октября 2017 г.). Иркутск: «Научное партнерство «Апекс», 2017. – 6 с.

15. Сингх С. Книга шифров. Тайная история шифров и их расшифровки/ Изд-во: Астрель, 2007. – 93 с.

16. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

17. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. 2008-02-15. М.: ФСТЭК России, 2008. 69 с.

18. Ильченко Л.М., Брагина Е.Ж., Егоров И.Э., Зайцев С.И. Расчет рисков информационной безопасности телекоммуникационного предприятия // Журнал Открытое Образование. – 2018. Т.22 №2. – С. 61-70.

19. Квантовое шифрование защитили от «атаки троянского коня» Режим доступа: http://nmir.net/news/2063-kvant-cript.html

20. Стойкость квантовых протоколов распределения ключей Режим доступа: https://rid.tusur.ru/conference/2012/themes/8/projects/175/discourses/269

21. Искусственный интеллект поможет хакерам усовершенствовать кибератаки Режим доступа: https://www.itweek.ru/ai/article/detail.php?ID=204144

22. SITA: Авиакомпании и аэропорты Китая переходят на новый уровень обслуживания пассажиров. Режим доступа:

https://www.aviapages.ru/news/205306-sita-aviakompanii-i-aeroporty-kitaya-perehodyat-na-novyy-uroven-obsluzhivaniya-passazhirov

23. Применение новых технологий в современных аэропортах. Режим доступа: https://golos.io/@konstantin/novyi-tekhnologii-i-aeroporty-budushego

24. Как ввести в заблуждение компьютер: коварная наука обмана искусственного интеллекта. Режим доступа https://habr.com/ru/post/405773/

25. Биометрическая аутентификация: защита систем и конфиденциальность пользователей. Режим доступа https://www.osp.ru/os/2012/10/13033122

26. Возможности и вызовы для блокчейн в новой индустриализации. Режим доступа: https://cyberleninka.ru/article/n/vozmozhnosti-i-vyzovy-dlya-blokcheyn-v-novoy-industrializatsii

27. Запутать робота: как и зачем люди обманывают искусственный интеллект. Режим доступа: https://www.forbes.ru/tehnologii/359591-zaputat-robota-kak-i-zachem-lyudi-obmanyvayut-iskusstvennyy-intellekt