Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Калмыков Максим Игоревич

СИСТЕМНЫЙ АНАЛИЗ СПУТНИКОВОЙ СВЯЗИ С ПОВЫШЕННОЙ ИМИТОСТОЙКОСТЬЮ НА ОСНОВЕ РАЗРАБОТКИ МЕТОДА ПОСТРОЕНИЯ СИСТЕМЫ ОПОЗНАВАНИЯ КОСМИЧЕСКОГО АППАРАТА

Специальность 05.13.01 – Системный анализ, управление и обработка информации (в технике и технологиях)

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук
профессор, заслуженный
работник высшей школы РФ
Пашинцев В.П.

Ставрополь – 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Обеспечение услугами связи таких глобальных проектов как освоение Северного морского пути, развертывание сил обеспечения безопасности в Арктике, создание информационно-телеметрических систем воздушного и наземного транспорта в высоких широтах невозможно без использования низкоорбитальных систем спутниковой связи (НССС). Для решения данных задач в настоящее время широко используются спутниковые системы связи «Iridium NEXT», «Гонец», «Эфир».

Одним из наиболее перспективных направлений применения НССС является освоение полезных ископаемых в районах Крайнего Севера. В этом случае НССС являются достаточно важной частью автоматизированных систем дистанционного мониторинга, контроля и управления (АСДМКУ), с помощью которых производится управление необслуживаемыми объектами добычи и транспортировки углеводородов, расположенных за Полярным Кругом. При этом для организации бесперебойной связи группировка НССС содержит от 48 до 60 космических аппаратов (КА).

Проводимые исследования принципов построения и алгоритмов работы автоматизированных систем дистанционного мониторинга, контроля и управления позволили обосновано отнести их к сложным информационным системам. Как и всякая сложная информационная система АСДМКУ обладает определенным набором уязвимостей. Использование данных уязвимостей позволит злоумышленнику нарушить правильную и эффективную работу такой сложной информационной системы управления.

В качестве основных источников угроз безопасности АСДМКУ можно выделить стихийные бедствия и аварии; сбои и отказы оборудования (технических средств) системы, ошибки проектирования и разработки

компонентов системы, ошибки персонала, возникающие в процессе эксплуатации, преднамеренные действия нарушителей [57].

Проведенные исследования показали, что среди структурно-функциональных элементов, входящих в состав автоматизированных систем дистанционного мониторинга, контроля и управления наибольшим числом уязвимостей обладают системы спутниковой связи. Это связано с тем, что расстояния между объектом управления и центром поддержки операций АСДМКУ составляют сотни километров, благодаря чему у нарушителя имеется потенциальная возможность нарушить эффективность работы НССС и всей АСДМКУ. Кроме того, в последние годы наблюдается тенденция увеличения числа низкоорбитальные системы спутниковой связи, используемых в комплексах дистанционного мониторинга, контроля и управления необслуживаемыми объектами экологически-опасных технологий, расположенными за пределами Полярного Круга. Это связано с постоянным расширением стран и транснациональных компаний, которые начинают массово осваивать месторождения Арктического шельфа, что способствует увеличению количества группировок низкоорбитальных спутников. Так как число космических аппаратов постоянно возрастает, то возникает ситуация, когда «чужой» спутник может оказаться в зоне видимости приемника спутниковой связи, который располагается на абонентском терминале предназначенного для управления необслуживаемым объектом экологически-опасных технологий. В результате этого спутник-нарушитель может дестабилизировать функционирование низкоорбитальной системы спутниковой связи ССС. Такая дестабилизация функционирования ССС может привести к выходу из строя объекта управления и спровоцировать экологическую катастрофу.

Очевидно, что эффективность функционирования низкоорбитальной системы спутниковой связи во многом зависит от выбора методов противодействия деструктивным воздействиям, которые могут быть выполнены нарушителем при воздействии на НССС. Проведенный анализ

основных методов деструктивного воздействия на низкоорбитальные системы спутниковой связи позволили разделить их на следующие группы.

Основу первый группы составляют методы радиоэлектронного подавления сигнала спутника путем блокировки передаваемого сигнала от КА и объекту управления и обратно. Для решения данной задачи в настоящее время широко применяются помехи. Проведенный анализ работ [12,46,51,63], позволил сделать вывод о том, что в настоящее время достаточно эффективно, применяются пассивные помехи. Особое место среди таких помех занимают гармонические непрерывные помехи, прицельные непрерывные шумовые помехи, заградительные непрерывные шумовые помехи.

Однако такие пассивные помехи нецелесообразно применять для подавления передачи ССС, используемых в комплексах мониторинга, контроля и управления объектами, расположенными районах Крайнего Севера. Это связано, во-первых, с удаленным расположением объектов управления, на которых находятся приемники ССС, а, во-вторых, для комплексов пассивного шумового подавления необходимо обеспечить прямую видимость со спутником связи, что за Полярным Кругом сделать достаточно затруднительно. Обобщая сказанное, можно сделать вывод о том, что такой подход к нарушению функционирования ССС в районах Крайнего Севера является низкоэффективным и затратным.

Наряду с пассивными помехами системами радиоэлектронной борьбы (РЭБ) широко используются активные помехи, которые можно разбить на две группы. Основу первой группы составляют активные маскирующие помехи, применение которых, во-первых, не позволяет приемнику радиосвязи обнаружить передаваемый сигнал и во-вторых, не позволяют провести эффективную обработку принятого сигнала. В состав второй группы входят активные имитирующие помехи. Такие помехи называют «интеллектуальными» помехами, которые способны подстраиваться под передаваемый сигнал, нарушая тем самым эффективную работу системы радиосвязи.

Однако, в условиях Крайнего Севера, территория которого является труднодоступной и малозаселенной, использование активных помех является нецелесообразным. Это связано с тем, что рассмотренные методы, способные дестабилизировать работу низкоорбитальной ССС, являются малоэффективными, так как для постановки различных видов радиопомех станциями РЭБ, которые располагаются за пределами Российской Федерации, требуются значительные финансовые и энергетические затраты. Таким образом, можно сделать вывод - несмотря на разнообразие пассивных и активных имитирующих помех, данный подход к нарушению работы системы спутниковой связи, применяемых в комплексах мониторинга, контроля и управления удаленным объектом, в арктических условиях практически не осуществим.

Ко второй группе деструктивных воздействий на системы спутниковой связи относятся различные способы, позволяющие имитировать или перехватывать «правильные» сигналы с последующим их навязыванием противнику. Главной целью таких способов, базирующихся на навязывании ложного или перехваченного сигнала, является подмена передаваемого сигнала.

В ряде работ по радиоэлектронной борьбе [12,46,51,72] рассматриваются способы, которые используют принцип перехвата и навязывания противнику перехваченных сигналов. Используя данные методы, спутник-нарушитель должен сначала перехватить передаваемые сигналы от космического аппарата, которые предназначены абонентскому терминалу необслуживаемому объекту. После этого такой перехваченный сигнал сохраняется в памяти спутника-нарушителя определенное время. Затем, спустя некоторый временной интервал, перехваченный сигнал передается приемнику ССС, который входит в состав абонентского терминала управления удаленным объектом. В этом случае приемник однозначно примет такой сигнал, а абонентский терминал приступит к исполнению команды управления. Это связано с тем, принятый сигнал будет иметь свою

соответствующую структуру, а его параметры будут полностью совпадать с параметрами сигналов, которые используются низкоорбитальной ССС, входящей в состав комплекса контроля, мониторинга управления. При определенных условиях это может привести к внештатной ситуации на необслуживаемом объекте добычи и транспортировки углеводородов. А неправильная работа системы управления таким удаленным объектом способна вызвать экологическую катастрофу, которая негативно скажется на природе Крайнего Севера.

Повысить имитостойкость низкоорбитальной системы спутниковой связи, то есть предотвратить навязывание перехваченного и задержанного сигнала, можно за счет применения системы опознавания космического аппарата (СОКА), которая перед началом сеанса связи будет проводить опознавание спутника. Если спутник имеет статус «свой», то система опознавания космического аппарата разрешает ему осуществлять обмен данными с абонентским терминалом. В противном случае – космическому аппарату в сеансе будет отказано.

Поэтому разработка метода построения системы опознавания космического аппарата, позволяющего повысить имитостойкость низкоорбитальной системы спутниковой связи, является актуальной задачей.

В ходе проведенных исследований было установлено, что настоящее время существует два вида систем опознавания «свой-чужой». К первой группе относятся системы «свой-чужой», которые для опознавания объекта используют неимитостойкие режимы работы. Проведенный анализ показал, что данная система опознавания обладает рядом недостатков:

– низкий уровень имитостойкости;

– относительно низкая пропускная способность, которая позволяла осуществлять одновременную работу 10 запросчиков и 10 ответчиков;

Из-за небольшого числа возможных комбинаций ответа такая система опознавания «свой-чужой» характеризуется вероятностью имитации противником сигнал «свой» за обзор равной $P_И = 0,1$.

Основу второй группы составляют системы «свой-чужой», в которых используется режим общего имитостойкого опознавания. Благодаря данному режиму работы снижается вероятность имитации противником сигнала «свой» до величины $P_И = 0,005$. Однако, имитостойкие системы опознавания все равно обладают достаточно низкой имитостойкостью. Повысить имитостойкость таких систем позволяет шифрование данных. Применение криптографического кодирования обеспечивает значительное уменьшение вероятности имитации противником сигнала «свой». Это связано со сложностью подбора ответного сигнала при использовании шифрования. Так при использовании зашифрованного сигнала, имеющего информационную часть равную 30 бит, вероятность имитации противником

Однако анализ условий функционирования элементов НССС позволяет сделать вывод о том, что использование методов шифрования в системах опознавания космического аппаратов невозможно. Так в системе опознавания «Пароль» для повышения имитостойкости секретные ключи необходимо менять ежедневно. Обеспечить своевременную смену ключей на орбите и на необслуживаемом объекте, где размещается запросчик системы «свой-чужой» возможно следующими способами:

– созданием достаточно большой базы данных секретных ключей, которая будет размещаться как на борту спутника, так и необслуживаемом объекте;

– организовать ежедневную передачу секретных ключей ответчику и запросчику с использованием закрытого канала.

Очевидно, что реализация первого решения может привести к компрометации секретных ключей в результате падения спутника или нарушения целостности объекта управления. В этом случае захват ключей обеспечит вскрытие всей системы опознавания «свой-чужой», что приведет к резкому снижению имитостойкости как самой системы, так и всей НССС.

Второе решение также является сложно реализуемым. Для организации своевременной доставки секретных ключей ответчику и запросчику

необходимо создавать закрытый канал связи, то есть дополнительно использовать аппаратуру шифрования. А это в свою очередь также требует использование периодически изменяемых секретных ключей.

Таким образом, налицо следующее **противоречие на практике**. С одной стороны, существующие системы опознавания, функционирующие без шифрования, не позволяют обеспечить высокую имитостойкость, а, с другой стороны, системы «свой-чужой», применяющие криптографические методы защиты информации шифрование, не могут быть использованы в системах опознавания КА.

Проведенный анализ выявленной проблемной ситуации показал, что данную проблему можно отнести к проблемам совершенствования и развития систем. Это связано с тем, что выявленная проблема имеет решение, которое направлено на повышение эффективности функционирования низкоорбитальной системы спутниковой. При этом это решение базируется на применении новых идей, связанных с построением систем опознавания КА, обладающих высокой имитостойкостью без использования методов шифрования. Согласно [5] такая проблема относится к слабоструктурированным проблемам, решение которых является объектом исследования системного анализа и синтеза.

Для решения выявленного противоречия на практике был проведен сравнительный анализ альтернативных методов опознавания, которые могут быть использованы в СОКА.

Так как методы построения системы опознавания космического аппарата во многом определяются протоколами опознавания, которые могут использоваться в СОКА. Значительный научный вклад в теорию построения протоколов опознавания протоколов внесли как отечественные, так и зарубежные ученые, среди которых можно выделить: Алферов А.П., Зубов А.Ю., Кузьмин А.С., Запечников С. В., Черемушкин А.В. Чмора А.Л., L. Guillou, J. Camenisch, A. Feige, A. Lysyanskaya, J. Quisquater, M. Michels, A. Fiat, A. Shamir и другие. Проведенные исследования и анализ работ

[15,67,77,83,96,98,100] позволили поделить все множество протоколов опознавания типа «запрос-ответ» на три класса. Основу первого класса составляют методы парольной опознавания. При использовании данных методов претендент и проверяющий владеют секретной информацией, с помощью которой и происходит опознавание субъекта. В зависимости от вида секретной информации и правила обмена этими данными различают протоколы опознавания, использующие многоразовые и секретные пароли. Однако, несмотря на минимальные временны затраты, необходимые на опознавание претендента, методы, использующие многоразовые и одноразовые секретные пароли, имеют недостатки. Во-первых, это наличие у проверяющей стороны базы данных, где хранятся все идентификаторы и пароли. Во-вторых, при реализации протокола опознавания необходимо осуществить передачу секретных ключей на обе стороны протокола по закрытому каналу связи. Учитывая, что проверяющая сторона системы опознавания космического аппарата, которая находится на необслуживаемом объекте, то возникают определенные трудности с организацией такого канал к каждому объекту.

Более высокой стойкостью к НСД обладают протоколы опознавания, составляющие вторую группу. Данные протоколы используют метод опознавания типа «запрос-ответ» [15,74]. В основу таких методов положен принцип, согласно которому претенденту должен убедить проверяющую сторону, что он относится к группе авторизованных абонентов. Для этого ему необходимо, ответить на запрос, который инициировала проверяющая сторона. При этом ответ должен определяться как вопросом, так и секретом известным только претенденту. При этом претендент не должен разгласить секрет, отвечая на поставленный вопрос. Однако таким протоколам присущи и недостатки. Так в процессе реализации протокола опознавания претенденту нарушитель может перехватить и запомнить передаваемые данные по каналу связи. После этого нарушитель пытается навязать претенденту запросы, с помощью которых он получит на них ответы. На основе анализа полученных

ответов злоумышленник способен определить данные о секрете. Кроме того, для повышения стойкости таких протоколов предлагается использовать симметричные криптосистемы.

В третью группу входят протоколы опознавания, использующие методы доказательства с нулевым разглашением знаний [76,77]. Как правило, такие протоколы опознавания характеризуются многошаговым итерационным доказательством. Одним из первых протоколов опознавания был протокол Фиат–Шамира. Чтобы снизить вероятность пропуска нарушителя предлагается выполнять процедуру опознавания W = 20 - 40 раундов. Сократить время опознавания претендента позволяет протокол Фейге-Фиат-Шамира. За счет использование параллельных вычислений с операндами разрядности n, требуемый уровень вероятности пропуска нарушителя достигается за меньшее количество повторов (раундов). Однако, несмотря на сокращение временных затрат на проведение опознавания, данные протоколы также нецелесообразно использовать при определении статуса космического аппарата в НССС. Большое число раундов обмена данными между ответчиком и запросчиком способствует повышению вероятности подбора ответа на поставленный вопрос запросчика.

Сократить число этапов проверки статуса космического аппарата позволяет разработанный метод опознавания, базирующийся на доказательстве с нулевым разглашением. За счет использования дополнительных истинных и зашумленных образов КА, полученных с использованием секретных операндов, находящихся на борту спутника, было достигнуто сокращение числа этапов проверки до двух. При этом для повышения имитостойкости данного протокола было предложено использовать заменяемые сеансовые ключи, которые вычисляются с помощью псевдослучайной функции (ПСФ).

Таким образом, налицо следующее **противоречие в теории.** Известные протоколы опознавания, построенные на основе методов типа «запрос-ответ», а также с помощью многоразовых и одноразовых паролей, не позволяют в

полной мере предотвратить навязывание имитирующих и ретрансляционных помех спутником-нарушителем. При этом метод опознавания, базирующийся на доказательстве с нулевым разглашением и использующий псевдослучайно-изменяемые сеансовые ключи, реализация которого позволяет при минимальном числе этапов провести опознавания космического аппарата, не нашел применения.

Проведенные исследования показали, что для повышения имитостойкости низкоорбитальной системы спутниковой связи существует множество альтернативных решений. Применение каждой альтернативы из данного набора позволяет в той или иной степени повысить имитостойкость НСС. Таким образом, возникают трудности, которые не позволяют впрямую при минимальных затратах решить поставленную задачу.

Найти выход из создавшейся ситуации позволяют использование методов системного анализа (СА). Как показано в работах [3,4,5,36,75] применение математического аппарата СА способствует проведению сравнительного анализа альтернативных решений. Полученные количественные оценки позволят выбрать наиболее эффективную альтернативу. Именно такое альтернативное решение позволит обеспечить устранения выявленных противоречий на практике и в теории. Устранение таких противоречий позволит обеспечить повышение имитостойкости низкоорбитальной системы спутниковой связи за счет применения разработанного метода построения системы опознавания космического аппарата. Поэтому в диссертационных исследованиях был использован научно-методологический аппарат (НМА) системного анализа. Применение метода сравнительного анализа альтернативных решений позволило обоснованно выбрать наиболее эффективное решение, применение которого обеспечит повышение имитостойкости низкоорбитальной системы спутниковой связи.

Объектом диссертационных исследований является низкоорбитальная система спутниковой связи.

Целью диссертационных исследований является повышение имитостойкости низкоорбитальной ССС за счет использования разработанного метода построения системы опознавания космического аппарата.

Предметом диссертационных исследований являются:

– протоколы опознавания типа «запрос-ответ», базирующиеся на доказательстве с нулевым разглашением знаний;

– методы построения запросно-ответных систем опознавания космического аппарата, использующие протоколы опознавания.

Научная задача диссертационных исследований состоит в применении научно-методологического аппарата СА при разработке метода построения системы опознавания космического аппарата, позволяющего повысить имитостойкость НССС за счет использования протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений.

Для решения поставленной общей научной задачи была проведена ее декомпозиция на ряд следующих **частных задач**:

1. Разработка протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений, обладающего меньшими временными затратами на опознавания спутника.

2. Разработка алгоритма проверки повторного использования сеансового ключа, применение которого не позволит снизить вероятность пропуска спутника-нарушителя.

3. Разработка структурной модели генератора псевдослучайной функции для выработки сеансового ключа системы опознавания космического аппарата.

4. Разработка метода построения системы опознавания космического аппарата, отличающегося от ранее известных более низкой вероятностью подбора ответа на вопрос запросчика за счет использования разработанного протокола опознавания, с нулевым разглашением сведений.

5. Разработка структурной схемы системы опознавания космического аппарата, реализованная на основе разработанного метода и протокола опознавания.

Методы исследований. В ходе решения научной задачи диссертационных исследований применялись методы теории системного анализа, теории построения протоколов опознавания, теории кодирования, теории конечных полей.

Достоверность и обоснованность полученных в диссертационной работе результатов и формулируемых на их основе выводов обеспечивается строгостью производимых математических выкладок, которые были получены с помощью научно-методического аппарата системного анализа, теории построения протоколов опознавания, теории кодирования, теории конечных полей. Справедливость полученных научных результатов относительно эффективности предложенных решений подтверждена теоретическим сравнением с уже существующими системами опознавания.

Научная новизна исследований заключается в следующем:

1. Разработан протокол опознавания КА, построенный на основе доказательства с нулевым разглашением сведений, обладающий меньшими временными затратами на определение статуса спутника за счет сокращения количества этапов выполнения по сравнению с ранее известными протоколами типа «запрос-ответ».

2. Разработан алгоритм проверки повторного использования сеансового ключа, отличающийся от ранее известных, тем, что позволяет провести проверку без его передачи по каналу связи.

3. Разработана структурная модель генератора псевдослучайной функции для выработки сеансового ключа системы опознавания космического аппарата, отличающаяся от ПСФ Наорра-Рейнголда меньшими временными затратами на получение выходных значений.

4. Разработан метод построения системы опознавания космического аппарата, отличающийся от ранее известных более низкой вероятностью

подбора ответа на вопрос запросчика за счет использования разработанного протокола опознавания, с нулевым разглашением сведений.

Практическая значимость результатов данной работы:

1. В ходе проведения диссертационных исследований был разработан протокол опознавания, который может быть использован в запросно-ответных системах «свой-чужой».

2. Разработан метод построения системы опознавания, обладающий высокой имитостойкостью. Данный метод может использован для построения запросно-ответных систем «свой-чужой», которые способны выполнять процедуру опознавания длительное время в автоматическом режиме.

3. Разработанная структурная модель генератора псевдослучайной функции может быть использована для построения генераторов, обладающих высокой криптостойкостью при использовании меньшего по длине ключа.

4. Выполнена разработка структурной схемы системы опознавания космического аппарата, которая обеспечивает определение статуса спутника за меньшее число итераций, что позволяет снизить вероятность пропуска спутника-нарушителя.

Основные положения, выносимые на защиту:

1. Протокол опознавания КА, построенный на основе доказательства с нулевым разглашением сведений, обладающий меньшими временными затратами на определение статуса спутника за счет сокращения количества этапов выполнения по сравнению с ранее известными протоколами типа «запрос-ответ».

2. Алгоритм проверки повторного использования сеансового ключа, отличающегося от ранее известных, тем, что позволяет провести проверку без его передачи по открытому каналу связи.

3. Структурная модель генератора псевдослучайной функции для выработки сеансового ключа системы опознавания космического аппарата,

отличающегося от ПСФ Наорра-Рейнголда меньшими временными затратами на получение выходных значений.

4. Метод построения системы опознавания космического аппарата, отличающийся от ранее известных более низкой вероятностью подбора ответа на вопрос запросчика за счет использования разработанного протокола опознавания, с нулевым разглашением сведений.

Объем и структура работы. Диссертационная работа состоит из введения, трех глав, заключения и приложений. Работа изложена на 172 страницах, включая 6 рисунков, 5 таблиц. Список литературы состоит из 101 наименования.

Во **введении** показана актуальность провидимых исследований связанных с повышением имитостойкости низкоорбитальной системы спутниковой связи, обосновано применение методологии системного анализа для разработки СОКА, применение которого позволит снизить вероятность пропуска спутника-нарушителя, определены объект и предмет диссертационных исследований, выполнена постановка цели и научной задачи диссертационной работы, представлены научная и практическая значимость проводимых исследований, а также основные положения, выносимые на защиту.

В **первой** главе проведен анализ научно-методического аппарата системного анализа, который позволил выделить основные этапы методик системного анализа. На основе методики системного анализа были исследованы основные принципы построения автоматизированных систем дистанционного мониторинга, контроля и управления. Показано, что для организации эффективного управления необслуживаемыми экологически-опасными объектами, которые размещаются в районах Крайнего Севера необходимо, использовать низкоорбитальные системы спутниковой связи. Проведен анализ угроз безопасности АСДМКУ. В качестве основных источников угроз безопасности были обоснованно выбраны системы спутниковой связи. Определен объект исследований. Проведен анализ

деструктивных методов, направленных на снижение имитостойкости низкоорбитальной системы спутниковой связи. Показано, что методы, позволяющие имитировать или перехватывать «правильные» сигналы управления с последующим их навязыванием приемнику ССС, позволяет нарушить эффективную работу ССС АСДМКУ. Определена цель диссертационных исследований. Проведен анализ основных методов построения систем опознавания «свой-чужой», который позволил выявить противоречие на практике. Показана актуальность разработки новых принципов построения системы распознавания спутника для низкоорбитальной группировки ССС. Проведен системный анализ альтернативных методов опознавания для системы опознавания космического аппарата, который позволил провести обоснование противоречия в теории. Проведена постановка научной задачи исследования. На основе проведенного анализа выбран показателя качества, позволяющего оценить эффективность разработанных решений, позволяющих повысить имитостойкость низкоорбитальной системы связи в условиях воздействия имитирующих помех. Произведена математическая постановка задачи исследования. Используя методы СА, была проведена декомпозиция главной научной задачи на ряд частных научных задач.

Вторая глава диссертации посвящена решению первой и второй частных задач исследований. Первая частная задача диссертационных исследований связана с разработкой протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений, обладающего меньшими временными затратами на опознавания спутника. Проведенный анализ реализаций протоколов опознавания Фиата-Шамира, Фейге-Фиат-Шамира, базирующихся на доказательстве с нулевым разглашением сведений, а также алгоритмов закрытия данных с открытым ключом показал, что они не позволяют обеспечить определение статуса КА за минимальное время. На основе проведенных исследований был разработан протокол опознавания, построенный на основе доказательства с нулевым разглашением знания,

который обладает меньшим количеством этапов опознавания. Проведенный сравнительный анализ показал, разработанный протокол позволяет выполнить процедуру опознавания за два этапа, что в 1,5 раза быстрее рассмотренного ранее протокола опознавания Шнорра. Вторая частная задача диссертационных исследований связана с разработкой алгоритма проверки повторного использования сеансового ключа в СОКА. Показано, что ситуация, когда сеансовый ключ S(j) не изменяет свое значение при изменении номера сеанса с j-го на (j+1)-й, приводит к повышению вероятности пропуска спутника-нарушителя. Чтобы устранить такую ситуацию был разработан алгоритм, позволяющий провести проверку повторного использования сеансового ключа S(j). В ходе диссертационных исследований был разработан такой алгоритм, отличающийся от ранее известных, тем, что позволяет провести проверку без передачи по открытому каналу связи сеансовых ключей. Если в процессе работы СОКА ответчик повторно использует сеансовый ключ, то реализуя разработанный алгоритм, проверяющая сторона получит открытый ключ спутника. Проведен сравнительный анализ эффективности работы системы опознавания космического аппарата, использующей разработанный алгоритма проверки повторного использования сеансового ключа и без применения данного алгоритма. Полученные результаты свидетельствуют о том, что не использование разработанного алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата приводит к увеличению вероятность подбора ответа на вопрос запросчика в $1{,}52 \cdot 10^5$ раз уже при разрядности ответа претендента равного 64 бит.

Третья глава диссертации посвящена решению третьей, четвертой и пятой частных задач исследований. Чтобы снизить вероятность подбора ответа на вопрос запросчика и повысить имитостойкость системы опознавания статуса космического аппарата, применяемой в ССС комплекса удаленного мониторинга, контроля и управления удаленным объектом было предложено использовать псевдослучайную функцию (ПСФ) для формирования

сеансового ключа S(j). Была разработана структурная модель генератора сеансовых ключей, которая позволяет сократить временные затраты на вычисление сеансового ключа в 1,21 раза по сравнению с алгоритмом ПСФ Наора-Рейнголда. Четвертая частная задача связана с разработкой метода построения системы опознавания космического аппарата, реализованного на основе протокола опознавания с нулевым разглашением. Были обоснованы основные этапы функционирования СОКА, использующей предложенный метод. Для оценки эффективности метода построения СОКА был проведен сравнительный анализ с разработанным ранее протоколом опознавания. При использовании разрядности модуля q равной 25 бит вероятность имитации противником сигнала «Свой» в СОКА в протоколе составит $P_{и} = 7{,}89 \cdot 10^{-31}$, а для разработанного метода $P_{и} = 2{,}35 \cdot 10^{-38}$. Таким образом, применение разработанного метода построения СОКА позволяет снизить вероятность имитации противником сигнала «Свой» в СОКА в $3{,}35 \cdot 10^{7}$ раз. Пятая частная задача диссертационных исследований связана с разработкой структурной схемы системы опознавания космического аппарата, использующей разработанный метод построения СОКА, реализованного на основе протокола опознавания нулевым разглашением. Для оценки эффективности разработанного метода был проведен сравнительный анализ с методами построения СОКА, которые используют другие протоколы опознавания, построенные на основе нулевого доказательства. В качестве альтернативных решений предлагается использовать протокол Фиат-Шамира, протокол Шнорра, а также разработанный протокол, представленный в диссертации. В качестве исходных данных было выбрана разрядность ответного сигнала равная 100 бит, при длине команды управления – 20 бит. Полученные результаты показали, что разработанный метод построения системы опознавания космического аппарата позволяет уменьшить вероятность навязывания имитационной помехи в $3{,}36 \cdot 10^{8}$ раз по сравнению с протоколом Фиат-Шамира, в $5{,}01 \cdot 10^{7}$ раз по сравнению с протоколом Шнорра, и в

$3{,}36 \cdot 10^7$ раз по сравнению с разработанным протоколом опознавания, который не использует алгоритм проварки двойного использования сеансового ключа. Таким образом, показано, что разработанный метод построения системы опознавания космического аппарата позволил повысить имитостойкость НССС по сравнению с альтернативными методами построения СОКА

В заключении кратко описаны научные и практические результаты, которые были получены в процессе выполнения диссертации.

Апробация диссертационной работы.

Основные результаты диссертационной работы докладывались и обсуждались на следующих научных конференциях: II международная научно-практическая конференция «Актуальные проблемы современной науки» (Ставрополь, 2013 г.), VI международная научно-технической конференции «Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-6)» (Ставрополь, 2014), Всероссийской научно-практической конференции «Развитие науки и техники: механизм выбора и реализации приоритетов» (Самара, 2018), Международной научно-практической конференции «Фундаментальные проблемы основных направлений научно - технических исследований: (Волгоград 2018 г.), REMS 2018, Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT (Stavropol - Dombay, 2018), Международная научно-практическая конференция «Актуальные проблемы современной когнитивной науки» (Таганрог, 2019).

Публикации. Основные результаты диссертации отражены в 15 печатных работах. Среди последних 5 статей опубликовано в рецензируемых научных журналах, входящих в перечень ВАК при Минобрнауки России, 2 статьи в научных изданиях, входящих в систему индексирования научных работ Scopus, 8 статей в научных изданиях, входящих в базу цитирования РИНЦ. Получено 2 патента РФ на изобретение, 2 свидетельства о государственной регистрации программ для ЭВМ.

Личный вклад соискателя. Представленные в диссертации результаты были получены при непосредственном участии автора. В качестве личного авторского вклада можно выделить разработку протокола опознавания, базирующегося на доказательстве с нулевым разглашением сведений, алгоритма проверки повторного использования сеансового ключа, отличающегося от ранее известных, тем, что позволяет провести проверку без его передачи по открытому каналу связи, разработку нейросетевых алгоритмов выполнения операций, метода построения системы опознавания космического аппарата, отличающийся от ранее известных более низкой вероятностью подбора ответа на вопрос запросчика за счет использования разработанного протокола опознавания, с нулевым разглашением сведений, структурной модели генератора псевдослучайной функции для выработки сеансового ключа системы опознавания космического аппарата, структурной схемы системы опознавания космического аппарата, применение которой позволяет снизить вероятность пропуска спутника-нарушителя за счет за счет использования разработанного протокола опознавания КА.

Результаты диссертационной работы были использованы при выполнении проекта по **гранту РФФИ № 17-37-50017 мол_нр** «Разработка и исследование принципов построения запросно-ответной системы распознавания спутника для повышения имитостойкости низкоорбитальных систем спутниковой связи» по **гранту РФФИ № 18-07-01020 а** «Разработка теоретических основ и принципов построения низкоорбитальных помехозащищенных систем спутниковой связи».

В заключении автор считает приятным долгом выразить огромную признательность научному руководителю доктору технических наук, профессору Пашинцеву Владимиру Петровичу за помощь в решении вопросов, возникавших за период длительной работы.

ГЛАВА 1 ФОРМАЛИЗАЦИЯ И ПОСТАНОВКА ЗАДАЧИ СИСТЕМНОГО АНАЛИЗА ПОВЫШЕНИЯ ИМИТОСТОЙКОСТИ НИЗКООРБИТАЛЬНЫХ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ

1.1 Основные этапы методики системного анализа

В настоящее время системный анализ является одним из наиболее перспективных направлений, позволяющим разрешить выявленные практические противоречия и проблемы, возникающих при разработке и эксплуатации сложных систем [3,4,5,36,75]. То есть при использовании методов системного анализа в качестве объекта выбираются сложные системы. При этом при разработке таких систем на начальном этапе ее создания у разработчиков может не хватать сведений, которые позволили бы определить и обосновать выбранное решение, которое способствовало достижению поставленной цели, а также устранению выявленной практической проблемы. Другими словами, для достижения поставленной цели необходимо провести формализованное описание сложной системы, осуществить разработку ее математической модели, а затем на основе сравнительного анализа возможных альтернативных путей решения обоснованно выбрать такой новый подход, применение которого устранит выявленную проблемы на практике.

Следует отметить, научно-методический аппарат СА характеризуется междисциплинарным подходом, применение которого позволяет решить сложную практическую проблему, возникающую при разработке и эксплуатации сложной системы. Таким образом, методы системного анализа позволяют объединить и сконцентрировать усилия группы самых разных по профилю специалистов, которые совместными усилиями пытаются решить сложную конкретную проблему. То есть применение НМА системного

анализа позволяет представить объект исследования в виде системы, сложность которой определяется не только количеством элементов, входящих в ее состав, но и количеством связей между ними. При этом в процессе устранения выявленной практической проблемы могут быть производиться изменения формального описания и моделирования системы, что позволяет провести выбор наиболее перспективного метода достижения поставленной цели [5,36].

Очевидно, что эффективность достижения поставленной цели СА во многом определяется правильным выбором этапов и последовательности решения задачи по устранению выявленного противоречия. При этом применение НМА СА позволяет обосновать методы, используемые для выполнения частных задач, которые определяются последовательностью этапов. При этом для достижения поставленной цели в СА предлагается осуществлять возврат к предыдущим этапам решения выявленной практической проблемы. Таким образом, обоснование последовательности этапов решения противоречия, выбор соответствующих методов и способов решения частных задач образуют методику системного анализа.

Благодаря этому системный анализ позволяет:

– установить и обосновать причинно-следственные связи, которые оказывают существенное влияние на практическую проблему;

– произвести разработку и исследование модели системы для выбора возможных решений проблемной ситуации;

– провести анализ возможных альтернатив решения выявленной системной проблемы, учитывая выдвинутые ограничения;

– обосновать выбранные рекомендации, позволяющие в максимальной степени достичь поставленной цели.

Анализ работ, посвященных применению методов системного анализа [8,34,36,66], показал, что в настоящее время наибольшее распространение получили следующие методики системного анализа, разработанные Э. Квейдом и С. Оптнером.

В работе [47] представлена методика системного анализа, которая была разработана Э. Квейдом. Для данной методики присуща следующая последовательность этапов.

Первый этап был посвящен постановке задачи исследований. На данном этапе производится формулировка выявленной практической проблемы, а также определяется граница предметной области проводимых исследований. На основе выявленных исходных данных, а также границ исследований выполняется постановка цели исследования.

Второй этап методики связан с выбором возможных альтернативных решений задачи исследований. На данном этапе на основе предварительных соображений выявляются альтернативные пути и методы, которые позволят успешно решить поставленные задачи. При этом проведенные исследования могут привести к отказу от выбранных альтернативных решений.

Третий этап связан с проведением исследований доступных для решения задачи ресурсов. Исследование имеющихся в распоряжение ресурсов, необходимых на решение задачи, является важным этапом. На данном этапе можно определить границы имеющихся ресурсов.

Четвертый этап посвящен разработке модели системы. С помощью данной модели можно провести исследования эффективности предложенных альтернативных решений. Моделирование в системном анализе занимает основное место, так как позволяет изучить основные свойства сложной системы без натурных испытаний последней.

Пятый этап посвящен обоснованию и выбору критериев оценки эффективности альтернатив. Очевидно, что данный этап является достаточно важным, так позволяет обоснованно выбрать соответствующий показатель качества, используя который можно оценить степень решения задачи исследования.

Шестой этап – это проведение сравнительного анализа альтернативных решений. На данном последнем этапе системного анализа осуществляется сравнение предлагаемых альтернативных путей решения поставленной задачи

с использованием выбранного показателя качества с последующим принятием решения.

В работах [9,71] показана методика системного анализа, разработанная С. Оптнером. Данная методика содержит следующие укрупненные этапы.

Первый этап методики связан с определением актуальности практической проблемы, стоящей перед системой. В этом случае считается, что проблема определяет два состояния системы. Первое состояние называется существующее состояние. Второе состояние системы называется предлагаемым. Под проблемой, которая стоит перед системой, принимают промежуток между существующим состоянием и предлагаемым. Чтобы осуществить переход от первого состояния ко второму состоянию необходимо произвести изменение состава системы и связей между ее элементами.

Второй этап методики связан с процедурой определения цели перехода от одного состояния системы к другому. В данной методике считается, что направление улучшения состояния системы должно выполняться только с использованием терминов требований. При этом выбранная цель должна отождествляться с предлагаемым состоянием системы.

Третий этап посвящен изучению структуры системы для определения слабых элементов и связей между ними этой системы, которые не позволяют достичь предлагаемое состояние. При этом необходимо учитывать структурные возможности системы.

Четвертый этап посвящен выявлению альтернативных решений, посвященных достижению поставленной цели. Очевидно, что при решении проблемы, стоящей перед системой, могут быть использовано множество альтернативных решений. При этом такая альтернатива может затрагивать несколько элементов, входящих в состав системы и не позволяющих ей перейти в предполагаемое состояние. Для оценки альтернатив используется критерий отбора, позволяющий обоснованно выбрать такое альтернативное решение, которое позволяет в наибольшей степени удовлетворить требованиям, предъявляемым к цели.

На пятом этапе методики системного анализа происходит разработка решения, позволяющего системе перейти из существующего состояния в предлагаемое. После выполнения процедур признания данного решения родителями системы происходит процесс выполнения выбранного решения. Заключительным подэтапом является проведение оценки эффективности реализации выбранного решения.

Проведенные исследования методик СА позволил сделать вывод о том, что, не смотря на определенные различия, они имеют идентичную структуру, которая содержит следующие обобщенные этапы.

Первый этап – постановка задачи СА, выбор цели исследований.

Второй этап – разработка моделей альтернативных решений для проведения их анализа.

Третий этап – обоснование критериев оценки.

Четвертый этап – сравнительный анализ альтернативных решений и выбор оптимального решения, позволяющего в максимальной мере достичь поставленной цели.

Очевидно, что первый этап применения методики СА является наиболее сложным. Это связано с тем, что на данном этапе необходимо определить объект исследований, сформулировать существующую практическую проблему, определить границы системы, выявить исходные данные, а также обозначить цель проводимых исследований.

На втором этапе методики системного анализа необходимо выявить основные альтернативные решения задачи. При этом необходимо рассмотреть существующие модели таких альтернативных подходов, исследование которых позволит обосновать соответствующий выбор. При этом на данном этапе может происходить как исключение определенных альтернативных решений, так и включение новых альтернатив.

Третий этап связан с обоснованным выбором критериев оценки, позволяющему оценить эффективность той или иной альтернативы решения поставленной задачи. Поэтому на данном этапе происходит выбор

соответствующего показателя качества, численное значение которого покажет насколько выбранная альтернатива позволяет достичь выбранную цель исследования.

На четвертом этапе производится сравнительный анализ альтернативных решений. При этом для выбора оптимального решения используется выбранный ранее критерий оценки. При этом необходимо учитывать обоснованные ранее ограничения на другие показатели качества функционирования объекта исследований. В результате проведенного сравнительного анализа возможных решений будет обоснованно выбрано оптимальное решение, позволяющее в максимальной мере достичь поставленную цель.

1.2 Формализация задачи системного анализа повышения имитостойкости НССС

1.2.1 Анализ уязвимостей АСДМКУ, работающих с необслуживаемыми объектами за Полярным Кругом

В современных условиях обеспечить эффективное управление сложными необслуживаемыми объектами, предназначенных для добычи и транспортировки нефти и газа, расположение которых определяется районами Заполярья, возможно только с помощью автоматизированных систем дистанционного мониторинга, контроля и управления (АСДМКУ). Проводимые исследования принципов построения и алгоритмов работы таких

комплексов [12,54,73] позволили обосновано считать, что их можно отнести к сложным информационным системам. Значит, справедливо утверждение, что АСДМКУ будут обладать определенным набором уязвимостей. Использование данных уязвимостей позволит злоумышленнику нарушить правильную и эффективную работы такой сложной информационной системы управления.

Очевидно, что обеспечение бесперебойной работы автоматизированных систем дистанционного мониторинга, контроля и управления относится к сложной научно-технической задаче. Чтобы решить данную задачу воспользуемся математическим аппаратом СА, в частности методом декомпозиции. Применение метода декомпозиции позволит изучить структуру автоматизированных систем дистанционного мониторинга, контроля и управления с целью выявления элементов, которые в наибольшей степени подвержены уязвимостям к деструктивным действиям.

В общем случае АСДМКУ, предназначенные для выполнения удаленного мониторинга, моделирования и контроля операционных процессов, включают в свой состав следующие структурно-функциональные элементы [1,2]:

– центр поддержки операций, объединяющий в своем составе высококвалифицированных специалистов, развитые технологические процессы, а также передовую технологию обработки данных, который предназначен для эффективного управления проводимых работ, обеспечивая при этом требуемые показатели безопасности освоения месторождений полезных ископаемых;

– абонентские терминалы (АТ), расположенные, как правило, на необслуживаемых объектах, которые предназначены для добычи и транспортировки углеводородов;

– систему спутниковой связи, которая используется для передачи данных телеметрического сопровождения и измерений, регистрируемых

приборами, установленными на удаленных необслуживаемых объектах управления.

Очевидно, что каждый структурно-функциональный элемент автоматизированной системы дистанционного мониторинга, контроля и управления обладает уязвимостями, способных привести к нарушению конфиденциальности, целостности или доступности передаваемых и обрабатываемых данных внутри данной системы. Таким образом, если суметь выявить такие уязвимости, то это позволит обосновать выбор таких мероприятий, которые будут способствовать снижению негативных последствий этих уязвимостей. Все это в конечном итоге приведет к повышению устойчивости системы мониторинга, контроля и управления к деструктивным воздействиям.

В качестве основных источников угроз безопасности АСДМКУ можно выделить [54,57,64]:

– стихийные бедствия и аварии;
– сбои и отказы оборудования (технических средств) системы;
– ошибки проектирования и разработки компонентов системы;
– ошибки персонала, возникающие в процессе эксплуатации;
– преднамеренные действия нарушителей и злоумышленников.

Достаточно подробно процедура определения основных угроз для автоматизированных систему управления приведена в работе [57]. Рассмотрим угрозы информационной безопасности, которые возникают в системах передачи и обработки информации.

Так как объекты добычи и транспортировки газа и нефти находятся в малодоступных областях Крайнего Сервера, которые также характеризуются низкой плотностью населения, то для эффективного управления такими сложными экологически-опасными объектами необходимо использовать системы спутниковой связи. В настоящее для обеспечения эффективной работы в состав ССС включают определенное количество космических аппаратов, которые объединяются в орбитальные группировки. При этом

такие группировки КА могут располагаться на орбитах, имеющих разную высоту. В зависимости от данных орбит различают следующие группировки спутников [38,43,48,52].

Основу первой группы составляют системы спутниковой связи, использующие высокоорбитальные, геостационарные орбиты. Для таких спутников характерно то, что период обращения таких геостационарных ССС будет равен 24 часам. Следовательно, такие спутники вращаются вокруг Земли, имея угловую скорость, которая соответствует угловой скорости вращения нашей планеты вокруг своей оси. Совпадение скоростей вращения приводит к тому, что такие КА располагаются над определенной точкой. Так как высота орбиты таких спутников составляет до 40000 км, то благодаря этому, достаточно три космических аппарата для организации связи почти со всеми точками планеты. Однако такие ССС обладают недостатками:

– из-за большой высоты орбиты для таких ССС характерна задержка данных при передаче по спутниковому каналу связи;

– при размещении приемо-передающих устройств ССС за пределами Полярного Круга достаточно сложно организовать устойчивую связь.

Основу второй группы ССС составляют среднеорбитальные группировки спутников. Как показало проведенное исследование среднеорбитальные группировки спутников располагаются на орбитах с высотой от 5000 до 15000 км. Очевидно, что снижение высоты орбиты ССС приводит к уменьшению зоны видимости и уменьшению интервала времени нахождения спутника в данной зоне. В результате требуется увеличение количества спутников в группировке. Поэтому для организации устойчивой связи необходимо, чтобы в состав такой группировки входили 10 - 12 спутников. Снижение высоты орбиты позволяет устранить один из недостатков, которые присущи высокоорбитальной группировке КА. Благодаря тому, что диапазон высоты орбиты находится в пределах 5000 - 15000 км, происходит уменьшение времени задержки сигнала в канале связи. При этом также уменьшаются затраты на вывод КА на орбиту. Однако, такие

ССС не позволяют в полной мере обеспечить достаточно устойчивую спутниковую связь с объектами, разложенными за Полярным Кругом.

Устранить данный недостаток позволяют КА, которые составляют основу третьей группы. К ним относятся низкоорбитальные группировки спутников [33,53,42]. Известно, что использование только таких группировок КА позволяет обеспечить достоверную связь с объектами, размещенных в районах Крайнего Севера. Однако снижение высоты орбиты приводит к тому, что период обращения низкоорбитальных спутников вокруг Земли будет находиться в пределах 85-130 минут. В результате этого время нахождения КА в зоне видимости приемной спутниковой станции составляет до 5-10 минут. Поэтому для организации устойчивой связи необходимо, чтобы в состав группировки входило 48-60 спутников. В результате для передачи данных необходимо, чтобы низкоорбитальные спутники устанавливали сеанс связи с приемником спутниковой связи, расположенной на необслуживаемом объекте управления последовательно и по очереди. Благодаря отмеченным достоинствам низкоорбитальные ССС широко используются для организации связи с удаленными объектами управления, которые находятся в районах Крайнего Севера.

В последние годы наблюдается тенденция увеличения числа низкоорбитальные системы спутниковой связи. Это связано с тем, что такие ССС широко используются в комплексах дистанционного мониторинга, контроля и управления необслуживаемыми объектами экологически-опасных технологий, расположенными за пределами Полярного Круга. При этом происходит постоянное увеличение числа стран и транснациональных компаний, которые начинают массово осваивать месторождения Арктического шельфа. Это в свою очередь приводит к увеличению количества группировок низкоорбитальных спутников. Так как число космических аппаратов, постоянно возрастает, то возникает ситуация, когда «чужой» спутник может оказаться в зоне видимости приемника спутниковой связи, который располагается на абонентском терминале предназначенного

для управления необслуживаемым объектом экологически-опасных технологий. В результате этого спутник-нарушитель может дестабилизировать функционирование низкоорбитальной системы спутниковой связи ССС. Такая дестабилизация функционирования ССС может привести к выходу из строя объекта управления и спровоцировать экологическую катастрофу.

Поэтому объектом исследования является низкоорбитальная система спутниковой связи.

Очевидно, что эффективность функционирования низкоорбитальной системы спутниковой связи во многом зависит от выбора методов противодействия деструктивным воздействиям, которые могут быть выполнены нарушителем при воздействии на НССС. Проведем анализ основных методов деструктивного воздействия на низкоорбитальные системы спутниковой связи.

1.2.2. Анализ деструктивных методов, направленных на снижение имитостойкости низкоорбитальной системы спутниковой связи

Как и всякая система, связанная с обработкой и передачей информации, система спутниковой связи обладает уязвимостями. Под уязвимостью системы спутниковой связи будем понимать недостатки технологии процесса передачи данных, мер и средств обеспечения информационной безопасности ССС, позволяющие нарушителю совершать действия, приводящие к реализации той или иной угрозы. Чтобы создать и реализовать эффективные механизмы защиты информации от НСД в ССС от различных угроз

безопасности необходимо выявить такие элементы системы, которые уязвимы в наибольшей степени.

Проведенный анализ предметной области [12,45,46,50,51,63,72] позволил провести кластеризацию дестабилизирующих воздействий на ССС. Все эти воздействия можно разбить на две класса. Основу первого класса воздействий на ССС будут составлять различные способы радиоэлектронного подавления сигнала. Основу второго класса дестабилизирующих воздействий будут составлять методы и способы, которые используют навязывание ложного образа сигнала.

Рассмотрим первую группу дестабилизирующих воздействий на ССС. В качестве главной цели методов и средств радиоэлектронного подавления сигнала спутника, располагающегося в низкоорбитальной группировке, можно выделить блокировку передаваемого сигнала от КА и объекту управления и обратно. В результате данного негативного воздействия на систему спутниковой связи ЦПО комплекса мониторинга, контроля и управления не способен правильно выбрать соответствующее управляющее воздействие на необслуживаемый объект.

Проведенный анализ работ [45,63] позволил сделать вывод о том, что в настоящее время достаточно эффективно, применяются пассивные помехи (ПП). Особое место среди пассивных помех, используемых в комплексах РЭБ, занимают следующие ПП:

- гармоническая непрерывные помехи (ГНП);
- прицельные непрерывные шумовые помехи (ПНШП).
- заградительные непрерывные шумовые помехи (ЗНШП).

Для получения пассивных помех, относящихся к первой группе гармонических непрерывных помех, применяют генераторы, работа которого представляется следующим выражением

$$U_{\text{ГНП}}(t) = U_{mm}\cos\left(\omega_{p2}t + \varphi_{p2}\right), \tag{1.1}$$

где $\omega_{p2} \in [\omega_0 - \pi\Delta f_2; \omega_0 + \pi\Delta f_2]$ – угловая частота помехи; U_{mm} – амплитуда гармонической непрерывной помехи; φ_{p2} - начальная фаза гармонической непрерывной помехи.

Анализируя выражение (1.1), можно сделать вывод о том, что по своей структуре такая непрерывная помеха является очень простой. В качестве достоинства гармонических непрерывных помех можно отметить то, что для ее постановки применяют генераторы гармонических колебаний. С целью повышения эффективности работы систем РЭБ, использующих пассивные непрерывные помехи, в работах [46,50] предлагают применять прицельные и заградительные непрерывные помехи.

Наибольшее распространение среди ПНШП и ЗНШП получила шумоподобная помеха (ШП) типа «квазибелый» шум. Данный вид пассивной помехи реализуют с помощью следующей математической модели, которая определяется выражением

$$U_{ШП}(t) = U_{mm}(t)\cos\left(\omega_{p1}t + \varphi_{p1}(t)\right), \qquad (1.2)$$

где $U_{mm}(t)$ - закон изменения огибающей шумоподобной помехи; $\varphi_{p1}(t)$ - закон изменения фазы шумоподобной помехи; ω_{p1} - средняя частота помехи; $\omega_{p1} \approx \omega_0; \omega_0 = 2\pi L$; L - несущая частота сигнала.

Помеха ШП типа «квазибелый шум», характеризуется достаточно простым алгоритмом ее выработки и постановки. Благодаря данному свойству шумоподобная помеха, как и рассмотренная ранее гармоническая непрерывная помеха, широко применяются в комплексах РЭБ.

Однако, обладая достаточно высокой простотой реализации, такие пассивные помехи нецелесообразно применять для подавления передачи ССС, используемых в комплексах мониторинга, контроля и управления объектами, расположенными районах Крайнего Севера. Это связано, во-первых, с удаленным расположением объектов управления, на которых находятся приемники ССС, а, во-вторых, для комплексов пассивного шумового

подавления необходимо обеспечить прямую видимость со спутником связи, что за Полярным Кругом сделать достаточно затруднительно. Обобщая сказанное, можно сделать вывод о том, что такой подход к нарушению функционирования ССС в районах Крайнего Севера является низкоэффективным и затратным.

Рассмотри группу активных помех (АП), которые позволяют достаточно эффективно блокировать канал связи системы спутниковой связи [45,63]. Очевидно, что применение таких помех позволит злоумышленнику получить достаточно хорошие результаты радиоэлектронного противодействия группировке низкоорбитальной ССС.

Преследуя главную цель радиоэлектронной борьбы, а также учитывая особенности применения средств РЭБ, было разработано множество активных помех. Все множество АП, которые могут привести к нарушению функционирование низкоорбитальной системы спутниковой связи, целесообразно разделить на две группы.

В основу первой группы входят активные маскирующие помехи (АМП) [46]. Характерной чертой данной группы помех являются их тактико-технические характеристики. Во-первых, они сначала не позволяют приемнику радиосвязи обнаружить передаваемый сигнал. А, во-вторых, АМП не позволяют провести эффективную обработку принятого сигнала. В зависимости от методов получения активные маскирующие помехи можно разделить наследующие виды:

– активные непрерывные шумовые помехи;
– последовательности детерминированных импульсных сигналов;
– хаотические импульсные помехи.

Рассмотрим данные виды активных помех. Амплитудно-модулированные шумовые помехи (АМШП) представляют собой незатухающие гармонические колебания, математическая модель которых определяется выражением

$$U(t) = U_{П}\left[1 + K_{а}\Delta U_{МОД}(t)\right], \qquad (1.3)$$

где $K_а$ - крутизна модуляционной характеристики передатчика; $\Delta U_{МОД}(t)$ - моделирующее направление, поступающее от генератора шума.

В ряде случаев кроме активных непрерывных шумовых помех в комплексах радиоэлектронной борьбы используют последовательности детерминированных импульсных сигналов [51]. Если $\{x[k]\}, k = 0, \pm 1, \pm 2, \ldots$ - последовательность детерминированных импульсных сигналов, то мгновенная мощность такого сигнала равна $\left|x[k]^2\right|$, а полная энергия определяется выражением

$$E_{x} = \sum_{k=-\infty}^{+\infty}\left|x[k]\right|^{2}. \qquad (1.4)$$

Тогда средняя мощность такой активной помехи - последовательности детерминированных импульсных сигналов $\{x[k]\}$ равна

$$P_{x} = \left\langle\left|x[k]\right|^{2}\right\rangle = \lim_{T\to\infty}\frac{1}{2T+1}\sum_{k=-T}^{T}\left|x[k]\right|^{2}. \qquad (1.5)$$

Наряду с рассмотренными выше помехами в комплексах РЭБ применяются активные помехи, которые относятся к хаотическим импульсным помехам [51]. Как правило, такие хаотические помехи характеризуются последовательностью радиоимпульсов с заданным заранее значениями частоты заполнения. При этом значения амплитуды и длительности помехи, а также интервалы между соседними импульсами могут изменяться случайным образом. На практике используется последовательность радиоимпульсов, имеющих одинаковую амплитуду и характеризующихся случайными изменениями длительности импульсов M_{τ} и временных интервалов между ними M_{Δ}. В этом случае имеем

$$M_{\tau} = \frac{\pi}{\sqrt{-\rho_{о}}}\left[1 - \Phi\left(\frac{\gamma}{\sqrt{2}}\right)\right]\exp\left(\frac{\gamma^{2}}{2}\right), \qquad (1.6)$$

$$M_{\Delta} = \frac{\pi}{\sqrt{-\rho_{o}}}\left[1 + \Phi\left(\frac{\gamma}{\sqrt{2}}\right)\right]\exp\left(\frac{\gamma^{2}}{2}\right), \qquad (1.7)$$

где $\rho_0 = \left.\frac{d_2\rho(\tau)}{d\tau^2}\right|_{\tau=0}$; $\rho(\tau)$ - коэффициент корреляции шума генератора; $\gamma = \frac{U_0}{\sigma_{ш}}$;

$\Phi(\gamma) = \frac{2}{\sqrt{\pi}}\int_0^{\gamma} e^{-x^2} dx$ - интеграл вероятности; $\sigma_{ш}$ - дисперсия шума.

Очевидно, что каждый рассмотренный вид АП по-своему воздействует на канал радиосвязи. Поэтому при выборе активной помехи, которая позволила бы эффективно воздействовать на канал передачи данных, необходимо учитывать целый ряд параметров, среди которых можно выделить:

- временные, спектральные, а также статистические характеристики используемого сигнала;

- отношение мощность сигнала к мощности помехи на входе приемника спутника низкоорбитальной ССС.

Чтобы достичь поставленные цели, с использованием активных шумоподобных помех, необходимо перед их применением провести радиоразведку. В качестве основных параметров радиосвязи, которые будут подвергнуты радиоразведки, можно выделить:

– несущая частота передаваемого сигнала;

– полоса пропускания канала радиосистемы;

– амплитуда передаваемого сигнала.

С целью повышения эффективности проведения радиоэлектронной борьбы кроме отмеченных выше помех в комплексах РЭБ используются активные имитирующие помехи (АИП) [46]. Характерной чертой АИП можно отметить цель их постановки. Чтобы нарушить работу систем радиосвязи АИП могут обеспечить перегрузку каналов передачи и обработки информации. Кроме того, такие помехи используются для навязывания ложной информации. К активным имитирующим помехам относятся:

– прицельная имитирующая помеха (ПИП);

– следящая имитирующая помеха (СИП);

– заградительная имитирующая помеха (ЗИП).

Рассмотрим данные активные имитирующие помехи. Такие помехи называют «интеллектуальными» помехами, которые способны подстраиваться под передаваемый сигнал, нарушая тем самым эффективную работу системы радиосвязи.

Для получения прицельной имитирующей помехи используют следующее выражение

$$U_{ПИП}(t) = K\ U_m Q_i(t - t_d - \Delta\tau)\sin\left[2\pi\left(L \pm \Delta f\right)\left(t - t_d - \Delta\tau\right) + \varphi\right], \qquad (1.8)$$

где K – коэффициент, учитывающий уровень ПИП.

Прицельная имитирующая помеха представляет собой процесс, подобный передаваемому сигналу, с частотным и временным рассогласованием, а также с фиксированным значением фазы огибающей манипулирующей функции.

Рассмотрим математическую модель получения следящей имитирующей помехи. Для получения данной помехи используется следующее выражение

$$U_{СИМ}(t) = K\ U_m Q\ (t - t_d - \tau(t))\sin\left[2\pi\left(L \pm \Delta f\right)\left(t - t_d - \tau(t)\right) + \varphi\right], \qquad (1.9)$$

где $\tau(t) = r(t)/c$ - расстояние от спутника до станции РЭБ.

Следует отметить, что следящая имитирующая помеха подобна прицельной имитирующей помехе, но с переменной начальной фазой манипулирующей функции, закон изменения которой соответствует изменению расстояния r(t) от КА до станции РЭБ.

Рассмотрим математическую модель получения заградительной имитирующей помехи. Для получения данной помехи используется следующее выражение

$$U_{ЗИП}(t) = \sum_{i=1}^{n_{RA}} K_i U_m Q_i(t - t_d - \tau))\sin\left[2\pi\left(L \pm \Delta f\right)\left(t - t_d - \tau\right)\right) + \varphi\right]. \qquad (1.10)$$

Следует отметить, что среди рассмотренных выше активных имитирующих помех наиболее простой по своей реализации выступает помеха тип ЗИП.

Наряду с активными и пассивными помехами комплексы РЭБ могут использовать различные способы, позволяющие имитировать или перехватывать «правильные» сигналы с последующим их навязыванием противнику. Такой подход к нарушению эффективной работы систем радиосвязи позволил создать вторую группу воздействия комплексов РЭБ на системы связи.

Главной целью таких способов, базирующихся на навязывании ложного или перехваченного сигнала, является подмена передаваемого сигнала. Рассмотрим особенности работы комплексов РЭБ, которые работаю с ложными сигналами. Основные принципы построения таких средств РЭБ показаны в работе [45]. Следует отметить, что применение такого подхода к построению радиоэлектронному противодействию системам связи требует значительных схемных и временных затрат на свою реализацию. Это связано с тем, что такие технические средства радиоэлектронной борьбы должны иметь возможность воспроизводить копии передаваемых сигналов в системах спутниковой связи. Для этого необходимо произвести тестирование приемников и передатчиков, используемых в ССС. В работах [45,63] показаны процедуры тестирования приемников и передатчиков для систем радиосвязи, выполняемые в лабораторных условиях при проведении сертификации и поверки средств связи. В данной работе достаточно подробно представлены основные технические блоки, которые можно использовать для проведения тестирования приемников и передатчиков. Очевидно, что использование таких средств в комплексах РЭБ при неправомерном их применении позволит навязать спутнику ложные сигналы. Применение таких средств тестирования связи приведет к нарушению эффективного обмена данных в системах спутниковой связи. Это связано с тем, что приемник ССС, который входит в состав абонентский терминала объекта добычи и транспортировки

углеводородов, будет считать принятые со спутника сигналы управления как «свои». После получения сигналов, имитирующих настоящие команды управления, абонентский терминал приступит к их исполнению, что привести к ситуации, когда объекта управления выйдет из строя. Чтобы усложнить такую задачу в работах [14,55,56] предлагается использовать специальные квазиортогональные сигналы, которые характеризуются повышенной структурной скрытностью. Кроме того, в данных работах, предлагается периодически менять структуру передаваемых сигналов. Таким образом, очевидно, что использование имитации передаваемых сигналов низкоорбитальными системами спутниковой связи требует значительных схемных и финансовых затрат на реализацию технических средств РЭБ.

В ряде работ по радиоэлектронной борьбе [45,63] рассматриваются способы, которые используют принцип перехвата и навязывания противнику перехваченных сигналов. Используя данные методы, спутник-нарушитель должен сначала перехватить передаваемые сигналы от космического аппарата, которые предназначены абонентскому терминалу необслуживаемому объекту. После этого такой перехваченный сигнал сохраняется в памяти спутника-нарушителя определенное время. Затем, спустя некоторый временной интервал, перехваченный сигнал передается приемнику ССС, который в состав абонентского терминала управления удаленным объекта. В этом случае приемник однозначно примет такой сигнал, а абонентский терминал приступит к исполнению команды управления. Это связано с тем, принятый сигнал будет иметь свою соответствующую структуру, а его параметры будут полностью совпадать с параметрами сигналов, которые используются низкоорбитальной ССС, входящей в состав комплекса контроля, мониторинга управления. При определенных условиях это может привести к внештатной ситуации на необслуживаемом объекте добычи и транспортировки углеводородов. А неправильная работа системы управления таким удаленным объектом способна вызвать экологическую катастрофу, которая негативно скажется на природе Крайнего Севера.

Чтобы не позволить спутнику-нарушителю навязать абонентскому терминалу перехваченную и задержанную команду необходимо не допустить обмен данными между таким космическим аппаратом и приемником ССС, находящимся на объекте управления. Для этого до начала сеанса связи целесообразно определить статус спутника. Такой подход не позволит допустить передачу данных с борта спутника-нарушителя. В результате применения системы опознавания «свой-чужой», спутник, который не имеет статус «свой», не сможет осуществлять сеанс связи с приемником ССС абонентского терминала удаленного объекта управления. При этом для навязывания задержанной команды управления спутнику-нарушителю необходимо будет подобрать правильный «ответ» на запрос, поступающий от запросчика системы «свой-чужой», расположенного на объекте управления.

Поэтому применение системы опознавания космического аппарата, используемой в низкоорбитальных системах спутниковой связи, является одним из наиболее эффективных методов противодействия навязыванию приемнику ССС удаленного объекта перехваченных и задержанных команд управления.

Поэтому целью диссертационных исследований является повышение имитостойкости низкоорбитальной ССС за счет использования метода построения системы опознавания космического аппарата, применение которого позволит снизить вероятность пропуска спутника-нарушителя.

1.2.3 Анализ проблемной ситуации повышения имитостойкости низкоорбитальной системы спутниковой связи на основе использования систем опознавания «свой-чужой»

В настоящее время известно множество систем опознавания «свой-чужой», которые нашли широкое применение во многих странах. Исходя из целей, которые ставятся перед такими системами, одной из основных сфер их применения являются Вооруженные Силы. Как правило, запросно-ответная система опознавания представляет собой программно-аппаратный комплекс, предназначенный для определения принадлежности идентифицируемого объекта (самолета, беспилотного летающего объекта, морских судов) [68].

Большинство запросно-ответных систем относятся к активным радиолокационным системам. В радиолокационных системах с активным ответом классификация проводится за счет отправки запроса объекту в различных режимах и анализа полученных ответов.

В настоящее время различают следующие виды опознавания [7]:

– общее опознавание;

– индивидуальное опознавание.

Запросно-ответные системы, использующие общее опознавание «свой-чужой», предназначены для определения принадлежности объекта определенной стране. Решение о принадлежности объекта осуществляется при получении на запросы необходимых сигналов ответа действующими кодами. Если полученные сигналы с действующими кодами полностью соответствуют требованиям системы опознавания, то статус объекта «свой». Если полученные сигналы с действующими кодами полностью не соответствуют требованиям системы опознавания, то статус объекта «чужой».

На практике широко используются запросно-ответные системы, использующие индивидуальное опознавание. При этом индивидуальное опознавание отлично от общего тем, что во время процедуры опознания происходит выделение отдельных объектов по какому-либо признаку (например, индивидуальный номер). Чтобы исключить угрозу использования системы злоумышленником, применяются различные средства для

засекречивания обмена данными.

Проведем анализ наиболее известных отечественных и зарубежных систем опознавания «свой-чужой». В Российской Федерации нашли широкое применение запросно-ответные системы «Кремний-2», которые достаточно распространены в Министерстве обороны РФ [6,43]. Различают два вида станций «Кремний 2». В первом случае применяется станция, имеющая название СРЗО-2. Данная станция представляет собой систему типа «запрос-ответ» для самолетов. Во втором случае применяется станция СРО-2, которая является только ответчиком. В работе [13] рассмотрены принципы работы данной системы «свой-чужой». Эта система радиолокационного опознавания самолетов использует для запросов и ответов одну несущую частоту в III диапазоне дециметровых волн. Данная система может функционировать в четырех режимах работы, а именно:

- режим неимитостойкого опознавания самолетов;
- режим контрольного запроса;
- режим индивидуального опознавания;
- режим «Бедствие».

С помощью первого режима работы запросно-ответной системы можно определить государственную принадлежность самолета. Для опознавания движущегося объекта используется радиолокационная станция. После получения координат такого объекта запросчик осуществляет передачу на частоте f_1 запросного сигнала. В качестве такого сигнала используются три радиоимпульса, имеющих фиксированную структуру. То есть временные интервалы между этими импульсами являются константанами. Данный сигнал принимается ответчиком с помощью ненаправленной антенны, а затем проводится его анализ во временной области (определяются временные интервалы между принятыми импульсами). После этого ответчик формирует ответный сигнал, который содержит три радиоимпульса. При этом первый радиоимпульс подвергается амплитудной модуляции гармоническим

сигналом, имеющим частоту F_{AM}. Изменяя значение частоты модуляции F_{AM} и временные интервалы между импульсами τ_1, τ_2, ответчик может получить 36 возможных комбинаций ответа, так как система имеет шесть вариантов частоты F_{AM} и шесть различных временных интервалов. Таким образом, за каждой комбинацией закреплен соответствующий сигнал ответчика. Выбранный ответный сигнал передается запросчику, который осуществляет проверку соответствия между принятым сигналов и используемой в текущий момент комбинацией. Для повышения точности процедуры опознавания она производится несколько раз. Очевидно, что имитостойкость данного режима работы определяется только периодической сменой действующих кодов сигнала ответчика на основе использования единого расписания смены кодов.

Второй режим работы запросно-ответной системы (запрос К) предлагается применять в условиях, когда противник пытается провести имитацию правильного ответа. Для этого в данном режиме работы запросчик передает объекту на три радиоимпульса, а четыре. В этом случае ответчик, соответствующий нашему объекту, не будет отвечать на полученный сигнал. При этом при попытке противника имитировать правильный ответ запросчик получит ответный сигнал, который показывает, что объект является своим. В этом случае полученный сигнал будет соответствовать ситуации, когда проверяемый объект является чужим.

При использовании третьего режима работы запросно-ответная система позволяет определить положение проверяемого объекта относительно других. Для этого в ответный сигнал, который соответствует первому режиму работы, добавляют четвертый импульс. При этом временной интервал задержки четвертого импульса позволяет путем подсветки выявить местоположение проверяемого объекта.

Четвертый режим используется для передачи запросчику данных об аварийной ситуации на объекте. Для этого используются два сигнала, промодулированных гармоническим колебанием с частотой F_{AM}.

На рисунке 1.1 показана структура неимитостойкой запросно-ответной системы «свой-чужой».

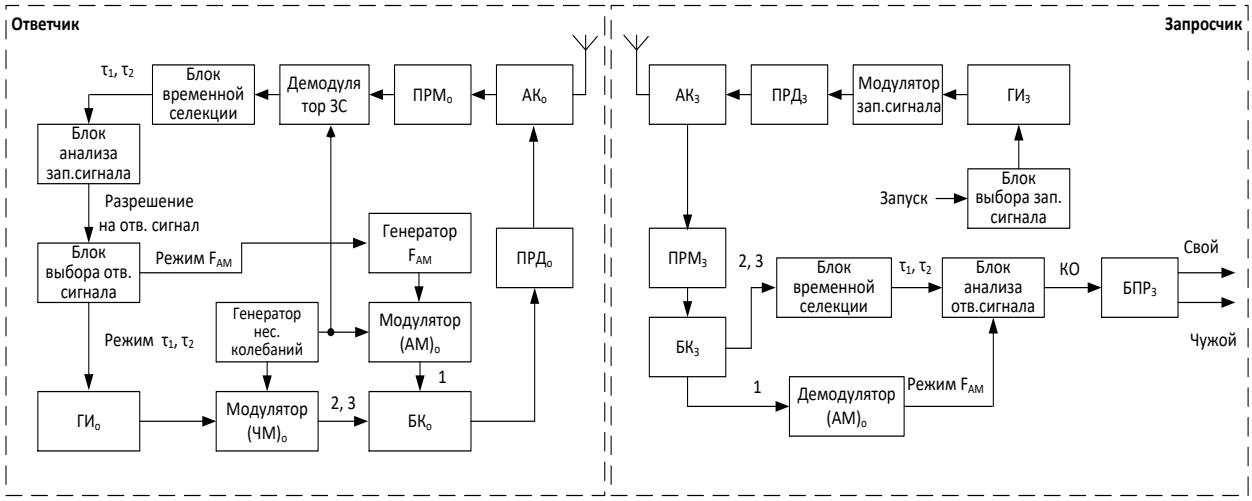

Рисунок 1.1 - Структура неимитостойкой запросно-ответной системы «свой-чужой»

Проведенный анализ работы [13] показал, что данная система опознавания обладает рядом недостатков:

– низкий уровень имитостойкости;

– относительно низкая пропускная способность, которая позволяла осуществлять одновременную работу 10 запросчиков и 10 ответчиков;

– достаточно низкая помехоустойчивость, из-за малой мощности передающих устройств ответчиков и запросчиков.

Из-за небольшого числа возможных комбинаций ответа такая система опознавания «свой-чужой» характеризуется вероятностью имитации противником сигнал «Свой» за обзор равной $P_{ИМ} = 0,1$.

Таким образом, очевидно, что использование такой запросно-ответной системы для повышения имитостойкости НССС является нецелесообразным.

Повысить имитостойкость позволяет система радиолокационного опознавания «Пароль» [40]. Данная система кроме рассмотренных выше режимов работы имеет и дополнительные. К ним можно отнести:

– режим общего неимитостойкого опознавания (1 режим VII диапазона);

– режим общего имитостойкого опознавания (2 режим VII диапазона);

– режим индивидуального опознавания (3 режим VII диапазона).

Характерной особенностью имитостойкой запросно-ответной системы является, во-первых, использование более высокого диапазона частот, что позволило повысить помехоустойчивость. Во-вторых, в данной системе для передачи запроса используется частота f_1, для передачи ответа применяются две частоты f_2 и f_3, что позволяет повысить пропускную способность системы. Рассмотрим работу системы в режиме общего неимитационного опознавания. Данный режим позволяет эффективно определять государственную принадлежность самолета в условиях работы многих систем опознавания. После обнаружения объекта запросчик передает ему четыре радиоимпульса, которые имеют постоянные временные интервалы между сигналами. Для этого запросчик использует частоту f_1. Первые три радиоимпульса передаются с помощью остронаправленной антенны. Четвертый импульс, который носит название импульс подавление боковых лепестков (ПБЛ), передается с помощью слабонаправленной антенны. Ответчик, получив данные радиоимпульсы, производит сравнение их амплитуд. Если амплитуда импульса ПБЛ будет меньше чем первых трех радиоимпульсов, то ответчик приступает к формированию ответа. При этом ответный сигнал будет передаваться с помощью двух частот f_2 и f_3. Для ответа в данном режиме существует 6 кодограмм, определяемых тремя вариантами длительности τ_1, τ_2 и двумя комбинациями частот. Очевидно, что обеспечить имитостойкость возможно за счет периодической смены ответных кодов.

Устранить данный недостаток позволяет использование режима общего имитостойкого опознавания. Данный режим позволяет определить государственный статус объекта даже в условиях работы имитации ответов противником. Для повышения имитостойкости предлагается использовать специальные методы кодирования запросного и ответного сигналов [13]. В

этом случае каждый день происходит случайная выборка N действующих кодов запросного сигнала из числа имеющихся $N_{общ} = 9^{11}$. Затем каждому выбранному коду запросного сигнала подбирается один из 16 возможных кодов ответного сигнала. Полученная таблица доставляется на все запросчики и ответчики. Данной таблицей будут пользоваться в течение целого дня для опознавания объекта. Благодаря данному режиму работы снижается вероятность имитации противником сигнала «свой» до величины $P_{ИМ} = 0{,}005$.

Проведенный анализ неимитостойкой и имитостойкой запросно-ответных систем «свой-чужой» показал, что данные системы обладают достаточно низкой имитостойкостью. Повысить ее возможно за счет использования методов шифрования. В работе [13] рассматривается работа системы опознавания «Пароль» с использованием засекречивающей аппаратуры опознавания (ЗАО-П). Данная аппаратура предназначена для формирования запросного сигнала (ЗС) в имитостойком режиме с использованием алгоритмов шифрования. Для работы системы «свой-чужой» используется запросный сигнал, который состоит из:

– группы синхроимпульсов, определяющих начало запросного сигнала (4 импульса);

– одного импульса подавления боковых лепестков, применение которого позволяет повысить пропускную способность системы;

– одного ключевого импульса, при наличии которого ответчик переходит на новый код;

– информационной группы, содержащей 30 позиций, в которых количество импульсов и их временная расстановка изменяются в каждом ЗС с использованием с помощью аппаратуры шифрования;

– группы из 8 импульсов, определяющих признак ответчика (ПОК), применение которых обеспечивает повышение достоверности, так как получается на основе информационной части.

Одновременно с запросчиком ответчик, зная закон построения,

производит формирование информационной части запросного сигнала. Затем для данной информационной части производится вычисление проверочной части ПОК. Получив запросный сигнал, ответчик производит сравнение принятого сигнала с вычисленным. При их совпадении ответчик формирует ответный сигнал, который передается запросчику. В противном случае – ответчик не осуществляет передачу.

На рисунке 1.2 представлена структура запросно-ответной системы, реализующей опознавание объекта с использованием методов шифрования. Данная система предназначена для установки на самолеты. Система «свой-чужой» состоит из запросчика и ответчика. В состав запросчика входят регистр запросчика Ргз, предназначенный для хранения вектора начального заполнения, счетчик запросчика Счз, кодовое вычислительное устройство КВУз, сумматор по модулю два Сумз, декодер ответного сигнала ДОСз, приемник ответного слова ПРМз, антенный коммутатор АКз, буферный регистр БРгз, шифратор запросчика Шз, блок памяти для хранения секретного ключа БПХКз, кодер запросного сигнала КЗСз, передатчик запросного сигнала ПРДз, генератор таковых импульсов ГТИз.

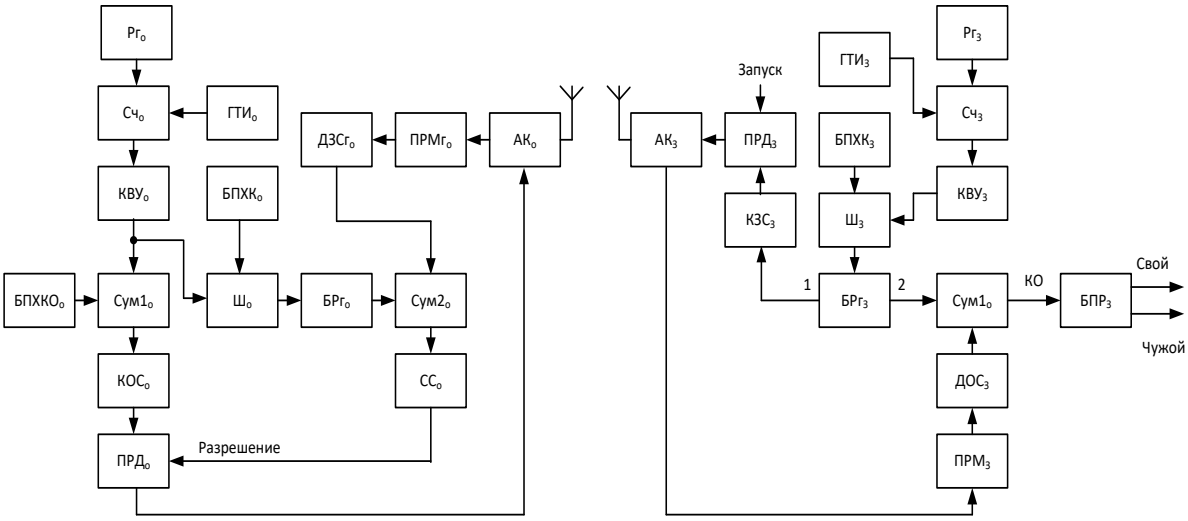

Рисунок 1.2 - Структура запросно-ответной системы, реализующей опознавание объекта с использованием методов шифрования

В состав ответчика системы «свой-чужой» входят регистр ответчика

Рго, предназначенный для хранения вектора начального заполнения, счетчик ответчика Счо, кодовое вычислительное устройство КВУо, первый сумматор по модулю два Сум1о, кодер ответного сигнала КОСо, передатчик ответного сигнала ПРДз, антенный коммутатор ответчика АКо, буферный регистр БРго, шифратор ответчика Шо, блок памяти для хранения секретного ключа БПХКо приемник запросного сигнала ПРМо, декодер запросного сигнала ДЗСз, второй сумматор по модулю два Сум2о, счетчик совпадения ССо, блок памяти для хранения кода объекта БПХКОо, генератор таковых импульсов ответчика ГТИо.

Система «свой-чужой» работает следующим образом. Ежедневно перед запуском самолета в ответчик, который располагается на борту объекта, заносятся текущие значения секретного ключа в БПХКо, кода объекта в БПХКОо, вектора начального заполнения в регистр Рго. Одновременно с этим аналогичный секретный ключ и вектор начального заполнения заносятся в БПХКз и Ргз запросчика. При включении ответчика и запросчика вектор начального заполнения в регистров Рго и Ргз записывается в счетчики Счо и Счз. Импульсы, поступающие с выходов генераторов тактовых импульсов ГТИо и ГТИз., изменяют синхронно значение счетчиков. Кодовые вычислительные устройства КВУо и КВУз, предназначены для генерации псевдослучайной последовательности чисел. Шифраторы Шо и Шз имеют одинаковую структуру, и алгоритмы их работы определяются симметричными секретными ключами.

Рассмотрим работу ответчика до поступления запросного сигнала. Выходное значение Счо поступает на вход кодового вычислительного устройства КВУо, которое с помощью алгебраических и логических преобразований, генерирует на выходе псевдослучайное число. Данное число с помощью первого Сум1о суммируются по модулю два с кодом объекта, хранящимся в БПХКОо. Результат суммирования подается на кодер ответного сигнала КОСо, который предназначен для преобразования двоичного кода в импульсный или частотный код. Результат преобразования поступает на

первый вход передатчика ответного сигнала ПРДз. Однако передача данного сигнала не осуществляется, так как на втором входе отсутствует сигнал управления, поступающий со счетчика совпадения ССо.

Кроме того, псевдослучайное число с выхода кодового вычислительного устройства КВУо поступает на вход шифратора ответчика Шо, который с помощью секретного ключа, хранящегося в БПХКо, производит его зашифрование. Результат криптографического преобразования записывается в буферный регистр БРго. Ответчик готов к процедуре опознавания.

В запросчике происходят следующие преобразования. Выходное значение Счз поступает на вход кодового вычислительного устройства запросчика КВУз, с выхода которого снимается псевдослучайное число. Данное число записывается в буферный регистр запросчика БРгз, а затем с первого его выхода поступает на шифратор запросчика Шз, который с помощью секретного ключа, хранящегося в БПХКз, производит зашифрование. Результат криптографического преобразования подается на вход кодера запросного сигнала КЗСз. Импульсный или частотный код запросного сигнала поступает на первый вход передатчика запросного сигнала ПРДз. Однако передача запросного сигнала не осуществляется, так как отсутствует команда «Запрос». Таким образом, представленная на рисунке 1.2 система опознавания готова к работе.

Сигнал «Запрос» может быть подан автоматически, в момент, когда неопознанный объект появляется в зоне видимости запросчика. В этом случае передатчик ПРДз подключается к антенному коммутатору запросчика АКз, и запросный сигнал посылается в эфир. Запросный сигнал принимается антенной ответчика и через антенный коммутатор АКо поступает приемник ПРМо. Затем запросный сигнал подается на декодер ДЗСо, с выхода которого снимается двоичный код. Полученная кодовая комбинация подается на первый вход второго сумматора по модулю два Сум2о, а на второй поступает зашифрованная кодограмма из буферного регистра БРго. Результат побитового суммирования подается на вход счетчика совпадения ССо. При

полном совпадении принятого запросного сигнала с сигналом, вычисленным ответчиком, ССо передает сигнал управления на второй вход передатчика ПРДо. Данный передатчик подключается к антенному коммутатору ответчика АКо, и ответный сигнал передается запросчику.

Запросчик, приняв ответный сигнал, через антенный коммутатор АКз передает его на вход приемника ПРМз. С выхода последнего ответный сигнал поступает на декодер ответного сигнала $ДОС_з$, который преобразует его в двоичный код. Полученная кодовая комбинация поступает на первый вход сумматора по модулю два $Сум_з$, где поразрядно складывается с зашифрованным числом, хранящимся в буферном регистре БРгз. Если полученный результат совпадает с кодом ответчика, то данному объекту присваивается статус «свой». В противном случае, объект считается чужим.

Проведенный анализ работы данной системы показал, что при использовании зашифрованного сигнала, имеющего информационную часть равную 30 бит, вероятность имитации противником сигнал «Свой» составит $P_{И} = 2^{-30} = 9{,}31 \cdot 10^{-10}$, в то время как имитостойкая система опознавания «свой-чужой» без шифрования обеспечивает РИ = 0,005. Таким образом, очевидно, что применение методов шифрования позволяет снизить вероятность имитации противником сигнал «Свой».

Следует отметить, что запросно-ответные системы опознавания используются не только в наших ВС РФ. В настоящее время известна система опознавания самолетов МК-XII, которая достаточно успешно применяется в Вооруженных Силах США [44]. Для повышения криптостойкости в запросно-ответной системе МК-XII введен «Режим-4», в котором используется псевдослучайный закон, определяющий соответствие между запросом и ответом. Дальнейшее совершенствование данной системы привело к появлению модификации МК-XIIA. Чтобы повысить имитостойкость в модифицированной системе МК-XIIA предлагается использовать криптографическое стандарт STANAG 4193 [6].

В работе [101] показана возможность расширения сферы применения системы опознавания. С целью снижения потерь от огня своих подразделений была разработана боевая система опознавания, кототрая получила название Battlefield Combat Identification System (BCIS). Предполагается, что Вооруженные Силы США будут применять данную систему опознавания на поле боя. Использование запросно-ответной системы позволит идентифицировать танки и боевые машины пехоты в реальном масштабе времени. Проведенные натурные испытания показали достаточно высокую эффективность работы такой системы опознавания. Однако систему не приняли на вооружения из-за ее высокой стоимости.

Рассмотрим перспективные решения по построению системы опознавания «свой-чужой». Для этого проведем патентный поиск среди отечественных и зарубежных решений.

В работе [95] повышение криптографической стойкости системы определения «свой-чужой» осуществляется на основе использования псевдослучайных последовательностей (ПСП). Для этого предлагается в запросчике и ответчике формировать последовательности 4 запросных и 4 ответных импульсов, которые имеют стандартные временные интервалы длительностью 10 мс. При этом временной интервал между этими импульсами определяется по закону ПСП. Кроме того, временное положение запросных и ответных импульсов также изменяется в пределах типового импульса по псевдослучайному закону последовательности. Для модуляции импульсов применяются 256-элементные псевдослучайные последовательности, которые меняются от импульса к импульсу.

Рассмотрим работу запросно-ответной системы, приведенной в патенте [58]. Представленная в работе система используется для определения принадлежности самолетов и других летательных объектов. Система опознавания «свой-чужой» состоит из запросчика и ответчика. Запросчик располагается на Земле. Ответчик располагается на подвижном объекте. Для эффективной запросно-ответной системы необходимо обеспечить

синхронизацию между ответчиком и запросчиком. При этом данная процедура должна производиться на Земле до запуска самолета или другого летательного аппарата с использованием соответствующего канала связи. Данный недостаток этой системы опознавания не позволяет его использовать для опознавания спутника.

Рассмотрим работу запросно-ответной системы, приведенной в патенте [58]. В данной работе рассмотрена имитостойкая запросно-ответная система. При этом для повышения ее имитостойкости в патенте предлагается использовать пароль и шифровальную колодку. Данная колодка имеет одинаковое количество входов и выходов. С целью повышения имитостойкости предлагается в данной колодке осуществлять операцию перестановки. В результате этого каждый из m входов колодки по определенному закону подключается к соответствующему из m выходов. Очевидно, что степень криптостойкости система опознавания «свой-чужой» определяется размерами колодки $m \times m$. Очевидно, что в процессе работы запросно-ответной системы необходимо периодически менять перестановку в шифровальной колодке.

Рассмотрим работу запросно-ответной системы, приведенной в патенте [91]. В данном патенте представлена запросно-ответная система, которая для защиты передаваемых данных от НСД в процессе опознавания статуса летательного аппарата использует специальные закодированные сигналы. В качестве недостатка данного способа опознавания «свой-чужой» можно отметить необходимость использования согласованных рубидиевых фильтров, для обеспечения высокой степени синхронизации сигналов. Реализовать данное требование в системе спутниковой связи довольно сложно.

Рассмотрим работу системы опознавания «свой-чужой», приведенной в патенте [60]. В данном патенте показан способ построения запросно-ответной системы на основе использования радиолокационного устройства. Данная система предназначена для опознавания статуса воздушных объектов. В

качестве основного недостатка этой запросно-ответной системы можно отметить, что такая система может определить только тип воздушного объекта. При этом представленная в работе система опознавания «свой-чужой» не способна определить статус данного объекта.

Рассмотрим работу запросно-ответной системы, приведенной в патенте [92]. В данном патенте предлагается новый способ опознавания летательных объектов с использованием лазерного излучения. Следует отметить, что представленный в работе способ идентификации статуса подвижных воздушных объектов, обладает недостатком, который связан с тем, что для его эффективной работы необходимо обеспечить прямую видимость и хорошие климатические условия. Таким образом, очевидно, что данный способ невозможно применить для идентификации спутника низкоорбитальной группировки.

В работе [93] предлагается для определения статуса объекта Для определения статуса объекта использовать зашифрованный 64 битовый код. Меняется каждые 24 часа. Основным недостатком данной системы «свой-чужой» является использование закрытого канала для передачи на объекты правильного идентификатора.

В работе [94] представлена система опознавания «свой-чужой». В данной системе для опознавания летательного объекта предлагается использовать благодаря источникам UV света, которые располагаются на самом объекте. Недостаток данного решения является то, что использовать источники UV света для определения статуса спутника невозможно.

Проведенный анализ альтернативных методов построения запросно-ответных систем опознавания позволил выявить следующую проблемную ситуацию. Известные принципы построения систем «свой-чужой» без использования методов криптографии не позволяют обеспечить требуемые уровни имитозащиты. Так при использовании системы опознавания без режима имитостойкого опознавания объекта вероятность имитации противником сигнал «Свой» будет составлять $P_И$ = 0,1. Улучшить данный

критерий позволяет система «свой-чужой», использующая режим общего имитостойкого опознавания. В результате этого вероятность имитации противником сигнал «Свой» снизилась до величины $P_И$ = 0,005. Однако полученное значение не позволяет коренным образом повысить имитостойкость низкоорбитальной системы спутниковой связи.

Качественным скачком в обеспечении высокой имитостойкости запросно-ответных систем является использование методов шифрования. Применение методов симметричной криптографии позволяет обеспечить вероятность имитации противником сигнал «Свой» равной $P_И = 2^{-L}$, где L – длина запросного сигнала. Так при использовании зашифрованного запросного сигнала, имеющего информационную часть равную 30 бит, вероятность имитации противником сигнал «Свой» составит $P_И = 2^{-30} = 9{,}31 \cdot 10^{-10}$. При этом очевидно, что увеличение размерности запросного сигнала приводит к повышению имитостойкости самой системы «свой-чужой». А это способствует снижению вероятности навязывания имитирующих и ретрансляционных помех. Таким образом, между имитостойкостью запросно-ответной системы «свой-чужой» и имитостойкостью НССС существует прямо пропорциональная зависимость. То есть решение, определенное из множества альтернативных методов построения системы «свой-чужой», которое позволит обеспечить самую минимальную вероятность имитации сигнала «Свой», будет считаться оптимальным для решения проблемы повышения имитостойкости НССС.

Однако анализ условий функционирования элементов НССС, во-первых, это невозможность временной посадки спутников на Землю, а, во-вторых, расположение приемо-передающих станций на объектах управления в малонаселенной местности, позволяют сделать вывод о том, что использование методов шифрования в системах опознавания космического аппаратов невозможно. Так в рассмотренной системе опознавания «Пароль» для повышения имитостойкости секретные ключи необходимо менять

ежедневно [13]. Обеспечить своевременную смену ключей на орбите и на необслуживаемом объекте, где размещается запросчик системы «свой-чужой» возможно следующими способами:

– созданием достаточно большой базы данных секретных ключей, которая будет размещаться как на КА, так и на необслуживаемом объекте;

– организовать ежедневную передачу секретных ключей ответчику и запросчику с использованием закрытого канала.

Очевидно, что реализация первого решения может привести к компрометации секретных ключей в результате падения спутника или нарушения целостности объекта управления. В этом случае захват ключей обеспечит вскрытие всей системы опознавания «свой-чужой», что приведет к резкому снижению имитостойкости как самой системы, так и всей НССС.

Второе решение также является сложно реализуемым. Для организации своевременной доставки секретных ключей ответчику и запросчику необходимо создавать закрытый канал связи, то есть дополнительно использовать аппаратуру шифрования. А это в свою очередь также требует использование периодически изменяемых секретных ключей.

Таким образом, налицо следующая проблема. С одной стороны, существующие системы опознавания, функционирующие без шифрования, не позволяют обеспечить высокую имитостойкость, а, с другой стороны, системы «свой-чужой», применяющие криптографические методы защиты информации шифрование, не могут быть использованы в СОКА.

Проведем анализ выявленной проблемной ситуации повышения имитостойкости НССС на основе использования системы опознавания космического аппарата. Очевидно, что данную проблему можно отнести к проблемам совершенствования и развития систем. Это связано с тем, что выявленная проблема имеет решение, которое направлено на повышение эффективности функционирования низкоорбитальной системы спутниковой. При этом это решение базируется на применении новых идей, связанных с построением систем опознавания КА, обладающих высокой имитостойкостью

без использования методов шифрования. Согласно [5] такая проблема относится к слабоструктурированным проблемам, решение которых является объектом исследования системного анализа и синтеза.

Очевидно, чтобы решить выявленное противоречие на практике необходимо провести сравнительный анализ альтернативных методов опознавания, которые могут быть использованы в СОКА. Выбор оптимального решения позволит разработать протокол опознавания КА, который позволит обеспечить высокую имитостойкость без использования методов шифрования.

1.2.4 Системный анализ альтернативных методов опознавания для системы опознавания космического аппарата

В настоящее время известно множество методов опознавания, которые применяются в различных областях. При этом каждая область, где используются такие методы, предъявляет к ним особые требования. Таким образом, учитывая предметную область применения протокола опознавания, можно определить, что структура такого протокола будет определяться, во-первых, объектом исследований, а, во-вторых, тем, что протокол будет использоваться на необслуживаемых объектах.

Рассмотрим объект управления, на котором будет размещаться запросная часть, разрабатываемой системы опознавания космического аппарата. Известно, что такой объект будет размещен в малонаселенной местности Крайнего Севера. Следовательно, в таких районах невозможно использование систем опознавания, в которых необходимо ежедневное участие человека. Значит разрабатываемая системы опознавания

космического аппарата должна иметь такой протокол опознавания, который позволял функционировать в течение длительного времени за счет самостоятельной выработки секретных сеансовых ключей. В результате этого система опознавания, размещенная на спутнике будет периодически изменять секретные сеансовые ключи, что позволит повысить информационную скрытность низкоорбитальной ССС. При этом вырабатываемые сеансовые ключи должны обладать высокой стойкостью к подбору. Это означает, что при получении таких сеансовых ключей должна использоваться псевдослучайная функция. При этом, система опознавания космического аппарата должна иметь возможность проверки длительности использования сеансового ключа. Ведь увеличение срока применения сеансового ключа, то есть попытка повторного его использования, приводит к увеличению вероятности навязывания ложных команд управления.

Обобщая сказанное выше, можно сделать вывод о том, что разрабатываемая СОКА должна использовать такие протоколы опознавания, которые бы позволяли обеспечить высокую имитостойкость к подбору ответа без использования методов шифрования.

Как показывают проведенные исследования и анализ работ [15,67,77,96,98,100] все множество протоколов опознавания целесообразно поделить на несколько классов. Основу первого класса составляют методы парольной опознавания. При использовании данных методов претендент и проверяющий владеют секретной информацией, с помощью которой и происходит опознавание субъекта. Различают протоколы опознавания, использующие многоразовые или одноразовые секретные пароли.

Основу протоколов опознавания, использующих многоразовые секретные пароли составляют методы, в которых происходит обмен фиксированных секретных данных. Данные методы позволяет достаточно просто произвести определение статуса претендента. При этом пароль, который предъявляет претендент не должен изменяться при различных сеансах проверки. Благодаря такому свойству система, использующая

парольную опознавания, должна иметь соответствующую базу данных, где хранятся все секретные пароли претендентов. Достоинством интерактивной системы доказательства, построенной на основе использования многоразовых секретных паролей, является достаточно простая реализация.

Благодаря данному свойству системы парольной опознавания нашли широкое применение во многих информационных системах. В том случае претендент P выполняет передачу проверяющему V личный идентификатор и многоразовый секретный пароль

$$P \to V: \quad (\text{ind } P, \text{pass } P), \tag{1.11}$$

где ind P – идентификатор претендента P; pass P – многоразовый секретный пароль претендента P; V – проверяющая сторона протокола.

Получив соответствующие значения ind P и pass P, проверяющая сторона V протокола проверяет претендента P. Однако в данном протоколе есть уязвимость, которая может быть использована при атаке «пассивный перехват пароля». Чтобы устранить эту потенциальную угрозу необходимо выполнить действия. Во-первых, использовать симметричные шифры

$$P \to V: \quad (\text{ind } P, E_k(\text{pass } P)), \tag{1.12}$$

где $E_k(\text{pass } P)$ –шифрование пароля претендента; k – секретный ключ.

Во-вторых, применить бесключевую хеш-функцию

$$P \to V: \quad (\text{ind } P, h(\text{pass } P)), \tag{1.13}$$

где $h(\text{pass } P)$ – хеш-образ пароля претендента P.

Анализ протоколов опознавания, определяемых выражениями (1.12) и (1.13), показывает, что нарушителю будет неизвестен только пароль претендента, а сам идентификатор доказывающего участника свободно передается по открытому каналу. Перехватив этот идентификатор P, нарушитель способен войти в систему. С целью предотвращения такой ситуации в работе [15] предлагается модифицировать протокол опознавания, использующий многоразовые секретные пароли, следующим образом

$$P \to V: \quad (\text{ind } P, h(\text{pass } P, \text{ind } P)). \tag{1.14}$$

Несмотря на минимальные временны затраты, необходимые на опознавание претендента, методы, использующие многоразовые секретные пароли, имеют недостатки. Во-первых, это наличие у проверяющей стороны V базы данных, где хранятся все идентификаторы и пароли или соответствующие им хеш-образы $h(\text{pass P})$. Во-вторых, при реализации протокола опознавания (1.12) необходимо осуществить передачу секретных ключей k на обе стороны протокола по закрытому каналу связи. Учитывая, что проверяющая сторона системы опознавания космического аппарата, которая находится на необслуживаемом объекте, то возникают определенные трудности с организацией такого канал к каждому объекту.

Для устранения недостатков, которые присущи многоразовым секретным паролям, были разработаны методы опознавания, в которых используются одноразовые пароли [15,67]. В настоящее время получили распространения два подхода к вычислению одноразовых паролей. При реализации первого подхода предлагается использовать набор одноразовых паролей, которые передаются как претенденту P, так и проверяющей стороне V. Для этого необходимо применять закрытый канал связи, не позволяющий провести перехват данного списка секретных паролей. В основу второго подхода положены методы итерационного получения одноразовых паролей. Для этого необходимо, чтобы претенденту P и проверяющей стороне V был доставлен секретный пароль $k_{pass}(t)$. Используя данный пароль, обе стороны протокола вырабатывают новый одноразовый пароль $k_{pass}^{P}(t+1)$ и $k_{pass}^{V}(t+1)$ соответственно. Затем претендент P передает свой одноразовый пароль $k_{pass}^{P}(t+1)$ проверяющей стороне V, которая производит сравнение $k_{pass}^{P}(t+1)$ и $k_{pass}^{V}(t+1)$. Однако данный протокол имеет недостаток, который выражается в угрозе перехвата одноразового пароля. Чтобы устранить такую угрозу в системах опознавания используется шифрование с ключом, который получается из текущего одноразового ключа $k_{pass}(t)$. В основу третьего

подхода положены методы итерационного получения одноразовых паролей на основе однонаправленной функции H, согласно

$$\begin{array}{l} 1.\ P, V: H(pass), H(H(pass)),... = H^n(pass) \\ 2.\ P, V: pass_i = H^{n-i}(pass). \\ 3.\ P \to V: \quad (ind\ P, i, pass_i) \end{array} \qquad (1.15)$$

где H(pass) – итерационный процесс получения пароля.

Однако, системы опознавания, которые используют одноразовые пароли, имеют недостатки. В качестве первого недостатка таких систем опознавания можно отметить необходимость использования защищенного канала связи, не позволяющего нарушителю выполнить перехват ключей. Вторым недостатком систем опознавания является угроза проведения атаки, основанной на подмене участника протокола. Таким образом, можно сделать вывод о том, что методы опознавания с использованием многоразовых и одноразовых паролей обладают достаточно слабой стойкостью к НСД, что не позволяет их применять в системах определения статуса КА.

Более высокой стойкостью к НСД обладают протоколы опознавания, использующие метод типа «запрос-ответ» [11,98]. В основу таких методов положен принцип, согласно которому претенденту P должен убедить проверяющую сторону V, что он относится к группе авторизованных абонентов. Для этого ему необходимо, ответить на запрос, который инициировала проверяющая сторона V. При этом ответ должен определяться как вопросом, так и секретом известным только претенденту P. При этом претендент не должен разгласить секрет, отвечая на поставленный вопрос.

Использование метода опознавания типа «запрос-ответ» позволяет разрабатывать протоколы, которые имеют две итерации. При этом для повышения стойкости таких протоколов предлагается использовать симметричные криптосистемы [76,77]. Тогда определение статуса претендента P можно представить следующим протоколом

$$\begin{array}{l} 1.\ V \to P: \quad b_V. \\ 2.\ P \to V: \quad E_{k_{HV}}(ind\ P, b_V) \end{array} \qquad (1.16)$$

где b_V – случайное число.

Наряду с симметричными шифрами при использовании метода «запрос-ответ» также широко применяются асимметричные шифры. В этом случае протокол опознавания будет расширен и имеет вид

$$\begin{aligned}
&1.\ P \to V: \quad E_{k_B}(b_P, \text{ind } P);\\
&2.\ V: \quad D_{k_V^*}(E_{k_B}(b_P, \text{ind } P));\\
&3.\ V \to P: \quad E_{k_V}(b_P, b_V);\\
&4.\ P: \quad D_{k_V^*}(E_{k_V}(b_P, b_V));\\
&5.\ P \to V: \quad E_{k_V}(b_V).
\end{aligned} \tag{1.17}$$

где b_V и b_P – случайные числа; k_V и k_V^* – открытый и секретный ключи участника V; k_P и k_p^* – открытый и секретный ключи претендента P.

Использование метода опознавания типа «запрос-ответ» позволило повысить стойкость протоколов к взлому. Однако таким протоколам присущи и недостатки. Так в процессе реализации протокола опознавания претенденту P нарушитель может перехватить и запомнить передаваемые данные по каналу связи. После этого нарушитель пытается навязать претенденту P запросы, с помощью которых он получит на них ответы. На основе анализа полученных ответов злоумышленник способен определить данные о секрете. Предотвратить такую атаку на систему опознавания возможно за счет использования протоколов, которые базируются на многошаговом итерационном доказательстве.

Одним из первых протоколов опознавания был протокол Фиат–Шамира [15,76,77,90]. В таблице 1.1 представлен раунд данного протокола.

Таблица 1.1 – Раунд протокола Фиат-Шамира

№	**Вычисление открытого и секретного ключей**		
	Претендент P	Центр	Проверяющая сторона V
1		p, g – простые числа; $M = p \cdot g$	
2	$s: \text{НОД}(s, M) = 1,$ где $1 \le s \le M - 1.$ $v = s^2 \bmod M$.		

3	$k_{секр} = \{s\}.$	$k_{откр} = \{M, v\}$	
		Опознавание	
1	r – случайное число где $1 \le к \le M - 1.$ $x = r^2 \bmod M.$	Число x передается проверяющей стороне V	
2		Число передается P	$e \in \{0, 1\}$
3	$y = r \cdot s^e \bmod M$	Число передается V	
4			Если y=0, то чужой. $y^2 = x \cdot v^e \bmod M$
	Процедура опознавания производится W раундов.		

В процессе опознавания этапы 1-4 повторяются многократно. Если данный протокол будет выполнен только один раз (один раунд опознавания), то вероятность ошибки второго рода (вероятность пропуска нарушителя) примет значение $P_{ПН} = 1/2$. Чтобы ее снизить, необходимо выполнить процедуру опознавания W раундов. Тогда вероятность пропуска нарушителя составит $P_{ПН} = 1/2^W$. Согласно [15,74] величина W, которая выступает в качестве параметра безопасности данного протокола опознавания, берется в пределах от 20 до 40. Претенденту P будет присвоен статус «свой», если при каждой проверке на 4 этапе будет получен положительный результат.

Выбор запроса $e \in \{0, 1\}$ необходим для получения ответа от претендента P на два вопроса. Первый вопрос необходим, чтобы показать, что претендент P владеет секретным ключом. Второй вопрос необходим, чтобы не допустить ситуации, когда недобросовестный проверяющий пытается обмануть честного претендента P. В зависимости от поставленного запроса, который выполняется на 3 этапе опознавания, претендент P вычисляет при e = 0 ответ $y = r$ или при e = 1 ответ $y = s \cdot r \bmod M$. Таким образом, претендент P в своем ответе демонстрирует знание секретного ключа s, не разглашая его проверяющей стороне V.

Для сокращения временных затрат была проведена его модификация [15]. В таблице 1.2 представлен один раунд протокола Фейге-Фиат-Шамира.

Таблица 1.2 – Раунд протокола Фейге-Фиат-Шамира

№	**Вычисление открытого и секретного ключей**		
	Претендент P	Центр	Проверяющая сторона V
1		p, g – простые числа; $M = p \cdot g$	
2	$s_i : НОД(s_i, M) = 1,$ где $1 \le s \le M - 1.$ $v_i = s_i^2 \bmod M.$		
3	$k_{секр} = s = \{s_1, s_2, ..., s_n\}.$	$k_{откр} = \{M, v\}$ $v = \{v_1, v_2, ..., v_n\}.$	
		Опознавание	
1	r_i – случайное число где $1 \le r_i \le M - 1.$ $X_i = r_i^2 \bmod M.$	Результат передается V	
2		$(e_{i1}, e_{i2}, ..., e_{in})$ передаются P	$(e_{i1}, e_{i2}, e_{i3}, ..., e_{in}) \in \{0,1\}^n$
3	$y_i \equiv r(s_1^{e_{i1}}, ..., s_k^{e_{ik}}) \bmod M$	Результат передается V	
4			Если y=0, то чужой. $x_i \equiv y_i^2 (v_1^{e_{i1}}, ..., v_k^{e_{ik}}) \bmod M$
	Процедура опознавания производится W раундов		

При этом использовании данного протокола вероятность пропуска нарушителя $P_{ПН} = 1/2^{nW}$. В работе [15] предлагается выбирать n = 5, W = 4.. Однако, несмотря на сокращение временных затрат на проведение опознавания, данные протоколы также нецелесообразно использовать при определении статуса космического аппарата в НССС.

Анализ работ [76,77] показал, что дальнейшее сокращение времени опознавания возможно, если использовать протокол опознавания Шнорра. В таблице 1.3 представлены принципы реализации данного протокола.

Таблица 1.3 – Протокол опознавания Шнорра

№	**Вычисление открытого и секретного ключей**		
	Претендент P	Центр	Проверяющая сторона V
1		P, H – простые числа; $H \mid (P-1)$	
2	Выбирается число K, где $1 < K \le P-1$ и $K^H \equiv 1 \bmod P$.		
3	B – секретный ключ, где $1 \le B \le H-1$		
4.	Вычисляется $У = K^{-B} \bmod P$		
3	$k_{секр} = B$	$k_{откр} = \{P, H, K, У\}$	
		Опознавание	
1	C – случайное число, где $1 \le C \le H-1$. $M = K^C \bmod P$.	Результат число M передается V	
2		Число передается претенденту P	Выбирается число E, где $1 \le E \le 2^T - 1$
3	Вычисляется ответ $A = (C + E \cdot Bx) \bmod H$	Ответ передается стороне V	
4			$X = K^A У^E \bmod P$ Если X = M, то «свой». Если $X \ne M$, то «чужой».

Несмотря на то, что данный протокол позволяет провести опознавание претендента за один цикл, тем не менее, он имеет недостаток. Это связано с тем, что для проведения опознавания требуется три обмена данными между претендентом и проверяющим. Сначала выполняется передача числа M от

претендента P к проверяющей стороне V. Затем проверяющий передает претенденту P вопрос E. Третья передача предназначена для доведения до проверяющей стороны V ответа A на поставленный вопрос E.

При этом очевидно, что чем больше число раундов обмена данными между ответчиком и запросчиком, тем выше вероятность подбора ответа на поставленный вопрос запросчика.

Сократить число этапов проверки претендента P позволяют протоколы опознавания с нулевым разглашением знаний, которые используются в системах электронных платежей. Так в работе [31] представлен протокол опознавания пользователя в банке для получения электронного кошелька. При этом для обеспечения более эффективной работы носителей электронных денежных средств (например, смарт-карт) за счет сокращения объема программного обеспечения предлагается использовать псевдослучайную функцию. Протокол снятия со счета электронной наличности представлен в работе [19]. В качестве основы предлагается использовать протокол опознавания, построенный на основе доказательства с нулевым разглашением и имеющим два этапа опознавания. Программная реализация данного протокола приведена в работе [26]. Протокол, позволяющий обеспечить выплату всей наличности электронного кошелька, использующий доказательство с нулевым разглашением знаний приведен в работе [30]. В работе [29] рассмотрены вопросы повышения имитостойкости протокола выплаты электронной наличности за счет использования разработанного алгоритма опознавания и модулярных кодов. опознавания. Программная реализация данного протокола приведена в работе [20]. В работе [25] показаны принципы построения протокола обмена данными на основе алгоритма слепой подписи.

Проведенный анализ работ показал, что в системах электронных платежей нашли достаточно широкое применение протоколы на основе доказательства с нулевым разглашением знаний. При этом процесс опознавания происходит за минимальное число этапов. Однако, обладая

высокой вычислительной сложностью при минимальном числе этапов опознавания, данные протоколы, использующие метод доказательства с нулевым разглашением знаний, не нашли применения в системах опознавания спутника НССС.

Таким образом, налицо следующее противоречие в теории**.** Известные протоколы опознавания, построенные на основе методов опознавания типа «запрос-ответ», а также с помощью многоразовых и одноразовых паролей, не позволяют в полной мере предотвратить навязывание имитирующих и ретрансляционных помех спутником-нарушителем. При этом метод опознавания, базирующийся на доказательстве с нулевым разглашением и использующий псевдослучайно-изменяемые секретные сеансовые ключи, реализация которого позволяет при минимальном числе этапов провести опознавания космического аппарата, не нашел применения.

Устранить данный недостаток возможно за счет разработки метода построения системы опознавания космического аппарата, которая использует протокол опознавания, базирующийся на доказательстве с нулевым разглашением сведений и имеющий два этапа определения статуса спутника.

1.3 Выбор и обоснование показателя оценки имитостойкости низкоорбитальный системы спутниковой связи

Для оценки эффективности применения различных альтернативных решений, направленных на повышение имитостойкости низкоорбитальной системы спутниковой связи, необходимо осуществить выбор показателя качества (ПК). Данные показатели должны выступать в качестве количественной меры, с помощью которой можно определить насколько

близко к поставленной цели позволяет применение того или иного альтернативного метода.

В работе [65] приведена классификация основных показателей качества, которая осуществляется по следующим признакам. По количеству описываемых свойств объекта исследования показатели качества разделяются на - единичные и комплексные ПК. По основным характеризуемым свойствам показатели качества подразделяются на ПК назначения и ПК надежности. Различают также прогнозируемые ПК, производственные ПК и эксплуатационные ПК, которые классифицируются по стадии определения. По способу определения показатели качества можно разбить на две группы – экспериментальные ПК и расчетные ПК.

В работе [39] предлагается другая классификация ПК, которая построена в зависимости от свойств исследуемого объекта. В этом случае получаем следующие классы ПК:

- показатели, предназначенные для оценки назначения объекта;
- показатели, характеризующие свойства надежности объекта;
- показатели качества, оценивающие технологичность;
- эргономические показатели качества;
- показатели безопасности.

Очевидно, что на выбор показателей качества должны оказывать и их свойства. Основные требования, которые предъявляются к показателям качества приведены в работе [37]. Очевидно, что выбранный ПК должен в наглядной форме отражать основные свойства объекта и предметов исследования и иметь простой физический смысл. Кроме того, такой показатель должен учитывать достижения, которые были получены современной наукой и техникой. При этом с помощью выбранного ПК исследователь мог бы достаточно провести измерение, контроль и необходимые вычисления.

Так как целью исследований является повышение имитостойкости низкоорбитальной системы спутниковой связи, то в диссертации был

проведен анализ показателе качества, которые используются для оценки имитостойкости радио систем.

В работе [8] для оценки имитостойкости командно-телеметрических радиолиний предлагается использовать вероятность навязывания сигнала, которая определяется выражением,

$$P_{нав}^{ком} = \frac{1}{M_f - M_{кс}} M_f^P M_{кс}^P, \quad (1.18)$$

где M_f^P и $M_{кс}^P$ – количество разрешенных частот форм сигналов, реализуемые системой связи; M_f и $M_{кс}$ – максимальное количество частот и форм сигналов, которые могут быть использованы данной системой связи.

Очевидно, что на величину вероятности навязывания имитационного сигнала влияет также интервал времени T, в течение которого происходит имитация сигнала. В работе [72] предлагается для оценки имитостойкости системы радиосвязи использовать следующее выражение

$$P_{нав}^{ком}(T) = \frac{1}{A_Z^k \cdot t_{ПИ}}, \quad (1.19)$$

где $t_{ПИ}$ – время, которое необходимо для выполнения одной попытки имитации; Z – множество сложных сигналов, используемой данной системой связи.

Другим показателем, позволяющим оценить имитостойкость системы связи является математическое ожидание времени опробования полного ансамбля возможных сложных сигналов. Согласно [8] данный показатель используют для оценки эффективности множества попыток имитации сигналов. Для вычисления данного показателя предлагается использовать

$$T_Б^{ком} = \frac{1}{2} Z \cdot t_{прд}, \quad (1.20)$$

где Z – параметр, оценивающий размерность ансамбля сигналов; $t_{прд}$. – время затрачиваемое на передачу имитационного сигнала.

При для вычисления данного времени $t_{прд}$. предлагается следующее выражение

$$t_{прд} = \frac{1}{R_{П}}, \qquad (1.21)$$

где $R_П$ – скорость имитационных воздействий на систему радиосвязи.

В работе [10] рассматриваются вопросы оценки имитостойкости каналов системы радиосвязи и управления, которые используют частотную модуляцию. В данной работе для оценки имитостойкости такой системы предлагается использовать показатель - вероятность битовой ошибки, значение которой определяется согласно

$$P_{в} = \frac{1}{2}\exp\left(-\frac{E_{В} + (1-2\rho)E_{П}}{2N_{0}}\right), \qquad (1.22)$$

где $E_В$ – энергия, которая требуется для передачи одного бит команды; N_0 – спектральная плотность мощности шума; $E_П$ – энергия помехи; ρ – коэффициент временной корреляции.

В работе [17] для оценки имитостойкости каналов управления беспилотных летательных аппаратов предлагается использовать вероятность имитонавязывания при выполнении одной попытки, которая определяется как отношение подпространства допустимых кодовых комбинаций к общему числу возможных кодовых комбинаций $\Omega_{общ}$. Тогда такой показатель задается выражением

$$P_{им} = \frac{\Omega_{ед}}{\Omega_{общ}} = \frac{F_{ед}S_{ед}}{F_{общ}S_{общ}}, \qquad (1.23)$$

где $S_{ед}$ – общее количество комбинаций сигнатуры системы; $F_{ед}$ – количество состояний вектора в частотном подпространстве $\Omega_{ед}$; $S_{общ}$ – максимальное возможное количество возможных комбинаций сигнатуры системы; $F_{общ}$ – максимальное возможное количество возможных реализаций сигнала в частотном пространстве.

В работах [45,46] для оценки стойкости систем радиосвязи к имитирующим и ретрансляционным помехам предлагается использовать вероятность успеха имитации, которая определяется отношением

$$P_{И} = \frac{N_{С}}{N_{Ш}}, \tag{1.24}$$

где $N_{с}$ – количество сообщений, которые подвигалось шифрованию; $N_{ш}$ – количество возможных криптограмм.

Из выражения (1.24) наглядно видно, что имитостойкость системы связи будет тем больше, чем меньше будет показатель $N_{с}$ и чем больше будет показатель $N_{ш}$.

Проведенный анализ основных показателей, используемых для оценки имитостойкости систем связи, показал, что чаще всего в качестве критерия имитостойкости выбирается вероятность навязывания дезинформирующего сигнала. Если положить, что длина кодограммы передаваемой НССС составляет $L_{С}$ бит, то вероятность подбора команды будет определяться выражением

$$P_{ПК} = \frac{1}{2^{L_{С}}}. \tag{1.25}$$

где $L_{С}$ – длина передаваемого сигнала.

Однако, введение дополнительной системы опознавания космического аппарата приведет к повышению имитостойкости НССС. В этом случае имитостойкость низкоорбитальной системы спутниковой связи будет зависеть как от вероятности навязывания передаваемого сигнала, так и от вероятности имитации ответа для системы «свой-чужой».

В этом случае имитостойкость НССС будет определяться вероятностью навязывания имитационной помехи

$$P_{НИП} = P_{ПК} \cdot P_{ПС}^{СОКА}, \tag{1.26}$$

где $P_{ПС}^{СОКА}$ – вероятность пропуска спутника-нарушителя системой «свой-чужой».

Если в процессе функционирования НССС спутник-нарушитель будет использовать ретрансляционную помеху, то вероятность навязывания дезинформирующего сигнала будет равна $P_{ПК} = 1$. Это связано с тем, что

спутнику-нарушителю нет необходимости имитировать передаваемый сигнал. Для нарушения работы НССС спутник произведет перехват сигнала, выполнит временную задержку, а затем произведет навязывание этого сигнала. Так как ретрансляционная помеха будет полностью соответствовать передаваемому сигналу, то имитостойкость низкоорбитальной системы спутниковой связи будет определяться только имитостойкостью системы опознавания космического аппарата. Тогда справедливо выражение

$$P_{НИП} = P_{ПС}^{СОКА}. \quad (1.27)$$

Так как целью исследований является повышение имитостойкости низкоорбитальной системы спутниковой связи за счет использования системы опознавания КА, применение которой позволит снизить вероятность навязывания имитируемых помех, а также перехваченных и задержанных команд управления спутником-нарушителем, то эффективность работы последней можно оценить с помощью целого ряда ПК. Очевидно, что эффективность работы системы опознавания спутника будет определяться множеством параметров, среди которых можно выделить методы опознавания, количество этапов, необходимых для распознавания спутника, способом построения такой системы, разрядность обрабатываемых данных, протоколы, позволяющие определить увеличение срока использования сеансовых ключей.

Таким образом, в качестве показателей качества, позволяющих оценить эффективность работы системы опознавания космического аппарата можно привести:

- количество раундов опознавания КА (W);
- количество этапов в протоколе опознавания (N);
- вероятность пропуска спутника-нарушителя;
- вероятность ошибки СОКА;
- вероятность ложного срабатывания СОКА;
- разрядность параметров протокола опознавания;

– вычислительная сложность (имитостойкость) протокола опознавания.

Проведенные исследования, а также учет выбранной цели исследований, позволили обоснованно выбрать в качестве показателя качества вероятность пропуска спутника-нарушителя для организации сеанса связи будет определяться выражением

$$P_{ПС} = \frac{N(i)}{N(max)} P_{И}, \qquad (1.28)$$

где $P_{И}$ – вероятность имитации противником сигнал «Свой» в СОКА; N(i) – количество этапов опознавания спутника при использовании i-го протокола опознавания; N(max) – максимальное количество этапов в протоколе опознавания, построенном на основе доказательства с нулевым разглашением знаний.

При этом вероятность имитации противником сигнал «Свой» в СОКА будет определяться разрядностью передаваемого сигнала от ответчика к запросчику

$$P_{И} = \frac{1}{2^{L}}, \qquad (1.29)$$

где L – разрядность ответного сигнала.

1.4 Постановка научной задачи исследований

Научная задача диссертационных исследований состоит в применении научно-методического аппарата СА при разработке метода построения системы опознавания космического аппарата, позволяющего повысить имитостойкость НССС за счет использования протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений.

Постановку задачи системного анализа повышения имитостойкости спутниковой связи на основе совершенствования метода построения системы опознавания космического аппарата можно представить следующим образом.

Известны множество протоколов опознавания $A=\{A_1,A_2,...,A_X\}$, количество раундов $W=\{W_1,W_2,\ldots,W_E\}$ и этапов $N=\{N_1,N_2,\ldots,N_M\}$ необходимых для выполнения протокола, разрядности команд управления $L_C=\{L_C^1,L_C^2,...L_C^R\}$, используемых модулей $Q=\{q_1,q_2,...,q_H\}$ и ответов на поставленные вопросы запросчиков $L=\{L_1,L_2,...,L_J\}$, а также множество алгоритмов реализации вычислений сеансовых ключей $G=\{G_1,G_2,...,G_K\}$. На ряд показателей СОКА наложены ограничения:

– разрядность используемых модулей q_i не должна быть больше предельно допустимого значения $q_{доп}$;

– разрядность ответов на поставленные вопросы запросчика L_i не должна быть меньше предельно допустимого значения $L_{доп}$.

Требуется разработать метод построения системы опознавания космического аппарата, использующего протокол опознавания с нулевым разглашением сведений, использование которого позволит повысить имитостойкость спутниковой связи при выполнении заданных ограничений.

Проведенная формализация задачи научных исследований позволяет определить ее математическую постановку. Рассмотренную в диссертации научную задачу исследований можно отнести к задачам, которые связаны с повышением эффективности или качества функционирования системы. Значит, в диссертации при определении математической постановки задачи исследования можно использовать формальное представление задачи, направленной на повышение качества функционирования системы, приведенной в работе [49]. Тогда имеем

Математическую постановку задачи исследования можно представить

$$\begin{aligned} &S\left(A, W, N, Q, L, G, L_C\right) \rightarrow \left\{\Delta P_{НИП}\right\} \mid, \Delta P_{НИП} > 0, \\ &L_i \geq L_{доп}, q_i \leq q_{доп}, \end{aligned} \tag{1.30}$$

где $S=\{S_1,\ldots, S_V\}$ – множество методов построения СОКА, применение которых позволяет повысить имитостойкость НССС; $\Delta P_{НИП} = P^{*}_{НИП} - P^{S_i}_{НИП}$ – снижение вероятности навязывания имитационной помехи НССС при использовании S_i метода построения системы опознавания КА; $P^{*}_{НИП}$ – вероятность навязывания имитационной помехи в НССС без использования СОКА; q_i – разрядность используемых модулей; L_i – разрядность ответов на поставленные вопросы запросчика; $q_{доп}$ и $L_{доп}$ – предельно допустимые значения разрядности модуля и ответного сигнала.

Чтобы обеспечить эффективное решение разработанной научной задачи диссертационных исследований воспользуемся методом СА – методом декомпозиции, с помощью которого будут получены частные задачи исследования.

Чтобы правильно провести декомпозицию разработанной научной задачи диссертационных исследований воспользуемся принципами построения «дерева целей». Согласно работе [34] построение дерева целей начинается с формулировки основной цели. Затем необходимо данную цель разбить на подцели, каждая из которых выступает в качестве средства, с помощью которого можно достичь главную цель. Главная цель диссертационных исследований связана с повышением имитостойкости низкоорбитальной системы спутниковой связи. Сформулируем подцель первого уровня. Проведенные исследования показали, что качественным скачком в повышении имитостойкости НССС в условиях имитационных и ретрансляционных помех является использование системы опознавания космического аппарата. Поэтому подцель первого уровня НССС связана с разработкой структуры системы опознавания КА, применение которой позволит повысить имитостойкость НССС в условиях воздействия имитирующих и ретрансляционных помех.

Для того чтобы разработать структуру запросно-ответной системы «свой-чужой» для низкоорбитальной системы спутниковой связи необходимо разработать метод построения такой системы. Поэтому подцель второго уровня связана с разработкой и совершенствованием метода построения системы опознавания космического аппарата, применение которого позволит повысить имитостойкость НССС.

Проведенный системный анализ альтернативных методов опознавания для системы опознавания космического аппарата показал, что эффективность работы СОКА, в первую очередь, зависит от используемого протокола опознавания. В ходе анализа было определено, что известные протоколы, построенные на основе методов опознавания типа «запрос-ответ», а также с помощью многоразовых и одноразовых паролей, не позволяют в полной мере предотвратить навязывание имитирующих помех и задержанных команд управления спутником-нарушителем. При этом метод опознавания, базирующийся на доказательстве с нулевым разглашением и использующий псевдослучайно-изменяемые секретные сеансовые ключи не нашел применения. Поэтому первая подцель третьего уровня связана с разработкой протокола опознавания с нулевым разглашением знаний, реализация которого позволяет при минимальном числе этапов провести определение статуса космического аппарата.

Использование сеансовых ключей при определении статуса КА позволяет уменьшить количество этапов опознавания. Однако если в процессе работы СОКА происходит повторное использование сеансового ключа, то передаваемые запросчику ответы будут частично совпадать. А это приводит к сокращению длины ответа L на $\log_2 q$ бит, где q – разрядность модуля. В результате повторного использования сеансового ключа увеличивается вероятность имитации противником сигнал «Свой» в СОКА, что негативно влияет на имитостойкость НССС. Поэтому вторая подцель третьего уровня связана с разработкой алгоритма проверки повторного использования сеансового ключа.

Очевидно, что имитостойкость разработанного протокола опознавания космического аппарата во многом определяется алгоритмом вычисления сеансовых ключей. Поэтому третья подцель третьего уровня посвящена разработке структурной модели генератора псевдослучайной функции для выработки сеансового ключа системы опознавания космического аппарата.

На рисунке 1.3 показано построенное дерево целей разработанной научной задачи диссертационных исследований. Применение разработанного дерева целей позволяет провести декомпозицию научной задачи исследований, которая характеризуется большой размерностью, а для ее решения требуются значительные вычислительные затраты, на пять частных задач исследования. Анализ рисунке 1.3. показывает, что подцели более низкого уровня подчинены и используются для достижения подцелей, находящихся на более высоком уровне. Очевидно, что последовательное достижение подцелей будет способствовать достижению выбранной (глобальной) цели диссертационных исследований.

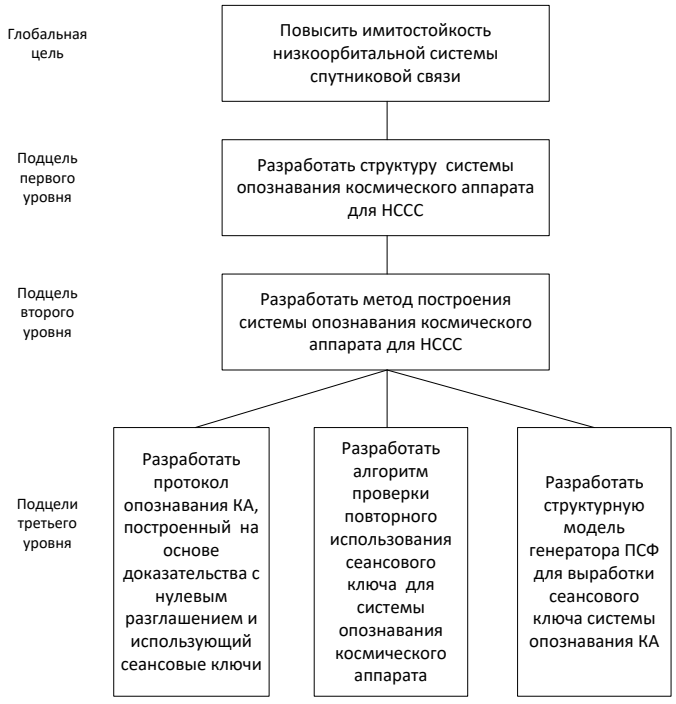

Рисунок 1.3 – Дерево целей разработанной научной задачи диссертационных исследований

Таким образом, используя метод системного анализа, были получены следующие частные задачи:

1. Разработка протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений, обладающего меньшими временными затратами на опознавания спутника за счет сокращения количества этапов выполнения по сравнению с ранее известными протоколами типа «запрос-ответ».

2. Разработка алгоритма проверки повторного использования сеансового ключа, отличающегося от ранее известных, тем, что позволяет провести проверку без его передачи по открытому каналу связи.

3. Разработка структурной модели генератора псевдослучайной функции для выработки сеансового ключа системы опознавания космического аппарата, отличающегося от ПСФ Наорра-Рейнголда меньшими временными затратами на получение выходных значений.

4. Разработка метода построения системы опознавания космического аппарата, отличающийся от ранее известных более низкой вероятностью подбора ответа на вопрос запросчика за счет использования разработанного протокола опознавания с нулевым разглашением сведений.

5. Разработка структурной схемы системы опознавания космического аппарата, характеризующейся меньшими временными затратами на определение статуса спутника за счет использования разработанного протокола опознавания КА.

Порядок следования частных научных задач исследований будут полностью совпадать с последовательностью их решения в диссертации. Таким образом, последовательное решение позволит выбрать наиболее оптимальное решение из множества альтернатив, применение которого позволит устранить проблему на практике.

Выводы

1. Как показывают проведенные исследования научно-методический аппарат системного анализа нашел широкое применение при решении сложных задач в самых различных областях. Это связано с тем, что методы СА характеризуются междисциплинарным подходом, применение которого позволяет решить сложную практическую проблему, возникающую при разработке и эксплуатации сложной системы. Проведенный анализ основных подходов к решению научных проблем сложных систем позволил выделить основные этапы методик системного анализа.

2. Проведен анализ принципов построения автоматизированных систем дистанционного мониторинга, контроля и управления, которые работают со сложными территориально-распределенными экологически-опасными объектами. Показано, что для организации эффективного управления такими необслуживаемыми объектами, размещенными в районах Крайнего Севера необходимо использовать низкоорбитальные системы спутниковой связи. В качестве основных источников угроз безопасности АСДМКУ были обоснованно выбраны системы спутниковой связи. Поэтому объектом исследования стала низкоорбитальная система спутниковой связи

3. Проведен анализ деструктивных методов, направленных на снижение имитостойкости низкоорбитальной системы спутниковой связи. Были рассмотрены алгоритмы постановки пассивных и активных помех комплексами РЭБ. Проведенные исследования показали, что данный подход к нарушению работы ССС, применяемых в комплексах мониторинга, контроля и управления удаленным объектом, в арктических условиях практически не осуществим. Были исследованы методы, позволяющие имитировать или перехватывать «правильные» сигналы с последующим их навязыванием противнику. Показано, что такой подход позволяет нарушить эффективную работу НССС. Определена цель диссертационных исследований, которая направлена на повышение имитостойкости низкоорбитальной системы спутниковой связи за счет использования системы опознавания КА, применение которой не позволит спутнику-нарушителю произвести

навязывание имитируемых помех, а также перехваченных и задержанных команд управления

4. Проведен анализ основных методов построения систем опознавания «свой-чужой», который позволил выявить противоречие на практике. Одним из наиболее эффективных способов противостоять навязыванию имитируемых помех, а также перехваченных и задержанных команд управления, передаваемых по каналам спутниковой связи, является опознавание космического аппарата перед началом сеанса связи спутник – объект управления. Однако существующие системы «свой-чужой» не позволяют проводить опознавание КА и не могут быть использованы в НССС. Показана актуальность разработки новых принципов построения системы распознавания спутника для низкоорбитальной группировки ССС.

5. Проведен системный анализ альтернативных методов опознавания для системы опознавания космического аппарата. В результате был определено противоречие в теории, которое состоит в том, что известные протоколы опознавания, построенные на основе методов опознавания типа «запрос-ответ», а также с помощью многоразовых и одноразовых паролей, не позволяют в полной мере предотвратить навязывание имитирующих помех и задержанных команд управления спутником-нарушителем, а методы опознавания, базирующиеся на доказательстве с нулевым разглашением, и обладающие высокой вычислительной сложностью при минимальном числе этапов опознавания космического аппарата, не нашли применения.

6. Проведен анализ известных показателей качества, позволяющих оценить имитостойкость системы передачи данных. На основе проведенного анализа был произведен выбор и обоснование показателя оценки имитостойкости низкоорбитальный системы спутниковой связи.

7. Проведена постановка научной задачи исследования, которая состоит в применении научно-методического аппарата системного при разработке метода построения системы опознавания космического аппарата, позволяющего повысить имитостойкость НССС за счет использования

протокола опознавания КА, построенного на основе доказательства с нулевым разглашением. Произведена математическая постановка задачи исследования. Для осуществления декомпозиции разработанной научной задачи диссертационных исследований было построено «дерево целей». Используя данный метод системного, была проведена декомпозиция главной научной задачи на пять частных научных задач.

ГЛАВА 2. РАЗРАБОТКА ПРОТОКОЛА ОПОЗНАВАНИЯ СПУТНИКА, ПОСТРОЕННОГО НА ОСНОВЕ ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ ЗНАНИЯ, ДЛЯ СИСТЕМЫ ОПОЗНАВАНИЯ КОСМИЧЕСКОГО АППАРАТА

2.1 Основные принципы реализации итерационных протоколов опознавания, использующих методы доказательства знаний

Первая частная задача диссертационных исследований связана с разработкой протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений, обладающего меньшими временными затратами на опознавания спутника за счет сокращения количества этапов выполнения по сравнению с ранее известными протоколами типа «запрос-ответ». Для решения данной частной задачи проведем исследование основных принципов реализации таких протоколов.

Проведенный анализ протоколов опознавания на основе парольных схем, показал, что они обладают уязвимостью. При использовании методов парольной опознавания злоумышленник может перехватить передаваемые сообщения, с помощью которых может представиться как легальный абонент. Недостаточной стойкостью к атакам и протоколы опознавания типа «запрос-ответ». Это связано с тем, что нарушитель может контролировать канал связи, по которому передаются вопросы от проверяющей стороны V и ответы от претендента P. В этом случае он может создать специальные запросы, а затем направить их претенденту. После этого, получив ответы и проанализировав их, злоумышленник сможет получить информацию о секрете, который известен претенденту P.

Чтобы устранить данную ситуацию были разработаны протоколы, использующие доказательства знаний, которые не позволяют разгласить секретные данные, известные претенденту P [84,86,90]. В данном протоколе участвуют две стороны. При этом проверяющая сторона V генерирует случайные вопросы, на которые должен ответить претендент P. Цель реализации данного протокола состоит в том, что претендент должен убедить проверяющую сторону V в истинности известному ему утверждения. Если претендент является авторизованным пользователем, то есть его утверждения верны, то при увеличении числа этапов проверки, вероятность правильного утверждения должна стремиться к единице. В противном случае, когда утверждение, выдвинутое претендентом P, является ложным, то вероятность правильности доказательства будет близка к нулю [74].

Как правило, реализация большинства протоколов доказательства с нулевым разглашением, требует выполнения несколько раундов проверки. При этом каждый такой раунд требует выполнения следующих этапов:

Первый этап. Претендент, обладающий определенным секретом S делает заявку E, которая передается проверяющей стороне V.

Второй этап. Проверяющая сторона V передает запрос B претенденту.

Третий этап. Претендент P вычисляет ответ Y на поставленный запрос.

На каждом раунде проверяющая сторона V принимает решение – является ли текущее доказательство претендента P истинным.

Рассмотрим основные принципы, которые положены в основу протоколов с нулевым разглашением. На первом этапе протокола претендент, владея секретом M, выбирает случайное число K_1. Затем производится вычисление однонаправленной функции, аргументами которой являются M и K, т.е. $E_1 = f_1(M, K_1)$. Полученное значение в виде заявки передается проверяющей стороне V. Благодаря данному принципу обеспечивается случайность и независимость получения заявки E_i на всех этапах протокола. На втором этапе протокола проверяющая сторона V выбирает несколько вопросов B_1, B_2, …B_W, где W – количество раундов в протоколе. Затем

проверяющая сторона V посылает первый вопрос B_1. На третьем этапе протокола претендент P отвечает на него, вычисляя следующую функцию $У_1 = f_2(B_1, M)$. Полученный ответ пересылается проверяющей стороне V, которая осуществляет проверку истинности данного ответа. На первом этапе вероятность пропуска нарушителя примет значение $P_{ПН} = 1/2$. Чтобы ее снизить, необходимо выполнить процедуру опознавания W раундов. Тогда вероятность пропуска нарушителя составит $P_{ПН} = 1/2^w$.

Рассмотрим основные протоколы опознавания с нулевым доказательством, реализующие. В работе [15] приведен протокола опознавания, известный как протокол опознавания Фиата-Шамира. Протокол содержит два алгоритма, первый из которых используется для получения секретного и открытого ключей:

1. Для генерации ключей выбираются два больших простых числа Q и G, которые держатся в секрете. Затем вычисляется произведение $M = Q \cdot G$. Полученное значение M - это частью открытого ключа.

2. Претендент P реализует следующие действия:

- осуществляет выбор случайного числа S, для которого выполняется

$$НОД(M, S) = 1, \tag{2.1}$$

где S – секретное число; $S \in \{1, 2, .., M-1\}$.

- производится выбор числа H, для которого выполняется условие

$$H = S^2 \bmod M. \tag{2.2}$$

где H – квадратичный вычет по модулю M.

Кроме того, выбранное число H имеет мультипликативную инверсию $H^{-1} \bmod M$. Значит для данного числа H справедливо

$$H \cdot H^{-1} \equiv 1 \bmod M. \tag{2.3}$$

Для данного протокола были получены: секретный ключ S и открытый ключ определяется набором чисел (M, H).

Для выполнения опознавания претендента Р используется второй алгоритм, входящий в состав протокола. Он включает следующие этапы:

1. Зная открытый ключ, претендент Р выбирает случайное число К, которое удовлетворяет условию $1 < K < M - 1$. Данное число называют обязательством. Используя обязательство, производится вычисление

$$E \equiv K^2 \bmod M. \tag{2.4}$$

После этого претендент Р пересылает число Е проверяющей стороне V протокола опознавания.

2. Проверяющая сторона V осуществляет выбор случайного числа В, из условия $B \in \{0,1\}$, которое передается претенденту Р.

3. Получив число В, претендент Р вычисляет выражение

$$У = K \cdot S^B \bmod M \tag{2.5}$$

Если выбранное значение В = 0, то на проверяющую сторону передается вычисленное значение $У = K$. Если полученный проверочный бит был равен В = 1, то на проверяющую сторону передается $У = K \cdot S \bmod M$.

4. После получения ответа «У» на вопрос «В» проверяющая сторона V проверяет правильность полученного ответа из условий:

– если проверочный вопрос В = 0, то вычисляются равенство

$$L = Y^2 \bmod M \tag{2.6}$$

– если проверочный вопрос В = 1, то вычисляются равенство

$$L = (Y^2 H) \bmod M \tag{2.7}$$

Претендент Р имеет статус «свой» при выполнении условия

$$L \equiv E \bmod M \tag{2.8}$$

В противном случае – претенденту Р присваивается статус «чужой».

В процессе опознавания этапы 1-4 повторяются многократно. Если данный протокол будет выполнен только один раз (один раунд аутнетификации), то вероятность ошибки второго рода (вероятность пропуска нарушителя) примет значение $P_{ПН} = 1/2$. Чтобы ее снизить, необходимо

выполнить процедуру опознавания W раундов. Тогда вероятность пропуска нарушителя составит $P_{ПН} = 1/2^{W}$. Согласно [15] величина W, которая выступает в качестве параметра безопасности данного протокола опознавания, берется в пределах от 20 до 40. Претенденту P будет присвоен статус «свой», если при каждой проверке на 4 этапе будет получен положительный результат. Пример реализации протокола приведен в Приложении А.

Основным недостатком рассмотренных протоколов является низкая скорость опознавание, которая связана с необходимостью выполнения W циклов проверки для обеспечения требуемого уровня стойкости к навязыванию ложного образа.

С целью сокращения времени реализации протокола Фиат-Шамира была проведена его модификация, которая получила название протокол Фейге-Фиат-Шамира [8,67,76]. В данном протоколе можно выделить два алгоритма. Первый связан с вычислением открытого и секретного ключей. Он включает в себя следующие этапы:

1. Для генерации ключей выбирается большое число M, которое равно

$$M = Q \cdot G \tag{2.9}$$

где Q и G – большие простые числа.

2. Претендент P выбирает числа s_i, которые являются взаимно простыми с вычисленные произведением M и удовлетворяющие условию $1 \le s_i \le M - 1$, где i = 1, 2, …, n. Затем вычисляются значения

$$\nu_i \equiv s_i^2 \bmod M \tag{2.10}$$

В результате секретным ключом данного протокола является набор $s = (s_1, s_2, s_3, ..., s_n)$. В качестве открытого ключа выступают число M и $\nu = (\nu_1, \nu_2, \nu_3, ..., \nu_n)$.

Алгоритм опознавания включает в себя следующие этапы.

1. Претендент P производит выбор случайного числа K_i, которое удовлетворяет условию $1 \le K_i \le M - 1$, где i = 1, 2, …, n. Затем вычисляются

$$E_i \equiv K_i^2 \bmod M \tag{2.11}$$

Данное значение пересылается на проверяющую сторону V.

2. Для проведения опознавания проверяющая сторона V выбирает значение проверочного бита $(B_{i1}, B_{i2}, B_{i3},..., B_{in}) \in \{0,1\}^n$, который отсылается претенденту P.

3. Претендент P вычисляет ответ с использованием проверочных битов

$$Y_i \equiv K_i (s_1^{B_{i1}}, s_2^{B_{i2}}, s_3^{B_{i3}},..., s_k^{B_{ik}}) \bmod M \tag{2.12}$$

Вычисленные значения пересылается на проверяющую сторону V.

4. Проверяющая сторона V осуществляет проверку правильности полученных ответов

$$E_i \equiv Y_i^2 (\nu_1^{B_{i1}}, \nu_2^{B_{i2}}, \nu_3^{B_{i3}},..., \nu_k^{B_{ik}}) \bmod M \tag{2.13}$$

Если выражение (2.13) является истинным, то делается вывод о том, что претендент P является «своим».

При использовании данного протокола количество повторов (раундов) будет равно W. При этом использование параллельных вычислений с операндами разрядности n позволяет достичь вероятности пропуска нарушителя равной $P_{ПН} = 1/2^{nW}$. В работе [15] показано, что разработчики предлагали выбирать следующие значения n = 5, W = 4. Таким образом, проведенная модификация протокола опознавания, позволила сократить число раундов с W=20 до W = 4. Однако, несмотря на сокращение временных затрат на проведение опознавания, данный протокол также нецелесообразно использовать при определении статуса космического аппарата в НССС.

Устранить данный недостаток возможно за счет использования протокола опознавания Шнорра, принципы реализации показаны в [74,77]. Для выполнения данного протокола необходимо:

1. Выбрать два простых числа P и H такие, что число H является делителем числа P-1. Для вычисления секретного и открытого ключа определяется число M из сравнения

$$M^{H} \equiv 1 \bmod P \qquad (2.14)$$

Зная число H, выбирается секретный ключ S из условия $1 < S \le H - 1$. Используя секретный ключ, вычисляется открытый ключ протокола

$$A = M^{-S} \bmod P \qquad (2.15)$$

Протокол опознавания включает в себя следующие этапы.

1. Претендент осуществляет выбор случайного числа K, которое принадлежит группе, порожденной числом H, т.е. $1 \le K \le H - 1$. Затем вычисляется число

$$E = M^{K} \bmod P \qquad (2.16)$$

Данное число E передается на проверяющую сторону V.

2. Проверяющий V производит выбор случайного числа B, которое удовлетворяет условию $1 \le B \le 2^{T} - 1$, где T – параметр (разработчики предлагали использовать T= 52 бит). Число T пересылается претенденту.

3. Претендент P, вычисляет ответ, используя число B, согласно

$$У = (K + S \cdot B) \bmod H \qquad (2.17)$$

Полученное число Y пересылается проверяющему V.

4. Проверяющий V, получив ответ Y от претендента, производит проверку ответа

$$X = M^{У} A^{B} \bmod P \qquad (2.18)$$

Если справедливо X = E, то претендент получает статус «свой». В противном случае – претендент получает статус «чужой».

Пример реализации протокола приведен в Приложении А. Несмотря на то, что данный протокол позволяет провести опознавание претендента за один цикл, тем не менее он имеет недостаток, который связан с трудностью подбора простого числа H, который должен быть делителем числа (P - 1).

Проведенные исследования основных принципов построения протоколов опознавания, базирующихся на доказательстве с нулевым разглашением знаний, показал, что они имеют хорошую имитостойкость.

Однако, рассмотренные протоколы типа «запрос-ответ» не обеспечивают максимальную скорость выполнения процедуры опознавания. Кроме того, для обеспечения высокой имитостойкости в данных протоколах требуется выполнять все операции с использованием больших модулей. Это связано с тем, что в них не применяются сеансовые ключи, которые бы менялись на разных сеансах опознавания. Поэтому необходимо разработать такой протокол, который бы позволил выполнить эту процедуру за меньшее количество этапов и использовал сеансовые ключи.

Сократить число этапов, выполняемых в протоколе для опознавания претендента P, можно, если воспользоваться алгоритмами закрытия данных с открытым ключом (АЗДОК). В работе [85] предложен алгоритм опознавания, который построен с использованием АЗДОК. В этом случае проверяющая сторона V должна знать открытый ключ претендента P, с помощью которого происходит закрытие информации. Чтобы провести опознавание претендента проверяющая сторона выбирает случайное число X, а затем с помощью открытого ключа претендента $K^{P}_{отк}$, преобразует его согласно

$$M = E_{K^{P}_{отк}}(X) \qquad (2.19)$$

где E – процедура закрытия открытого текста.

Полученное зашифрованное сообщение M передается претенденту P. Очевидно, что получить из переданного сообщения M случайное число X возможно только при условии знания секретного ключа, с помощью которого происходит расшифрование. То есть подтвердить свой статус сможет только тот претендента P, который знает соответствующий открытому ключу $K^{P}_{отк}$ секретный ключ $K^{P}_{секр}$. Получив данное сообщение, претендент расшифровывает его с помощью своего секретного ключа $K^{P}_{секр}$ согласно

$$X^{*} = D_{K^{P}_{секр}}(M) \qquad (2.20)$$

где D – процедура расшифрования.

После того, как было получено случайное число X, претендент P передает его проверяющей стороне V. В результате этого проверяющая сторона V получает число $X = X^*$, которое передавалось претенденту P.

Из приведенного алгоритма видно, что такой протокол опознавания можно выполнить с помощью двух этапов, что позволяет повысить скорость выполнения процедуры опознавания претендента P. Так как проверяющая сторона V больше не получает новой информации от претендента P, то угроза утечки данных о значении секретного ключа $K^P_{секр}$ претендента P отсутствует. А совпадение передаваемого в сообщении M случайного числа X с принятым от претендента P числа X^*, позволяет сделать вывод о том, что последний является легитимным.

Использование данного алгоритма проверки позволяет в протоколах с нулевым разглашением секрета реализовать такой механизм, с помощью которого претендента P, который является владельцем ключа $K^P_{отк}$, можно удостоверить до расшифрования полученного сообщения M в том, что проверяющая сторона V знает случайное число X.

В работе [52] представлен двухэтапный протокол опознавания с нулевым разглашением знаний, построенный на основе алгоритма открытого шифрования RSA. В данном протоколе выбираются два простых числа r и q, которые генерируются случайным образом. Затем находится их произведение

$$R_A = q \cdot r \tag{2.21}$$

и значение функции Эйлера от этого произведения

$$\varphi(R_A) = \varphi(q \cdot r) = (q-1)(r-1) \tag{2.22}$$

Для реализации протокола выбирают число Y, которое является взаимно простым с функцией Эйлера произведения R_A, то есть справедливо $НОД(Y, \varphi(R_A)) = 1$. В работе предлагается выбрать размер числа Y равный 32 разрядам. В результате этого получается открытый ключ $K^P_{отк} = (R_A, Y)$, который известен претенденту P.

На основании открытого ключа производится выбор секретного ключа согласно

$$K_{секр}^{P} = Y^{-1} \bmod \varphi(R_A) \qquad (2.23)$$

После вычисления значения секретного ключа $K_{секр}^{P}$ выбранные простые числа r и q подвергаются уничтожению.

Тогда процедура опознавания в данном протоколе с нулевым доказательством знаний, построенным на основе алгоритма RSA, состоит из следующих этапов.

Первый этап. Проверяющая сторона V выбирает случайное число X, которое удовлетворяет условию $X < R_A$. А затем происходит вычисление сообщения M с использованием открытого ключа $K_{отк}^{P} = (R_A, Y)$ претендента согласно выражения

$$M = X^{K_{отк}^{P}} \bmod R_A \qquad (2.24)$$

Вычисленное значение пересылается претенденту P.

Второй этап. Получив сообщение M претендент P, используя свой секретный ключ $K_{секр}^{P}$, производит обратное преобразование, согласно

$$X^{*} = M^{K_{секр}^{P}} \bmod R_A \qquad (2.25)$$

Вычисленное значение X^{*} пересылается проверяющей стороне V, которая производит сравнение этого числа с числом X переданным ранее претенденту P. Если выполняется условие $X = X^{*}$, то претенденту P присваивается статус «свой».

Однако данный протокол обладает уязвимостью. Это связано с тем, что нарушитель может навязать претенденту P случайное сообщение C^{*}, представив его как зашифрованное случайное число X. В результате выполнения протокола претендент P произведет расшифрование полученного сообщения C^{*} с помощью своего секретного ключа $K_{секр}^{P}$, а результат передаст нарушителю. В результате этого произойдет утечки информации о секретном ключе претендента P. Чтобы устранить данный недостаток предлагается

использовать хэш-функции, а также специальные метки, которые добавляются к случайному числу X.

В стандарте [85] регламентируется алгоритм построения протокола опознавания с нулевым доказательством знаний на основе АЗДОК с использованием хеш-функции. В данном протоколе проверяющая сторона V формирует запрос, представляющий собой пару значений (M, H), где M – шифртекст случайного числа X, который получен с помощью АЗДОК, H – значение хэш-функции, вычисленное от сообщения X, т.е. $H = h(X)$. Использование в запросе хеш-функции позволяет претенденту P удостовериться в том, что извлеченное из зашифрованного сообщения M случайное число X было создано проверяющей стороной V. Для этого претендент должен вычислить хеш-функцию от расшифрованного числа X^*, а затем сравнить со значением $H = h(X)$, которое находилось в запросе.

В соответствии с [85] в состав протокола опознавания с нулевым разглашением знаний входят следующие этапы:

Первый этап. Проверяющая сторона V выбирает случайное число X, а затем выполняет его зашифрование с помощью выражения (2.24). Затем производится вычисление хеш-функции числа X, т.е. $H = h(X)$. Полученные значения (M, H) передаются претенденту P.

Второй этап. Претендент P, получив данный запрос (M, H), с помощью своего секретного ключа $K_{секр}^{P}$, производит расширование с использованием алгоритма (2.25). Вычисленное значение X^* подвергается хешированию. В результате получается $H^* = h(X^*)$. Данное значение сравнивают с значением хеш-функции H, поступившей от проверяющей стороны V. Если справедливо равенство $H = H^*$, то претендент P убеждается в том, что число X известно проверяющей стороне V. После этого полученное число X^* передается проверяющему V. Проверяющая сторона V производит сравнение этого числа с числом X переданным ранее претенденту P. Если выполняется условие $X = X^*$, то претенденту P присваивается статус «свой».

Наряду с хеш-функцией в протоколах опознавания могут быть использованы специальные метки. В работе [52] представлен протокол опознавания с нулевым разглашением на основе RSA, в котором используются 128-битовой метки. Данные метки определяются условием

$$\mu \equiv R_A \bmod 2^{128} \tag{2.26}$$

Таким образом, в модификации протокола будут использованы специальные метки, которые представляют собой 128 младших битов числа R_A. В этом случае протокол реализуется следующим образом.

Первый этап. Проверяющая сторона V выбирает случайное число X, которое удовлетворяет условию

$$\log_2\left(\frac{R_A}{2}\right) < \log_2 X < \log_2 R_A - \log_2 \mu \tag{2.27}$$

Затем метка μ добавляется к случайному числу X. Полученный результат зашифровывается с помощью открытого ключа претендента P, согласно

$$M = (X \| \mu)^{K^P_{отк}} \bmod R_A . \tag{2.28}$$

Вычисленное значение пересылается претенденту P.

Второй этап. Получив сообщение M претендент P, используя свой секретный ключ $K^P_{секр}$, производит обратное преобразование, согласно

$$X^* \| \mu^* = M^{K^P_{секр}} \bmod R_A \tag{2.29}$$

где μ^* − младшие 128 битов расшифрованного сообщения.

Претендент P сравнивает данное значение битовой строки μ^* с имеющимся у него значением μ, вычисленным согласно (2.3). Если справедливо $\mu^* = \mu$, то претендент P передает значение X^* проверяющей стороне V, которое является ответом на поставленный вопрос M. Если выполняется условие $\mu^* \neq \mu$, то претендент P передает сообщение о получении некорректного запроса. При выполнении равенства $X = X^*$, проверяющая сторона V присваивает претенденту P статус «свой».

В работе [11] представлен протокол опознавания с нулевым разглашением знаний, в котором обосновывается выбор меток, которые включаются в сообщение X. Предлагается выбирать метки μ, размер которых находится в пределах от 80 до 512 бит. Такая размерность меток позволит обеспечить вероятность пропуска нарушителя, будет равна $P_{ПН} = 1/2^{\mu}$. Следует также отметить, что использование специальных меток позволяет сократить схемные и временные затраты на опознавание, так как проверяющей стороне V и претенденту P не надо будет вычислять хэш-функции.

Несмотря на то, что стандарт [85] в настоящее время является действующим, предложенные методы построения протоколов опознавания с нулевым разглашением знаний на основе асимметричных алгоритмов шифрования не может быть использован в системе опознавания КА. Это связано с тем, что для реализации таких протоколов необходимо, чтобы на борту спутника находился свой секретный ключ $K^{P}_{секр}$, с помощью которого он сможет доказать свой статус проверяющей стороне V. Значит, у каждого запросчика, которые находятся на необслуживаемых объектах управления, должна быть база открытых ключей космических аппаратов. При этом для обеспечения требуемого уровня вероятности пропуска нарушителя необходимо их периодически заменять, что будет достаточно сложно выполнить. Поэтому в основе разрабатываемого протокола опознавания КА должен быть использованы другие принципы построения.

2.2 Разработка протокола опознавания, построенного на основе доказательства с нулевым разглашением знания

Прежде чем перейдем к разработке протокола опознавания, построенного на основе доказательства с нулевым разглашением знания, имеющего минимальное количество этапов для определения статуса КА обоснуем принципы, на которые будут положены в основу протокола.

Во-первых, учитывая требования, которые предъявляются к протоколам опознавания, следует отметить, что претендент Р должен обладать определенным секретом, который известен только ему. В качестве такого секрета может выступить долгосрочный секретный ключ $K_{секр}$. .

Во-вторых, чтобы усложнить возможность нарушителю определить значение секретного ключа необходимо, чтобы с данным ключом выполнялись такие вычисления, которые бы соответствовали сложности решения задачи дискретного логарифма. В качестве таких преобразований можно выбрать возведение в степень по модулю большого простого числа.

В-третьих, в рассмотренных ранее примерах реализации протоколов опознавания с нулевым разглашением знаний для обеспечения достаточно малого значения вероятность пропуска нарушителя предлагается многократно выполнять сам алгоритм опознавания. Однако, это может негативно сказаться на вероятности ложного срабатывания системы опознавания. В результате многократного обмена запросами и соответствующими ответами, на сигналы, которые передаются по радиоканалу, будут воздействовать помехи. Такое воздействие приведет к искажению переданной комбинации. В результате этого запросчик, размещенный на объекте управления, будет воспринимать свой спутник как нарушитель и откажет ему в организации сеанса связи. Для устранения данной ситуации необходимо, чтобы в разработанном протоколе опознавания без разглашений знаний использовались сеансовые ключи S(j), j = 1, 2, …. При этом при изменении номера сеанса j эти ключи должны меняться на основе псевдослучайного закона.

В-четвертых, в разрабатываемом протоколе наряду с истинными значениями секретного ключа $K_{секр}$ и сеансового ключа S(j) на j-ом сеансе, необходимо использовать их зашумленные образы $K^*_{секр}$ и $S^*(j)$. При этом величины $\Delta K_{секр}(j), \Delta S(j)$, используемые для такого зашумления должны постоянно изменяться.

В-пятых, в разрабатываемом протоколе наряду с истинными образами спутника, которые получаются на основе секретного ключа $K_{секр}$ и сеансового ключа S(j), необходимо использовать зашумленные образы, которые вычисляются с использованием зашумленных значений секретных параметров $K^*_{секр}$ и $S^*(j)$.

В-шестых, при ответе на поставленный вопрос, поступивший от запросчика, необходимо использовать как значения секретного ключа $K_{секр}$ и сеансового ключа S(j), так и их зашумленные образы $K^*_{секр}$ и $S^*(j)$. Так как в протоколе участвуют два секретных параметра $K_{секр}$ и S(j), то претендент P должен предоставить два ответа.

В-седьмых, ответы на поставленный вопрос должны вычисляться таким образом, чтобы при выполнении проверки на стороне запросчика был получен зашумленный образ спутника.

Для обеспечения требуемого уровня сложности вычисления значений секретных параметров $K_{секр}$ и S(j) предлагается воспользоваться вычислительно-сложной операцией возведения в степень по модулю. В работе [15], что данная операция имеет вычислительную сложность, соответствующую задачам распознавания Диффи-Хеллмана. Известно, что в основу стойкости задачи Диффи-Хеллмана положена сложность нахождения дискретного логарифма.

Выберем в качестве модуля q большое простое число. Найдем такое число $g < q$, с помощью которого можно получить все элементы

мультипликативной группы по модулю q. Тогда вычисление истинного образа претендента P можно реализовать на основе выражения

$$C(j) = g^{K_{секр}} g^{S(j)} \bmod q \qquad (2.30)$$

Затем необходимо провести зашумление значений секретного ключа $K_{секр}$ и S(j). Для этого воспользуемся значениями $\Delta K_{секр}(j), \Delta S(j)$, которые будут изменяться при каждом сеансе. В результате получаем следующие выражения

$$\begin{aligned} K^*_{секр}(j) &= (K_{секр} + \Delta K_{секр}(j)) \bmod \varphi(q), \\ S^*(j) &= (S + \Delta S(j)) \bmod \varphi(q), \end{aligned} \qquad (2.31)$$

где $K^*_{секр}$ и $S^*(j)$ – зашумленные образы параметров протокола $K_{секр}$ и S(j) соответственно; φ(q) – функция Эйлера числа q.

Тогда зашумленный образ претендента P будет определяться на основе выражения

$$C^*(j) = g^{K^*_{секр}} g^{S^*(j)} \bmod q \qquad (2.32)$$

Истинный и зашумленный образы претендента P будут использованы при проверке его статуса. Чтобы провести опознавание претендента P проверяющая сторона V задает вопрос, в качестве которого используется случайное число d(j) < q. При этом данный запрос должен изменяться при смене сеанса.

Получив запрос d(j), претендент P должен ответить на поставленный вопрос. Для этого предлагается разработать такие выражения, в которых в качестве аргументов используются истинные $K_{секр}$, S(j) и зашумленные $K^*_{секр}$, $S^*(j)$ значения параметров протокола опознавания, а также запрос d(j). Так как в протоколе используются два аргумента это секретный ключ $K_{секр}$ и сеансовый ключ S(j), то в протоколе должно быть получено два ответа. В этом случае каждый ответ будут зависеть и от секретного параметра, известного только претенденту P, и от заданного запроса d(j). В качестве таких выражений можно выбрать

$$\begin{aligned} r_1(j) &= (K^*_{секр}(j) - d(j)K_{секр}) \bmod \varphi(q), \\ r_2(j) &= (S^*(j) - d(j)S(j)) \bmod \varphi(q), \end{aligned} \qquad (2.33)$$

где $r_1(j)$ и $r_2(j)$ – ответы на поставленный вопрос d(j).

Для осуществления проверки претендент P должен передать истинный C(j), зашумленный $C^*(j)$ образы претендента, а также два ответа $r_1(j)$ и $r_2(j)$ на поставленный вопрос d(j).

Для проверки правильности полученных ответов проверяющая сторона V использует выражение, в котором должны участвовать истинный C(j), зашумленный $C^*(j)$ образы претендента, два ответа $r_1(j)$ и $r_2(j)$, а также поставленный вопрос d(j). Для этого необходимо истинный C(j) образ претендента P возвести в степень d(j) по модулю q. А затем полученный результат умножить на два сомножителя, значения которых получаются путем возведения числа g в степень $r_1(j)$ и $r_2(j)$ по модулю q. Учитывая выражение, используемое для получения ответов (2.33), результатом должен стать зашумленный $C^*(j)$ образ претендента P. То есть для проверки ответов можно использовать следующее выражение

$$Y(j) = C(j)^{d(j)} g^{r_1(j)} g^{r_2(j)} \bmod q \qquad (2.34)$$

Если вычисленное значение будет удовлетворять условию $Y(j) = C^*(j)$, то это означает, что претендент P подтвердил проверяющей стороне V, что он владеет секретными параметрами $K_{секр}$ и S(j), при этом не раскрывая их значение. Если условие $Y(j) = C^*(j)$ не выполняется, то это означает, что претендент P имеет статус «чужой».

Рассмотренные выше требования к протоколу опознавания космическому аппарату, построенному на доказательстве с нулевым разглашением знаний, позволили разработать протокол опознавания спутника. Данный протокол достаточно полно приведен в работе [28]. В таблице 2.1 представлен разработанный протокол опознавания космического аппарата для НССС.

Таблица 2.1 – Протокол опознавания космического аппарата

Предварительный этап			
	P (претендент)	Центр доверия	V (проверяющий)
1 2	$K_{секр}$ – секретный ключ, $K_{секр} = \{1, 2,\ldots, q - 1\}$; S – вектор для вычисления сеансового ключа $S = \{1, 2, \ldots, q - 1\}$.	q – простое число g – первообразный элемент мультипликативной группы q	
Рабочий этап			
	P (претендент)		V (проверяющий)
1	Вычисление сеансового ключа $S(j) = F(S)$; $S(j) = \{1, 2,\ldots, q - 1\}$; F – псевдослучайная функция.		
2	Вычисляется истинный статус $C(j) = g^{K_{секр}} g^{S(j)} \bmod q$.		
3	Зашумление параметров $K^*_{секр}(j) = (K_{секр} + \Delta K_{секр}(j)) \bmod \varphi(q)$, $S^*(j) = (S + \Delta S(j)) \bmod \varphi(q)$, где $\{\Delta U, \Delta S\} = \{1, 2,\ldots, q - 1\}$.		
4	Вычисляется зашумленный статус претендента $C^*(j) = g^{K^*_{секр}} g^{S^*(j)} \bmod q$.		
Опознавание космического аппарата			
1			Выбирается вопрос $d(j) = \{1, 2,\ldots, q - 1\}$.
2	Отвечает на вопрос «d(j)» $r_1(j) = (K^*_{секр}(j) - d(j)K_{секр}) \bmod \varphi(q)$, $r_2(j) = (S^*(j) - d(j)S(j)) \bmod \varphi(q)$.		
			Получает параметры $(C(j), C^*(j), r_1(j), r_2(j))$
Проверка полученного ответа на поставленный вопрос d(j)			
1			Проверяется правильность ответов на вопрос «d(j)» $Y(j) = C(j)^{d(j)} g^{r_1(j)} g^{r_2(j)} \bmod q$

			Y(j) = C*(j) – статус «свой» Y(j) ≠ C*(j) – нарушитель

Рассмотрим пример применения данного протокола в системе опознавания статуса космического аппарата. Пусть в качестве простого числа выбираем q = 19. Для мультипликативной группы, порожденной данным простым числом, существует первообразный элемент g = 2. Вычислим элементы данной мультипликативной группы.

$2^0 = 1$	$2^3 = 8$	$2^6 = 7$	$2^{10} = 17$	$2^{13} = 3$	$2^{16} = 5$
$2^1 = 2$	$2^4 = 16$	$2^7 = 14$	$2^{11} = 15$	$2^{14} = 6$	$2^{17} = 10$
$2^2 = 4$	$2^5 = 13$	$2^8 = 9$	$2^{12} = 11$	$2^{15} = 12$	$2^{18} = 1$

Пусть значение секретного ключа будет равно $К_{секр} = 10$. Пусть значение сеансового ключа системы опознавания равно S(j) = 15. Для вычисления истинного статуса претендента Р при выполнении j-го сеанса воспользуемся выражением (2.30). В результате получаем значение

$$C(j) = g^{K} g^{S(j)} \bmod q = (2^{10} \cdot \cdot 2^{15}) \bmod 19 = 2^{25} \bmod 19 = 14.$$

Произведем зашумление секретных параметров. Для этого воспользуемся выражением (2.31). Выберем следующие значения для зашумления параметров $\Delta K(j) = 5, \Delta S(j) = 8$.

В результате поучаем зашумленные значения

$$K^*(j) = (K + \Delta K(j)) \bmod \varphi(q) = (10 + 5) \bmod \varphi(19) = 15,$$
$$S^*(j) = (S(j) + \Delta S(j)) \bmod \varphi(q) = (15 + 8) \bmod \varphi(19) = 5.$$

Используя полученные значения, вычислим зашумленный статус спутника согласно (2.32). Тогда получаем

$$C^*(j) = g^{K^*} g^{S^*(j)} \bmod q = (2^{15} \cdot 2^5) \bmod 19 = 2^2 \bmod 19 = 4.$$

В процессе перемещения по орбите спутник появился в зоне видимости приемника ССС, который входит в состав абонентского терминала необслуживаемого объекта управления. Для проверки статуса данного спутника запросчик передает вопрос d(j) = 7. Получив вопрос d(j) = 7,

ответчик, находящийся на борту спутника, используя выражент (2.33) приступает к ответу на вопрос.

$$r_1(j) = (K^*(j) - dK) \bmod \varphi(q) = (15 - 7 \cdot 10) \bmod 18 = -1 \bmod 18 = 17,$$
$$r_2(j) = (S^*(j) - dS(j)) \bmod \varphi(q) = (5 - 7 \cdot 15) \bmod 18 = -10 \bmod 18 = 8.$$

После вычисления ответов ответчик передает запросчику истинный и зашумленный статусы, а также два ответа на поставленный вопрос d(j) = 7. Запросчик, воспользовавшись выражением (2.34), приступает к проверке ответов на поставленный вопрос

$$Y(j) = C^d g^{r_1^*(j)} g^{r_2(j)} \bmod q = (14^7 \cdot 2^{17} \cdot 2^8) \bmod 19 = 2^2 \bmod 19 = 4.$$

Результат проверки показал, что $Y(j) = C^*(j) = 4$. То есть проверка ответов совпала с зашумленным статусом спутника. В результате этого запросчик принимает решение о том, что статус космического аппарата – «свой». Полученные результаты свидетельствуют о возможности использования данного протокола типа «запрос-ответ», базирующийся на доказательстве с нулевым разглашением знаний, в системе опознавания статуса космического аппарата.

При этом разработанный протокол позволяет выполнить процедуру опознавания за два этапа, что в 1,5 раза быстрее рассмотренного ранее протокола опознавания Шнорра. То есть, разработанный протокол типа «запрос-ответ» обеспечивают максимальную скорость выполнения процедуры опознавания. Кроме того, использование сеансовых ключей S(j), позволяет повысить имитостойкость протокола опознавания по сравнению с ранее известными. На этом решение первой частной задачи исследования закончено.

2.3 Разработка алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата

Вторая частная задача диссертационных исследований связана с разработкой алгоритма проверки повторного использования сеансового ключа в СОКА. Очевидно, что ситуация, когда сеансовый ключ S(j) не изменяет свое значение при изменении номера сеанса с j-го на (j+1)-й, может привести к снижению вероятности имитации противником сигнала «Свой» в СОКА $P_{И}$. Это связано с тем, что вероятность подбора ответа зависит от длины ответа L и разрядности, используемого модуля, с помощью которого выполняется вычисление ответа. В этом случае вероятность

$$P_{И} = 1/2^{L} \tag{2.35}$$

Анализ выражения (2.35) показывает, что вероятность подбора ответа на вопрос запросчика $P_{И}$, будет возрастать, если при ответе на поставленный вопрос, часть его не будет изменяться. Если в процессе работы СОКА не происходит изменение значения сеансового ключа S(j) при изменении номера сеанса с j-го на (j+1)-й, то получаем, что истинный статус спутника также не будет изменяться, т.е.

$$\begin{aligned} C(j) &= g^{K_{секр}} g^{S(j)} \bmod q, \\ C(j+1) &= g^{K_{секр}} g^{S(j)} \bmod q. \end{aligned} \tag{2.36}$$

Таким образом, имея равенство C(j) = C(j+1), получаем, что длина ответа, который выдает претендент P проверяющей стороне V, сократится на $\lceil \log_2 q \rceil$ двоичный разрядов. Тогда имеем

$$P_{И} = \frac{1}{2^{L-\lceil \log_2 q \rceil}} \tag{2.37}$$

Чтобы устранить такую ситуацию необходимо разработать алгоритм проверки повторного использования сеансового ключа S(j), отличающегося от ранее известных, тем, что позволяет провести проверку без его передачи ключа по открытому каналу связи.

Чтобы выполнить проверку необходимо в протокол включить дополнительный параметр T(j), который зависит от сеансового ключа S(j). Пусть $T(j) = kS(j) \bmod q$, где k – целое число. В процессе j-го сеанса опознавания претендент P должен также получить дополнительное случайное число, которое X(j) < q. Используя данное число претендент P вычисляет равенство, с помощью которого центр поддержки операций автоматизированной системы дистанционного мониторинга, контроля и управления сможет выявить повторное применение сеансового ключа. В составе данного выражения должен использоваться секретный ключ $К_{секр}$ спутника. Тогда получаем равенство

$$M(j) = (К_{сек} + T(j)X(j)) \bmod q \qquad (2.38)$$

где X(j) – случайное число, которое получил претендент на j-ом сеансе.

Вычисленное значение M(j) и запрос X(j) передаются в центр поддержки операций АСДМКУ. Очевидно, что однократное выполнение выражения (2.38) не позволит ЦПО автоматизированной системы дистанционного мониторинга, контроля и управления сможет выявить повторное применение сеансового ключа. Поэтому при выполнении следующего сеанса (j+1)-го сеанса опознавания претендент P от проверяющей стороны V получает другое случайное число X(j+1) < q. Затем претендент P вычисляет равенство

$$M(j+1) = (К_{сек} + T(j)X(j+1)) \bmod q \qquad (2.39)$$

Вычисленное значение M(j+1) и запрос X(j+1) передаются в центр поддержки операций АСДМКУ. В результате в ЦПО получают следующую систему уравнений

$$\begin{cases} M(j) = (К_{сек} + TX(j)) \bmod q \\ M(j+1) = (К_{сек} + TX(j+1)) \bmod q \end{cases} \qquad (2.40)$$

В результате решения такой системы уравнения центр поддержки операций АСДМКУ сможет получить значение секретного ключа космического аппарата.

Очевидно, что такой алгоритм проверки повторного использования сеансового ключа позволяет определить такую ситуацию, без его передачи сеансового ключа S(j) по открытому каналу связи. Однако, недостатком такого алгоритма является возможность вычисления секретного ключа $К_{секр}$ спутника. Это может негативно сказаться на защищенности всей системы опознавания космического аппарата НССС.

В работе [81] представлен алгоритм, позволяющий определить правильность генерации сеансового ключа S(j) и параметра T(j), используемого для проверки повторного использования сеансового ключа. Перед началом проверки претендент имеет значения сеансового ключа S(j) и параметра T(j), которые были вычислены согласно

$$S(j) = g^{a_S} \bmod q \tag{2.41}$$

$$T(j) = g^{a_T} \bmod q \tag{2.42}$$

где $a_S(j) = \prod_{n=1}^{m} \frac{1}{S_n + К_n} \bmod q$; $a_T(j) = \prod_{n=1}^{m} \frac{1}{T_n + К_n} \bmod q$; S_n, T_n и $К_n$ – n–й блок, полученный при разбиении параметров S(j), K и T(j) на m частей.

Для выполнения проверки проверяющая сторона V пересылает претенденту случайное число, которое $r \in Z_q$.

После претендент P приступает к вычислению ответов на вопрос r

$$a_s^*(j) = (a_s(j) - r) \bmod q \tag{2.43}$$

$$a_T^*(j) = (a_T(j) - r) \bmod q \tag{2.44}$$

Вычисленные значения претендент использует для вычисления затемненных образов S(j) и T(j)

$$S^*(j) = g^{a_S^*} \bmod q \tag{2.45}$$

$$T^*(j) = g^{a_T^*} \bmod q \tag{2.46}$$

После этого претендент P определяет произведение истинных и затемненных образов

$$S(j)T(j) \bmod q = g^{a_S} К_U g^{a_T} \bmod q = К_U g^{(a_S + a_T) \bmod \varphi(q)} \bmod q \tag{2.47}$$

$$S^*(j)T^*(j) \bmod q = g^{a_S^*} К_U g^{a_T^*} \bmod q = К_U g^{\left(a_S^* + a_T^*\right) \bmod \varphi(q)} \bmod q \qquad (2.48)$$

Затем результаты $(S(j)T(j), S^*(j)T^*(j))$ пересылаются проверяющей стороне V. После этого проверяющая сторона V приступает к вычислению отношения

$$A(j) = \frac{S(j)T(j)}{S^*(j)T^*(j)} = \frac{К_U g^{\left(a_S + a_T\right) \bmod \varphi(q)}}{К_U g^{\left(a_S^* + a_T^*\right) \bmod \varphi(q)}} = g^{2r} \bmod q \qquad (2.49)$$

Если вычисленное значение A(j) соответствует равенству

$$A'(j) = \left(g^r\right)^2 \bmod q = A(j) \qquad (2.50)$$

то это свидетельствует о том, что представленные S(j) и параметр T(j), который используется для проверки повторного использования S(j), сгенерированы правильно.

Однако данный алгоритм проверки не позволяет определить на каком спутнике произошел сбой, и он повторно использует сеансовый ключ S(j). Поэтому необходимо разработать алгоритм, применение которого позволило проверяющей стороне получить значение открытого ключа спутника.

В работе [27] предложен алгоритм, позволяющий провести проверку повторного использования сеансового ключа без передачи по открытому каналу связи как его самого, так и секретного ключа $К_{секр}$ спутника. Так как для генерации сеансового ключа S(j) будет использоваться псевдослучайная функция, то очевидно, что вычисления параметра T(j) должна также использоваться аналогичная ПСФ. При этом алгоритм проверки надо построить таким образом, чтобы в результате проверки в ЦПО был получен только открытый ключ КА.

Очевидно, что системе опознавания космического аппарата претендент P, который размещается на борту спутника должен сам осуществлять генерацию, как сеансовых ключей S(j), так и параметра T(j), зависящего от значения j-го сеансового ключа. Таким образом, очевидно следующее преобразование $S(j) = F_S(j)$, где $F_s(j)$ – функция, позволяющая определить j-ый сеансовый ключ, используя параметр S. Для вычисления параметра T(j),

позволяющего установить повторное использование сеансового ключа S(j) в СОКА, используется выражение $T(j) = F_T(j, К_{сек}, S(j))$. Таким образом, вычисленное значение параметра T(j) будет определяться исходным параметром T, секретным ключом спутника $К_{сек}$, а также сеансовым ключом S(j). Очевидно, чтобы обеспечить достаточно высокую стойкость к НСД необходимо, чтобы при вычислении значений S(j) и T(j) использовалась псевдослучайная функция (ПСФ), которая имеет следующие свойства:

– отсутствует корреляция между соседними аргументами функции j и j+1 и полученными результатами $F_S(j)$ и $F_S(j+1)$;

– ПСФ имеет достаточно простую аппаратную и программную реализацию;

– аппаратная реализация ПСФ поддерживает конвейерную организацию вычислений.

Для разработки алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата воспользуемся ПСФ, приведенной в работах [82,101]. Для получения сеансового ключа воспользуемся следующим выражением

$$S(j) = g^{\frac{1}{S(j-1)+К_{сек}}} \bmod q \qquad (2.51)$$

где S(j-1) – значение сеансового ключа на предыдущем сеансе связи; $S = S(0)$ – исходный параметр для вычисления сеансовых ключей; $К_{секр}$ – секретный ключ спутника.

Для вычисления параметра T(j), позволяющего установить повторное использование сеансового ключа S(j) в СОКА, воспользуемся следующим выражением

$$T(j) = g^{\frac{1}{S(j-1)+К_{сек}+T}} \bmod q \qquad (2.52)$$

где T – исходный параметр для получения T(j).

Разработанный алгоритм проверки повторного использования сеансового ключа в системе опознавания космического аппарата состоит из следующих этапов.

1. Претендент P для проведения опознавания вычисляет значения сеансового ключа S(j), согласно выражения (2.51), а также значение параметра проверки T(j) на основе равенства (2.52).

2. После выполнения j-го сеанса опознавания проверяющая сторона V делает дополнительный запрос, в качестве которого используется случайное число $X(j) < q$.

3. Претендент P, получив данный запрос, вычисляет не него ответ согласно выражения

$$M(j) = K_{отк}\left(g^{\frac{1}{S(j-1)+K_{сек}+T}} \right)^{X(j)} \bmod q \qquad (2.53)$$

4. Значения $M(j), X(j)$ передаются проверяющей стороне.

5. Претендент P для проведения опознавания вычисляет значения сеансового ключа S(j+1), согласно выражения (2.51), а также значение параметра проверки T(j+1) на основе равенства (2.52).

6. После выполнения (j+1)-го сеанса опознавания проверяющая сторона V делает дополнительный запрос, в качестве которого используется случайное число $X(j+1) < q$.

7. Претендент P, получив данный запрос, вычисляет на него ответ согласно выражения

$$M(j+1) = K_{отк}\left(g^{\frac{1}{S(j-1)+K_{сек}+T}} \right)^{X(j+1)} \bmod q \qquad (2.54)$$

8. Значения $M(j+1), X(j+1)$ передаются проверяющей стороне.

9. Проверяющая сторона выполняет проверку повторного использования сеансового ключа в системе опознавания космического аппарата, используя следующие выражение

$$W = \left| \left(\frac{(M(j))^{X(j+1)}}{(M(j+1))^{X(j)}} \right)^{(X(j+1)-X(j))^{-1}} \right|_q^+ \qquad (2.55)$$

Если в результате вычисления будет получен открытый ключ космического аппарата $К_{отк}$, то это свидетельствует о том, что данный спутник повторно использовал сеансовый ключ S(j) при выполнении процедуры опознавания.

Рассмотрим ситуацию, когда была нарушена работа генератора ПСФ, с помощью которого вычислялись значения сеансовых ключей S(j). В этом случае значения соседних сеансовых ключей S(j) и S(j+1) будут совпадать

$$S(j) = g^{\frac{1}{S(j-1)+K_{сек}}} \bmod q = g^{\frac{1}{S(j)+K_{сек}}} \bmod q = S(j+1) \qquad (2.56)$$

при выполнении условия $S(j) = S(j+1) = \hat{S}$.

Очевидно, что передавать сеансовые ключи по открытому каналу для проверки нельзя. Поэтому воспользуемся параметрами T(j) и T(j+1), позволяющими установить повторное использование сеансового ключа S(j) в СОКА. В этом случае значения данных параметров будут также совпадать, так как при выполнении условия $S(j) = S(j+1) = \hat{S}$ справедливо

$$T(j) = g^{\frac{1}{S(j-1)+K_{сек}+T}} \bmod q = g^{\frac{1}{S(j)+K_{сек}+T}} \bmod q = T(j+1) \qquad (2.57)$$

Тогда при получении первого запроса X(j) < q, ответ претендента P будет определяться из выражения

$$M(j) = К_{отк} \left(g^{\frac{1}{\hat{S}+K_{сек}+T}} \right)^{X(j)} \bmod q \qquad (2.58)$$

При получении второго запроса от проверяющей стороны X(j+1) < q, претендент вычислит ответ, согласно

$$M(j+1) = К_{отк} \left(g^{\frac{1}{\hat{S}+K_{сек}+T}} \right)^{X(j+1)} \bmod q \qquad (2.59)$$

Для удобства обозначим

$$B = \left(g^{\frac{1}{\hat{S}+K_{сек}+T}} \right) \bmod q \qquad (2.60)$$

Рассмотрим выполнение проверки повторного использования сеансового ключа в системе опознавания космического аппарата, реализованного согласно выражению (2.55). В этом случае получаем

$$W = \left| \left(\frac{(M(j))^{X(j+1)}}{(M(j+1))^{X(j)}} \right)^{(X(j+1)-X(j))^{-1}} \right|_q^+ = \left| \left(\frac{(K_{отк} B^{x(j)})^{X(j+1)}}{(K_{отк} B^{x(j+1)})^{X(j)}} \right)^{(X(j+1)-X(j))^{-1}} \right|_q^+ =$$

$$= \left| \left(\frac{K_{отк}^{X(j+1)} B^{X(j)X(j+1)}}{K_{отк}^{X(j)} B^{X(j+1)X(j)}} \right)^{(X(j+1)-X(j))^{-1}} \right|_q^+ = \left| \left(\frac{K_{отк}^{X(j+1)}}{K_{отк}^{X(j)}} \right)^{(X(j+1)-X(j))^{-1}} \right|_q^+ = \qquad (2.61)$$

$$\left| \left(K_{отк}^{X(j+1)-X(j)} \right)^{\frac{1}{X(j+1)-X(j)}} \right|_q^+ = K_{отк}.$$

Вычисленное значение открытого ключа спутника позволяет определить соответствующий КА и произвести перезапуск генератора выработки сеансовых ключей.

Проведем сравнительный анализ системы опознавания космического аппарата, использующей разработанный алгоритм проверки повторного использования сеансового ключа и СОКА без применения данного алгоритма. Пусть простое число q имеет разрядность, равную $\log_2 q = 16$ бит. При использовании разработанного протокола опознавания на основе доказательства с нулевым разглашением знания проверяющей стороне передаются следующие значения: истинный статус претендента C(j), зашумленный статус претендента $C^*(j)$, а также два ответа $r_1(j), r_2(j)$. Так как все вычисления проводились по модулю q, размерность такого сигнала, передаваемого претендентом составит L = 64 бит. Тогда согласно выражения (1.20) вероятность имитации противником сигнала «Свой» в СОКА будет равна $P_И(1) = 2^{-64} = 5{,}421 \cdot 10^{-20}$.

Рассмотрим ситуацию, когда СОКА не использует разработанный алгоритм проверки повторного использования сеансового ключа. Очевидно,

что если в процессе работы СОКА не происходит изменение значения сеансового ключа S(j) при изменении номера сеанса с j-го на (j+1)-й, то получаем, что истинный статус спутника также не будет изменяться, т.е.

$$C(j) = g^{K_{секр}} g^{S(j)} \bmod q,$$
$$C(j+1) = g^{K_{секр}} g^{S(j)} \bmod q.$$

В результате этого при неизменной длине ответа проверяющей стороне, равной L = 64 бит, первых 16 бит не будут изменять свое значение. Таким образом, имея равенство C(j) = C(j+1), получаем, что длина ответа, который выдает претендент P проверяющей стороне V, сократится на $\lceil \log_2 q \rceil$ двоичный разрядов. Тогда имеем

$$P_{ПО}^{СОКА}(2) = \frac{1}{2^{L-\lceil \log_2 q \rceil}} = \frac{1}{2^{48}} = 3{,}552 \cdot 10^{-15}$$

Таким образом, полученные результаты свидетельствуют о том, что не использование разработанного алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата приводит к увеличению вероятность подбора ответа на вопрос запросчика в $1{,}52 \cdot 10^{5}$ раз.

На этом решение второй частной задачи исследования закончено.

Выводы

1. Первая частная задача диссертационных исследований связана с разработкой протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений, обладающего меньшими временными затратами на опознавания спутника. Для решения данной частной задачи был проведем анализ основных принципов реализации протоколов опознавания Фиата-Шамира, Фейге-Фиат-Шамира,

базирующихся на доказательстве с нулевым разглашением сведений. Проведенные исследования показали, что для обеспечения требуемого уровня вероятности подбора ответа данные протоколы выполняются многократно. Так для протокола Фиата-Шамира требуется выполнить от 20 до 40 раундов опознавания.

2. Для сокращения числа этапов, выполняемых в протоколе для опознавания претендента P, был проведен анализ алгоритмов закрытия данных с открытым ключом. Проведенные исследования показали, что эти методы построения протоколов опознавания с нулевым разглашением знаний не могут быть использован в системе опознавания КА. Это связано с тем, что для реализации таких протоколов необходимо, чтобы на борту спутника находился свой секретный ключ $K_{секр}^{P}$, с помощью которого он сможет доказать свой статус проверяющей стороне V. Значит, у каждого запросчика, которые находятся на необслуживаемых объектах управления, должна быть база открытых ключей космических аппаратов. При этом для обеспечения требуемого уровня вероятности пропуска нарушителя необходимо их периодически заменять, что будет достаточно сложно выполнить.

3. На основе проведенных исследований были определены основные принципы построения протокола опознавания КА. Используя данные принципы, был разработан протокол опознавания, построенный на основе доказательства с нулевым разглашением знания, который обладает меньшим количеством этапов опознавания. должен быть использованы другие принципы построения. Проведенный сравнительный анализ показал, разработанный протокол позволяет выполнить процедуру опознавания за два этапа, что в 1,5 раза быстрее рассмотренного ранее протокола опознавания Шнорра. На этом решение первой частной задачи исследования закончено.

4. Вторая частная задача диссертационных исследований связана с разработкой алгоритма проверки повторного использования сеансового ключа в СОКА. Очевидно, что ситуация, когда сеансовый ключ S(j) не изменяет свое значение при изменении номера сеанса с j-го на (j+1)-й, может привести к

повышению вероятности пропуска спутника-нарушителя $P_{ПС}^{СОКА}$. Чтобы устранить такую ситуацию был разработан алгоритм, позволяющий провести проверку повторного использования сеансового ключа S(j). В ходе диссертационных исследований был разработан такой алгоритм, отличающийся от ранее известных, тем, что позволяет провести проверку без передачи по открытому каналу связи сеансовых ключей. Если в процессе работы СОКА ответчик повторно использует сеансовый ключ, то реализуя разработанный алгоритм проверяющая сторона получит открытый ключ КА.

5. В диссертации проведен сравнительный анализ эффективности работы системы опознавания космического аппарата, использующей разработанный алгоритма проверки повторного использования сеансового ключа и без применения данного алгоритма. Полученные результаты свидетельствуют о том, что не использование разработанного алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата приводит к увеличению вероятность подбора ответа на вопрос запросчика в $1{,}52 \cdot 10^5$ раз уже при разрядности ответа претендента равного 64 бит. На этом решение второй частной задачи исследования закончено.

ГЛАВА 3 РАЗРАБОТКА СИСТЕМЫ ОПОЗНАВАНИЯ КОСМИЧЕСКОГО АППАРАТА, ПОСТРОЕННОГО НА ОСНОВЕ ПРОТОКОЛА ОПОЗНАВАНИЯ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ ЗНАНИЙ

3.1 Разработка структурной модели генератора для выработки сеансового ключа системы опознавания космического аппарата

В рассмотренных в разделе 2.1 диссертации протоколах опознавания, базирующихся на основе доказательства с нулевым разглашением знаний, применяется только секретный ключ. Для повышения имитостойкости низкоорбитальной ССС было предложено использовать сеансовые ключи, которые бы изменяли свое значение через определенные интервалы времени. При использовании разработанного протокола опознавания сеансовые ключи участвуют в вычислениях:

- истинного статуса C(j) претендента P;
- зашумленного статуса C^{*}(j)претендента P;
- второго ответа на поставленный запрос d(j).

Таким образом, очевидно, что качества выработки сеансового ключа во многом зависит имитостойкость разработанного протокола опознавания. Рассмотрим основные методы и алгоритмы, которые можно использовать для получения сеансового ключа.

В настоящее время известно множество генераторов, с помощью которых можно формировать псевдослучайную последовательность (ПСП) чисел. В работе [16] приведен метод позволяющий получить ПСП чисел на основе линейных конгруэнтных генераторов. Алгоритм работы таких

генераторов задается выражением

$$S(j+1) = (AS(j) + B) \bmod p \qquad (3.1)$$

где S(j) – j-ый член ПСП чисел; S(j+1) – последующий член ПСП чисел; A – множитель; B – приращение (инкремент); p – модуль.

Обобщая выражение (3.1), получаем закон генерирования ПСП чисел

$$S(j+k) = \left(A^k S(j) + \frac{A^k - 1}{A - 1} B \right) \bmod p \qquad (3.2)$$

В результате выполнения алгоритма (3.20) получается линейная конгруэнтная последовательность чисел. Из выражений (3.1) и (3.2) наглядно видно, что величина периода линейного конгруэнтного генератора определяется величиной выбранного модуля p. Чтобы обеспечить максимальный период линейная конгруэнтная ПСП чисел необходимо, выполнение условий:

– переменные B и p должны иметь наибольший общий делитель равный единице, т.е. $НОД(B, p) = 1$;

– число (A - 1) должно быть кратным простому числу C, которое является делителем числа p;

– число (A - 1) должно быть кратным 4, если модуль p кратен числу 4.

Проведенные исследования показали, что достоинством линейных конгруэнтных генераторов ПСП чисел являются хорошие статистические свойства. Однако такие генераторы нельзя отнести к криптостойким. При выполнении теста «распределения на плоскости» полученный результат имеет четко решетчатую структуру.

С целью уменьшения решетчатости результатов преобразования в работах [16,100] предлагалось использовать полиномиальные конгруэнтные генераторы ПСП чисел. Алгоритм работы таких генераторов задается

$$S(j+1) = (A_i S^i(j) + A_{i-1} S^{i-1}(j) + \ldots + A_1 S^i(j) + B) \bmod p \qquad (3.3)$$

Для получения максимального периода ПСП чисел необходимо выполнение следующих условий:

– переменные B и p должны иметь наибольший общий делитель равный единице, т.е. $\text{НОД}(B, p) = 1$;

– числа A_1 и A_2 должны быть кратным простому числу C, которое является нечетным делителем числа p;

– значение числа равно $A_2 = (A_1 - 1) \bmod 4$ при условии, что p кратно 4;

– значение числа равно $A_2 = (A_1 - 1) \bmod 2$ при условии, что p кратно 2;

– значение числа равно $A_3 \neq 3B \bmod 9$ при условии, что p кратно 9.

Как показал анализа работ [8,67] применение полиномиальных генераторов не позволило существенно снизить решетчатость распределения чисел на плоскости.

В работе [77] представлен алгоритм работы генератора с квадратичным остатком. Данный генератор позволяет получить ПСП чисел на основе использования алгоритма BBS. Для работы генератора выбирают два больших числа A и B. Они должны удовлетворять следующим условиям:

$$A \equiv 3 \bmod 4, \quad B \equiv 3 \bmod 4 \tag{3.4}$$

$$\text{rest}\frac{A}{4} = 3, \quad \text{rest}\frac{B}{4} = 3 \tag{3.5}$$

Затем находится произведение $M = AB$ - число Блюма. После этого выбирается случайное число S, такое что $\text{НОД}(S, M) = 1$. Затем производится вычисление стартового числа генератора согласно

$$S(0) \equiv S^2 \bmod M \tag{3.6}$$

На j –ом шаге работы генерация числа определяется выражением

$$S(j) \equiv S^2(j-1) \bmod M \tag{3.7}$$

В обобщенном виде вычисление числа на j –ом шаге работы генератора задается выражением

$$S(j) \equiv S_0^{2^j \bmod \varphi M} \bmod M \tag{3.8}$$

где $S_0 = S(0)$.

Применение данного генератора позволяет устранить недостатки рассмотренных ранее генераторов ПСП чисел. Однако он требует достаточно высоких временных затрат на вычисление псевдослучайных чисел. При этом появление быстрого алгоритма факторизации приведет к снижению стойкости данного алгоритма BBS.

В работе [16] предлагается для получения последовательности псевдослучайных чисел использовать рекуррентный генератор последовательности чисел (РГПЧ), который задается стандартом ГОСТ 28147-89. Данный рекуррентный генератор предназначен для получения 64-битовых псевдослучайных чисел. Принцип его работы состоит в следующем.

Исходное 64-битовое число разбивается на два полублока, размер которых равен 32. При этом старший и младший полублоки подвергаются независимой обработке согласно

$$\begin{aligned} &\Omega_i = (\Omega_i^0, \Omega_i^1), \left|\Omega_i^0\right| = \left|\Omega_i^1\right| = 32, \\ &\Omega_{i+1}^0 = f_1(\Omega_i^0), \Omega_{i+1}^1 = f_2(\Omega_i^1), \end{aligned} \tag{3.9}$$

где f_1, f_2 – функция преобразования; Ω_i – элемент рекуррентной последовательности; Ω_i^0 – младший полублок размером 32 бит; Ω_i^1 – старший полублок размером 32 бит.

В результате такого подхода создается два РГПЧ, которые независимо обрабатывают старший и младший полублоки исходного числа.

При этом рекуррентные преобразования старшего полублока определяются выражением

$$\Omega_{i+1}^1 = (\Omega_i^1 + C_1 - 1) \bmod (2^{32} - 1) + 1 \tag{3.10}$$

где $C_1 = 1010104_{16}$ – константа в 16-ричной системе счисления.

Рекуррентные преобразования второго полублока определяются выражением

$$\Omega_{i+1}^0 = (\Omega_i^0 + C_0) \bmod 2^{32} \tag{3.11}$$

где $C_0 = 1010101_{16}$ – константа в 16-ричной системе счисления.

Характерной чертой выражения (3.10) является то, что при возникновении ситуации, когда при получении результата $(2^{32}-1)\bmod(2^{32}-1)=0$ в регистр буде записано число $2^{32}-1$. Такой подход позволяет получить период для старшего полублока равный $T_1=2^{32}-1$. При этом период для младшего полублока составит $T_0=2^{32}$. В результате этого период для данного РГПЧ составит $T_{\text{РГПЧ}}=2^{32}(2^{32}-1)$.

Однако данный генератор невозможно использовать для получения сеансовых ключей S(j) для системы опознавания космического аппарата, так как он применялся в отечественном стандарте шифрования ГОСТ 28147-89.

В работе [70] представлен алгоритм работы инверстного конгруэтного генератора. Характерной чертой такого генератора является то, что с целью повышения стойкости предлагается использовать обратную функцию, которая получается с использованием линейных комбинаций, состоящей из предыдущих чисел. В этом случае используется следующее равенство

$$S(j+1)=(AS^{-1}(j)+C)\bmod q \qquad (3.12)$$

где $S(j)\neq 0$.

Если значение S(j) = 0, то значение, снимаемое с выхода генератора, будет равно S(j+1) = C.

Как известно, наличие мультипликативного обратного элемента возможно, если генератор работает в конечном поле Галуа GF(q). При этом соблюдается следующее условие $S(j)S^{-1}(j)=1\bmod q$. Для эффективной работы такого генератора необходимо, чтобы выполнялись условия $\text{НОД}(S(0), q)=1$ и $\text{НОД}(A, q)=1$. В этом случае добиться максимального периода ПСП чисел можно, если выбранный многочлен $F(s)=s^2-Cs-A$ относится к примитивным многочленам конечного поля Галуа GF(q).

Следует отметить, что благодаря своим достоинствам, были разработаны генераторы, использующие полиномы более высокой степени. Тогда алгоритм работы таких генераторов определяется выражением

$$S(j+1) = \sum_{i=0}^{r} ((A(i)S^{i-r}(j) + C) \bmod q \qquad (3.13)$$

Как показано в работе [16] данные генераторы ПСП чисел проходят успешно большинство тестов, проводимых на проверку случайности выходного отклика. Однако, данные генераторы обладают недостатком. Он связан с трудоемкостью отыскания мултипликативного обратного элемента в конечном поле Галуа. Как правило, трудоемкость такой операции составляет $O(N^2) = O((\log_2 q)^2)$.

Достаточно широкое применение нашли генераторы, построенные на основе регистров сдвига с линейной обратной связью. Данный тип генераторов ПСП чисел характеризуется достаточно простой схемной реализацией, высокой скоростью вычисления чисел, хорошими статистическими характеристиками получаемой последовательности. Для таких генераторов ПСП чисел справедливо следующее выражение

$$S(j+1) = T^k S(j) \qquad (3.14)$$

где S(j) – вектор, задаваемый состояниями регистра сдвига в j-ый момент времени; T^k – квадратная матрица, характеризующаяся порядком q.

Такую матрицу можно представить в следующем виде

$$T^k = \begin{pmatrix} a_1 & a_2 & \dots & a_{q-1} & a_q \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}. \qquad (3.15)$$

Однако, данные генераторы нецелесообразно использовать для получения сеансовых ключей S(j) для системы опознавания космического аппарата. Это связано с тем, что состояние регистра сдвига будет определяться элементом конечного поля Галуа GF(q), значение которого определяется порождающим полиномом. Тогда, если нарушитель узнает порождающий полином, то сможет достаточно легко вычислить значения сеансовых ключей.

Чтобы снизить вероятность подбора сеансового ключа S(j) и повысить имитостойкость системы опознавания статуса космического аппарата,

применяемой в ССС комплекса удаленного мониторинга, контроля и управления удаленным объектом, можно за счет использования псевдослучайной функции.

В настоящее время широкое применение нашла ПСФ Наора-Рейнголда. В работах [87-100] представлены принципы построения математической модели, применение которой позволяющая получить псевдослучайную последовательность целых чисел, вычисленных по модулю простого числа q. Стойкость данной псевдослучайной функции базируется на сложности решения проблемы Диффи-Хеллмана. Чтобы вычислитель псевдослучайные числа, построенные с помощью ПСФ Наора-Рейнголда, необходимо использовать n-битную двоичную строку и секретный ключ. Тогда вычислительная сложность ПСФ Наора-Рейнголда будет определяться умножениями по модулю, число которых равно n-1, а также одной операцией возведения в степень первообразного элемента по модулю q. Таким образом, для получения псевдослучайных чисел с помощью ПСФ Наора-Рейнголда применяется выражение

$$F((s_1,...,s_n),(g,x_1,...,x_n)) = g^w \bmod p \qquad (3.16)$$

где $(x_1,...,x_n)$ - входная последовательность; g – первообразный элемент, с помощью которого вычисляются элементы мультипликативной группы; $(s_1,...,s_n)$ - секретный ключ; $w = \prod_{i=1}^{n} x_i^{s_i}$.

Очевидно, что недостатком реализации ПСФ Наора-Рейнголда является необходимость выполнения n-1 умножений по модулю q, которые и определяют стойкость ПСФ.

В работах [18,19] была предложена ПСФ, которая позволяет устранить данный недостаток. В данной работе был проведен анализ основных принципов построения псевдослучайных функций. На основе полученных результатов был предложен алгоритм реализации ПСФ, которая для получения псевдослучайного целого числа использовала входную

последовательность $(x_1,...,x_n)$ и ключ $(g,s_1,...,s_n)$. В этом случае алгоритм формирования такой псевдослучайной функции можно представить в виде следующего выражения

$$F((s_1,...,s_n,g),(x_1,...,x_n)) = g^{\left(\prod_{i=1}^{m}(s_i+x_i)\right)^{-1}} \bmod q \qquad (3.17)$$

где g – первообразный элемент, образующий мультипликативную группу ненулевых остатков по модулю q.

В работе приведено доказательство теорем, которые показывают, что разбиение исходных аргументов, имеющих диапазон равный n разрядов, на m блоков, характеризующихся меньшим числом разрядов $\log_2 L$, где L определяется как $x \in \{1,..L\}$. Таким образом, исходная область определения, которая имеет размер 2^n, разбивается на совокупность $m = n/\log_2 L$ областей, имеющих размер L. В результате использования такой ПСФ будет сокращено число умножений по модулю в $\log_2 L$ раз. При этом ПСФ, формирование которой определяется выражением (3.17) обеспечивает стойкость аналогичную стойкости ПСФ Наора-Рейнголда при меньшей в $\log_2 L$ раз длине ключа. Кроме того, для реализации такой ПСФ требуется меньший объем памяти, которая будет использована для получения последовательности псевдослучайных целых чисел.

Благодаря отмеченным достоинствам псевдослучайная функция, алгоритм вычисления которой задается выражением (3.17), была выбрана для получения сеансового ключа S(j) и параметра проверки T(j) в разработанном методе построения системы опознавания космического аппарата, построенном на основе протокола опознавания нулевым разглашением значения функция. Для формирования ПСФ была разработана структурная схема генератора, предназначенного для выработки сеансового ключа системы опознавания космического аппарата, которая представлена в работе [61]. На рисунке 3.1 представлена структурная модель генератора

псевдослучайной функции, реализующего вычисление сеансового ключа согласно выражения

$$S(j) = g^{\left(\prod_{i=1}^{n}(S_i\,(j-1)+K_i)\right)^{-1}} \bmod q \qquad (3.18)$$

Структурная модель генератора ПСФ содержит два входа, на которые подаются сеансовый S(j-1) и секретный $К_{секр}$ ключи, три регистра (Рег.1 – Рег.3), сумматор по модулю q (Сум), блок вычисления обратного элемента (БВОЭ), умножитель по модулю q (Умн), блок возведения в степень (БВС).

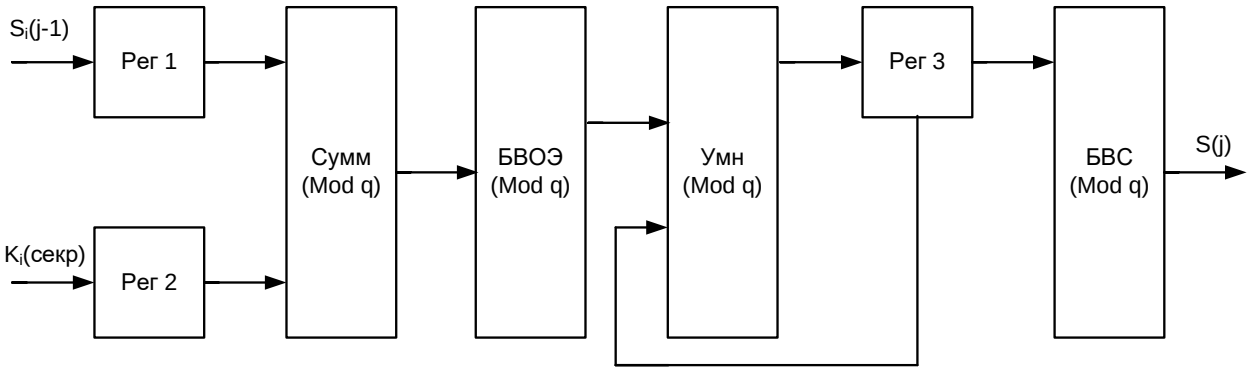

Рисунок 3.1 – Структурная модель генератора псевдослучайной функции, реализующего вычисление сеансового ключа

Для вычисления сеансового ключа S(j) на первый вход подается значение предыдущего сеансового ключа S(j-1). Данное значение поступает последовательно поблочно $S_i\,(j-1)$, где i = 1,2,…,n. При этом длина блока составляет $\log_2 S_i\,(j-1) = \log_2 L$ бит. Текущий блок заносится в первый регистр (Рег 1). Одновременно с этим на второй вход подается значение секретного ключа $К_{секр}$, размерность которого не превышает $\lceil \log_2 q \rceil$ разрядов. При этом секретный ключ также подается поблочно по $\log_2 L$ бит. Текущий блок секретного ключа заносится во второй регистр (Рег 2).

С выхода первого и второго регистров значения текущих блоков $S_i\,(j-1)$ и K_i подаются на входы сумматора по модулю q (Сумм). С выхода данного сумматора снимаются значения $(S_i\,(j-1)+K_i) \bmod q$, которое поступает на

вход блока вычисления обратного элемента по модулю q (БВОЭ). Данный блок реализует выполнение операции

$$a_i^{-1} = \left(\frac{1}{S_i(j-1) + K_i} \right) \bmod q \qquad (3.19)$$

Вычисленное значение a_i^{-1} поступает на первый вход умножителя по модулю q (Умн), на второй вход которого поступает промежуточный результат умножения. Для хранения промежуточного результат используется третий регистр (Рег 3).

После выполнения n раундов преобразований вычисленное значение показателя степени

$$w = \prod_{i=1}^{n} \left(\frac{1}{S_i(j-1) + K_i} \right) \bmod q \qquad (3.20)$$

подается на блок, реализующий возведение в степень по модулю q (БВС). С выхода данного блока снимается значение сеансового ключа S(j).

Рассмотрим пример. Пусть значение модуля q = 11. В качестве первообразного элемента для мультипликативной группы, состоящей из ненулевых вычетов по модулю q = 11, выбираем число g = 2. Пусть значение секретного ключа равно $K_{секр} = 11_{10}$. Данное значение подается на первый вход генератора ПСФВ качестве предыдущего значения сеансового ключа, поступившего на второй вход генератора ПСФ, выбираем число $S(j-1) = 10_{10}$. Значение сеансового ключа S(j-1) поступает на второй вход генератора ПСФ. Представляем данные значения в двоичной форме. В результате этого имеем $K_{секр} = 11_{10} = 1011_2$ и $S(j-1) = 10_{10} = 1010_2$.

Пусть секретный $K_{секр}$ и сеансовые S(j-1) ключи подаются на входы поблочно. При этом длина блока будет равна двум бит. Представим эти ключи в виде двух блоков, длиной по 2 бита каждый. Имеем

$$K_1 = 10_2 = 2_{10},\ K_2 = 11_2 = 3_{10},\ S_1(j-1) = 10_2 = 2_{10},\ S_1(j-1) = 10_2 = 2_{10}.$$

В результате этого на первом такте работы генератора на вход будут поступать значения $К_1 = 10_2 = 2_{10}$ и $S_1(j-1) = 10_2 = 2_{10}$. Данные числа подаются на входы первого и второго регистров соответственно, с выходов которых поступят на входы сумматора по модулю q = 11. После выполнения операции сложения с выхода сумматора снимается число

$$a_1 = (К_1 + S_1(j-1)) \bmod q = (2+2) \bmod 11 = 4$$

Одновременно с выполнением операции умножения на входы генератора ПСФ поступают вторые блоки ключей $К_2 = 11_2 = 3_{10}$ и $S_2(j-1) = 10_2 = 2_{10}$, которые записываются в первый и второй регистры соответственно.

Вычисленная сумма подается на вход блока вычисления обратного элемента по модулю q = 11. Данный блок реализует выполнение операции (3.37). В результате имеем

$$a_1^{-1} = \left(\frac{1}{S_1(j-1) + К_1} \right) \bmod q = \left| \frac{1}{4} \right|_{11}^{+} = 3$$

Одновременно с этим в сумматоре по модулю q = 11 определяется сумма вторых блоков, которая равна

$$a_2 = (К_2 + S_2(j-1)) \bmod q = (3+2) \bmod 11 = 5$$

Вычисленное значение обратного элемента первого блока a_1^{-1} поступает на первый вход умножителя по модулю q, на второй вход которого подается единица из третьего регистра Рег 3. В результате получается промежуточный результат

$$w_1 = \prod_{i=1}^{1} \left(\frac{1}{S_i(j-1) + К_i} \right) \bmod q = |3 \cdot 1|_{11}^{+} = 3$$

Полученный промежуточный результат записывается в Рег.3. Одновременно с этим вычисленная сумма a_2 подается на вход блока вычисления обратного элемента по модулю q = 11. Данный блок реализует выполнение операции (3.37). В результате имеем

$$a_2^{-1} = \left(\frac{1}{S_2(j-1) + K_2} \right) \bmod q = \left| \frac{1}{5} \right|_{11}^{+} = 9$$

Вычисленное значение обратного элемента первого блока a_2^{-1} поступает на первый вход Умн. по модулю q, на второй вход которого подается w_1 из третьего регистра Рег 3. В результате получается промежуточный результат

$$w = \prod_{i=1}^{2} \left(\frac{1}{S_i(j-1) + K_i} \right) \bmod q = \left| 3 \cdot 9 \right|_{11}^{+} = 5$$

Вычисленное значение показателя степени подается на блок, реализующий возведение в степень по модулю q согласно (3.36). Тогда

$$S(j) = g^{\left(\prod_{i=1}^{n} (S_i(j-1)+K_i) \right)^{-1}} \bmod q = \left| 2^5 \right|_{11}^{+} = 10$$

Если при вычислении значения сеансового ключа использовалась ПСФ Наора-Рейнголда, то необходимо было выполнить n-1 умножений по модулю q. При использовании модуля q =43 разрядность операндов будет равна шести. Тогда число операций умножения будет равно n=5. Использование разработанной структурной модели генератора позволяет сократить число умножений по модулю до двух. Таким образом, временные затраты на вычисление сеансового ключа были сокращены в 1,21 раза по сравнению с алгоритмом ПСФ Наора-Рейнголда. При этом при увеличении разрядности модуля q эффективность использования разработанного генератора будет возрастать.

3.2 Разработка метода построения системы опознавания космического аппарата, реализованного на основе протокола опознавания нулевым разглашением

Представленный в разделе протокол опознавания, построенный на основе доказательства с нулевым разглашением знаний позволяет определять статус космического аппарата за минимальное время. Для повышения эффективности разработанного протокола опознавания было предложено использовать в его структуре сеансовые ключи S(j), где j – номер сеанса опознавания. При этом использование двух этапов опознавания способствует снижению вероятности ложного срабатывания системы опознавания космического аппарата по сравнению с ранее известными протоколами опознавания без разглашения знаний.

Для повышения эффективности работы системы опознавания космического аппарата был предложен алгоритм проверки повторного использования сеансового ключа в системе опознавания космического аппарата. Использование такого алгоритма позволяет проверяющей стороне определить ситуацию, когда из-за сбоев или отказа генератора сеансовый ключ S(j) используется многократно. При этом данный алгоритм позволяет выявить такую ситуацию без передачи сеансовых ключей на приемную сторону. Очевидно, что отказ от использования такого алгоритма в работе СОКА приводит к увеличению вероятность подбора ответа на вопрос запросчика.

Таким образом, отмеченные выше результаты решения двух первых частных задач исследований должны быть учтены при разработке метода построения системы опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением.

Для обеспечения требуемого уровня сложности определения секретных параметров протокола нарушителем, которая должна быть сравнимой с вычислительной сложности задач распознавания Диффи-Хеллмана, воспользуемся операцией возведения в степень по модулю. При этом в состав секретных параметров кроме $K_{секр}$ и S(j) необходимо ввести T(j), который используется в алгоритме проверки повторного использования сеансового ключа в СОКА.

Значит на начальном этапе разрабатываемого метода построения системы опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением, необходимо также выбрать большое простое число q, которое образует мультипликативную группу. Среди элементов группы надо выбрать элемент g < q, с помощью которого можно получить все элементы мультипликативной группы по модулю q. При этом при вычислении истинного статуса претендента P при выполнении j-го сеанса опознавания необходимо добавить секретный параметр T(j). Тогда истинный статус претендента P может быть задан выражением (2.30)

Очевидно, что выражение (2.30) имеет стойкость сравнимую со стойкостью задачи Диффи-Хеллмана. То есть ее сложность будет соответствовать сложности нахождения дискретного логарифма [15,96,83].

Затем для вычисления зашумленного статуса претендента P необходимо выполнить процедуру зашумления значений секретных параметров $K_{секр}$, S(j) и T(j). Для этого необходимо использовать случайные величины $\Delta K_{секр}(j), \Delta S(j), \Delta T(j)$, которые удовлетворяют условию $\{\Delta K_{секр}(j), \Delta S(j), \Delta T(j)\} \le q-2$. При этом для обеспечения более высокой стойкости к подбору ответа запросчика данные случайные значения должны изменяться при каждом сеансе. Для получения зашумленных секретных параметров можно воспользоваться выражением (2.31).

Для вычисления зашумленного статуса претендента P в разрабатываемом методе построения системы опознавания космического

аппарата, построенного на основе протокола опознавания нулевым разглашением можно воспользоваться выражением (2.32) с учетом нового параметра T(j). При этом истинный статус C(j) и зашумленный статус $C^*(j)$ для выполнения j-го сеанса опознавания должны храниться в памяти претендента P.

Согласно разработанного протокола опознавания без разглашения знаний процедура опознавания должна также содержать два этапа. Для проведения процедуры опознавания претендента P проверяющая сторона V передает запрос, в качестве которого используется случайное число d(j), которое удовлетворяет условию $d(j) < q$.

Второй этап опознавания связан с вычислением претендентом P ответов на поставленный запрос d(j). При этом число ответов должно увеличиться на единицу. Это связано с тем, что в ответ должен зависеть как от запроса d(j), так и от секретных параметров. В разработанном протоколе опознавания в качестве секретных параметров использовались секретный ключ $K_{секр}$ и сеансовый ключ S(j). Поэтому претендент P вычислял два ответа на запрос d(j). Очевидно, что использование в разрабатываемом методе построения системы опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением, алгоритма проверки повторного использования сеансового ключа требует получить ответ, в котором будет использоваться секретный параметр T(j). Таким образом, количество ответов увеличивается до трех. В качестве прототипа можно использовать выражение (2.33). Затем для осуществления проверки претендент P должен передать истинный C(j), зашумленный $C^*(j)$ статусы претендента, а также три ответа на поставленный вопрос d(j).

Как и в разработанном протоколе опознавания без разглашения знаний при проверке правильности полученных ответов проверяющая сторона V использует выражение, в котором должны участвовать истинный C(j), зашумленный $C^*(j)$ образы претендента, три ответа, а также поставленный вопрос d(j). Учитывая выражение (2.33), которое использовалось для

вычисления ответов, необходимо выполнить следующие действия. Во-первых, истинный C(j) образ претендента P возвести в степень d(j) по модулю q. В результате этого получим

$$(C(j))^{d(j)} \bmod q = (g^{K_{секр}} g^{S(j)} g^{T(j)})^{d(j)} \bmod q = g^{d(j)K_{секр}} g^{d(j)S(j)} g^{d(j)T(j)} \bmod q \quad (3.21)$$

Во вторых, необходимо число g возвести в степень по модулю q, где в качестве показателей степени будут использованы ответы на поставленный вопрос. Тогда получаем

$$g^{r_1(j)} \bmod q = g^{K^*_{секр}(j) - d(j)K_{секр}} \bmod q \quad (3.22)$$

$$g^{r_2(j)} \bmod q = g^{S^*(j) - d(j)S(j)} \bmod q \quad (3.23)$$

$$g^{r_3(j)} \bmod q = g^{T^*(j) - d(j)T(j)} \bmod q \quad (3.24)$$

Чтобы в результате при проверке правильности ответов проверяющей стороной был получен зашумленный статус претендента P необходимо перемножить выражения (3.21)-(3.24). Результатом данной операции будет

$$Y(j) = (C(j))^{d(j)} g^{r_1(j)} g^{r_2(j)} g^{r_3(j)} \bmod q = g^{K^*_{секр}} g^{S^*(j)} g^{T^*(j)} \bmod q \quad (3.25)$$

Анализ выражения (3.25) показывает, что если претендент P имеет статус «свой», то полученный результат будет совпадать с зашумленным статусом, т.е. $Y(j) = C^*(j)$. В противном случае, полученный результат Y(j) будет свидетельствовать о том, что претендент P имеет статус «чужой».

На основе проведенных исследований был разработан метод построения системы опознавания космического аппарата, использующий протокол опознавания нулевым разглашением, который представлен в работах [23,79]. Данный метод построения системы опознавания состоит из следующих этапов.

Первый этап. Для работы системы опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением, выбирается большое простое число q. В результате этого вычислительные устройства, входящие в состав СОКА, реализуют арифметические операции по модулю q. При этом каждый ответчик имеет собственный секретный ключ

$K_{секр}$, который размещается в памяти ответчика. Кроме этого в память в вычислительного устройства ответчика вводятся секретные параметры S и T, с помощью которых можно вычислить сеансовые ключи и проверить сроки их применения. При этом число S используется для получения сеансовых ключей S(j), где $S = \{1, 2, ..., q-2\}$. Число T применяется для получения параметра T(j), который используется в алгоритме проверки повторного использования сеансового ключа в системе опознавания космического аппарата для проверки сеансового ключа, где $T = \{1, 2, ..., q-2\}$. Чтобы получить значения сеансовых параметров S(j) и T(j), в разработанном методе предлагается использовать псевдослучайную функцию.

В разработанном методе построения системы опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением, предлагается использовать псевдослучайную функцию вида

$$F((s_1,...,s_n),(g,x_1,...,x_n)) = g^{\left(\frac{1}{\prod_{i=1}^{n}(s_i+x_i)}\right)} \quad (3.26)$$

где $(x_1,...,x_n)$ – входная последовательность генератора ПСФ; $(g,s_1,...,s_n)$ – секретный ключ ПСФ.

Наряду с секретным ключом $K_{секр}$, который размещается на борту космического аппарата, в системе опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением, используется открытый ключ $K_{отк}$. Данный ключ находится в центре поддержки операций. В разработанном методе величина открытого ключа задается выражением

$$K_{отк} = g^{K_{секр}} \bmod q \quad (3.27)$$

С помощью данного открытого ключа при выполнении алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата ЦПО может определить КА, у которого произошел сбой в работе генератора выработки сеансовых ключей S(j).

Второй этап. Перед проведением j-го сеанса опознавания космического аппарата необходимо вычислитель значения сеансового ключа S(j) и параметра T(j). В работах [19,20,30,61] представлены реализации псевдослучайной функции, определяемой выражением (3.26). В этом случае значения секретных параметров будут определяться согласно равенствам

$$S(j) = g^{\left(\prod_{i=1}^{n}(S_i(j-1)+K_i)\right)^{-1}} \bmod q \qquad (3.28)$$

$$T(j) = g^{\left(\prod_{i=1}^{n}(S_i(j-1)+K_i+T_i)\right)^{-1}} \bmod q \qquad (3.29)$$

где K_i – i-ый блок секретного ключа $K_{секр}$ спутника; T_i – i-ый параметра T, используемого для проверки повторного использования сеансового ключа; $S(j-1) = \{S_1(j-1) \| S_2(j-1) \| ... \| S_n(j-1)\}$; $S_i(j-1)$ – i-ый блок j-го сеансового ключа; n – количество блоков в аргументе S(j); m_i – количество разрядов в блоке; $\lceil \log_2 q \rceil = m_i n$.

После получения значений сеансового ключа S(j) и параметра T(j) ответчик с помощью вычислительного устройства производит вычисление истинного статуса космического аппарата согласно

$$C(j) = g^{K_{секр}} g^{S(j)} g^{T(j)} \bmod q \qquad (3.30)$$

Полученное значение истинного статуса заносится в блок памяти, входящей в состав ответчика СОКА. В качестве такой памяти может быть использован регистр.

Третий этап. Для вычисления зашумленного статуса космического аппарата необходимо провести изменение значений секретных параметров спутника $K_{секр}$, S(j) и T(j). Для этого необходимо использовать случайные величины, которые удовлетворяют условию $\{\Delta K_{секр}(j), \Delta S(j), \Delta T(j)\} \le q-2$.

В этом случае процедура зашумления значения секретного ключа определяется выражением

$$K_{секр}(j) = K_{секр} + \Delta K(j) \bmod \varphi(q) \qquad (3.31)$$

где $\varphi(q)$ – функция Эйлера числа q; $\Delta K(j)$ – величина зашумления истинного значения секретного ключа $K_{секр}$ на j-ом сеансе.

Тогда зашумление сеансового ключа S(j) определяется выражением

$$S^*(j) = S(j) + \Delta S(j) \bmod \varphi(q) \qquad (3.32)$$

где $\Delta S(j)$ – величина зашумления истинного значения сеансового ключа S(j) на j-ом сеансе.

Процесс зашумления параметра T(j) проводится согласно выражения

$$T^*(j) = T(j) + \Delta T(j) \bmod q \qquad (3.33)$$

где $\Delta T(j)$ – величина зашумления истинного значения параметра T(j) на j-ом сеансе опознавания.

Вычисленные согласно (3.31)-(3.33) зашумленные секретные параметры используются для определения зашумленного статуса КА

$$C^*(j) = g^{K^*(j)} g^{S^*(j)} g^{T^*(j)} \bmod q \qquad (3.34)$$

Полученное значение зашумленного статуса КА заносится в блок памяти, входящей в состав ответчика СОКА. В качестве такой памяти может быть использован регистр.

В результате выполнения этих этапов ответчик готов к проведению процедуры опознавания.

Рассмотрим сам двухэтапный процесс опознавания статуса космического аппарата.

Первый этап опознавания. Пусть в зоне видимости запросчика, который располагается на необслуживаемом объекте, появился космический аппарат. Запросчик производит генерацию «запросного числа» d(j), которое после пересылается ответчику.

Второй этап опознавания. Ответчик, расположенный на борту космического аппарата, получает запрос d(j), а затем производит вычисление трех ответов. На данном этапе следующие выражения

$$r_1(j) = (K^*_{секр}(j) - d(j) K_{секр}) \bmod \varphi(q) \qquad (3.35)$$

$$r_2(j) = (S^*(j) - d(j)S(j)) \bmod \varphi(q) \quad (3.36)$$

$$r_3(j) = T^*(j) - d(j)T(j) \bmod \varphi(q) \quad (3.37)$$

где $\varphi(q)$ – функция Эйлера числа q.

После получения трех ответов на поставленный вопрос **d**(j) ответчик осуществляет передачу следующих параметров:

- значение истинного статуса C(j) космического аппарата;
- значение зашумленного статуса $C^*(j)$ космического аппарата;
- три вычисленных ответа $r_1(j)$, $r_2(j)$, $r_3(j)$.

Процесс опознавания космического аппарата путем проверки правильности полученных ответов.

Первый этап проверки статуса КА. Запросчик получает от ответчика сигнал, который содержит истинный статус C(j) спутника, зашумленный статус $C^*(j)$ и три вычисленных ответа $r_1(j)$, $r_2(j)$, $r_3(j)$. Затем он производит проверку полученных данных с помощью выражения

$$Y(j) = (C(j))^{d(j)} g^{r_1(j)} g^{r_2(j)} g^{r_3(j)} \bmod q \quad (3.38)$$

Затем запросчик проводит сравнение вычисленного значения Y(j) с зашумленным статусом $C^*(j)$, полученным от ответчика космического аппарата. Если вычисленное значение Y(j) равно величине $C^*(j)$, то есть $Y(j) = C^*(j)$, то запросчик принимает решение, что статус данного космического аппарата «свой». После этого начинается сеанс связи между объектом управления и спутником.

Если полученное при проверке значение Y(j) отличается от величины зашумленного статуса $C^*(j)$, т.е. $Y(j) \neq C^*(j)$, то запросчик принимает решение, что статус данного космического аппарата «чужой» и ему отказывает в сеансе связи с объектом управления.

Рассмотрим пример выполнения разработанного метода построения системы опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением.

Первый этап. Пусть в качестве простого числа выбираем q = 19. Для мультипликативной группы, порожденной q = 19, существует первообразный элемент g = 2. Вычислим элементы данной мультипликативной группы.

$2^0 = 1$	$2^3 = 8$	$2^6 = 7$	$2^{10} = 17$	$2^{13} = 3$	$2^{16} = 5$
$2^1 = 2$	$2^4 = 16$	$2^7 = 14$	$2^{11} = 15$	$2^{14} = 6$	$2^{17} = 10$
$2^2 = 4$	$2^5 = 13$	$2^8 = 9$	$2^{12} = 11$	$2^{15} = 12$	$2^{18} = 1$

Пусть ответчик, который располагается на борту КА, имеет собственный секретный ключ $K_{секр}$ =3, который размещается в памяти ответчика. В память в вычислительного устройства ответчика вводятся секретные параметры S = 6 и T = 17, с помощью которых можно вычислить сеансовые ключи и проверить сроки их применения.

Наряду с секретным ключом $K_{секр}$ в системе опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением, используется открытый ключ $K_{отк}$, который находится в центре поддержки операций. Тогда получаем

$$K_{отк} = g^{K_{сек}} \bmod q = 2^3 \bmod 19 = 8$$

Данный ключ находится в центре поддержки операций

Второй этап. Перед проведением j = 1 сеанса опознавания КА необходимо вычислитель значения первого сеансового ключа S(j=1) и первого параметра T(j=1). Для получения их значений воспользуемся псевдослучайной функцие1. Тогда

$$S(1) = g^{\frac{1}{S(0)+K_{секр}}} \bmod q = 2^{\frac{1}{6+3}} \bmod 11 = 2^{\frac{1}{9}} \bmod 11 = 2^{17} \bmod 11 = 10$$

$$T(1) = g^{\frac{1}{S(0)+K_{секр}+T}} \bmod q = 2^{\frac{1}{6+3+17}} \bmod 11 = 2^{\frac{1}{7}} \bmod 11 = 2^{11} \bmod 11 = 15$$

где S(0) = S = 6.

После получения значений сеансового ключа S(1) и параметра T(1) ответчик с помощью вычислительного устройства производит вычисление истинного статуса космического аппарата согласно (3.48). Тогда

$$C(1) = g^{K_{секр}} g^{S(1)} g^{T(1)} \bmod q = 2^3 \cdot 2^{10} \cdot 2^{15} \bmod 19 = 2^{10} \bmod 19 = 17$$

Полученное значение истинного статуса заносится в блок памяти, входящей в состав ответчика СОКА.

Третий этап. Для вычисления зашумленного статуса космического аппарата проводим зашумление секретных параметров спутника $K_{секр}$, S(1) и T(1). Пусть случайные величины равны $\Delta K_{секр}(1) = 4, \Delta S(1) = 6, \Delta T(1) = 5$.

Тогда согласно (3.31) зашумленное значение секретного ключа равно

$$K_{секр}(1) = (K_{секр} + \Delta K(1)) \bmod \varphi(q) = |3 + 4|_{18}^{+} = 7$$

Зашумление сеансового ключа S(1) проводится согласно (3.32). Тогда

$$S^{*}(1) = (S(1) + \Delta S(1)) \bmod \varphi(q) = |10 + 6|_{18}^{+} = 16$$

Зашумления параметра T(1) проводится согласно (3.33). Тогда имеем

$$T^{*}(1) = (T(1) + \Delta T(1)) \bmod q = |15 + 5|_{18}^{+} = 2$$

Вычисленные зашумленные секретные параметры используются для определения зашумленного статуса КА согласно (3.33). Тогда

$$C^{*}(1) = g^{K^{*}(1)} g^{S^{*}(1)} g^{T^{*}(1)} \bmod q = |2^7 \cdot 2^{16} \cdot 2^2|_{19}^{+} = |2^7|_{19}^{+} = 14$$

Полученное значение зашумленного статуса КА заносится в блок памяти, входящей в состав ответчика СОКА. В результате выполнения этих этапов ответчик готов к проведению процедуры опознавания.

Рассмотрим реализацию двухэтапного процесса опознавания статуса космического аппарата с помощью полученных данных.

Первый этап опознавания. При появлении спутника в зоне видимости запросчика, который располагается на необслуживаемом объекте, последний генерирует «запросное число» d(1) = 4. Данный запрос передается ответчику.

Второй этап опознавания. Ответчик, получив запрос d(j) = 4, производит вычисление первого ответа

$$r_1(1) = (K^{*}_{секр}(1) - d(1)K_{секр}) \bmod \varphi(q) = |7 - 4 \cdot 3|_{18}^{+} = |-5|_{18}^{+} = 13$$

Для вычисления второго ответа используем равенство (3.36). Тогда

$$r_2(1) = (S^*(1) - d(1)S(1)) \bmod \varphi(q) = \left|16 - 4 \cdot 10\right|_{18}^{+} = \left|-6\right|_{18}^{+} = 12$$

Для вычисления третьего ответа используем равенство (3.37). Тогда

$$r_3(1) = T^*(1) - d(1)T(1) \bmod \varphi(q) = \left|2 - 4 \cdot 15\right|_{18}^{+} = \left|-4\right|_{18}^{+} = 14$$

После получения трех ответов на вопрос $d(1) = 4$ответчик осуществляет передачу следующих параметров

$$(C(1) = 17, C^*(1) = 14, r_1(1) = 13, r_2(1) = 12, r_3(1) = 14)$$

Этап проверки статуса КА. Запросчик получает от ответчика сигнал $(C(1) = 17, C^*(1) = 14, r_1(1) = 13, r_2(1) = 12, r_3(1) = 14)$. Для проверки правильности полученных ответов воспользуемся выражением (3.38). Тогда

$$Y(1) = (C(1))^{d(1)} g^{r_1(1)} g^{r_2(1)} g^{r_3(1)} \bmod q = \left|17^4 \cdot 2^{13} \cdot 2^{12} \cdot 2^{14}\right|_{19}^{+} = \left|2^7\right|_{19}^{+} = 14$$

Так как вычисленное значение $Y(1) = C^*(1) = 14$, то запросчик принимает решение, что статус данного космического аппарата «свой».

Для оценки эффективности метода построения СОКА был проведен сравнительный анализ с разработанным ранее протоколом опознавания. При использовании разрядности модуля q равной 25 бит вероятность имитации противником сигнала «Свой» в СОКА в протоколе составит $P_{И} = 7{,}89 \cdot 10^{-31}$, а для разработанного метода $P_{И} = 2{,}35 \cdot 10^{-38}$. Таким образом, применение разработанного метода построения СОКА позволяет снизить вероятность имитации противником сигнала «Свой» в СОКА в $3{,}35 \cdot 10^7$ раз. При этом, при использовании разработанного метода построения системы опознавания космического аппарата, построенного на основе протокола опознавания нулевым разглашением, не требуется знания секретного ключа спутника. На основе разработанного метода будет решена пятая частная задача исследований.

3.3 Разработка структурной схемы системы опознавания

космического аппарата, построенной на основе протокола опознавания нулевым разглашением

Представленные выше результаты решения частных задач исследования стали основной для решения пятой частной задачи, которая посвящена разработке структурной схемы системы опознавания космического аппарата. Таким образом, при разработке данной структурной схемы будут использованы:

– разработанный протокол опознавания, построенный на основе доказательства с нулевым разглашением сведений, обладающий меньшими временными затратами на опознавания спутника [21,79]

– разработанный алгоритм проверки повторного использования сеансового ключа, отличающегося от ранее известных, тем, что позволяет провести такую проверку без его передачи по открытому каналу связи [27,85];

– разработанный метод построения системы опознавания космического аппарата, отличающийся от ранее известных более низкой вероятностью подбора ответа на вопрос запросчика за счет использования разработанного протокола опознавания, с нулевым разглашением сведений [22];

– разработанная структурная модель генератора псевдослучайной функции для выработки сеансового ключа системы опознавания космического аппарата, которая отличается от ПСФ Наорра-Рейнголда меньшими временными затратами на получение S(j) [62,72].

Система опознавания космического аппарата, построенная на основе разработанного метода, использующего протокол опознавания нулевым разглашением приведена в работе [62]. Она состоит из двух частей:

– ответчик СОКА;

– запросчик СОКА.

Рассмотрим более подробно каждую из частей структурной схемы СОКА. Ответчик системы опознавания космического аппарата размещается на борту космического аппарата, входящего в состав группировки низкоорбитальной системы спутниковой связи. Согласно разработанному методу построения СОКА на данную часть системы возлагаются следующие операции.

На первом этапе работы СОКА ответчик производит вычисление сеансовых ключей согласно

$$S(j) = \left| g^{\left(\prod_{i=1}^{n} (S_i\,(j-1)+K_i) \right)^{-1}} \right|_q^+ \qquad (3.39)$$

$$T(j) = \left| g^{\left(\prod_{i=1}^{n} (S_i\,(j-1)+K_i+T_i) \right)^{-1}} \right|_q^+ \qquad (3.40)$$

Таким образом, в состав ответчика должны входить генераторы вычисления сеансового ключа S(j) и параметра T(j), использующие разработанную структурную модель генератора в п.3.2.

На втором этапе разработанного метода построения СОКА ответчик после получения значений сеансового ключа S(j) и параметра T(j) производит вычисление истинного статуса космического аппарата согласно

$$C(j) = \left\| g^{K_{секр}} \right|_q^+ \left| g^{S(j)} \right|_q^+ \left| g^{T(j)} \right|_q^+ \Big|_q^+ \qquad (3.41)$$

Полученное значение истинного статуса заносится в блок памяти, входящей в состав ответчика СОКА. В качестве такой памяти может быть использован регистр.

На третьем этапе ответчик сначала производит зашумление секретных параметров спутника $K_{секр}$, S(j) и T(j). Данные искаженные значения секретных параметров будут использованы вычисления зашумленного статуса космического аппарата. Процедура зашумления определяется выражением

$$\begin{aligned} K_{секр}(j) &= \left|K_{секр} + \Delta K(j)\right|^{+}_{\varphi(q)} \\ S^{*}(j) &= \left|S(j) + \Delta S(j)\right|^{+}_{\varphi(q)} \\ T^{*}(j) &= \left|T(j) + \Delta T(j)\right|^{+}_{\varphi(q)} \end{aligned} \qquad (3.42)$$

где $\varphi(q)$ – функция Эйлера числа q; $\Delta K(j)$, $\Delta S(j)$, $\Delta T(j)$ – случайные значения зашумления на j-ом сеансе; $\{\Delta K_{секр}(j), \Delta S(j), \Delta T(j)\} \le q-2$.

Таким образом, в состав структурной схемы системы опознавания КА должны войти три вычислительных устройства (ВУ), реализующих выражение (3.42). Кроме того, необходимо наличие трех блоков памяти для хранения значений зашумления $\{\Delta K_{секр}, \Delta S, \Delta T\} \le q-2$.

На четвертом этапе работы ответчика происходит определение зашумленного статуса КА согласно

$$C^{*}(j) = \left\| g^{K^{*}(j)} \right|^{+}_{q} \left| g^{S^{*}(j)} \right|^{+}_{q} \left| g^{T^{*}(j)} \right|^{+}_{q} \Big|^{+}_{q} \qquad (3.43)$$

Анализ выражений (3.41) и (3.42) показывает, что для получения значений истинного и зашумленного статусов КА можно использовать одно вычислительное устройство. При этом необходимо в состав СОКА ввести блок коммутации, который позволит подключать регистры, где хранятся истинные значения $K_{секр}$, S(j) и T(j), сначала к вычислительному устройству, реализующего получение истинного статуса КА согласно (3.41), а затем к вычислительным устройствам, реализующим операцию зашумления этих параметров согласно (3.42).

Так как значения истинного и зашумленного статуса космического аппарата вычисляются на разных этапах на одном вычислительном устройстве, то в состав структурной модели необходимо ввести второй коммутатор, который последовательно подключает выход ВУ ко входам регистров для хранения C(j) и $C^{*}(j)$.

Рассмотрим функционирование ответчика при определении статуса космического аппарата. Получив от запросчика запрос d(j), который записывается в третий регистр, ответчик приступает к вычислению ответов

$$r_1(j) = \left| K^*_{\text{секр}}(j) - \left| d(j) K_{\text{секр}} \right|^+_{\varphi(q)} \right|^+_{\varphi(q)}$$

$$r_2(j) = \left| S^*(j) - \left| d(j) S(j) \right|^+_{\varphi(q)} \right|_{\varphi(q)} \qquad (3.44)$$

$$r_2(j) = \left| T^*(j) - \left| d(j) T(j) \right|^+_{\varphi(q)} \right|_{\varphi(q)}$$

Значит, в состав ответчика СОКА необходимо ввести три вычислительных устройства, реализующих (3.44), а также три регистра, предназначенных для хранения ответов $r_1(j)$, $r_2(j)$ и $r_3(j)$.

На рисунке 3.2 представлена структурная схема ответчика системы опознавания космического аппарата. В состав ответчика системы опознавания космического аппарата входят первый блок памяти ($БП_1$), предназначенный для хранения секретных параметров $K_{\text{секр}}$, S и T, блок вычисления сеансового ключа (БВСК), два блока коммутации ($БК_1$, $БК_2$), первое вычислительное устройство ($ВУ_1$), используемое для вычисления истинного и зашумленного статуса КА, три блока памяти ($БП_2$ – $БП_4$), предназначенные для хранения параметров зашумления $\Delta K(j)$, $\Delta S(j)$, $\Delta T(j)$, три сумматора по модулю φ(q), реализующих зашумление секретных параметров согласно (3.42), восемь регистров ($Рег_1$ – $Рег_8$), три вычислительных устройства ($ВУ_2$ – $ВУ_4$), предназначенных для вычисления ответов согласно (3.44).

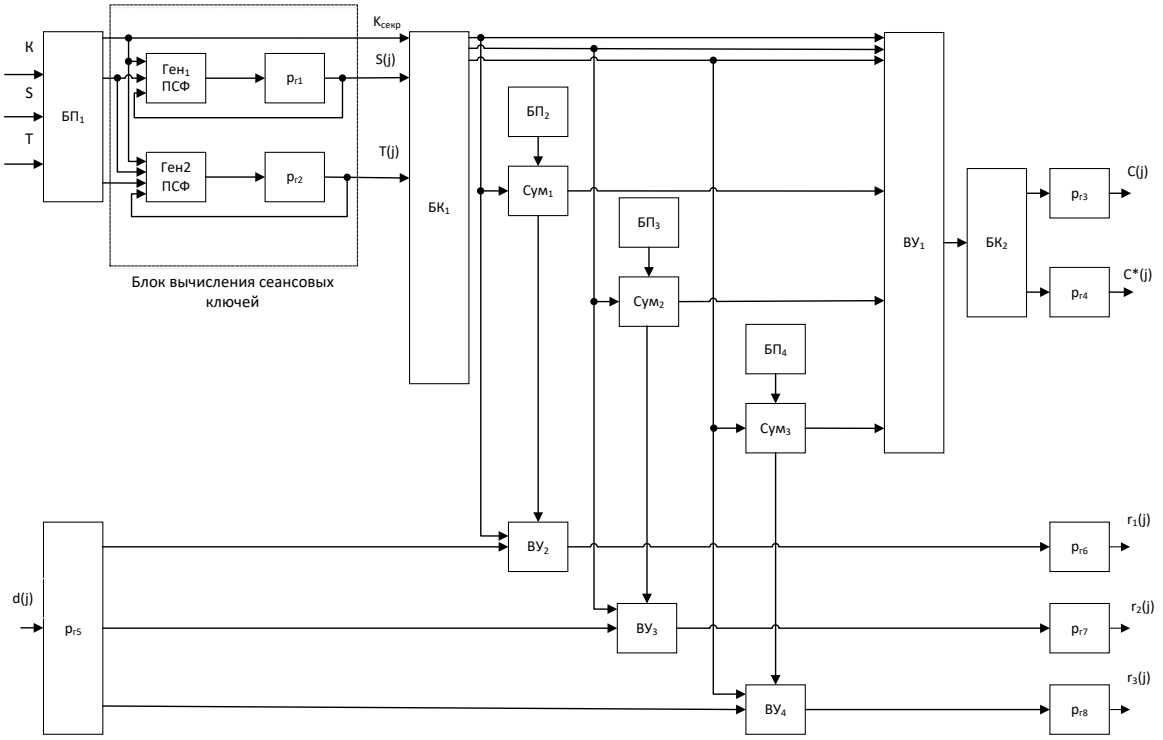

Рисунок 3.2 – Структурная схема ответчика системы опознавания космического аппарата

Запросчик, входящий в состав системы опознавания космического аппарата, размещается на необслуживаемом объекте. Рассмотрим процедуры, которые он выполняет. На первом этапе опознавания, когда в зоне видимости станции спутниковой системы связи появился космический аппарат, запросчик производит генерацию «запросного числа» d(j), которое после пересылается ответчику. Таким образом, в состав запросчика должен входить генератор «запросного числа» d(j)**,** в качестве которого можно использовать представленный в разделе 3.2 генератор ПСФ. Для хранения случайного числа d(j) используется первый регистр.

После вычисления ответов на поставленный вопрос согласно (3.44) ответчик передает запросчику истинный и зашумленный статусы и три ответа. Для их хранения в состав запросчика ввели пять регистров.

На основе полученного ответа запросчик производит проверку правильности ответов на поставленный вопрос

$$Y(j) = \left\| (C(j))^{d(j)} \right|_q^+ \left| g^{r_1(j)} \right|_q^+ \left| g^{r_2(j)} \right|_q^+ \left| g^{r_3(j)} \right|_q^+ \Big|_q^+ \qquad (3.45)$$

Анализ выражения (3.45) показывает, что в состав запросчика необходимо ввести четыре блока, реализующих операцию возведения в степень по модулю. После этого выполняется операция умножения по модулю q. Следовательно, в состав запросчика необходимо ввести умножитель по модулю q.

Затем запросчик проводит сравнение вычисленного значения Y(j) с зашумленным статусом $C^*(j)$, полученным от ответчика космического аппарата. Значит, для выполнения данной операции необходимо использовать вычитатель по модулю q. Если вычисленное значение Y(j) равно величине $C^*(j)$, то есть $C^*(j) - Y(j) \bmod q = 0$, то запросчик принимает решение, что статус данного космического аппарата «свой». После этого начинается сеанс связи между объектом управления и спутником.

На рисунке 3.3 представлена структурная схема запросчика системы опознавания космического аппарата. В состав запросчика входят генератор ПСФ, предназначенный для генерации числа d(j), который может быть реализован на основе разработанного генератора ПСФ в разделе 3.2, первый регистр ($Рг_1$) для хранения числа d(j), блок коммутации ($БКЗ_1$), пять регистров, предназначенных для хранения значений, поступивших от ответчика СОКА ($Рег_2$ – $Рег_6$), четыре блока возведения в степень по модулю q ($БВС_1$ – $БВС_4$), умножитель по модулю q (Умн), сумматор по модулю q (Сум.), блок принятия решения (БПР).

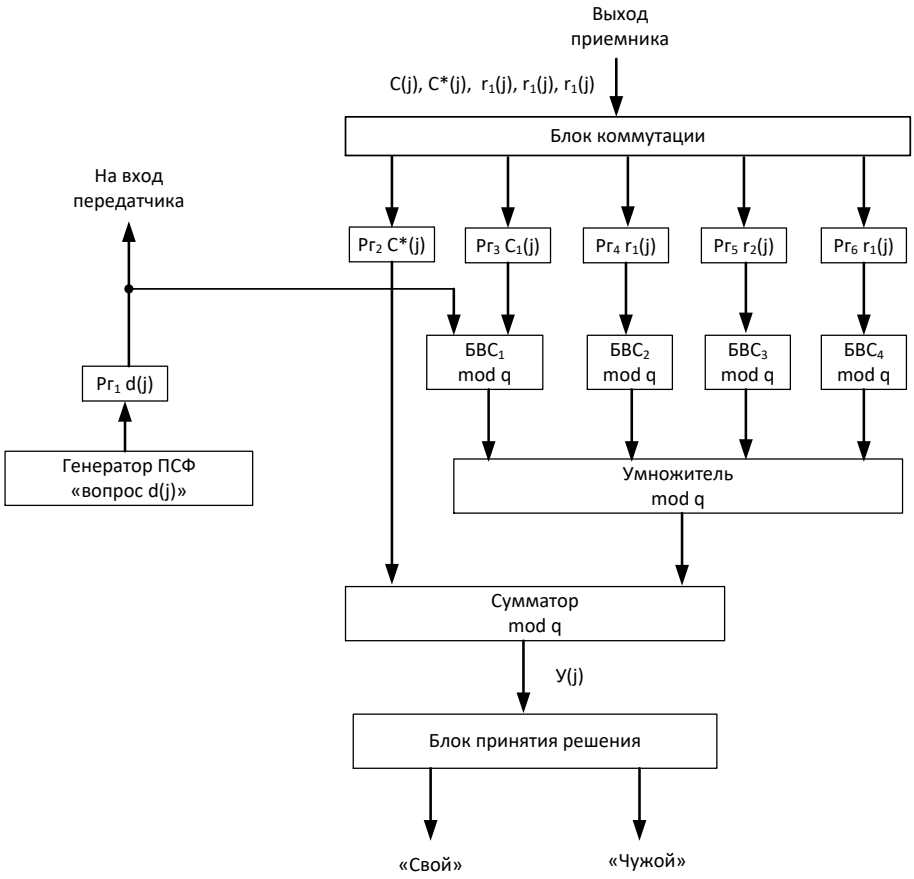

Рисунок 3.3 – Структурная схема запросчика системы опознавания космического аппарата

Для оценки эффективности разработанного метода проведем сравнительный анализ с методами построения СОКА, которые используют другие протоколы опознавания, построенные на основе нулевого доказательства. Для этого воспользуемся целевой функцией, определяемой выражением (1.30).В качестве альтернативных решений предлагается использовать протокол Фиат-Шамира, протокол Шнорра, а также разработанный протокол, представленный в диссертации. Для оценки имитостойкости НССС воспользуемся выражением (1.26). В этом случае имитостойкость низкоорбитальной системы спутниковой связи будет зависеть как от вероятности навязывания передаваемого сигнала, так и от вероятности имитации ответа для системы «свой-чужой». Тогда при длине команды управления 20 бит вероятность подбора команды составит $P_{ПК} = 2^{-20} = 9{,}54 \cdot 10^{-7}$. Для определения имитостойкости НССС согласно (1.26)

необходимо вычислить вероятность пропуска космического аппарата СОКА. Для этого воспользуемся выражениями (1.28) и (1.29). Согласно (1.29) вероятность имитации противником сигнала «Свой» в СОКА $P_И$ определяется длиной ответного сигнала. В работах [69,97] представлены сервисы, позволяющие определить временные затраты на реализацию взлома пароля, путем прямого перебора. Так, используя процессор Core i5-6600K, при длине пароля равной 56 бит потребуется два дня, при длине 64 бит - 12 дней, а при длине 96 бит будет затрачено 33 года. Выберем разрядность ответного сигнала равную 100 бит. Тогда вероятность имитации противником сигнала «Свой» в СОКА будет равна $P_И = 2^{-100} = 7{,}89 \cdot 10^{-31}$.

В разработанном протоколе опознавания космического аппарата ответ на поставленный вопрос состоял из истинного статуса C(j), зашумленного статуса $C^*(j)$ и двух ответов на вопрос $r_1(j), r_2(j)$, которые передаются запросчику с борта спутника. Так как данные значения вычисляются по модулю q. Следовательно, для получения данной разрядности ответа достаточно использовать 25-разрядный модуль.

В разработанном методе построения СОКА ответный сигнал состоит из истинного статуса $C(j)$, зашумленного статуса $C^*(j)$ и трех ответов на вопрос $r_1(j), r_2(j), r_3(j)$. В этом случае разрядность ответного сигнала увеличивается до 125 бит. Тогда вероятность имитации противником сигнала «Свой» в СОКА будет равна $P_И = 2^{-125} = 2{,}35 \cdot 10^{-38}$.

Если положить условие, что временные затраты на реализацию этапов опознавания на основе разработанного протокола и альтернативных протоколов совпадают, то для вычисления вероятность пропуска спутника-нарушителя воспользуемся выражением (1.28). Проведенные исследования показали, что максимальное количество этапов опознавания используется в протоколе Фиат-Шамира. Пусть N(max) = N(1) = 20. Тогда протокол Шнорра для опознавания КА потребует N(2) = 3 этапа, а разработанный протокол опознавания – N(3) = 2 этапа. В разработанном методе построения СОКА

также используется N(4) = 2 этапа. В таблице 3.1 представлены результаты сравнительного анализа альтернативных решений построения СОКА на основе протоколов опознавания с нулевым разглашением.

Таблица 3.1 – Сравнительный анализ альтернативных СОКА

Протоколы	Фиат-Шамира	Шнорра	Разработанный протокол опознавания	Разработанный метод построения СОКА
Разрядность команды, бит	20	20	20	20
Вероятность $P_{ПК}$	$9{,}54 \cdot 10^{-7}$	$9{,}54 \cdot 10^{-7}$	$9{,}54 \cdot 10^{-7}$	$9{,}54 \cdot 10^{-7}$
Разрядность модуля, бит	$\log_2 q=100$	$\log_2 q=100$	$\log_2 q = 25$	$\log_2 q = 25$
Вероятность $P_{И}$	$7{,}89 \cdot 10^{-31}$	$7{,}89 \cdot 10^{-31}$	$7{,}89 \cdot 10^{-31}$	$2{,}35 \cdot 10^{-38}$
Максимальное число этапов	$N_{max} = 20$	$N_{max} = 20$	$N_{max} = 20$	$N_{max} = 20$
Число этапов	N(1) = 20	N(2) = 3	N(3) = 2	N(4) = 2
Вероятность пропуска КА	$7{,}89 \cdot 10^{-31}$	$1{,}18 \cdot 10^{-31}$	$7{,}89 \cdot 10^{-32}$	$2{,}35 \cdot 10^{-39}$
Вероятность навязывания ИП	$7{,}53 \cdot 10^{-37}$	$1{,}12 \cdot 10^{-37}$	$7{,}53 \cdot 10^{-38}$	$2{,}24 \cdot 10^{-45}$

Анализ таблицы 3.1. показывает, что разработанный метод построения системы опознавания космического аппарата позволяет уменьшить вероятность навязывания имитационной помехи в $3{,}36 \cdot 10^{8}$ раз по сравнению с протоколом Фиат-Шамира, в $5{,}01 \cdot 10^{7}$ раз по сравнению с протоколом Шнорра, и в $3{,}36 \cdot 10^{7}$ раз по сравнению с разработанным протоколом опознавания, который не использует алгоритм проварки двойного использования сеансового ключа. Таким образом, разработанный метод

построения системы опознавания космического аппарата позволил повысить имитостойкость НССС по сравнению с альтернативными методами построения СОКА.

Выводы

1. Чтобы снизить вероятность подбора ответа на вопрос запросчика и повысить имитостойкость системы опознавания статуса космического аппарата, применяемой в ССС комплекса удаленного мониторинга, контроля и управления удаленным объектом было предложено использовать псевдослучайную функцию для формирования сеансового ключа S(j). На основе проведенных исследований была выбрана ПСФ, которая характеризуется меньшим числом операций умножения по сравнению с псевдослучайной функцией Наора-Рейнголда. На основе алгоритма вычисления ПСФ была разработана структурная модель генератора для выработки сеансового ключа системы опознавания космического аппарата. Проведенный сравнительный анализ показал, что уже при использовании шестиразрядного модуля q разработанная структурная модель позволяет сократить временные затраты на вычисление сеансового ключа в 1,21 раза по сравнению с алгоритмом ПСФ Наора-Рейнголда. При этом при увеличении разрядности модуля q эффективность использования разработанного генератора будет возрастать.

2. Четвертая частная задача исследований связана с разработкой метода построения системы опознавания космического аппарата, реализованного на основе протокола опознавания нулевым разглашением. Были обоснованы основные этапы функционирования СОКА, использующей предложенный метод. Для оценки эффективности метода построения СОКА был проведен сравнительный анализ с разработанным ранее протоколом опознавания. При

использовании разрядности модуля q равной 25 бит вероятность имитации противником сигнала «Свой» в СОКА в протоколе составит $P_{и} = 7{,}89 \cdot 10^{-31}$, а для разработанного метода $P_{и} = 2{,}35 \cdot 10^{-38}$. Таким образом, применение разработанного метода построения СОКА позволяет снизить вероятность имитации противником сигнала «Свой» в СОКА в $3{,}35 \cdot 10^{7}$ раз

3. Пятая частная задача диссертационных исследований связана с разработкой структурной схемы системы опознавания космического аппарата, использующей разработанный метод построения СОКА, реализованного на основе протокола опознавания нулевым разглашением. Известно, что система опознавания космического аппарата состоит из двух частей – ответчика, который находится на борту спутника, и запросчика, который размещается на необслуживаемом объекте управления. В диссертации были представлены структурные модели ответчика и запросчика, реализующие разработанный алгоритм опознавания.

4. Для оценки эффективности разработанного метода был проведен сравнительный анализ с методами построения СОКА, которые используют другие протоколы опознавания, построенные на основе нулевого доказательства. В качестве альтернативных решений предлагается использовать протокол Фиат-Шамира, протокол Шнорра, а также разработанный протокол, представленный в диссертации. В качестве исходных данных было выбрана разрядность ответного сигнала равная 100 бит, при длине команды управления – 20 бит. Полученные результаты показали, что разработанный метод построения системы опознавания космического аппарата позволяет уменьшить вероятность навязывания имитационной помехи в $3{,}36 \cdot 10^{8}$ раз по сравнению с протоколом Фиат-Шамира, в $5{,}01 \cdot 10^{7}$ раз по сравнению с протоколом Шнорра, и в $3{,}36 \cdot 10^{7}$ раз по сравнению с разработанным протоколом опознавания, который не использует алгоритм проварки двойного использования сеансового ключа. Таким образом, разработанный метод построения системы опознавания

космического аппарата позволил повысить имитостойкость НССС по сравнению с альтернативными методами построения СОКА.

ЗАКЛЮЧЕНИЕ

В современных АСДМКУ, предназначенных для контроля и управления необслуживаемыми объектами добычи и транспортировки углеводородов, расположенных за Полярным кругом, широко используют низкоорбитальные системы спутниковой связи. Так расстояния между объектом управления и центром поддержки операций АСДМКУ составляют сотни километров, то НССС обладают наибольшим числом уязвимостей, используя которые нарушитель может нарушить работу системы спутниковой связи. Поэтому повышение имитостойкости низкоорбитальной системы спутниковой связи является актуальной задачей. На основе проведенного системного анализа были выявлены основные деструктивные воздействия на НССС, среди которых особое место занимают методы, которые построены на принципах перехвата и навязывания перехваченных сигналов. Повысить имитостойкость низкоорбитальной системы спутниковой связи, то есть предотвратить навязывание перехваченного и задержанного сигнала, можно за счет применения системы опознавания космического аппарата СОКА, которая перед началом сеанса связи будет проводить опознавание спутника. Если спутник имеет статус «свой», то система опознавания космического аппарата разрешает ему осуществлять обмен данными с абонентским терминалом. В противном случае – космическому аппарату в сеансе будет отказано.

Для решения поставленной задачи проведен анализ основных методов построения систем опознавания «свой-чужой». Полученные результаты свидетельствуют о том, что существующие системы опознавания «свой-чужой» не позволяют определить статус КА и не могут быть использованы в НССС. Показана актуальность разработки новых принципов построения системы распознавания спутника для низкоорбитальной группировки ССС.

Проведен системный анализ альтернативных методов опознавания для системы опознавания космического аппарата. В результате был определено противоречие в теории, которое состоит в том, что известные протоколы опознавания, построенные на основе методов опознавания типа «запрос-ответ», а также с помощью многоразовых и одноразовых паролей, не позволяют в полной мере предотвратить навязывание имитирующих помех и задержанных команд управления спутником-нарушителем, а методы опознавания, базирующиеся на доказательстве с нулевым разглашением, и обладающие высокой вычислительной сложностью при минимальном числе этапов опознавания космического аппарата, не нашли применения.

Проведена постановка научной задачи исследования. на основе проведенного анализа был выбран показателя качества, позволяющего оценить эффективность разработанных решений, позволяющих повысить имитостойкость низкоорбитальной системы связи в условиях воздействия имитирующих помех. Произведена математическая постановка задачи исследования. Используя метод научно-методического аппарата СА, была проведена декомпозиция главной научной задачи на ряд частных научных задач.

Первая частная задача диссертационных исследований связана с разработкой протокола опознавания КА, построенного на основе доказательства с нулевым разглашением сведений, обладающего меньшими временными затратами на опознавания спутника. Для решения данной частной задачи был проведем анализ основных принципов реализации протоколов опознавания Фиата-Шамира, Фейге-Фиат-Шамира, базирующихся на доказательстве с нулевым разглашением сведений. Проведенные исследования показали, что для обеспечения требуемого уровня вероятности подбора ответа данные протоколы выполняются многократно. Так для протокола Фиата-Шамира требуется выполнить от 20 до 40 раундов опознавания.

Для сокращения числа этапов, выполняемых в протоколе для опознавания претендента P, был проведен анализ алгоритмов закрытия данных с открытым ключом. Проведенные исследования показали, что эти методы построения протоколов опознавания с нулевым разглашением знаний не могут быть использован в системе опознавания КА. Это связано с тем, что для реализации таких протоколов необходимо, чтобы на борту спутника находился свой секретный ключ, с помощью которого он сможет доказать свой статус проверяющей стороне V. Значит, у каждого запросчика, которые находятся на необслуживаемых объектах управления, должна быть база открытых ключей космических аппаратов. При этом для обеспечения требуемого уровня вероятности пропуска нарушителя необходимо их периодически заменять, что будет достаточно сложно выполнить.

На основе проведенных исследований были определены основные принципы построения протокола опознавания КА. Используя данные принципы, был разработан протокол опознавания, построенный на основе доказательства с нулевым разглашением знания, который обладает меньшим количеством этапов опознавания. должен быть использованы другие принципы построения. Проведенный сравнительный анализ показал, разработанный протокол позволяет выполнить процедуру опознавания за два этапа, что в 1,5 раза быстрее рассмотренного ранее протокола опознавания Шнорра. На этом решение первой частной задачи исследования закончено.

Вторая частная задача диссертационных исследований связана с разработкой алгоритмом проверки повторного использования сеансового ключа в СОКА. Очевидно, что ситуация, когда сеансовый ключ S(j) не изменяет свое значение при изменении номера сеанса с j-го на (j+1)-й, может привести к повышению вероятности подбора ответа $P_{по}$. Чтобы устранить такую ситуацию был разработан алгоритм, позволяющий провести проверку повторного использования сеансового ключа S(j). В ходе диссертационных исследований был разработан такой алгоритм, отличающийся от ранее

известных, тем, что позволяет провести проверку без передачи по открытому каналу связи сеансовых ключей. Если в процессе работы СОКА ответчик повторно использует сеансовый ключ, то реализуя разработанный алгоритм проверяющая сторона получит открытый ключ КА.

В диссертации проведен сравнительный анализ эффективности работы системы опознавания космического аппарата, использующей разработанный алгоритма проверки повторного использования сеансового ключа и без применения данного алгоритма. Полученные результаты свидетельствуют о том, что не использование разработанного алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата приводит к увеличению вероятность подбора ответа на вопрос запросчика в $1{,}52 \cdot 10^5$ раз уже при разрядности ответа претендента равного 64 бит. На этом решение второй частной задачи исследования закончено.

Чтобы снизить вероятность подбора ответа на вопрос запросчика и повысить имитостойкость системы опознавания статуса космического аппарата, применяемой в ССС комплекса удаленного мониторинга, контроля и управления удаленным объектом было предложено использовать псевдослучайную функцию для формирования сеансового ключа S(j). На основе проведенных исследований была выбрана ПСФ, которая характеризуется меньшим числом операций умножения по сравнению с псевдослучайной функцией Наора-Рейнголда. На основе алгоритма вычисления ПСФ была разработана структурная модель генератора для выработки сеансового ключа системы опознавания космического аппарата. Проведенный сравнительный анализ показал, что уже при использовании шестиразрядного модуля q разработанная структурная модель позволяет сократить временные затраты на вычисление сеансового ключа в 1,21 раза по сравнению с алгоритмом ПСФ Наора-Рейнголда. При этом при увеличении разрядности модуля q эффективность использования разработанного генератора будет возрастать. Таким образом, третья частная задача диссертационных исследований успешно решена.

Четвертая частная задача, связана с разработкой метода построения системы опознавания космического аппарата, реализованного на основе протокола опознавания нулевым разглашением. Были обоснованы основные этапы функционирования СОКА, использующей предложенный метод. Для оценки эффективности метода построения СОКА был проведен сравнительный анализ с разработанным ранее протоколом опознавания. При использовании разрядности модуля q равной 25 бит вероятность имитации противником сигнала «Свой» в СОКА в протоколе составит $P_{и} = 7{,}89 \cdot 10^{-31}$, а для разработанного метода $P_{и} = 2{,}35 \cdot 10^{-38}$. Таким образом, применение разработанного метода построения СОКА позволяет снизить вероятность имитации противником сигнала «Свой» в СОКА в $3{,}35 \cdot 10^{7}$ раз.

Пятая частная задача диссертационных исследований связана с разработкой структурной схемы системы опознавания космического аппарата, использующей разработанный метод построения СОКА, реализованного на основе протокола опознавания нулевым разглашением. Известно, что система опознавания космического аппарата состоит из двух частей – ответчика, который находится на борту спутника, и запросчика, который размещается на необслуживаемом объекте управления. В диссертации были представлены структурные модели ответчика и запросчика, реализующие разработанный алгоритм опознавания.

Для оценки эффективности разработанного метода был проведен сравнительный анализ с методами построения СОКА, которые используют другие протоколы опознавания, построенные на основе нулевого доказательства. В качестве альтернативных решений предлагается использовать протокол Фиат-Шамира, протокол Шнорра, а также разработанный протокол, представленный в диссертации. В качестве исходных данных было выбрана разрядность ответного сигнала равная 100 бит, при длине команды управления – 20 бит. Полученные результаты показали, что разработанный метод построения системы опознавания

космического аппарата позволяет уменьшить вероятность навязывания имитационной помехи в $3{,}36 \cdot 10^{8}$ раз по сравнению с протоколом Фиат-Шамира, в $5{,}01 \cdot 10^{7}$ раз по сравнению с протоколом Шнорра, и в $3{,}36 \cdot 10^{7}$ раз по сравнению с разработанным протоколом опознавания, который не использует алгоритм проверки двойного использования сеансового ключа. Таким образом, разработанный метод построения системы опознавания космического аппарата позволил повысить имитостойкость НССС по сравнению с альтернативными методами построения СОКА.

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

АЗДОК – алгоритм закрытия данных с открытым ключом;

АИП –активные имитирующие помехи;

АМП – активные маскирующие помехи;

АП - активные помехи;

АМШП – амплитудно-модулированные шумовые помехи;

АСДМКУ – автоматизированная система дистанционного мониторинга, контроля и управления

ГНП – гармоническая непрерывные помехи;

ЗИП – заградительная имитирующая помеха;

ЗНШП – заградительные непрерывные шумовые помехи;

ЗС – запросный сигнал;

КА – космический аппарат;

НМА - научно-методологический аппарат;

НСД – несанкционированный доступ;

НССС – низкоорбитальная система спутниковой связи;

ПБЛ – подавление боковых лепестков;

ПИП – прицельная имитирующая помеха;

ПК – показателя качества;

ПНШП – прицельные непрерывные шумовые помехи;

ПП – применяются пассивные помехи;

ПСП – псевдослучайные последовательности;

ПСФ – псевдослучайная функция

РЭБ – радиоэлектронная борьба;

СА – системный анализ;

СИП – следящая имитирующая помеха;

СОКА – система опознавания космического аппарата;

ССС – система спутниковой связи;

ЦПО – центр поддержки операций;

ШП – шумоподобная помеха.

СПИСОК ЛИТЕРАТУРЫ

1. Автоматизированная система дистанционного контроля и управления. Техническое описание [Электронный ресурс]. – Режим доступа: https://ntca2i.ru/info/articles/ob-avtomatizirovannoy-sisteme-kontrolya-i-upravleniya-asdku/.

2. Автоматизированная система дистанционного управления нефтяными месторождениями [Электронный ресурс]. – Режим доступа: http://aistsoft.ru/passport/gorno-hahtnoe_i_dobyvayushchee_oborudovanie/sistema_ avtomatizirovannaya_dispetcherskogo_upravl.htm

3. Антонов, А.В. Системный анализ [Текст] / А.В. Антонов. – М. : Высшая школа, 2004. – 454 с.

4. Анфилатов, В.С. Системный анализ в управлении / В.С. Анфилатов. – М. : Горячая линия–Телеком, 2007. – 421 с.

5. Асланов, М.А. Системный анализ и принятие решений в деятельности учреждений реального сектора экономики, связи и транспорта / М.А. Асланов и др. – М. : Экономика, 2010. – 406 с.

6. Бережной, В.А. Государственное опознавание: настоящее и будущее [Электронный ресурс] / В.А. Бережной, В.А. Иванцов, Е.А. Соломенин. – Режим доступа: http://old.nationaldefense.ru/110/754/index.shtml? id=4877

7. Буренок, В.М. Направления развития системы опознавания / В.М. Буренок, В.И. Москаленко, Е.А. Соломенин // Вооружение и экономика. – 2012. – № 1 (17). – С. 3-7.

8. Волкова, В.Н. Теория систем и системный анализ [Текст] / В.Н. Волкова, А.А. Денисов. – М. : Юрайт, 2015. – 616 с.

9. Воронов, Д.В. Критерии оценки имитостойкости командно-телеметрических радиолиний / Д.В. Воронов // Системы обработки информации. – 2007. – № 4 (62). – С. 14-16.

10. Дворников, С.В. Оценка имитостойкости каналов управления с частотной модуляцией / С.В. Дворников // Информация и космос. – 2016. – №1. – С. 32-35.

11. Демьянчук, А.А. Алгоритмы открытого шифрования в протоколах с нулевым разглашением секрета / А.А. Демьянчук, Д.Н. Молдовян, А.А. Молдовян // Вопросы защиты информации. – 2013. – № 2. – С. 22-27.

12. Дятлов, А.П. Радиоэлектронная борьба со спутниковыми радионавигационными системами / А.П. Дятлов, П.А Дятлов, Б.Х. Кулибякин. – М. : Радио и связь, 2004. – 412 с.

13. Ермаков, С.Н. Устройство и эксплуатация наземных средств системы государственного опознавания / С.Н. Ермак, С.Н. Касанин, О.А. Хожевец. – Минск : БГУИР, 2017. – 230 с.

14. Жук, А.П. Разработка методики повышения структурной скрытности сигналов спутниковых радионавигационных систем / А.П. Жук, Д.В. Орёл // Вестник Ставропольского государственного университета. – 2010. – №70(5). – С. 44–52.

15. Запечников, С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности / С. В. Запечников. – М. : Горячая линия-Телеком, 2011. – 256 с.

16. Иванов, М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с.

17. Иванов, Р.В. Оценка имитостойкости каналов управления беспилотными летательными аппаратами / Р.В. Иванов // Фундаментальные науки. Информационные технологии. – 2016. – № 4. – С. 37 – 42.

18. Калмыков, И.А. Системный подход к применению псевдослучайных функций в системах защиты информации / И.А. Калмыков, О.И. Дагаева, Д.О. Науменко, О.В. Вельц // Вестник Северо-Кавказского федерального университета. – 2012. – № 3 (32). – С. 26-34.

19. Калмыков, М.И Разработка алгоритма, использующего псевдослучайную функцию для протоколов доказательства с нулевым разглашением / М.И. Калмыков, О.И. Дагаева // Актуальные проблемы современной науки: материалы II международной научно-практической конференции. – Ставрополь, 2013. – С. 162-165.

20. Калмыков, М.И. Протокол опознавания покупателя на основе доказательства с нулевым разглашением для систем электронных платежей / Д.В. Гостев, М.И. Калмыков, Е.П. Степанова, Е.В. Топоркова // Свидетельство о государственной регистрации программ для ЭВМ № 2015612379 от 24.12.2014 регистрация 18.02.2015.

21. Калмыков, М.И. Алгоритм имитозащиты для систем удаленного мониторинга и управления критическими технологиями / М.И. Калмыков, Д.О. Науменко, И.А. Калмыков, О.В. Вельц // Известия ЮФУ. Технические науки. – 2014. – №2. – С. 181-187.

22. Калмыков, М.И. Методы защиты передаваемой информации для системы удаленного контроля и управления высокотехнологическими объектами / В.П. Пашинцев, И.А. Калмыков, О.В. Вельц, М.И. Калмыков // Вестник Северо-Кавказского федерального университета. – 2014. – № 2. – С. 30-35.

23. Калмыков, М.И. Применение помехоустойчивого протокола аутентификации космического аппарата для низкоорбитальной системы спутниковой связи / В.П. Пашинцев, А.В. Ляхов, М.И. Калмыков // Инфокоммуникационные технологии. – 2015. − № 2. − С. 183-190.

24. Калмыков, М.И. Применение псевдослучайной функции в электронных коммерческих системах / М.И. Калмыков, О.И. Дагаева, И.А. Калмыков // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы III Всероссийской научно-практической конференции. – Волгоград, 2014. – С. 57-61.

25. Калмыков, М.И. Протокол обмена данных с использованием алгоритма слепой подписи для инфокоммуникационных систем // М.И. Калмыков, О.В. Вельц, И.А. Калмыков, А.Г. Вельц // Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-6): сборник научных трудов шестой международной научно-технической конференции. – Ставрополь, 2014. – С. 235-240.

26. Калмыков, М.И. Протокол снятия со счета электронных денег/ М.И. Калмыков, Е.С. Голубь, И.А. Калмыков // Свидетельство о государственной регистрации программ для ЭВМ № 2013618054, от 29.08.2013.

27. Калмыков, М.И. Разработка алгоритма проверки повторного использования сеансового ключа в системе опознавания космического аппарата / М.И. Калмыков // Фундаментальные основы науки: сборник научных трудов по материалам II Международной научно-практической конференции. – Таганрог, 2018. – С. 9-15.

28. Калмыков, М.И. Разработка протокола аутентификации спутника для системы опознавания космического аппарата / М.И. Калмыков // Актуальные проблемы современной когнитивной науки: сборник статей Международной научно-практической конференции. – Таганрог, 2019. – С. 48-51.

29. Калмыков, М.И. Разработка протокола выплаты электронной наличности с использованием модулярной арифметики / М.И. Калмыков, Е.В. Топоркова, Н.П. Борода, С.А. Сирота // Международный журнал экспериментального образования. – 2015. – № 4-2. – С. 341-343.

30. Калмыков, М.И. Расширение методов защиты систем электронной коммерции на основе модулярных алгебраических схем / М.И. Калмыков, А.Б. Саркисов, И.А. Калмыков, А.В. Макарова // Известия ЮФУ. Технические науки. – Таганрог, 2014. – №2. – С. 218-225.

31. Калмыков, М.И. Реализация протоколов защиты данных в системах электронных денег на основе применения псевдослучайной функции / М.И. Калмыков, О.И. Дагаева // Актуальные проблемы современной науки:

материалы II международной научно-практической конференции. – Ставрополь, 2013. – С. 152-155.

32. Калмыков, М.И. Схемная реализация генератора псевдослучайной функции повышенной эффективности / М.И. Калмыков, Е.В. Петрова, И.А. Калмыков, Е.П. Степанова // Инфокоммуникационные технологии в науке, производстве и образовании (Инфоком-6): сборник научных трудов шестой международной научно-технической конференции. – Ставрополь, 2014. – С. 240-243.

33. Камнев, В.Е. Спутниковые сети связи [Текст] / В.Е. Камнев, В.В. Черкасов, Г.В. Чечин. – М.: «Альпина Паблишер», 2004. – 536 с.

34. Карпеев, Д.О. Риски систем: оценка и управление [Текст] / Под ред. Ю.Н. Лаврухина, Д.О Карпеев, В.Н. Асеев О.А. Остапенко. – М. : Горячая линия – Телеком, 2007. – 247 с.

35. Качала, В.В. Общая теория систем и системный анализ [Текст] / В.В. Качала – М. : Горячая линия – Телеком, 2017. – 432 с.

36. Качала, В.В. Основы теории систем и системного анализа [Текст] / В.В. Качала. – М. : Горячая линия – Телеком, 2008. – 189 с.

37. Качественные показатели, их достижение и анализ [Электронный ресурс]. – Режим доступа: http://fb.ru/article/205003/kachestvennyie-pokazateli-ih-dostijenie-i-analiz.

38. Квантор, Л.Я. Расцвет и кризис спутниковой связи / Л.Я. Квантор // Электросвязь. – Москва, 2007. – № 7. – С. 45-51.

39. Классификация показателей качества [Электронный ресурс]. – Режим доступа: http://lyubimyj.ru/biznes-i-finansy/klassifikaciya-pokazatelej-kachestva.

40. Корякин, О.А. Как создавалась секретная советская система опознавания «свой-чужой» [Электронный ресурс] / О.А. Корякин. – Режим доступа: https://topwar.ru/72473-kak-sozdavalas-sekretnaya-sovetskaya-sistema-opoznavaniya-svoy-chuzhoy.html.

41. Кремний-2. Станции СРО-2 и СПЗО-2. Техническое описание [Электронный ресурс]. – Режим доступа: https://armyman.info/books/id-861.html.

42. Крылов, А.А. Анализ создания и развития низкоорбитальных систем спутниковой связи [Электронный ресурс] / А.А. Крылов. – Режим доступа: http://www.tssonline.ru/articles2/Oborandteh/analiz-sozdania-i-razvitiya - nizkoorbitalnih-sistem-spytnikovoi-svyazi.

43. Кукк, К.И. Спутниковая связь: прошлое, настоящее, будущее [Текст] / К.И. Кукк. – М. : Горячая линия – Телеком, 2017. – 256 с.

44. Куликов, А.В. «Свой-чужой» за рубежом. Состояние, перспективы развития и применение системы опознавания в иностранных государствах [Электронный ресурс] / А.В. Куликов. – Режим доступа: http://www.vko.ru/koncepcii/svoy-chuzhoy-za-rubezhom.

45. Куприянов, А.И. Радиоэлектронная борьба. Основы теории [Текст] / А.И. Куприянов, Л.Н. Шустов. – М. : Вузовская книга, 2011. – 800 с.

46. Куприянов, А.И. Радиоэлектронные системы в информационном конфликте [Текст] / А.И. Куприянов, А.В. Сахаров. – М.: Вузовская книга, 2003. – 643 с.

47. Лаборатория системного анализа [Электронный ресурс]. – Режим доступа: http://systems-analysis.ru.

48. Локшин, В.А. Спутниковое непосредственное вещание: новые горизонты / В.А. Локшин // Технологии и средства связи. – 2015. – № 2. – С. 60-65.

49. Макаренко, С.И. Краткий справочник научных терминов и обозначений / С.И. Макаренко. – СПб. : Наукоемкие технологии, 2019. – 241 с.

50. Максимов, М.В. Защита от радиопомех [Текст] // М. В. Максимов. – М. : «Сов. радио», 1976, – 496 с.

51. Меркулов, В.И. Защита радиолокационных систем от помех [Текст] / под ред. А.И. Канащенкова и.В.И. Меркулова. – М.:Радиотехника, 2003 – 472 с.

52. Молдовян, А.А. Протоколы аутентификации с нулевым разглашением секрета [Текст] / А.А. Молдовян, Д.Н. Молдовян, А.Б. Левина. – СПб. : Университет ИТМО, 2016. – 55 с.

53. Немировский, М.С Основы построения систем спутниковой связи [Текст] / М.С. Немировский, Б.А. Локшин, Д.А. Аронов. – М. : Горячая линия – Телеком, 2017. – 432 с.

54. Организация мониторинга систем безопасности территориально рассредоточенных объектов связи на базе оборудования ИСО «ОРИОН» [Электронный ресурс]. – Режим доступа: http://bolid.ru/support/articles.

55. Орёл, Д.В. Моделирование стохастических систем квазиортогональных сигналов для защищённых глобальных спутниковых радионавигационных систем / Д.В. Орёл // Вестник Ставропольского государственного университета. Научный журнал «Вестник СГУ». – 2011. – №75(4). – С. 111-116.

56. Орёл, Д.В. Разработка метода моделирования систем двоичных квазиортогональных кодовых последовательностей для глобальных навигационных спутниковых систем / Д.В. Орёл // Вестник Северо-Кавказского федерального университета. – 2013. – № 3(36). – С. 26-30.

57. Остапенко, О.А. Риски систем: оценка и управление [Текст] / Под ред. Ю.Н. Лаврухина. Д.О Карпеев, В.Н. Асеев. – М. : Горячая линия – Телеком, 2007. –247 с.

58. Пат. 2189610 Российская федерация, МПК7 G01S13/52. Система опознавания «свой-чужой» [Текст] / Сивов, В.А., Моисеев В.Ф. заявитель и патентообладатель Военная академия ракетных войск стратегического назначения им. Петра Великого. – №2000132255/09 ; заявл. 22.12.2000 ; опубл. 20.09.2002. – 5 с.

59. Пат. 2191403 Российская Федерация, МПК7 G01S13/78, G01S13/74. Система опознавания «свой-чужой» [Текст] / Моисеев, В.Ф., Сивов В.А. заявитель и патентообладатель Военная академия Ракетных войск стратегического назначения им. Петра Великого. – № 003124994/09 ; заявл. 11.08.2003 ; опубл. 20.06.2005. – 5 с.

60. Пат. 2324201 Российская Федерация, МПК G01S13/78. Устройство радиолокационного распознавания воздушных объектов [Текст] / Бляхман А.Б. ; заявитель и патентообладатель Федеральное государственное унитарное предприятие «Нижегородский научно-исследовательский институт радиотехники». – № 2006115013/09 ; заявл. 02.05.2006 ; опубл. 10.05.2008, Бюл. № 13. – 5 с.

61. Пат. 2562373 Российская Федерация, МПК G06F 7/72. Генератор псевдослучайной функции / Калмыков И.А., Дагаева О.И., Калмыков М.И. ; заявитель и патентообладатель ФГАОУ ВПО «Северо-Кавказский федеральный университет». – № 2013144483/08; заявл. 03.10.2013; опубл. 10.09.2015, Бюл. № 25. – 5 с.

62. Пат. 2570700 Российская Федерация, МПК G01S13/78. Способ построения системы опознавания «свой-чужой» на основе протокола с нулевым разглашением [Текст] / Калмыков М.И. ; заявитель и патентообладатель Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». – № 2014128068/07 ; заявл. 08.07.2014 ; опубл. 10.12.2015, Бюл. № 34. -– 11 с.

63. Перунов, Ю.М. Радиоэлектронное подавление информационных каналов систем управления оружием [Текст] / Ю.М. Перунов, К.И. Фомичев, Л.И. Юдин. – М. : Радиотехника, 2008. – 435 с.

64. Плетнев, П.В Методика оценки рисков информационной безопасности / П.В. Плетнев, В.М. Белов // Доклады ТУСУРа. – Томск, 2012. №1 (25) часть 2. – С. 83-86.

65. Показатели качества продукции [Электронный ресурс]. – Режим доступа: http://www.grandars.ru/college/biznes/pokazateli-kachestva-p.html.

66. Ракитов, А.И. Системный анализ и аналитические исследования: руководство для профессиональных аналитиков [Текст] / А.И. Ракитов, Д.А. Бондяев, И.Б. Романов, С.В. Егерев, А.Ю. Щербаков. – М. : Возрождение, 2009. – 443 с.

67. Рябко, Б.Я. Криптографические методы защиты информации [Текст] / Б.Я. Рябко, А.Н. Фионов – М.: Горячая линия-Телеком, 2012. – 229 с.

68. Свой-чужой на службе России [Электронный ресурс]. – Режим доступа: http://www.rt-online.ru/aticles/51010.

69. Сервис демонстрации времени взлома конкретного пароля методом brute-force [Электронный ресурс]. – Режим доступа: https://rb.ru/news/bruteforce.

70. Слеповичев, И.И. Генераторы псевдослучайных чисел [Текст] / И.И. Слеповичев. – Саратов : СГУ, 2017. – 118 с.

71. Сурмин, Ю.П. Теория систем и системный анализ: Учеб. пособие. [Текст] / Ю.П. Сурмин – Киев : МЛУП, 2003. – 368 с.

72. Тузов, Г.И. Помехозащищенность радиосистем со сложными сигналами [Текст] / Г.И. Тузов, В.А. Сивов, В.И. Прытков и др. – М. : Радио и связь, 1985. – 264 с.

73. Центр поддержки операций компании Шлюмберже [Электронный ресурс]. – Режим доступа:http://www.slb.ru/page.php?code=28.

74. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости [Текст] / А.В. Черемушкин. – М. : Издательский центр «Академия», 2009. – 272 с.

75. Чернышов, В.Н. Теория систем и системный анализ [Текст] / В.Н. Чернышов, А.В. Чернышов. – Тамбов : ТГТУ, 2008. – 96 с.

76. Чмора, А.Л. Современная прикладная криптография [Текст] / А.Л. Чмора. – М. : Гелиос АРБ, 2002. – 256 с.

77. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер. – М. : Издательство ТРИУМФ, 2003. – 816 с.

78. Шумский, А.А. Системный анализ в защите информации [Текст] / А.А. Шумский, А.А. Шелупанов. – М. : Гелиос АРВ, 2005. – 224 с.

79. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication / V.P. Pashintsev, I.A. Kalmykov, A.P. Zhuk, M.I. Kalmykov, D.N. Rezenkov // International Journal of Mechanical Engineering and Technology. – 2018. – №9 (5). – P. 958-965.

80. Battlefield Combat Identification System [Электронный ресурс]. – Режим доступа: http://www.globalsecurity.org/military/systems/ground/bcis.htm.

81. Development of the protocol «ELECTRONIC CASH» with inspection correction rules of the electronic e-cash number for e-Commerce systems // I.A. Kalmykov, V.A. Lapina, N.V. Kononova, M.I. Kalmykov // Proceedings of REMS 2018^Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT. – 2018. – P. 11-21.

82. Efficient construction of (distributed) verifiable random functions / Y. Dodis. – Springer: PKC, 2003. – P. 1-17.

83. Fast signature generation with a Fiat Shamir-Like scheme / C.P. Schnorr., H. Ong // Advances in Cryptology. Eurocrypt. – 1991. – P. 432-440.

84. Hannu, A. P. Zero Knowledge Protocols and Small System [Электронный ресурс]. – Режим доступа: http://www.tml.tkk.fi /Opinnot/Tik-110.501/1995/zeroknowledge.html.

85. ISO/IEC 9798-5:2009 Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques.

86. Menezes, A. Handbook of Applied Cryptography [Текст] / A. Meneze, P. Oorschot, S. Vanstone. – CRC Press, 1996. – p. 816.

87. Naor Moni and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. In FOCS’97 [Электронный ресурс]. – Режим доступа: http://www.wisdom.weizmann.ac.il/~naor/PAPERS/gdh_abs.html.

88. Number-theoretic constructions of efficient pseudorandom functions / M. Naor, O. Reingold // In Proceedings of the 38th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society Press. – Los Alamitos, Calif., 1977. – P. 458-467.

89. Number-Theoretic Constructions of Efficient Pseudo-Random Functions / M. Naor, O. Reingold // Journal of the ACM. – 2004. – Vol. 51, No. 2. – P. 231-262.

90. On the (In) security of the Fiat-Shamir Paradigm. / S. Goldwasser, Y. Kalai // FOCS. – 2003. – P. 102-114.

91. Patent No.: US 8,750,517 B2 United States, H04LK L/00. Friend or foe detection [Текст] / Kymissis I. ; assignee The Trustees of Columbia University in City of New York. – Appl. No. 12/682,216 ; PCT Filed Oct. 9, 2008 ; PCT Pub. Date Apr. 16. – 15 p.

92. Patent US 20100309039 United States, GOIS I.3/74. Identification friend or foe (iff) system [Текст] / Cornelia F., Thomas H. ; assignee Raytheon Company, Waltham. – Appl. No. 12/792,991 ; Filed Jun. 3, 2010 ; Pub. Date Dec. 9, 2010. – 12 p.

93. Patent US 5745575 A United States, HO4L 9/32, G01S 13/74. Identification friend or foe (IFF) system using variable codes [Текст] / William F. Robert A. Freddie M. ; assignee The United States of America as represented by the Secretary of the Army. – Appl. No. 668,608 ; Filed May 20, 1996 ; Date of Patent Apr. 28, 1998. – 5 p.

94. Patent US 6,664,915 B1 United States, G01S 13/78. Identification friend or foe system in clouding short range UV shield [Текст] / Daniel A. ; assignee The United States of America as represented by the Secretary of the Navy. – Appl. No 10/173,526 ; Filed Jun. 10, 2002 ; Date of Patent Dec. 16, 2003. – 6 p.

95. Patent US 8325081 B2 United States, GO1S 13/78. Identification friend or foe (IFF) system [Текст] / Cornelia F., Thomas H. ; assignee Raytheon Company. – Appl. No. 12/792,991 ; Filed Jun. 3, 2010 ; Dec. 4, 2012. – 12 p.

96. Schneir, B. Applied cryptography. Protocols, algorithms and source code in C [Текст] / B. Schneir – NY. : John Wiley & Sons Inc., 1996. – 786 p.

97. Secure password check [Электронный ресурс]. – Режим доступа: https://password.kaspersky.com.

98. Smith, R. Authenticaton: From Passwords to Public Keys [Текст] / R. Smith. – NY. : Addison-Wesley Publishing Company Inc., 2002. – 352 p.

99. Stallings, W. Network and Internetwork Security: principles and practice, Second Edition [Текст] / W. Stallings. – Prentice-Hall Inc., 1999. – 459 p.

100. Synthesizers and their application to the parallel construction of pseudo-random functions / M. Naor, O. Reingold // Journal of Computer and System Sciences. – 1999. – Vol. 58, No. 2. – P. 336-375.

101. Verifiable Random Function with Short Proofs an Keys / Y. Dodis, A. Yampolsky. – Springer: PKC, 2005. – P. 416-431.

Приложение А

Реализация протоколов опознавания, построенных на основе доказательства с нулевым разглашением данных

А.1 Пример реализации протокола опознавания Фиата-Шамира

Рассмотрим пример реализации данного протокола опознавания. Пусть выбраны два простых числа Q = 5, G = 7. Тогда их произведение будет равно M = 35.

Определим квадратичные вычеты по модулю M = 35. Квадратным вычетом является число, удовлетворяющее следующему выражению

$$S^2 = H \bmod M \qquad (A.1)$$

где $1 \le S \le n$.

В ходе проведенных исследований были найдены следующие значения квадратичных вычетов

$$S = \{1, 4, 6, 9, 11, 14, 15, 16, 21, 25, 29, 30, 34\}.$$

Если значение числа H = 16. Тогда обратное мультипликативное значение числа равно его $H^{-1}=11$, так как

$$(16 \cdot 11) \bmod 35 = 176 \bmod 35 = 1$$

Вычислим значение секретного ключ, используя выражение (2.2). Тогда получаем S = 9, так как $9^2 \bmod 35 = 81 \bmod 35 = 11$.

Таким образом, получили открытые ключи (M, H) = (35, 11).

Рассмотрим алгоритм опознавания для данного протокола. Данный порядок операций, выполненный один раз называется аккредитацией.

1. Пусть претендент P выбирает случайное числа K из условия $K \in \{1, 2, .., M-1\}$. Пусть K=8. Затем претендент вычисляет значение используя (2.4). Тогда имеем

$$E = K^2 \bmod M = 8^2 \bmod 35 = 29$$

Данное значение E=29 передается проверяющему B как свидетельство.

2. Проверяющий абонент V выбирает случайное число B = 0. Данное значение передается претенденту P.

3. Претендент P производит вычисление, используя равенство (2.5). Так как значение проверочного бита B = 0, то проверяющему абоненту V будет передано число Y = K = 8.

4. Проверяющий V, получив ответ, производит проверку согласно условия (2.6). Так как значение проверочного бита B = 0, то абонент V вычисляет

$$L = Y^2 \bmod M = 8^2 \bmod 35 = 29$$

Так как полученное значение делает истинным выражение (2.8), т.е. $L = E = 29 \bmod 35$, то проверяющий абонент V делает вывод - претендент P имеет статус «свой».

Рассмотрим ситуацию, когда проверяющий V пересылает претенденту P значение проверочного бита B = 1. Тогда получаем.

3. Претендент P производит вычисление, используя равенство (2.5). Так как значение B = 1, то проверяющему абоненту V будет передано число

$$H = (KS) \bmod M = (8 \cdot 9) \bmod 35 = 2$$

4. Проверяющий V, получив ответ, производит проверку согласно условия (2.7). Так как значение проверочного бита B = 1, то абоненту V необходимо вычислить

$$L = (Y^2 H) \bmod M = (2^2 \cdot 16) \bmod 35 = 29$$

Так как полученное значение делает истинным выражение (2.8), т.е. $L = E = 29 \bmod 35$, то проверяющий абонент V делает вывод - претендент P имеет статус «свой».

A.2 Пример реализации протокола опознавания Шнорра

Пусть претендент выбрал простое число P = 29. Тогда второе простое число H, должно быть делителем числа (P - 1) = 28. В этом случае можно

выбрать простое число H = 7. Воспользуемся выражением (2.14) для вычисления числа Мравное . Проведенные исследования позволили выбрать число M = 7.

Претендент P выбирает значение секретного ключа равное S = 5. Используя секретный ключ, вычисляется часть открытого ключа протокола

$$A = M^{-S} \bmod P = \left|7^{-5}\right|_{29}^{+} = \left|7^{23}\right|_{29}^{+} = 20$$

Тогда открытый ключ протокола опознавания будет равен $(A, P, M) = (20, 29, 7)$. Данный открытый ключ должен быть доступен проверяющей стороне V.

Рассмотрим процедуру опознавания претендента.

1. Пусть претендент P сначала выбирает случайное число K = 3, а затем вычисляет число E, используя выражение (2.16)

$$E = M^{K} \bmod P = \left|7^{3}\right|_{29}^{+} = 24$$

Полученный результат E = 24 претендент P передает проверяющему V.

2. Проверяющая сторона V выбирает случайное число B = 4. Данное число по каналу связи поступает претенденту P.

3. Претендент P, получив вопрос B = 4, приступает к вычислению ответа на основе выражения (2.17)

$$Y = (K + S \cdot B) \bmod H = \left|3 + 4 \cdot 5\right|_{7}^{+} = 2$$

Полученное число Y пересылается проверяющему V.

4. Проверяющий V, получив ответ Y от претендента P, производит проверку ответа

$$X = M^{Y} A^{B} \bmod P = \left|7^{2} \cdot 20^{4}\right|_{29}^{+} = 24$$

В результате проверка ответа показала, что справедливо X = E = 24. Это означает, что претендент P получает статус «свой».

А.3 Пример применения разработанного протокола в системе опознавания КА

Пусть выбрано простое число q = 37. В качестве первообразного элемента выбираем число $g = 2$, с помощью которого были получены все элементы, задаваемой q = 37. В таблице А.1 представлены элементы мультипликативной группы.

Таблица А.1 – Элементы мультипликативной группы по модулю 37

x	$\left\|g^x\right\|_q^+$	x	$\left\|g^x\right\|_q^+$	x	$\left\|g^x\right\|_q^+$	x	$\left\|g^x\right\|_q^+$	x	$\left\|g^x\right\|_q^+$	x	$\left\|g^x\right\|_q^+$
1	$2^1=2$	7	17	13	15	19	35	25	20	31	22
2	$2^1=4$	8	34	14	30	20	33	26	3	32	7
3	8	9	31	15	23	21	29	27	6	33	14
4	16	10	25	16	9	22	21	28	12	34	28
5	32	11	13	17	18	23	5	29	24	35	19
6	27	12	26	18	36	24	10	30	11	36	1

Пусть в качестве секретного ключа выбрано число U = 11. В качестве сеансового ключа выбираем число S(j) = 9. Для проведения проверки, позволяющей определить увеличение срока применения сеансового ключа S(j), выбираем число T(j) = 7. Вычислим значение истинного статуса космического аппарата. Тогда имеем

$$C(j) = g^U g^{S(j)} g^{T(j)} \bmod q = (2^{11} \cdot 2^9 \cdot 2^7) \bmod 37 = 2^{27} \bmod 37 = 6$$

Для проведения процесса зашумления выберем следующие случайные величины $\Delta U(j) = 3, \Delta S(j) = 22, \Delta T(j) = 14$. В результате получаем

$$U^*(j) = (U + \Delta U(j)) \bmod q = (11 + 3) \bmod 37 = 14,$$
$$S^*(j) = (S(j) + \Delta S(j)) \bmod q = (9 + 22) \bmod 37 = 31,$$
$$T^*(j) = (T(j) + \Delta T(j)) \bmod q = (7 + 14) \bmod 37 = 21.$$

С помощью вычисленных параметров определим зашумленный статус КА. Тогда имеем

$$C^*(j) = g^{U^*(j)} g^{S^*(j)} g^{T^*(j)} \bmod q = (2^{14} \cdot 2^{31} \cdot 2^{21}) \bmod 37 = 2^{30} \bmod 37 = 11$$

Рассмотрим процесс опознавания КА.

Запросчик, который размещается на необслуживаемом объекте, выбирает случайное число d = 23. Для опознавания космического аппарата запросчик передает вопрос ответчику, который находится на борту спутника.

Получив число d = 23, ответчик производит вычисления ответов на данный вопрос. Тогда имеем

$$r_1(j) = (U^*(j) - dU) \bmod \varphi(q) = |14 - 23 \cdot 11|_{36}^{+} = |-23|_{36}^{+} = 13;$$
$$r_2(j) = (S^*(j) - dS(j)) \bmod \varphi(q) = |31 - 23 \cdot 9|_{36}^{+} = |-32|_{36}^{+} = 4;$$
$$r_3(j) = (T^*(j) - dT(j)) \bmod \varphi(q) = |21 - 23 \cdot 7|_{36}^{+} = |-32|_{36}^{+} = 4.$$

Получив ответы на поставленный вопрос d = 23, ответчик передает запросчику следующий сигнал (6, 11, 13, 4, 4). Данный сигнал содержит истинный и зашумленный статусы космического аппарата, а также три ответа на случайный вопрос d = 23.

Запросчик проверяет правильность ответов

$$Y(j) = C^d g^{r_1^*(j)} g^{r_2(j)} g^{r_3(j)} \bmod q = |6^{23} \cdot 2^{13} \cdot 2^4 \cdot 2^4|_{37}^{+} = |2^{30}|_{37}^{+} = 11$$

Так вычисленное значение равно зашумленному статусу космического аппарата, то запросчик присваивает данному спутнику статус «свой».