УДК 681.32:007.5
DOI: 10.15587/1729-4061.2022.254545

Розробка крипто-кодових конструкцій на ldpc-кодах

С. С. Погасій, С. П. Євсеєв, О. С. Жученко, О. В. Мілов, В. П. Лисечко, О. В. Коваленко, М. Ю. Костяк, А. Ф. Волоков, О. В. Лезік, В. А. Сусукайло

Приведені результати розробки постквантових алгоритмів крипто-кодових конструкцій Мак-Еліса та Нідеррайтера на кодах LDPC (Low Density Parity Check) із малою щільністю перевірок на парність. В умовах стрімкого зростання обчислювальних можливостей мобільних технологій та створення на їх базі бездротових Mesh-, сенсорних-мереж, технологій Інтернет-речей, smart-технологій актуальною проблемою стає забезпечення безпеки інформації. При цьому виникає необхідність розгляду безпеки у двох контурах внутрішньому (безпосередньо всередині інфраструктури мережі) та зовнішньому (хмарних технологіях). У таких умовах необхідно комплексувати загрози як на внутрішній контур безпеки, так і на зовнішній контур. Це дозволяє не лише враховувати гібридність та синергізм сучасних цільових загроз, але й враховувати рівень значущості (ступінь секретності) інформаційних потоків та інформації, що циркулює як у внутрішньому, так і зовнішньому контурі безпеки. Пропонується концепція побудови безпеки на основі двох контурів. Для забезпечення безпеки бездротових мобільних каналів пропонується використовувати крипто-кодові конструкції Мак-Еліса та Нідеррайтера на LDPC-кодах, що дозволяє інтегруватися у технології забезпечення вірогідності стандартів IEEE 802.15.4, IEEE 802.16. Такий підхід дозволяє забезпечити необхідний рівень послуг безпеки (конфіденційності, цілісності автентичності) в умовах повномасштабного квантового комп'ютера. Розглядаються практичні технології забезпечення безпеки, на основі пропонованих крипто-кодових конструкцій, IP-телефонії в онлайн режимі та системи "Розумний дім" на основі використання внутрішнього сервера.

Ключові слова: крипто-кодові конструкції, коди з малою щільністю перевірок на парність, концепція безпеки.

1. Введение

Создание современных синтезированных сетей основывается на гибридизации технологий беспроводных мобильных и социо-киберфизических систем на основе Интернет вещей. Классические компьютерные системы и технологии интегрируют элементы Интернет вещей и формируют принципиально новые направления развития ИТ-индустрии, smart-технологии, которые объединяют все достижения мобильных, беспроводных и социо-киберфизических систем. Однако стремительное расширение mesh-, сенсорных сетей с использованием стандартов беспроводных каналов: мобильных технологий LTE (Long-Term Evolution – долго-

срочная эволюция), IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth не обеспечивает безопасность информационных потоков. В погоне за сверхскоростями в таких каналах не обеспечиваются услуги конфиденциальности и целостности. Протокол Diameter обеспечивает взаимодействие между клиентами в целях аутентификации, авторизации и учёта различных сервисов безопасности, однако имеет существенные недостатки с точки зрения современных кибератаках. Для обеспечения безопасности в киберфизических системах на основе интернет вещей используется стандарт KNX (ISO/IEC 14543) на основе использования VPN-каналов (шифрование AES–128, –256). Однако все механизмы обеспечения безопасности не обеспечат требуемый уровень безопасности в постквантовый период (появление полномасштабного квантового компьютера). Специалисты NIST США выдвигают сомнения в стойкости современных симметричных и несимметричных криптосистем (включая алгоритмы и на эллиптических кривых) на основе квантовых алгоритмов Гровера и Шора. В таких условиях постквантовые криптоалгоритмы на основе синтеза теорий помехоустойчивого кодирования и защиты информации – крипто-кодовые конструкции (CCC - crypto code constructs) – могут рассматриваться как альтернативный механизм обеспечения безопасности. Такие конструкции являются гибридами, т.к. формирование несимметричной криптосистемы (криптостойкость основывается не теоретико-сложностной задаче – декодирование случайного кода) обеспечивается на основе использования алгебраических кодов. По оценке специалистов NIST США для обеспечения криптостойкости формирование помехоустойчивых кодов необходимо над полем Галуа (GF 2^{10}–2^{13}), что даже при современных вычислительных ресурсах довольно сложный вопрос. Использование в беспроводных киберфизических системах требует значительного сокращения поля, что позволит с одной стороны обеспечить снижение энергоёмкости, а с другой стороны требует необходимого уровня криптостойкости. Таким образом, для киберфизических систем на основе беспроводных мобильных технологий необходимы криптосистемы, которые обеспечат требуемый уровень криптостойкости в постквантовый период, энергоемкость, которая позволит использовать в смарт-технологиях, а также обеспечить полный спектр услуг безопасности.

Кроме этого, возникает необходимость рассмотрения концепции двух контуров безопасности (внутреннего – непосредственно инфраструктура сети, и внешнего – облачные платформы – сервера управления киберфизическими системами) в условиях интеграции сетей и облачных технологий.

2. Обзор литературы и постановка проблемы

Криптосистемы, основанные на кодах, были признаны многообещающими альтернативами асимметричной криптографии. Это объясняется тем, что обеспечиваемая ими безопасность основана на хорошо известных NP-трудных проблемах и по-прежнему демонстрируют высокую производительность для широкого диапазона вычислительных платформ. Основным недостатком схем на основе ко-

да, включая популярные предложения Мак-Элиса и Нидеррайтера, являются большие ключи, размер которых по своей сути определяется базовым кодом. Криптосистема Мак-Элиса одна из старейших криптосистем с открытым ключом, которую невозможно взломать. Ее простота и эффективность делают ее очень интересным кандидатом для постквантовой эры, поскольку предполагается, что она защищена от атак квантового компьютера.

В [1] анализируется криптосистема Мак-Элиса, рассматриваются ее основы, достоинства и недостатки, представлены некоторые основные концепции теории кодирования, необходимые для понимания криптосистемы Мак-Элиса. Основное внимание в работе уделено протоколу шифрования на основе кода. Предполагается, что криптосистема устойчива к квантовым атакам с полиномиальным временем. Отмечается, что у криптосистемы Мак-Элиса существует проблема, связанная с размером ключа [2], а также со времени дешифрования. Поэтому предприняты попытки уменьшения размера ее ключа, но повышения ее защиты от известных атак и снижения времени шифрования и дешифрования.

Предлагается криптосистема на основе Мак-Элиса, которая использует коды Гоппы, семейство, используемое в оригинальном Мак-Элисе, и коды LDPC (Low Density Parity Code – коды с низкой плотностью проверок на чётность), семейство кодов, основанное на графах и позволяющее быстро выполнять декодирование на аппаратном уровне. Эта новая конструкция обеспечивает быстрое шифрование и дешифрование как программно, так и аппаратно и очень хорошо масштабируется для больших сообщений, решая указанную выше проблему. Кроме того, с помощью этой конструкции можно уменьшить размер ключа более чем в десять раз по сравнению с исходным Мак-Элисе. В качестве дальнейшего направления работы предлагается поиск способов еще большего уменьшения размера ключа криптосистемы Мак-Элиса, что имеет большое значение, если ожидается замена текущих криптографических протоколов квантово-устойчивыми протоколами.

В [3] предложено использовать квазициклические коды MDPC (Moderate-Density Parity-Check Codes – коды умеренной плотности с проверкой на четность), которые обеспечивают очень компактное представление ключа. В работе [4] исследуются новые реализации схемы Мак-Элиса с использованием кодов QC-MDPC (Quasi-cyclic MDPC – квази-циклические MDPC), адаптированных для встраиваемых устройств, оценивается и улучшаются различные подходы к декодированию кодов QC-MDPC. Поэтому текущие исследования нацелены на альтернативные коды, которые обеспечивают более компактное представление ключей, но при этом сохраняют свойства безопасности криптосистемы. В частности, предложено использовать QC-MDPC коды в качестве такой альтернативы.

Почти все известные асимметричные криптосистемы опираются на два класса фундаментальных проблем, а именно на проблему факторизации и проблему дискретного логарифмирования (эллиптическая кривая). Благодаря эффективному алгоритму Шора, который решает обе проблемы на квантовых компьютерах, стало очевидным, что необходимо готовить большее разнообразие примитивов открыто-

го ключа на тот случай использования квантовых компьютеров. В [5] представлены возможности применения квантового компьютера для решения проблем кодирования и шифрования. В качестве недостатка отмечается нестабильность хранимой и обрабатываемой информации, а также ограниченное время ее существования.

Наиболее многообещающие альтернативы подразделяются на криптографию на основе кода и криптографию на основе хеширования. Основным недостатком многих предлагаемых криптосистем в этих классах является их низкая эффективность и практичность из-за больших размеров ключа или сложных вычислений по сравнению с классическими криптосистемами. Это особенно актуально для небольших и встроенных систем, где память и вычислительная мощность являются дефицитными ресурсами. Было показано, что криптосистемы на основе кода, такие как хорошо зарекомендовавшие себя предложения Мак-Элиса и Нидеррайтера, могут значительно превосходить классические асимметричные криптосистемы на встроенных системах. В [6] исследуется реализация схемы Мак-Элиса во встроенных системах, что считалось проблемой из-за необходимости хранения больших ключей. В [7] описываются методы систематического проектирования встроенного сопроцессора для постквантовой защищенной криптосистемы Мак-Элиса. Совместная разработка аппаратного и программного обеспечения нацелена на практическую реализацию McEliece на недорогих встраиваемых платформах. Оптимизация конструкции происходит при выборе системных параметров, преобразований алгоритмов, выбора архитектуры и арифметических примитивов.

В [8] отмечается, что большинство часто внедряемых криптосистем с открытым ключом доказали свою безопасность на основе предполагаемой сложности двух математических задач: факторизации произведения двух больших простых чисел и вычисления дискретных логарифмов. Считается, что обе задачи вычислительно неразрешимы на обычном компьютере. Однако квантовый компьютер, способный выполнять вычисления на нескольких тысячах кубитов, мог бы решить обе проблемы с помощью алгоритма Шора. Утверждается, что основным недостатком криптосистемы с открытым ключом Мак-Элиса является очень большой открытый ключ, состоящий из нескольких сотен тысяч битов. Еще одним недостатком схемы Мак-Элиса, как и многих других схем, является то, что она не является семантически безопасной. Предлагается реализация криптосистемы с открытым ключом, которая семантически безопасна и использует в 40 раз меньший открытый ключ и в пять раз меньший секретный ключ по сравнению с более ранними реализациями.

Это превосходство достигается за счет очень длинных ключей (часто более 50 кбайт).

Несмотря на то, что схемы шифрования на основе кода были предложены более 30 лет назад, они почти не встречаются в каких-либо (обусловленных затратами) реальных приложениях из-за их больших секретных и открытых ключей. Первоначальное предложение Роберта Мак-Элиса для схемы шифрования на основе кода предполагало использование двоичных кодов Гоппы, но в целом можно было

использовать любой другой линейный код. В то время как другие типы кодов могут иметь такие преимущества, как более компактное представление, большинство предложений, использующих другие коды, оказались менее безопасными. В [9] представлена конструкция криптосистемы, основанная на обобщенных кодах Шриваставы, большом классе, который включает в себя коды Гоппы как особый случай. Такой подход позволяет использовать относительно короткие открытые ключи, не будучи уязвимыми для известных структурных атак.

В исследовании [10] исследуются различные производные криптосистемы Мак-Элиса и изучаются их структурные недостатки. Спроектирована эффективная структурная атака на криптосистему Мак-Элиса, основанная на алгеброгеометрических кодах, определенных на эллиптических кривых. Эта атака основана на алгоритме Сидельникова и Шестакова, который решает соответствующую проблему для кодов Рида-Соломона. Представленный алгоритм является эвристическим с полиномиальным временем. Показано, что криптосистема Сидельникова, основанная на двоичных кодах Рида-Малера, ненадежна. Основная идея предлагаемой атаки состоит в том, чтобы использовать тот факт, что слова минимального веса в коде Рида-Малера обладают очень специфическими свойствами. Эта атака основана на способности находить слова минимального веса в коде, что в данном конкретном случае намного проще, чем обычное декодирование. Атака имеет субэкспоненциальное время выполнения, если порядок кода сохраняется фиксированным, и взламывает большие ключи, как предложил Сидельников, менее чем за час на стандартном ПК.

Криптосистема Нидеррайтера представляет собой независимо разработанный вариант предложения Мак-Элиса, который доказал свою эквивалентность с точки зрения безопасности [11]. Многие предложения уже пытались решить проблему больших ключей, заменяя первоначально используемые двоичные коды Гоппы (безопасными) кодами, которые позволяют более компактные представления. Так, в [12] предлагаются новые параметры для криптосистем Мак-Элиса и Нидеррайтера, обеспечивающие стандартные уровни защиты от всех известных атак. Новые параметры учитывают улучшенную атаку; введение списочного декодирования для двоичных кодов Гоппы; и возможность выбора длины кода, которая не является степенью двойки. Результирующие размеры открытого ключа значительно меньше, чем предыдущие варианты выбора параметров для того же уровня безопасности. А в [13] представлены эффективные реализации вариантов Мак-Элиса с использованием квазидиадических кодов. Следует отметить представление безопасных параметров для классической схемы шифрования Мак-Элиса, основанной на квазидиадических обобщенных кодах Шриваставы, и последовательное преобразование схемы в защищенный протокол, применяя преобразование Фуджисаки-Окамото.

Несмотря на заявления о том, что многие попытки оказались неудачными, а для немногих оставшихся практически нет общедоступных реализаций [14], ряд публикаций опровергают это утверждение. В статье [15] предлагается новый подход к исследованию безопасности криптосистемы Мак-Элиса, основанной на ис-

пользовании кодов, исправляющих ошибки. Отмечается, что с момента ее изобретения не было разработано ни одной эффективной атаки, которая позволила бы восстановить закрытый ключ. Доказано, что закрытый ключ криптосистемы удовлетворяет системе биоднородных полиномиальных уравнений. Это свойство обусловлено особым классом рассматриваемых кодов, которые являются альтернативными кодами. Заявлено, что реализация описанной алгебраической атаки в системе компьютерной алгебры Magma позволяет найти секретный ключ за незначительное время практически для всех предлагаемых задач. В [16] предложен новый общий способ уменьшения размера открытого ключа с помощью квазициклических кодов. Рассматривается метод сокрытия структуры секретной порождающей матрицы путем выбора сначала подкода подполя квазициклического кода, определенного в большом алфавите, а затем путем случайного сокращения выбранного подкода. Безопасность предлагаемого варианта связана с трудностью декодирования случайного квазициклического кода.

В [17] предложен алгоритм, основанный на “семействах случайных разностей”, который позволяет строить очень большие наборы эквивалентных кодов. Разработан обширный криптоанализ для проверки уровня безопасности, достижимого за счет выбранного выбора параметров системы. Предложенная схема обеспечивает удовлетворительную надежность системы при уменьшенном размере ключа и повышенной скорости передачи. Более того, установлено, что новая криптосистема может быть достаточно быстрой, чтобы оправдать ее принятие в качестве альтернативы широко распространенным решениям, таким как RSA. В [18] рассматривается возможное включение квазициклических кодов проверки четности с низкой плотностью в криптосистему Мак-Элиса, чтобы проверить совместное действие безопасности/контроля ошибок, которое потенциально может быть достигнуто этой схемой. Поскольку линейность преобразования закрытого ключа в открытый подвергает систему риску атаки полного взлома, представлены и обсуждаются подходящие условия, адаптированные для этого класса кодов. В [19] авторы приходят к выводу, что некоторые семейства кодов QC-LDPC (Quasi-cyclic LDPC – квазициклические LDPC), основанные на матрицах циклических перестановок, неприменимы из-за проблем с безопасностью. Однако другие коды, основанные на подходе «разностных семейств», могут обеспечить хороший уровень защиты от вторжений.

Полученные результаты позволили сформировать вывод, заключающийся в том, что Мак-Элис, основанный на LDPC-кодах, не считается хорошим выбором [20].

В работе [21] предлагается два варианта криптосистемы Мак-Элиса. Первый вариант основывается на MDPC кодах умеренной плотности с проверкой на четность, а другой – на квазициклических кодах MDPC. Коды MDPC представляют собой коды LDPC с более высокой плотностью, чем те, которые обычно используются для телекоммуникационных приложений. Как правило, это приводит к ухудшению способности исправления ошибок. Однако в криптографии на основе кода не обязательно интересует исправление многих ошибок. Вместо этого важно

только число, которое обеспечивает адекватный уровень безопасности, условие, которому удовлетворяют коды MDPC. Такой подход имеет множество преимуществ. При разумном предположении коды MDPC сводят проблему распознавания ключей Мак-Элиса к проблеме декодирования линейных кодов. Поскольку атаки сообщений на схему Мак-Элиса также сводятся к этой проблеме, безопасность нашей схемы имеет то преимущество, что она опирается на хорошо изученную проблему теории кодирования.

Все криптосистемы, основанные на сложности факторизации или дискретного логарифмирования, могут быть атакованы за полиномиальное время с помощью квантового компьютера [22]. Это угрожает большинству, если не всем криптосистемам с открытым ключом, развернутым на практике, таким как RSA или DSA. Криптография на основе кода считается квантово-устойчивой и поэтому рассматривается как жизнеспособная замена этим схемам в будущих приложениях. Тем не менее, независимо от их так называемой «постквантовой» природы, криптосистемы на основе кода предлагают другие преимущества даже для современных приложений. Эти преимущества реализуются за счет превосходной алгоритмической эффективности, которая на несколько порядков выше, чем у традиционных схем.

Криптосистема Мак-Элиса – кодовая криптосистема, первоначально предложенная с использованием кодов Гоппы. Его безопасность основана на двух допущениях: неразличимости семейства кодов и трудности декодирования общего линейного кода [23]. Проблема декодирования – хорошо изученная NP-полная задача, которая по-прежнему считается сложной. С другой стороны, проблема неразличимости обычно является самой слабой и сильно зависит от выбора семейства кодов. В качестве примера такой хрупкости в [24] представлен распознаватель для высокоскоростных кодов Гоппы (подобных тем, которые первоначально были предложены для цифровой подписи [25] и для некоторых реалистичных параметров безопасности криптосистем Мак-Элиса). Хотя это не представляет собой практической атаки, предполагается, что коды Гоппы не окажутся оптимальным выбором для криптографии на основе кода.

Коды MDPC кажутся очень удобными для криптографических целей. При разумном предположении, что различение (квазициклического) кода MDPC от (квазициклического) случайного линейного кода равносильно установлению существования кодовых слов с малым весом в его двоичном коде, мы показываем, что эти коды уменьшают длину ключа Мак-Элиса. Таким образом, безопасность предложенного в [21] варианта Мак-Элиса зависит только от одной хорошо изученной проблемы теории кодирования. Это сильный аргумент в пользу предлагаемой схемы, и его нужно сравнить со сценарием для кодов Гоппы. Различение кодов Гоппы не обязательно является сложной проблемой. Хотя это не обязательно ведет к практической атаке, это показывает, что алгебраические коды не являются оптимальным выбором для криптографии.

В [26] предлагаются методы оптимизации декодирования для кодов MDPC и рассматривается несколько эффективных реализаций криптосистемы QC-MDPC McEliece. Они включают в себя высокоскоростные и легкие архитектуры для реконфигурируемого оборудования, эффективные стили кодирования для микроконтроллера ARM Cortex-M4, а также новые высокопроизводительные программные реализации, которые полностью используют векторные инструкции. На основании данных, приведенных в публикации, можно сделать вывод, что шифрование McEliece в сочетании с кодами QC-MDPC не только обеспечивает высокопроизводительные реализации, но также позволяет создавать облегченные конструкции на широком спектре различных платформ.

В контексте криптографии с открытым ключом криптосистема Мак-Элиса представляет собой очень разумное решение, основанное на сложности проблемы декодирования, которая, как считается, способна противостоять в условиях появления квантовых компьютеров. Несмотря на это, первоначальная криптосистема Мак-Элиса, основанная на кодах Гоппы, вызвала ограниченный интерес в практических приложениях, отчасти из-за некоторых ограничений, налагаемых этим весьма особым классом кодов.

В [27] развивается последнее предложение, введением декодирования с инвертированием битов для кодов QC-LDPC, что приводит к значительному снижению сложности декодирования за счет умеренных потерь с точки зрения производительности исправления ошибок. Производительность декодирования с инвертированием битов можно легко предсказать с помощью теоретических аргументов, и это помогает определить размеры системы без необходимости длительного численного моделирования. Также рассматриваются наиболее эффективные из известных на сегодняшний день процедур атаки и аналитически оценивается их коэффициент работы. Таким образом, предоставляются инструменты, которые позволяют разработчику легко найти наилучший набор системных параметров для оптимизации компромисса между безопасностью и сложностью. Предложенная модификация направлена на преодоление основных недостатков исходной системы, при этом позволяя достичь удовлетворительного уровня безопасности.

В [28] утверждается, что наиболее эффективным способом преодоления недостатков криптосистемы Мак-Элиса была бы замена кодов Гоппы другими семействами кодов, что позволило бы получить более компактное представление их характеристических матриц и увеличить скорость кодирования. К сожалению, хотя существует несколько семейств кодов с такими характеристиками, лишь в очень немногих случаях можно заменить коды Гоппы, не подвергаясь серьезным недостаткам безопасности.

В [29] предложено использовать дополнительный параметр ключевых данных – вектор инициализации (набор недопустимых векторов положения вектора ошибки). Для противодействия атакам Сидельникова предлагается использовать модифицированные (укороченные) алгеброгеометрические (эллиптические) коды MEC (modified (shortened) algebrogeometric (elliptic) codes). Для этого необходимо ис-

пользовать второй дополнительный вектор инициализации (набор позиций для сокращения вектора ошибки). На основе модификации классической схемы Нидеррайтера на недвоичных кодах предложены прикладные алгоритмы генерации и расшифровки криптограммы в модифицированной Нидеррайтером крипто-кодовой системе на основе модифицированных (укороченных) эллиптических кодов и программного обеспечения. В [30] предложены механизмы безопасности на основе модифицированных крипто-кодовых систем Нидеррайтера и Мак-Элиса, которые позволяют обеспечить надежность (на основе использования эллиптических кодов с исправлением ошибок) и безопасность передаваемых данных.

В работе [31] представлены гибридные крипто-кодовые конструкции (hybrid crypto-code constructs, HCCC) Мак-Элиса и Нидеррайтера на ущербных кодах, которые используют алгоритмы нанесения ущерба и формирования ущербного текста и ущерба. Такой подход обеспечивает снижение энергоемкости в реализации, однако требует дополнительного канала передачи ущерба.

В [32] для обеспечения безопасности систем критической инфраструктуры предлагается использовать гибридные крипто-кодовые конструкции на основе модифицированных асимметричных крипто-кодовых систем Мак-Элиса на дефектных кодах. Это позволяет получить максимальное количество эмерджентных свойств при минимальных затратах ресурсов на инициирование в системный синергетический эффект обеспечения безопасности. Основным отличием от известных подходов к построению гибридных криптосистем является использование модифицированных асимметричных крипто-кодовых систем вместо симметричных криптосистем. Для усиления стойкости и “уменьшения” мощности алфавита (размерность поля GF (2^6–2^8)) для построения модифицированных крипто-кодовых конструкций (CCC – crypto code constructs) Мак-Элиса используются системы на дефектных кодах.

Таким образом, проведенный анализ использования постквантовых алгоритмов показал, что в зависимости от степени секретности информации, уровня оперативности передачи данных и ее актуальности для обеспечения услуг безопасности могут использоваться CCC на LDPC-кодах. Кроме этого, использование CCC Мак-Элиса и Нидеррайтера на MEC (modified (shortened) algebrogeometric (elliptic) codes – модифицированные (укороченные) алгеброгеометрические (эллиптические) коды) возможен в технологиях smart-, mesh-, сенсорных сетях для обеспечения услуг конфиденциальности, и целостности только во внутреннем контуре безопасности. Такой подход не позволяет в полной мере обеспечить требуемый уровень криптостойкости в постквантовый период, энергоемкости, а также оперативности и не требует дополнительных затрат с точки зрения реализации.

3. Цель и задачи исследования

Целью работы является разработка крипто-кодовых конструкций Мак-Элиса и Нидеррайтера на кодах с малой плотностью проверок на четность. Такой подход позволит сформировать двухконтурную систему безопасности сетей на основе мо-

бильных технологий и обеспечить услуги безопасности, как во внутреннем, так и во внешнем контуре системы безопасности на основе постквантовых алгоритмов.

Для достижения цели работы необходимо решить следующие задачи:

– разработать концепцию безопасности беспроводных сетей на основе мобильных технологий;

– разработать математические модели построения крипто-кодовых конструкций Мак-Элиса и Нидеррайтера на LDPC-кодах;

– разработать способы практической реализации крипто-кодовых конструкций Мак-Элиса и Нидеррайтера.

4. Материалы и методы исследования

Для обеспечения безопасности в постквантовый период – появление полномасштабного квантового компьютера, специалистами НИСТ предлагается использовать постквантовые алгоритмы. Такие алгоритмы требуют для симметричных криптосистем увеличение до 512 бит ключевых последовательностей (при этом обеспечивается безопасное время около 60 лет), либо использование постквантовых несимметричных криптосистем (PQAS – post-quantum asymmetric cryptosystems). Среди конкурсантов третьего тура конкурса выделяются алгоритмы, построенные на комплексировании теории помехоустойчивого кодирования и криптографии. На рис. 1 представлены структурные схемы крипто-кодовых конструкций Мак-Элиса и Нидеррайтера на алгеброгеометрических кодах (эллиптических кодах над полем GF (2^8), которые обеспечивают защиту от атаки Сидельникова и снижение энергоемкости. Кроме этого они интегрированно обеспечивают исправление ошибок в информационной последовательности [33]. Обе крипто-кодовые конструкции строятся по принципу использования теории помехоустойчивого кодирования и ортогональности матриц G – порождающей матрицы линейного кода, и H – проверочной матрицы линейного кода. В качестве ключевой последовательности в обеих крипто-кодовых конструкциях используются матрицы маскировки:

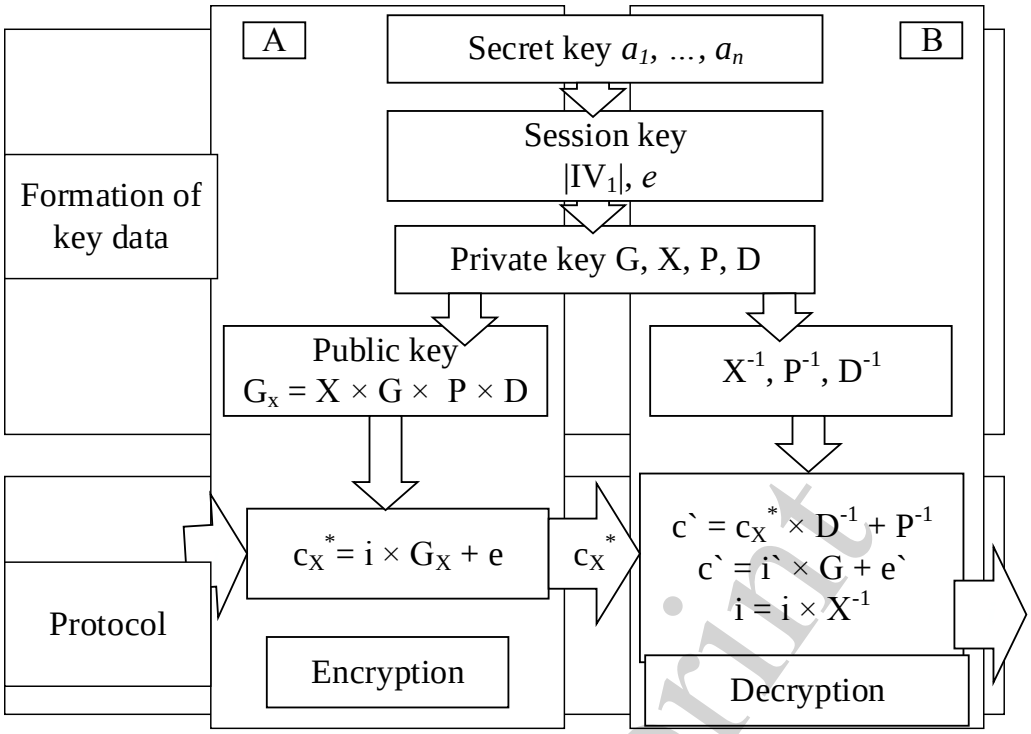
– X – маскирующая невырожденная случайно равновероятно сформированная источником ключей $k \times k$ матрица с элементами из $GF(q)$;

– P – перестановочная случайно равновероятно сформированная источником ключей $n \times n$ матрица с элементами из $GF(q)$;

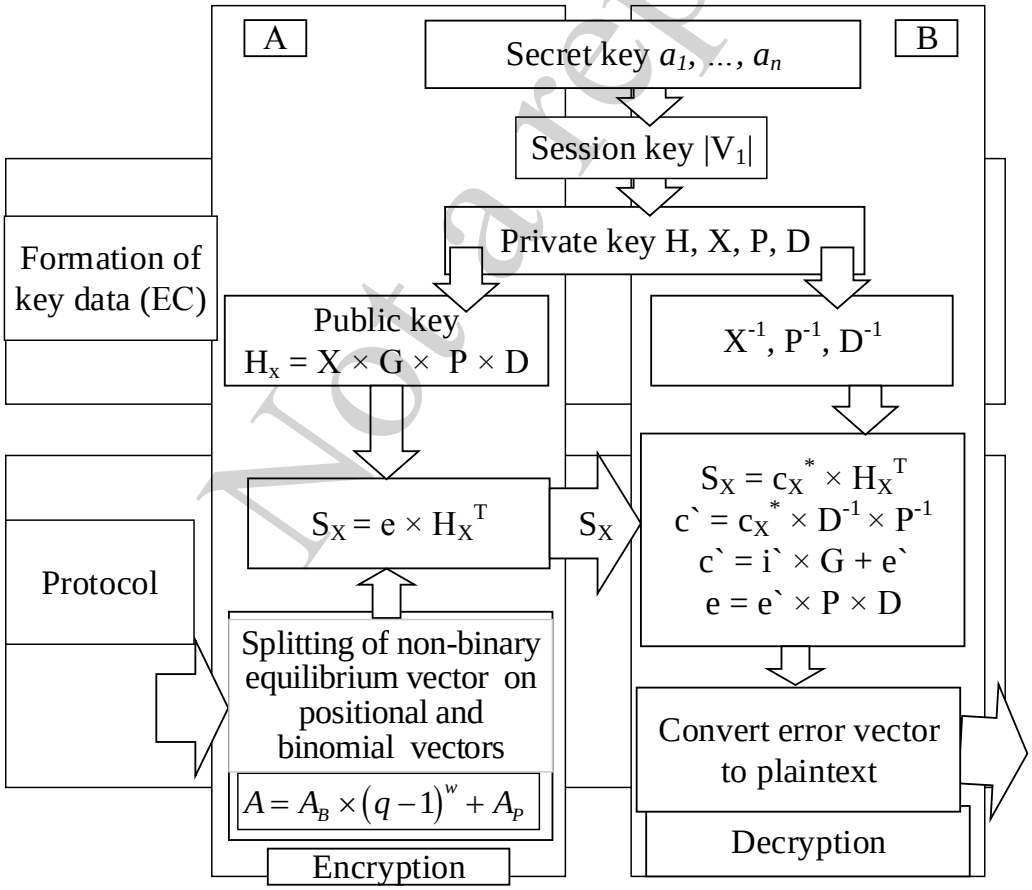
– D – диагональная сформированная источником ключей $n \times n$ матрица с элементами из $GF(q)$;

– G – порождающая матрица размерностью $k \times n$ (*CCC* Мак-Элиса);

– H – проверочная матрица размерностью $r \times n$. Кроме этого, отличительной особенностью *CCC* Нидеррайтера является предварительное использование равновесного кодирования, что позволяет обеспечить практически относительную скорость кодирования равную единице.



Крипто-кодовая конструкция Мак-Элиса на ЕС



Крипто-кодовая конструкция Нидеррайтера на ЕС

Рис. 1. Структурные схемы ССС Мак-Элиса и Нидеррайтера

Однако *CCC* Мак-Элиса обеспечивает интегрированно (одним механизмом) исправление ошибок $0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor$ (вес Хемминга (число ненулевых элементов) вектора ошибки – *e* не превышает исправляющей способности используемого алгебраического блокового кода. Использование *MEC* в крипто-кодовых конструкциях обеспечивает требуемый уровень криптостойкости, за счет использования векторов инициализации (IV_i, где *i* – номера символов укорочения или удлинения), а также позволяет обеспечить их построение над GF (2^6). В работах [29, 32] приведены математические модели и практические алгоритмы их реализации, а также результаты исследований их криптостойкости. Использование гибридных крипто-кодовых конструкций на основе ущербных кодов позволяет снизить уровень энергоемкости (строятся над полем GF (2^4), и обеспечить требуемый уровень криптостойкости, за счет использования двухканальной криптографии [30–32]. Однако их использование в смарт-технологиях и стандартах беспроводных мобильных сетей затруднительно, из-за необходимости дополнительной конвертации *m*-ичных кодовых последовательностей в бинарные и наоборот, что требует дополнительных энергозатрат. Для решения данного вопроса предлагается использовать коды LDPC для построения крипто-кодовых конструкций.

Коды LDPC используются в современных стандартах передачи данных, таких как DVB-S2, Gigabit Ethernet, WiMAX, Wi-Fi. Это обеспечивает их использование в любой системе связи, например, в космических коммуникациях, микроволновых системах связи, цифровом спутниковом телевидении.

Формирование регулярных LDPC кодов определено последовательной процедурой [34–42]. Регулярный код LDPC с длиной блока *n* формируется на основе проверочной матрицы *H*, которая характеризуется постоянным числом единиц в строке W_r и постоянным числом единиц в столбце W_c. Проверочная матрица *H* имеет низкую плотность единиц (плотность единиц считается низкой, если удельная часть единиц составляет менее 50 % всех элементов проверочной матрицы).

На основании заданных параметров *n*, W_r, W_c изменяются корректирующие свойства кода *t*, бит. При этом положение единиц в проверочной матрице *H* формируется на основе случайных перестановок столбцов базовой подматрицы, содержащей только одну единицу в каждом столбце. При этом скорость регулярного LDPC-кода в зависимости от параметров проверочной матрицы определяется по формуле:

$$r_k = \frac{n - \left(n \cdot \frac{W_c}{W_r} - (W_c - 1) \right)}{n} = 1 - \frac{W_c}{W_r} + \frac{W_c - 1}{n}, \qquad (1)$$

где n – длина кодовой последовательности, W_r – число единиц в строке проверочной матрицы H, W_c – число единиц в столбце проверочной матрицы H; r_k – скорость кодирования регулярного LDPC-кода.

В то же время, матрицы H LDPC кода одинакового размера и с одинаковыми параметрами могут порождать коды с разным кодовым расстоянием d и исправляющей способностью t.

Проверочная матрица LDPC кода может быть представлена в виде:

$$H = \begin{bmatrix} H_1 \\ \hline \pi_1(H_1) \\ \hline \vdots \\ \hline \pi_{Wc-1}(H_1) \end{bmatrix}, \quad (2)$$

где H_1 – базовая подматрица, $\pi_1(H_1)$ – подматрицы, полученные путём случайной перестановки столбцов базовой подматрицы H_1, i=1, 2, …, $W_{c\,1}$.

Проверочную матрицу H можно привести к виду:

$$H = \left[A \middle| I_{n-k} \right], \quad (3)$$

где A – некоторая фиксированная ((n–k)×k) – матрица с 0 и 1 (уже не являющаяся разреженной единицами), а $I_{n\text{-}k}$ – единичная матрица размера ((n–k)×(n–k)).

Матрица генерирования кодовых слов G слов имеет вид:

$$G = \left[I_k \middle| - A^T \right]. \quad (4)$$

Если матрица H представлена в виде (3), то матрица G (4) легко получается из матрицы H путем преобразований методом Гаусса.

Таким образом, с учетом выражений (1)–(4) и структурных схем ССС Мак-Элиса и Нидеррайтера возможно использование постквантовых криптосистем доказуемой стойкости для обеспечения безопасности информации в беспроводных сетях на основе мобильных технологий [43].

Для обеспечения безопасности в киберфизических системах и смарт-технологиях, как правило используется стандарт KNX (ISO/IEC 14543), который обеспечивает услуги безопасности – конфиденциальность и целостность данных [44–51]. На рис. 2, 3 представлены основные принципы обеспечения безопасности на основе использования стандарта KNX.

Стандарт KNX IP Secure позволяет аутентифицировать и шифровать телеграммы KNX в IP-сетях. При этом как правило формируется туннелирование, что обеспечивает конфиденциальность информации. Механизмы KNX IP Secure пред-

ставляют собой дополнительную защитную оболочку (оболочку), которая защищает весь трафик данных KNXnet/IP.

Однако KNX IP Secure не так уж и безопасна, есть возможность отслеживать сеть, записывать отправленные пакеты и легко их повторять, т. к. соединители линий с функцией “Security Proxy” нет. Кроме этого, использование при формировании туннелирования алгоритма AES-128 в постквантовый период не обеспечит требуемый уровень защиты даже внутреннего контура.

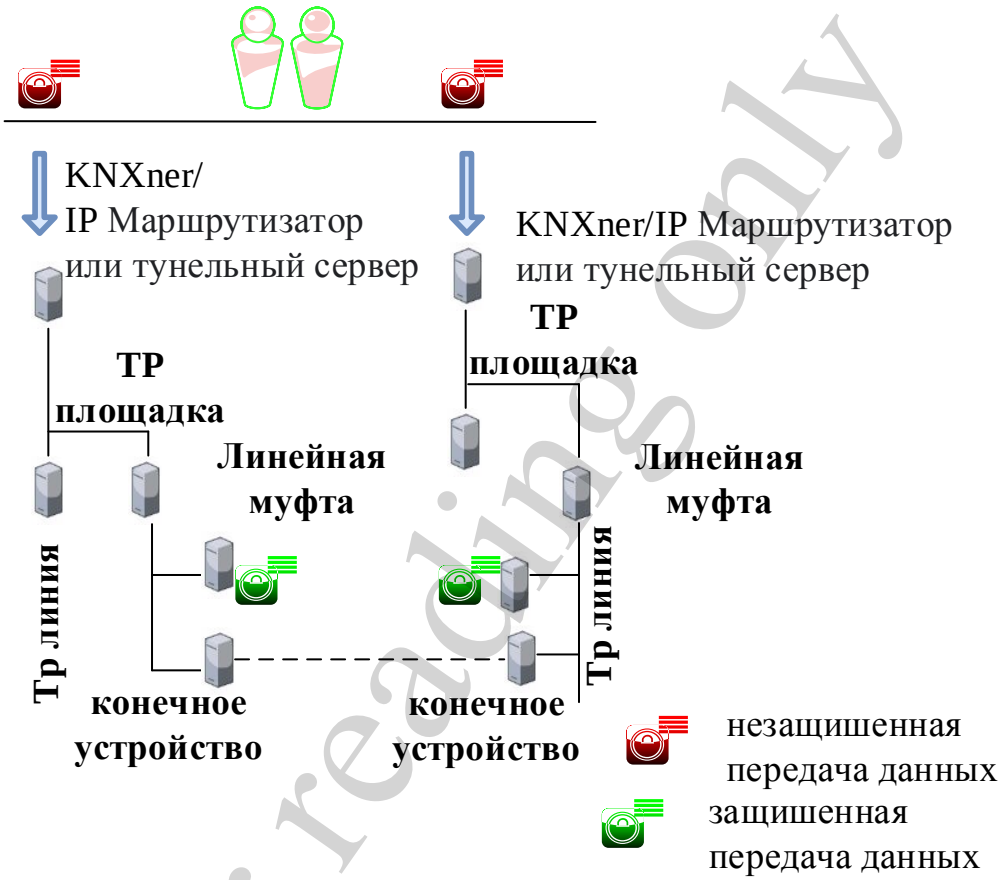


Рис. 2. Обеспечение безопасности в мобильных беспроводных каналах на основе KNX

На рис. 3 представленный протокол взаимодействия на основе беспроводного мобильного Интернета подтверждает возможность обеспечения конфиденциальности данных только во внутреннем контуре безопасности – внутри инфраструктуры сети. Однако во внешнем контуре безопасности стандарт не предполагает обеспечение услуг. Предполагается, что этим занимаются технологии безопасности внутри облачных платформ. Что с учетом доступности спецслужб развитых стран ставится под сомнение. Таким образом, система управления, которая размещена и реализована на основе облачных технологий (внешний контур безопасности), не в полной мере безопасна. С появлением квантовых компьютеров ста-

вится под сомнение возможность выполнения в полном объеме функций с учетом безопасности.

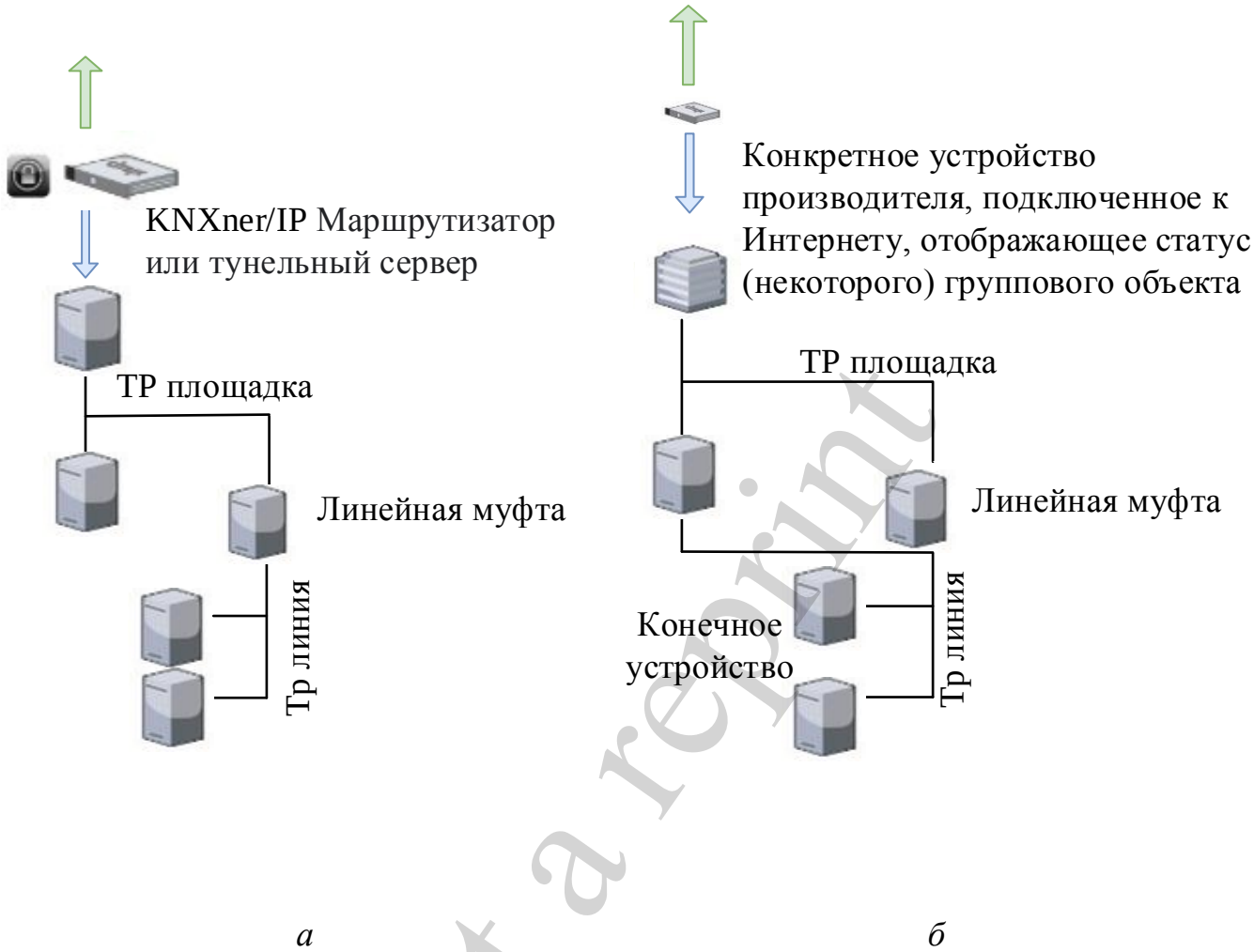


Рис. 3. KNX Data Secure: *а* – KNX IP Secure; *б* – KNX Data Secure

KNX Data Secure позволяет защитить данные пользователя от несанкционированного доступа и манипуляций с помощью механизмов шифрования и аутентификации. Устройства KNX Data Secure используют более длинный формат телеграмм KNX (расширенные кадры), чем обычные устройства, для передачи аутентифицированных и зашифрованных данных.

KNX Data Secure использует режим CCM (счетчик с кодом аутентификации сообщения цепочки блоков шифра) со 128-битным шифрованием AES, что позволяет обеспечить целостность информации. Однако предлагаемые варианты использования стандарта KNX обеспечивает только целостность и не обеспечивает конфиденциальность информации, что существенно снижает общий уровень безопасности циркулирующих в беспроводных мобильных сетях информационных потоков.

Для обеспечения аутентичности в мобильных беспроводных технологиях и сетях используется протокол Diameter. Протокол Diameter имеет предопределен-

ный набор общих атрибутов и назначает каждому атрибуту соответствующую семантику. Эти AVP (Attribute-Value-Pair – пара атрибут-значение) передают подробности AAA (AAA – authentication, authorization, accounting) (такую информацию как маршрутизация, безопасность и возможности) между двумя Diameter-узлами. Кроме того, каждая пара AVP ассоциируется с форматом AVP Data Format, который определен в протоколе Diameter (например, OctetString, Integer32), поэтому значение каждого атрибута должно следовать формату данных [52–56]. Однако протокол Diameter также как и предшествующие протоколы мобильных сетей разработан без учета требований безопасности. поэтому ему присущи практически все угрозы, что и самой технологии “G”.

Разработчики в погоне за сверхскоростями, не задумываются, что развитие вычислительной техники позволяет злоумышленникам (кибертеррористам) “расширить спектр и границы” угроз. Другими словами, рассматривать применение данной технологии для организации “окна” в корпоративные сети и/или локальные сети пользователей.

Как показывает практика, в сетях на основе протокола Diameter возможны атаки, направленные на отказ в обслуживании, раскрытие информации об абонентах и сети оператора, а также мошенничество в отношении оператора.

Кроме этого, злоумышленник может принудительно перевести устройство абонента в режим 3G – и проводить дальнейшие атаки уже на менее защищенную систему SS7.

Целями атак являются прослушивание голосовых вызовов, перехват SMS и осуществление мошеннических схем в отношении абонентов [57, 58]. Таким образом, отсутствие криптоалгоритмов для обеспечения услуг конфиденциальности, целостности приводит к выделению следующих классов “классических” атак (рис. 4).

При этом конфиденциадьность подразумевает защиту данных от пассивных атак при их передаче, целосность – защиту данных при хранении, а аутентичность – подлинность источника сообщения.

Анализ рис. 4 показывает, что при наличии в мобильных беспроводных технологиях только данного протокола не решаются задачи конфиденциальности и целостности. Использование механизмов стандарта KNX обеспечивает эти услуги только внутри инфраструктуры киберфизических систем, и не обеспечивает защиту во внешнем контуре безопасности – платформе на основе облачных технологий. В табл. 1 приведены основные характеристики беспроводных мобильных и компьютерных сетей и услуги безопасности на основе стандарта KNX и протокола Diameter.

Анализ табл. 1 показывает, что в условиях появления полномасштабного квантового компьютера услуги во внутреннем контуре безопасности ставятся под сомнение, из-за квантовых алгоритмов взлома симметричных и несимметричных алгоритмов. Кроме этого, в мобильных технологиях на основе протокола Diameter обеспечиваются только услуги AAA. В современных условиях гибридности и синергизма кибератак это позволяет беспрепятственно получать несанкционирован-

ный доступ как во внутренний, так и во внешний контуры безопасности и практически реализовывать целевые атаки на киберфизические системы.

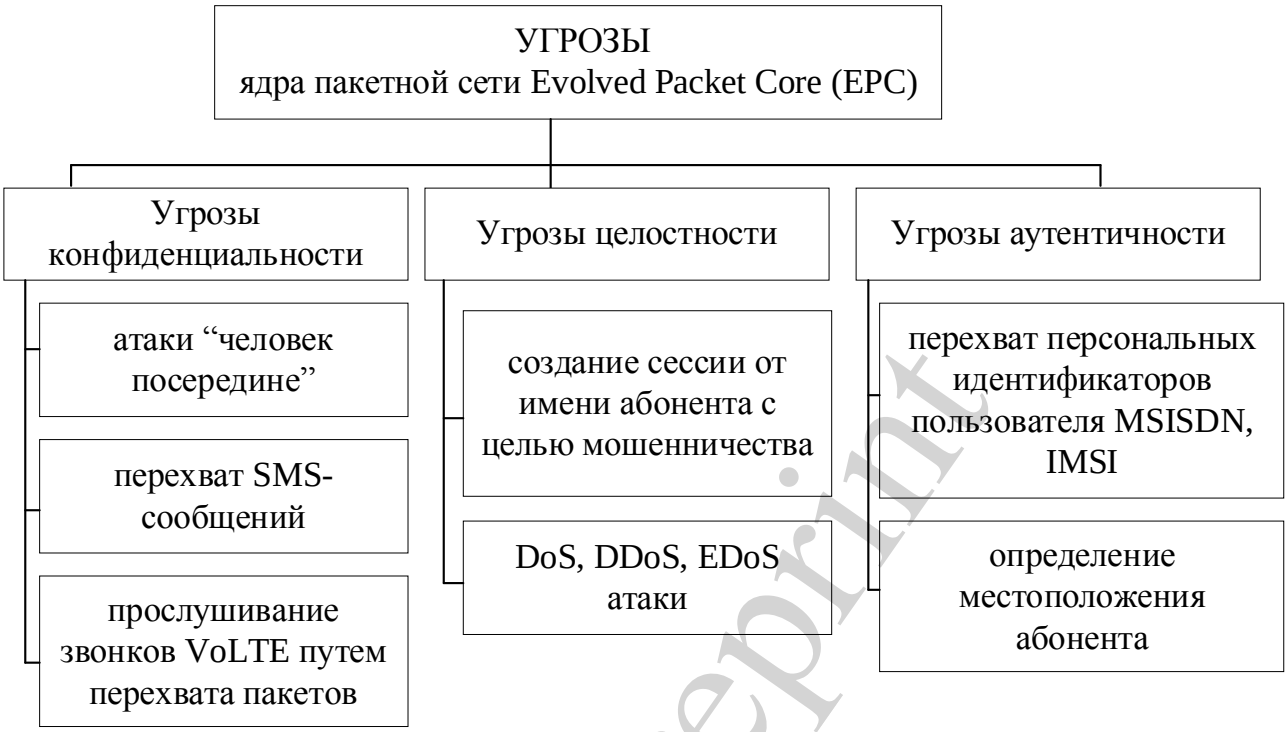


Рис. 4. Основные типы атак на Evolved Packet Core

Для обеспечения развития технологий mesh-, сенсорных сетей с использованием стандартов беспроводных каналов: мобильных технологий LTE, IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth необходимы новые подходы обеспечения услуг безопасности. В условиях появления квантового компьютера (возможного снижения “доверия” к современным криптосистемам на основе симметричной и несимметричной криптографии (включая и криптографию на эллиптических кривых) необходимо не только использование постквантовых криптоалгоритмов, но и новый подход к обеспечению безопасности формируемых на основе синтеза социо-киберфизических систем (socio-cyber-physical systems – SCFS), которые стремительно развиваются на основе смарт- и Интернет-вещей- технологиях.

Для обеспечения услуг безопасности в условиях современных угроз предлагается концепция двухконтурной безопасности на основе постквантовых алгоритмов – крипто-кодовых конструкций Мак-Элиса и Нидеррайтера. При этом предлагается использовать комплексированные решения использования тех или иных кодов в крипто-кодовых системах на основе градации степени секретности информации в социо-киберфизических системах. В табл. 2 приведены соотношения времени и степени секретности информации.

Таблица 1

Таблица технических характеристик беспроводных сетей

Технология	Дальность приема передачи, м	*V*, б/с	топология	Спектр передачи	Модуляция	услуги безопасности									
						до PQ					в PQ				
						C	*I*	*A*	A_u	*B*	*C*	*I*	*A*	A_u	*B*
LTE (4G)	до 13400	до 100 Мбит/с	AIPN	600 МГц до 2,5 ГГц	64QAM	–	–	+	+	–	–	–	–	–/+	–
LTE (5G)	500	20 Гбит/с	Гетерогенная опорная сеть	от 30 ГГц до 300 ГГц	256-QAM	–	–	+	+	–	–	–	–	–/+	–
IEEE 802.11 ac (WiFi 5)	500	до 7 Гбит/с	P2MP	5 ГГц	256-QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.11ax, Wi-Fi 6		9607 Мбит/с	P2MP	5 ГГц	1024-QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.16	5000	32 Мбит/с– 134 Мбит/с	mesh	10-66 ГГц	64QAM O-QPSK	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.16m (Wi-MAX2)	6000	90 Мбит/с– 179 Мбит/с	mesh	11 ГГц	64QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.15.1 Bluetooth 5	200	2–6 Мбит/с	mesh	2,4-2,485 ГГц	64QAM	+	+	+	+	–	–	–	–	–/+	–
IEEE 802.15.4	1000	250 кбит/с	P2P Cluster tree	2,4-2,483 ГГц	BPSK O-QPSK	+	+	+	+	–	–	–	–	–/+	–

Примечание: C – конфиденциальность; *I* – целостность; *A* – доступность; *Au* – аутентичность, *B* –причастность

Такой подход позволит своевременно обеспечивать требуемый уровень безопасности с учетом степени секретности информации и/или безопасного времени, которое необходимо для обеспечения услуг конфиденциальности.

Таблица 2
Соотношение времени и степени секретности информации

Степень секретности информации	Время	Предлагаемые коды для *CCC*
критическая	до 1 года	*MEC*, ущербные коды
высокая	до 1 месяца	*MEC*
средняя	до 1 часа	*EC*
низкая	до 10 минут	*EC*
очень низкая	до 1минуты	LDPC

Таким образом, возникает необходимость формирования концепции безопасности на основе двух контуров (внутреннего – непосредственно безопасности элементов инфраструктуры сети) и внешнего – платформы управления на основе облачных технологий.

5. Результаты разработки концепции безопасности беспроводных сетей на основе крипто-кодовых конструкций

5. 1. Разработка концепции безопасности беспроводных сетей на основе мобильных технологий

Для обеспечения безопасности современных беспроводных сетей и систем, основанных на их инфраструктуре, необходимо учитывать комплексирование внутренней инфраструктуры элементов сети (внутренний контур) и внешней инфраструктуры управления, основанной на облачных платформах.

Синтез внутреннего и внешнего контуров обеспечивает оперативность, энергоемкость и относительную безопасность (каждый контур строит безопасность на своих механизмах и принципах), с одной стороны. С другой стороны, отсутствуют возможности контроля не только механизмов безопасности, которые используются, но и оценки текущего состояния защищенности информационных потоков, которые циркулируют и хранятся в контуре. На рис. 5 представлена структурная схема концепции двухконтурной безопасности социо-киберфизических систем.

Системы безопасности социо-киберфизических систем в большинстве случаев ориентированы на объекты критической инфраструктуры (банковско-финансовый сектор, топливно-энергетический комплекс, сети жизнеобеспечения, телекоммуникации и сети связи, комплекс безопасности и обороны, и т. п.). Для обеспечения безопасности таких систем необходимо учитывать два класса угроз. Первый класс – это угрозы и их комплексирование с методами социальной инженерии внутренней инфраструктуры (внутренний контур безопасности). Второй

класс – угрозы внешнего контура (облачные технологии, которые обеспечивают не только управление социо-киберфизическими системами и сетями, но и хранение/дублирование базы данных). В работах [31, 59] предложены методологические основы построения систем безопасности с учетом синергизма и гибридности современных целевых атак на объекты критической инфраструктуры, что позволяет обеспечить безопасность во внутреннем контуре.

Для обеспечения безопасности всей системы защиты необходимо учитывать угрозы внутреннего и внешнего контуров:

– угрозы внутреннего контура с учетом гибридности и синергизма [59]:

$$W^{SCPS\ ISL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg} = W^{SCPS\ ISL\ C}_{synerg} \cap W^{SCPS\ ISL\ I}_{synerg} \cap \cap W^{SCPS\ ISL\ A}_{synerg} \cap W^{SCPS\ ISL\ Au}_{synerg} \cap W^{SCPS\ ISL\ Inv}_{synerg}, \quad (5)$$

где $W^{SCPS\ ISL\ C}_{synerg}$ – синергия угроз на услугу конфиденциальности, $W^{SCPS\ ISL\ I}_{synerg}$ – синергия угроз на услугу целостности, $W^{SCPS\ ISL\ A}_{synerg}$ – синергия угроз на услугу доступности, $W^{SCPS\ ISL\ Au}_{synerg}$ – синергия угроз на услугу аутентичности, $W^{SCPS\ ISL\ Inv}_{synerg}$ – синергия угроз на услугу причастности.

– угрозы внешнего контура с учетом гибридности и синергизма:

$$W^{SCPS\ ESL}_{\text{hybrid}\ C,I,A,Au,Af\ synerg} = W^{SCPS\ ESL\ C}_{synerg} \cap W^{SCPS\ ESL\ I}_{synerg} \cap \cap W^{SCPS\ ESL\ A}_{synerg} \cap W^{SCPS\ ESL\ Au}_{synerg} \cap W^{SCPS\ ESL\ Inv}_{synerg}, \quad (6)$$

где $W^{SCPS\ ESL\ C}_{synerg}$ – синергия угроз на услугу конфиденциальности, $W^{SCPS\ ESL\ I}_{synerg}$ – синергия угроз на услугу целостности, $W^{SCPS\ ESL\ A}_{synerg}$ – синергия угроз на услугу доступности, $W^{SCPS\ ESL\ Au}_{synerg}$ – синергия угроз на услугу аутентичности, $W^{SCPS\ ESL\ Inv}_{synerg}$ – синергия угроз на услугу причастности.

Каждый элемент информационных ресурсов $I_{A_i} \in \{I_A\}$ может быть описан вектором $I_{A_i} = \left(Type_i, A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}, \beta_i\right)$. $Type_i$ – тип информационного актива, описывается множеством базовых значений: $Type_i$={CI_i, PD_i, CD_i, TS_i, StR_i, $PubI_i$, $ContI_i$, PI_i}, где CI_i – конфиденциальная информация, PD_i – платежные документы, CD_i – кредитные документы, TS_i – коммерческая тайна, StR_i – статистические отчеты, $PubI_i$ – общедоступная информация, $ContI_i$ – управляющая информация, PI_i – персональные данные. $A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}$ – услуги безопасности (A_i^C – конфиденциальность, A_i^I – целостность, A_i^A –доступность, A_i^{Au} – аутентичность, A_i^{Inv} – принадлежность); β_i – метрика соотношения времени и степени секретности информации для актива (критическая – 1,0; высокая – 0,75; средняя – 0,5; низкая – 0,25; очень низкая – 0,01).

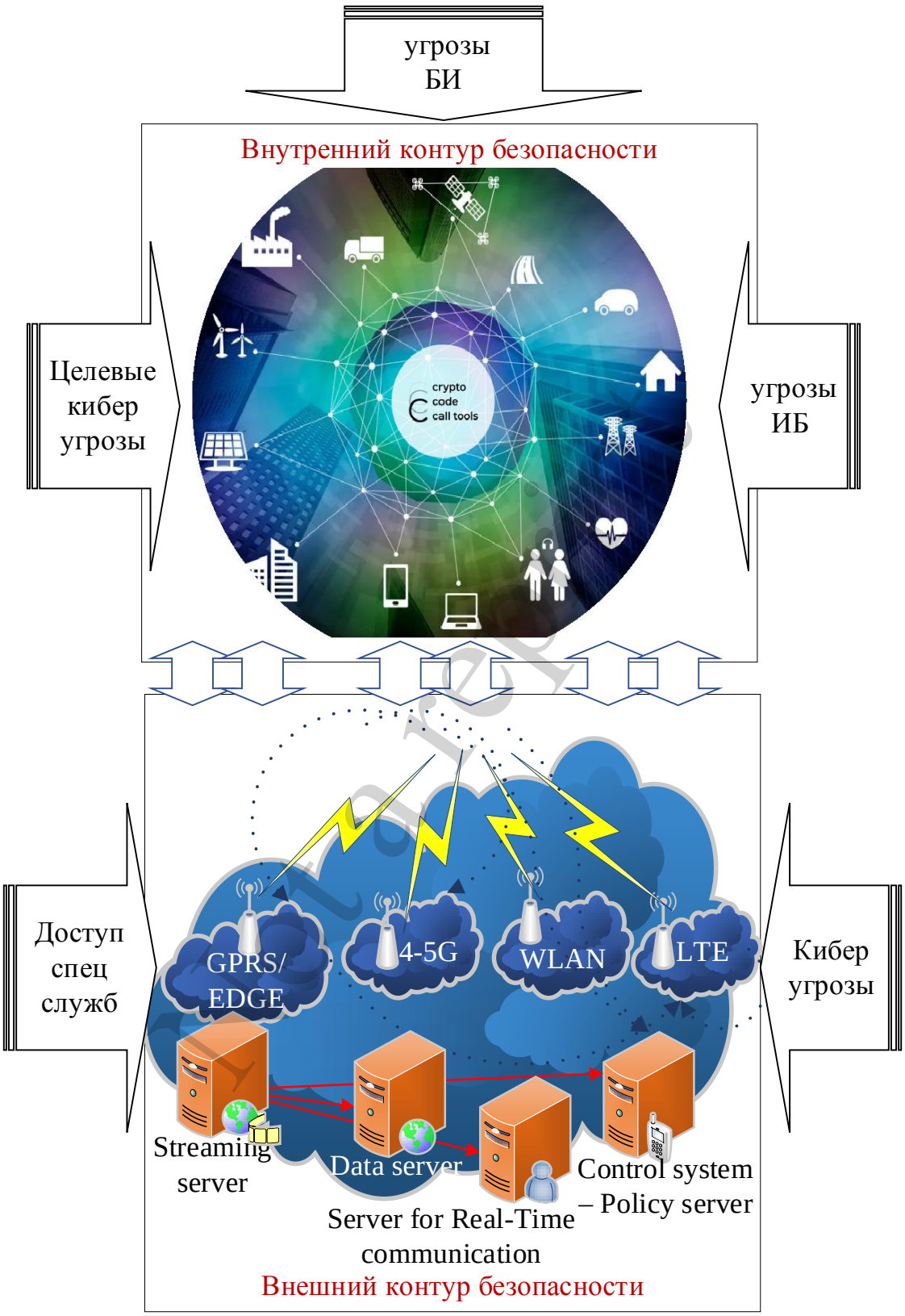


Рис. 5. Структурная схема концепции двухконтурной безопасности социо-киберфизических систем

Тогда общий (текущий) уровень защищенности социо-киберфизических систем на основе беспроводных мобильных технологий описывается выражением:

– для аддитивной свертки

$$L_{W_{\text{security}}^{SCPS}} = \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ISL}} \sum_{i=1}^{8} \left(I_{A_i} \times \beta_i \right) + \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ESL}} \sum_{i=1}^{8} \left(I_{A_i} \times \beta_i \right); \quad (7)$$

– для мультипликативной свертки

$$L_{W_{\text{security}}^{SCPS}} = 1 - \left\lceil 1 - \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ISL}} \sum_{i=1}^{8} \left(I_{A_i} \times \beta_i \right) \right\rceil \times \left\lceil 1 - \sum_{W_{\text{hybrid}\,C,I,A,Au,Af\,synerg}^{SCPS\ ESL}} \sum_{i=1}^{8} \left(I_{A_i} \times \beta_i \right) \right\rceil. \quad (8)$$

В (7), (8) индекс i относится к соответствующему типу информационного актива, а внешнее суммирование производится по всем угрозам внутреннего и внешнего контуров.

Предлагаемая Концепция двух контуров безопасности обеспечивает комплексирование и учитывает возможности целевых кибератак, их синергизм, гибридность и возможность комплексирования в условиях роста вычислительных ресурсов и расширения спектра смарт-технологий.

5. 2. Разработка математических моделей крипто-кодовых конструкций Мак-Элиса и Нидеррайтера на LDPC-кодах

Для реализации крипто-кодовых конструкций на LDPC-кодах воспользуемся подходами работ [29–31, 60].

Исходными данными для математических моделей *CCC* Мак-Элиса и Нидеррайтера являются:

– множество открытых текстов для *CCC* Мак-Элиса $M = \left\{ M_1, M_{2,} \ldots M_{q^k} \right\}$, где $M_i = \{ I_0, I_{h_1}, \ldots I_{h_j}, I_{k\text{-}1} \}$, $\forall I_j \in GF(q)$, h_j – информационные символы равные нулю, $|h| = \frac{1}{2} k$, т. е. I_i=0, $\forall I_i \in h$; для *CCC* Нидеррайтера $M_i = \left\{ e_0, e_{h_1,} \ldots e_{h_k}, e_{e-1} \right\}$, $\forall e_e \in GF(q)$, h_e – символы вектора ошибки, которые равняются нулю, $|h| = \frac{1}{2} e$, то есть e_i=0, $\forall e_i \in h$. На основе алгоритма равновесного кодирования открытый текст преобразуется в вектор ошибки;

– множество закрытых текстов (кодограмм) для *CCC* Мак-Элиса $C = \left\{ C_1, C_2, ..., C_{q^k} \right\}$, где $C_i = \left(c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}} \right)$, $\forall c^*_{X_j} \in GF(q)$; для *CCC* Нидеррайтера $S = \left\{ S_0, S_1, ... S_{q^r} \right\}$, где $S_i = \left\{ S^*_{X_0}, S^*_{h_1}, ... S^*_{h_j}, S^*_{X_r} \right\}$, $\forall S_{X_r} \in GF(q)$;

– множество прямых отображений (на основе использования открытого ключа – порождающей/проверочной матрицы LDPC–коду:

а) для *CCC* Мак-Элиса – $\phi=(\phi_1, \phi_2, \ldots, \phi_s)$, где $\phi_i : M \to C_{k-h_j}$, $i=1, 2,\ldots, s$;

б) для *CCC* Нидеррайтера – $\varphi=(\varphi_1, \varphi_2, \ldots, \varphi_r)$, где $\varphi_i : M \to S_{r-h_e}$, $i=1, 2, \ldots, e$;

– множество обратных отображений (на основе использования закрытого (личного) ключа – матриц маскировки):

а) для *CCC* Мак-Элиса – $\phi^{-1} = \left\{ \phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1} \right\}$, где $\phi_i^{-1} : C_{k-h_j} \to M$, $i = 1, 2, ..., s$;

б) для *CCC* Нидеррайтера – $\varphi^{-1} = \left\{ \varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_r^{-1} \right\}$, де $\varphi_i^{-1} : S_{r-h_e} \to M$, $i = 1, 2, ..., e$.

– множество ключей, параметризирующих прямые отображения (открытый ключ уполномоченного пользователя):

а) для *CCC* Мак-Элиса – $KU_i = \left\{ KU_1, KU_2, ..., KU_S \right\} = \left\{ G_1^{LDPC}, G_2^{LDPC}, ..., G_S^{LDPC} \right\}$, где $G^{LDPC_i}_{X_{a_i}}$ – порождающая $n \times k$ матрица замаскированного под случайный код. Матрица определяется из ортогональности матриц порождающей и проверочной.

б) для *CCC* Нидеррайтера – $KU_i=\{KU_1, KU_2, \ldots, KU_r\}=\{H_1, H_2, \ldots, H_r\}$, где $H^{LDPC_i}_{X_{a_i}}$ – проверочная $(N\text{-}K)\times N$ матрица определяет $(N–K)$ проверочных символов $P_1, P_2, \ldots, P_{N\text{-}K}$ в виде линейной комбинации информационных символов d_k, $k=1, 2, \ldots, K$;

– множество личных (закрытых) ключей пользователей:

$$KR = \left\{ KR_1, KR_2, ..., KR_r \right\} = \left\{ \left\{ X, P, D \right\}_1, \left\{ X, P, D \right\}_2, ..., \left\{ X, P, D \right\}_r \right\},$$

$$\left\{ X, P, D \right\}_i = \left\{ X^i, P^i, D^i \right\},$$

где X^i – маскирующая невырожденная случайно равновероятно сформированная источником ключей $k\times k$ матрица с элементами из $GF(q)$; P^i – перестановочная случайно равновероятно сформированная источником ключей $n\times n$ матрица с элементами из $GF(q)$; D^i – диагональная сформированная источником ключей $n\times n$ матрица с элементами из $GF(q)$. За счет того, что диагональная матрица равна единичной матрице, значением можно пренебречь, что дает уменьшение емкости и сложности вычисления.

Открытый ключ формируется путем перемножения матриц маскировки на порождающую/проверочную матрицы:

– для *CCC* Мак-Элиса – $G_{X_{a_i}}^{LDPCu} = X^u \times G^{LDPCu} \times P^u,\ u \in \{1,2,\ldots,s\}$;

– для *CCC* Нидеррайтера – $H_{X_{a_i}}^{LDPCu} = X^u \times H^{LDPCu} \times P^u,\ u \in \{1,2,\ldots,r\}$.

В канал связи поступает:

– для *CCC* Мак-Элиса – кодовое слово: $C_j = M_i \times G_{X_{a_i}}^{LDPCu^T} + e$, где e – дополнительный сеансовый ключ каждой информационной посылки;

– для *CCC* Нидеррайтера – синдромная последовательность:

$$S^* = (e_n) \times H_{X_{a_i}}^{LDPC^T}.$$

На приемной стороне уполномоченный пользователь, знающий матрицы маскировки, использует быстрый алгоритм на основе мягкого декодирования.

На рис. 6 представлена структурная схема декодирования полученной последовательности на основе мягкого декодирования.

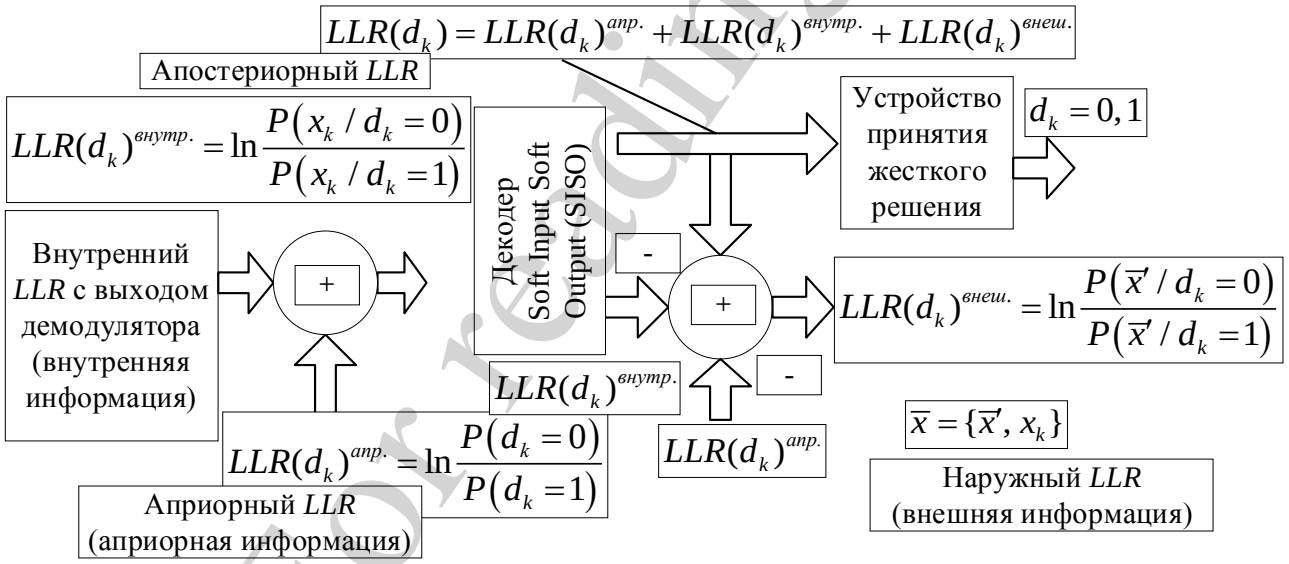


Рис. 6. Схема декодирования на основе мягкого решения

На схеме введены следующие обозначения: *LLR – log-likelihood ratio* (логарифм отношения правдоподобия); d_k – символ кодового слова, $d_{ij} \in \{0, 1\}$, $x_k=(2d_k-1)+p_k$, p_k – случайная величина, имеющая нормальное распределение с нулевым средним значением.

Анализ рис. 8 показывает, что мягкое решение представляет собой логарифм отношения правдоподобия (апостериорный LLR). Мягкое решение можно представить совокупностью априорной, внутренней и внешней информации. Принятие

жесткого решения для некоторого символа осуществляется на основе апостериорного LLR. Знак логарифма по отношению к правдоподобию определяет жесткое решение, а величина – надежность этого решения.

Проверочная матрица имеет размерность $(N–K)\times N$ и позволяет выразить $(N–K)$ проверочных символов $P_1, P_2, \ldots, P_{N-K}$ в виде линейной комбинации информационных символов d_k, k=1, 2, …, K, то есть определяет проверочные уравнения:

$$\begin{cases} P_1 = c_{11}d_1 \oplus c_{21}d_2 \oplus \ldots \oplus c_{k1}d_K, \\ P_2 = c_{12}d_1 \oplus c_{22}d_2 \oplus \ldots \oplus c_{k2}d_K, \\ \ldots \\ P_{N-K} = c_{1\,N-K}d_1 \oplus c_{2\,N-K}d_2 \oplus \ldots \oplus c_{K\,N-K}d_K, \end{cases} \tag{9}$$

где c_{ij} – элементы подматрицы A, $c_{ij}\in\{0,1\}$. Если d_k, k=1, 2, …, K – статистически независимые символы, принимающие значения 0 и 1 и которые, в общем случае, соответствуют информационным символам блокового кода, а $\beta_k=(2d_k–1)=\pm1$.

При таком формате результат добавления символов β_k по модулю два будет выглядеть так:

$$\begin{cases} \beta_1 \oplus \beta_2 = -1, \text{если } \beta_1 = \beta_2, \\ \beta_1 \oplus \beta_2 = +1, \text{если } \beta_1 \neq \beta_2. \end{cases} \tag{10}$$

Тогда логарифм отношения правдоподобия суммы по модулю – два символов β_k – $LLR(\beta_1 \oplus \beta_2 \oplus \ldots \oplus \beta_K)$ можно записать следующим образом [60]:

$$LLR(\beta_1 \oplus \beta_2 \ldots \oplus \beta_k \oplus \ldots \oplus \beta_K) = \ln\left[\frac{\sum_k e^{LLR(\beta_k)}}{1+\prod_k e^{LLR(\beta_k)}}\right]. \tag{11}$$

Выражение (11) можно аппроксимировать как:

$$\begin{aligned} &LLR(\beta_1 \oplus \beta_2 \ldots \oplus \beta_k \oplus \ldots \oplus \beta_K) \approx \\ &\approx -1 \cdot \left[\prod_k \operatorname{sign}\{LLR(\beta_k)\}\right]\left[\min_k \{|LLR(\beta_k)|\}\right], \end{aligned} \tag{12}$$

где функция sign(•) возвращает знак своего аргумента.

Каждое проверочное уравнение (9) позволяет выразить один символ (независимо от того, является ли он информационным или проверочным) через сумму по модулю два всех других символов, входящих в это проверочное уравнение.

Исходными данными алгоритма являются: проверочная матрица H блочного (N, K) кода, последовательность мягких решений для информационных и проверочных символов с выхода демодулятора.

Алгоритм декодирования LDPC-кодах:

Шаг 1. Определяем оценку надежности для каждого кодового символа (для каждого информационного и проверочного символа) кодового слова на основании мягких решений по выходу демодулятора путем вычисления их абсолютной величины (пренебрегаем знаком мягких решений в последовательности выхода демодулятора).

Шаг 2. Для строки проверочной матрицы H с номером i, i=1… N–K:

1) находим кодовый символ, соответствующий ненулевому (единичному) значению элементов строки с номером i матрицы H. Это значит, что кодовый символ входит в состав проверочного уравнения, определяемого строкой с номером i, и имеет самое низкое значение оценки надежности (наименее надежный символ). Фиксируем номер столбца j, j=1… N проверочной матрицы H, которому соответствует найденный наименее надежный символ;

2) преобразуем проверочную матрицу H путем линейного комбинирования ее строк. Линейное комбинирование производится с целью исключения зависимости других проверочных уравнений (определяемых другими строками проверочной матрицы) от найденного наименее надежного символа. Это будет достигнуто, когда столбец матрицы H с номером j будет иметь только одну единицу, содержащуюся именно в рассматриваемой строке с номером i;

3) повторяем предварительные процедуры 1 и 2 для каждой из строк проверочной матрицы H, после чего переходим к следующему шагу.

Шаг 3. Осуществляем жесткое декодирование K символов, имеющих наивысшее значение для оценки надежности (наиболее надежные символы).

Шаг 4. Для каждого из K наиболее надежных символов:

1) находим мягкие решения с использованием двух пробных кодовых последовательностей (гипотез). Одна пробная последовательность формируется путем повторного кодирования результата жесткого декодирования K наиболее надежных символов, полученных на Шаге 3 (первая гипотеза). Другая формируется путем повторного кодирования результата жесткого декодирования K наиболее надежных символов, полученных на шаге 3, но с дополнительной инверсией символа, для которого находится мягкое решение (вторая гипотеза);

2) находим жесткое решение на основании мягкого решения, полученного на предварительной процедуре.

Шаг 5 (необязательный). Обновляем оценку надежности каждого кодового символа и переходим к Шагу 1 на следующую итерацию.

Таким образом, представленный алгоритм позволяет обеспечить оперативность выполнения декодирования и обеспечивает использование LDPC-кодов в крипто-кодовых конструкциях Мак-Элиса и Нидеррайтера. Такой подход позволяет варьировать, в зависимости от степени секретности информации в выборе помехоустойчивого кода для крипто-кодовых конструкций, и обеспечения требуемого уровня безопасности.

5. 3. Разработка способов практической реализации крипто-кодовых конструкций Мак-Элиса и Нидеррайтера

Примерами практической реализации таких систем является, предлагаемый в работе [60] протокол обеспечения безопасности голосовых сообщений в онлайн режиме на основе *CCC* Мак-Элиса и Нидеррайтера на *EC* (*MEC*), который представлен на рис. 7. На рис. 8 представлена практическая реализация предлагаемой Концепции и крипто-кодовых конструкций на LDPC-кодах. Предлагаемый протокол обеспечения безопасности в киберфизических системах (“Умный дом”) основывается на использовании двухконтурной концепции безопасности и постквантовых алгоритмах.

Так, на рис. 7 для обеспечения безопасности голосовых сообщений предлагается использовать программно-аппаратный шифратор, который встраивается в гарнитуру наушников (предлагается использовать Bluetooth-наушники) и обеспечивает шифрование цифрового сообщения на основе *CCC* Мак-Элиса. После чего зашифрованное сообщение передается через Bluetooth-канал в мобильный гаджет. При этом используются стандартные протоколы мобильного Интернет-канала GSM. Это позволяет обеспечивать конфиденциальность разговора без учета требований канала связи, требований производителей гарнитуры и мобильных гаджетов, не учитывать модификации, как Bluetooth-канала, так и технологии мобильного Интернет.

Кроме этого, использование программно-аппаратной реализации шифратора в виде чипсета позволяет существенно снизить затраты на производство и реализацию данного подхода. Для обеспечения безопасности в наушниках записывается только сеансовый пароль в зависимости от роли (отправитель, получатель), которые записываются из мобильного приложения.

После окончания разговора они удаляются. При этом в чипсете реализуется шифратор на *CCC* Мак-Элиса. Обеспечение безопасности передачи ключевых данных между мобильным приложением и сервером обеспечивается *CCC* Нидеррайтера. Для обеспечения безопасности серверной части после генерации ключей для проведения разговора и их передачи отправителю и получателю – проводится обнуление ОП сервера, что обеспечивает туннелирование канала между пользователями. Секретные ключи крипто-кодовых конструкций Мак-Элиса и Нидеррайтера меняются с разными промежутками времени, и являются OTP-ключами (сеансовыми ключами).

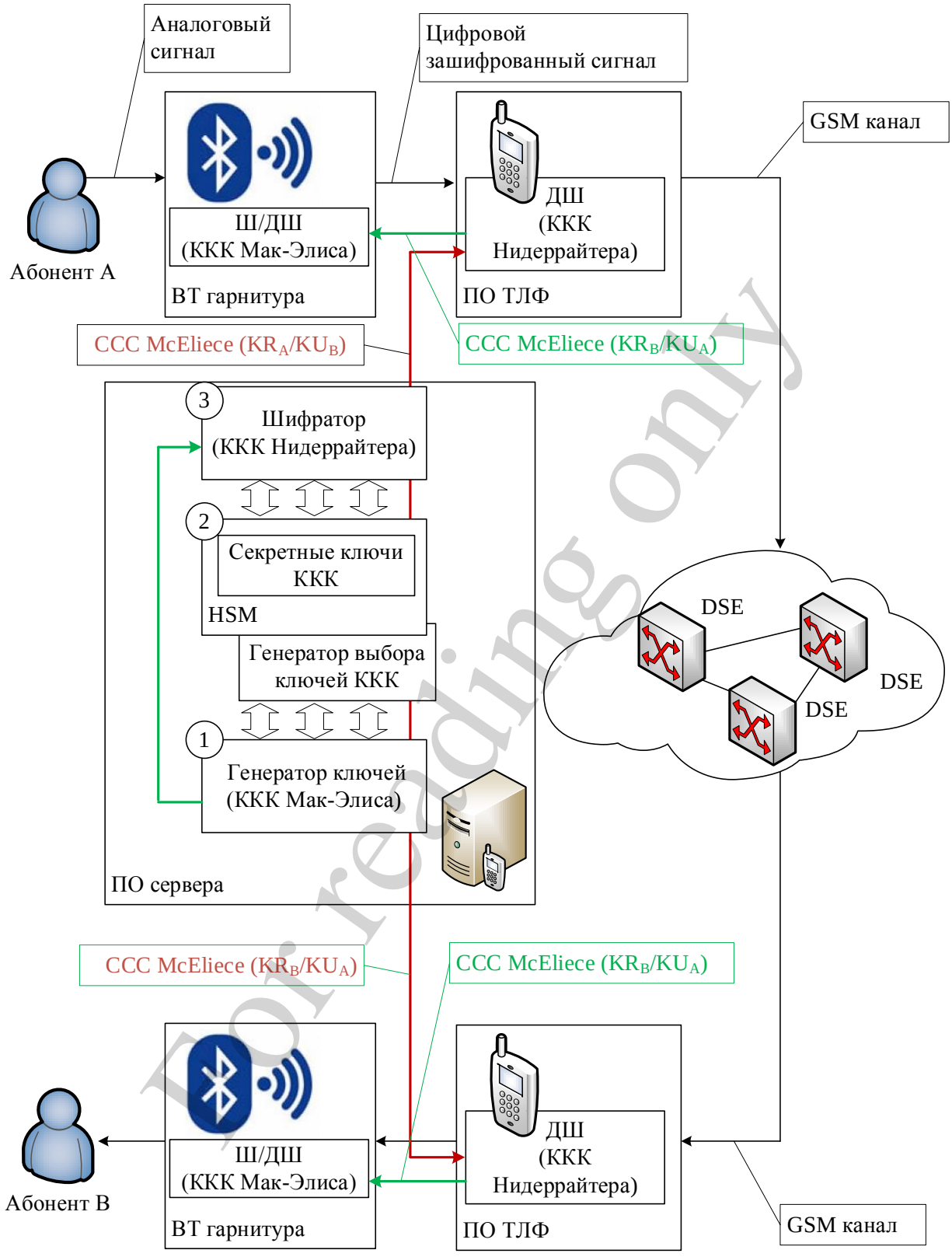


Рис. 7. Структурная схема построения двухконтурной системы защиты информации на *CCC* для обеспечения конфиденциальности голосовых сообщений

Рассмотрим протокол обеспечения безопасности голосового сообщения на основе постквантовых алгоритмов:

АБОНЕНТ А (инициатор звонка).

1. Открывает ПО ТЛФ и в списке абонентов находи соответствующего абонента (АБОНЕНТ В)

2. Отправляет запрос абоненту В через сервер.

3. Получает на ПО тлф через закрытый канал (используется шифрование на основе *CCC* Нидеррайтера на *EC*) личный ключ, и открытый ключ абонента В.

4. Подтверждает готовность к разговору. При этом из ПО тлф по Bluetooth-каналу передается личный ключ (KR_A) и открытый ключ KU_B.

5. В Bluetooth-наушниках в шифраторе (Ш/ДШ) происходит запись ключа.

6. После записи ключа формируется сигнал о готовности.

7. После подтверждения о готовности абонента В осуществляется разговор.

ПО СЕРВЕРА.

1. По запросу абонента А в (2) Генератор выбора ключей *CCC* рандомно выбирает параметры ключей и передает в (1).

2. В (1) поступают из GSM секретные ключи (матрицы маскировки – X, P, D, и порождающая матрица G^{EC}).

3. В (1) формируются KR_A (личный ключ *CCC* Мак-Элиса абонента А) и KU_A (открытый ключ абонента А).

4. По отклику абонента В формируется открытый ключ KU_B и передается абоненту А.

5. В (3) из (1) поступают сгенерированные KR_A и KU_A, после передачи ключей в (1) стираются данные.

6. В (3) шифруются KR_A и KU_A, KU_B.

7. Из (3) отправляются соответственно KR_A, KU_B – абоненту А (абонент, который инициирует звонок), KU_A – абоненту В (абонент, которому звонят), после передачи ключей в (3) стираются данные.

АБОНЕНТ В (получатель звонка).

1. Получает запрос от сервера в ПО тлф на передачу открытого ключа (KU_A).

2. Подтверждает запрос на сервер, отправляет KR_B.

3. Получает на ПО тлф через закрытый канал (используется шифрование на основе *CCC* Нидеррайтера на EC) открытый ключ KU_A.

4. Подтверждает готовность к разговору. При этом из ПО тлф по Bluetooth-каналу передается открытый ключ (KU_A).

5. В Bluetooth-наушниках в дешифраторе (Ш/ДШ) происходит запись ключа.

6. После записи ключа формируется сигнал о готовности.

7. После подтверждения о готовности абонент В передает сигнал на сервер о готовности к разговору.

Таким образом, предложенный протокол обеспечивает закрытие мобильного Интернет-канала с использованием комплекса программно-аппаратных средств. Использование аппаратного решения закрытия (шифрования) голосового сообще-

ния в гарнитуре наушников обеспечит противодействие практически всех угроз, а использование сервера ключей обеспечивает туннельный режим, что исключает возможность “подслушки” голосовых сообщений.

На рис. 8 для обеспечения безопасности в киберфизических системах предлагается использовать *ССС* Мак-Элиса и Нидеррайтера на LDPC-кодах.

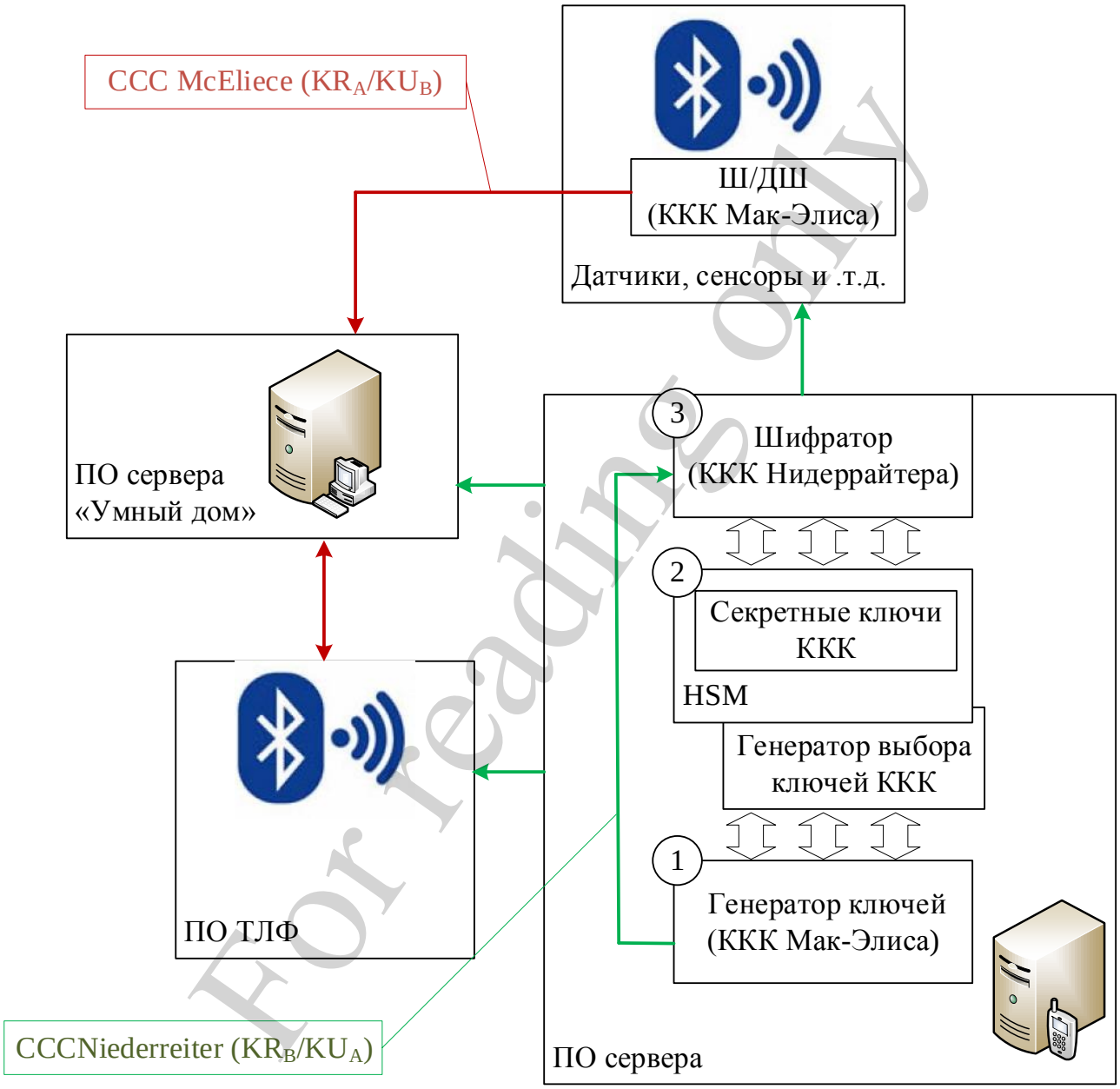


Рис. 8. Структурная схема построения двухконтурной системы защиты системы “Умный дом” на основе *ССС*

Использование данных постквантовых несимметричных криптосистем обеспечит требуемый уровень защищенности при обеспечении услуг безопасности. Использование LDPC кодов позволяет без существенных изменений использовать

мобильные беспроводные технологии на основе стандартов IEEE802.11ac, IEEE802.11ax, IEEE802.16m, IEEE802.15.1, IEEE802.15.4. Система умный дом управляет комплексом автономных систем, каждая из которых управляет определенными устройствами в доме, соединяя их общую киберфизическую систему. Однако для обеспечения безопасности внешнего контура (системы управления и хранения информации) предлагается использовать разработанный сервер, который физически размещается в доме.

Каждая система отправляет пакет данных на локальный сервер, что позволяет управлять домом в отсутствии интернета, находясь в той же локальной сети (будучи подключенным к WI-FI-роутеру). Информация в сети киберфизической системы передается по открытым беспроводным каналам с шифрованием на основе *CCC* Мак-Элиса и Нидеррайтера на LDPC-кодах.

Такой подход обеспечивает услуги безопасности, а за счет использования локального сервера управления обеспечивает снижение вероятности целевых атак на получение несанкционированного доступа к системе управления “Умным домом”. Также подход обеспечивает требуемый уровень безопасности при использовании мобильных приложений управления, на основе использования *CCC* Мак-Элиса и Нидеррайтера на LDPC-кодах. Для обеспечения безопасности базы данных могут использоваться *CCC* Мак-Элиса и Нидеррайтера на *EC* (*MEC*), что значительно затруднит возможность реализации кибератак класса R2L (Remote to Local (user) Attack – удаленная атака на локального пользователя).

6. Обсуждение результатов применения крипто-кодовые конструкций Мак-Элиса и Нидеррайтера на LDPC-кодах

Предлагаемый подход обеспечения в *SCFS* основан на Концепции двухконтурной построения системы защиты безопасности, постквантовых алгоритмах – крипто-кодовых конструкциях Мак-Элиса и Нидеррайтера на различных кодах. Такой подход обеспечивает комлексированный системный подход в построении двух контуров системы защиты информации, учитывает признаки синергизма и гибридности целевых атак и обеспечивает полноценное целенаправленное развитие смарт-технологий и технологий на основе беспроводных мобильных систем. В табл. 2 приведены сравнительные характеристики использования крипто-кодовых конструкций в постквантовый период, с учетом комплексирования с различными стандартами беспроводных и мобильных Интернет-технологий, а также с учетом критичности (степени секретности) информации.

Анализ табл. 2 показывает, что применение классических (симметричных) криптосистем на основе блочных и поточных шифров (которые используются в стандарте KNX) не обеспечивают услуги конфиденциальности и целостности в полном объеме. Применение для обеспечения распределения ключевых данных для симметричных криптосистем, а также услуг аутентичности и причастности. Кроме этого, использование криптосистем на основе эллиптических кривых также

не обеспечивает требуемый уровень стойкости к алгоритмам взлома на основе квантовых вычислений.

Таблица 2

Сравнительные характеристики беспроводных и мобильных интернет-технологий

Технология	Обеспечение услуг безопасности					Степень секретности информации (β_i)				
	A_i^C	A_i^I	A_i^A	A_i^{Au}	A_i^{Inv}	1,0	0,75	0,5	0,25	0,01
LTE (4G), LTE (5G)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11 ac (WiFi 5)	–	–	+	–/+	–/+	–	–	–	–	–
IEEE 802.11ax, Wi-Fi 6+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.16+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE802.16m (WiMAX2)	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.1 Bluetooth 5+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
IEEE 802.15.4+KNX	–/+	–/+	+	–/+	–/+	–	–	–	+	+
Мобильные технологии+*CCC* на *EC* (*MEC*)	+	+	+	+	+	+	+	+	+	+
Мобильные технологии+*HCCC* на *EC* (*MEC*)	+	+	+	+	+	+	+	+	+	+
Мобильные технологии+*CCC* на *LDPC-кодах*	+	+	+	+	+	–	–	+	+	+

Таким образом, для обеспечения безопасности в *SCFS* предлагается использовать постквантовые алгоритмы – крипто-кодовые конструкции, которые, в отличие, от современных механизмов услуг безопасности (стандарты KNX, IEEE802.11h, IEEE802.16e – используют симметричные алгоритмы шифрования) позволяют обеспечить требуемый уровень криптостойкости. Кроме этого, крипто-кодовые конструкции на предлагаемых алгебраических и/или алгеброгеометрических кодах позволяют интегрированно обеспечить повышение уровня достоверности (за счет своих свойств исправления ошибок), оперативность (по скорости криптопреобразований совместимы с алгоритмами симметричной криптографии) и требуемый уровень энергоемкости, результаты сравнительных исследований по критериям криптостойкости, оперативности, энергоемкости приведены в работах [29–32]. Синтез предлагаемой Концепции с предлагаемыми технологиями на основе *CCC* (*HCCC*) позволит не только обеспечить требуемый уровень основных критериев современных беспроводных сетей, но и принципиально изменить методологические основы построения систем безопасности в *SCFS*.

7. Выводы

1. Развитие вычислительных ресурсов, квантовых компьютеров и бурный рост использования беспроводных и мобильных технологий позволяет формировать и развивать смарт-технологии, новые форматы сетей, которые основываются на их синтезе с классическими сетями. Однако, в погоне за сверхскоростями и цифровизацией разработчики не уделяют должного внимания безопасности таких систем. Формирование социо-киберфизических систем на основе комплексирования и синтеза беспроводных технологий и мобильных Интернет-технологий, с Интернет-вещами, с одной стороны, обеспечивают дальнейшее развитие цифровых услуг. С другой стороны, формируют незащищенные критические точки, которые используют киберпреступники в коростных целях. Появление полномасштабного квантового компьютера только усугубляет возможность обеспечить требуемый уровень безопасности. Кроме этого, использование облачных технологий требует переоценки подходов к формированию системы безопасности. В таких условиях, предлагаемый подход использования двухконтурной системы безопасности является актуальным и своевременным. Предлагаемая концепция позволяет не только учитывать признаки синергизма и гибридности современных угроз, но и обеспечивает объективный подход к оценке текущего уровня защищенности в социо-киберфизических системах.

2. Использование для обеспечения безопасности постквантовых криптосистем-крипто-кодовых конструкций обеспечивает своевременный переход на алгоритмы постквантового периода. Такой подход обеспечивает требуемый уровень защищенности услуг безопасности, а использование различных кодов, позволяет с учетом стоимости (степени секретности) информации обеспечить ее безопасность при использовании современных стандартов беспроводных каналов связи. При этом стоимость безопасности предлагается оценивать не количественной оценкой ущерба при ее компрометации, а временем ее актуальности, что позволяет варьировать использованием в *ССС* помехоустойчивых кодов.

3. Практические способы реализации постквантовых алгоритмов обеспечивает решение комплекса задач – обеспечения требуемого уровня безопасности (при реализации услуг безопасности), оперативности и достоверности информационных потоков. Использование как программных, так и программно-аппаратных реализаций *ССС* Мак-Элиса и Нидеррайтера на различных кодах позволяет выделить их в отдельное направление обеспечения услуг безопасности и достоверности. Такой подход существенно может упростить вопросы безопасности в бурно развивающихся направлений *SCFS*, смарт- и mesh- технологиях.

Литература

1. Branco, P. de M. (2017). A new LDPC-based McEliece cryptosystem. Tecnico Lisboa, 79. URL: https://fenix.tecnico.ulisboa.pt/downloadFile/1970719973967111/Thesis.pdf
2. Engelbert, D., Overbeck, R., Schmidt, A. (2007). A Summary of McEliece-Type Cryptosystems and their Security. Journal of Mathematical Cryptology, 1 (2). doi: https://doi.org/10.1515/jmc.2007.009
3. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P. S. L. M. (2012). MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes. URL: https://eprint.iacr.org/2012/409.pdf
4. Baldi, M., Bodrato, M., Chiaraluce, F. (2008). A New Analysis of the McEliece Cryptosystem Based on QC-LDPC Codes. Security and Cryptography for Networks, 246–262. doi: https://doi.org/10.1007/978-3-540-85855-3_17
5. Chang, K. (2012). I.B.M. Researchers Inch Toward Quantum Computer. The New York Times. URL: http://www.nytimes.com/2012/02/28/technology/ibm-inch-closer-on-quantum-computer.html?_r=1&hpw
6. Eisenbarth, T., Güneysu, T., Heyse, S., Paar, C. (2009). MicroEliece: McEliece for Embedded Devices. Cryptographic Hardware and Embedded Systems - CHES 2009, 49–64. doi: https://doi.org/10.1007/978-3-642-04138-9_4
7. Ghosh, S., Delvaux, J., Uhsadel, L., Verbauwhede, I. (2012). A Speed Area Optimized Embedded Co-processor for McEliece Cryptosystem. 2012 IEEE 23rd International Conference on Application-Specific Systems, Architectures and Processors. doi: https://doi.org/10.1109/asap.2012.16
8. Heyse, S. (2011). Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices. Lecture Notes in Computer Science, 143–162. doi: https://doi.org/10.1007/978-3-642-25405-5_10
9. Persichetti, E. (2012). Compact McEliece keys based on quasi-dyadic Srivastava codes. Journal of Mathematical Cryptology, 6 (2). doi: https://doi.org/10.1515/jmc-2011-0099
10. Minder, L. (2007). Cryptography Based on Error Correcting Codes. Lausanne. doi: https://doi.org/10.5075/epfl-thesis-3846
11. Overbeck, R., Sendrier, N. (2009). Code-based cryptography. Post-Quantum Cryptography, 95–145. doi: https://doi.org/10.1007/978-3-540-88702-7_4
12. Bernstein, D. J., Lange, T., Peters, C. (2008). Attacking and Defending the McEliece Cryptosystem. Lecture Notes in Computer Science, 31–46. doi: https://doi.org/10.1007/978-3-540-88403-3_3
13. Cayrel, P.-L., Hoffmann, G., Persichetti, E. (2012). Efficient Implementation of a CCA2-Secure Variant of McEliece Using Generalized Srivastava Codes. Lecture Notes in Computer Science, 138–155. doi: https://doi.org/10.1007/978-3-642-30057-8_9

14. Misoczki, R., Barreto, P. S. L. M. (2009). Compact McEliece Keys from Goppa Codes. Lecture Notes in Computer Science, 376–392. doi: https://doi.org/10.1007/978-3-642-05445-7_24

15. Faugère, J.-C., Otmani, A., Perret, L., Tillich, J.-P. (2010). Algebraic Cryptanalysis of McEliece Variants with Compact Keys. Lecture Notes in Computer Science, 279–298. doi: https://doi.org/10.1007/978-3-642-13190-5_14

16. Berger, T. P., Cayrel, P.-L., Gaborit, P., Otmani, A. (2009). Reducing Key Length of the McEliece Cryptosystem. Lecture Notes in Computer Science, 77–97. doi: https://doi.org/10.1007/978-3-642-02384-2_6

17. Baldi, M., Chiaraluce, F. (2007). Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes. 2007 IEEE International Symposium on Information Theory. doi: https://doi.org/10.1109/isit.2007.4557609

18. Baldi, M., Chiaraluce, F., Garello, R. (2006). On the Usage of Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. 2006 First International Conference on Communications and Electronics. doi: https://doi.org/10.1109/cce.2006.350824

19. Baldi, M., Chiaraluce, F., Garello, R., Mininni, F. (2007). Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem. 2007 IEEE International Conference on Communications. doi: https://doi.org/10.1109/icc.2007.161

20. Monico, C., Rosenthal, J., Shokrollahi, A. (2000). Using low density parity check codes in the McEliece cryptosystem. 2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060). doi: https://doi.org/10.1109/isit.2000.866513

21. Otmani, A., Tillich, J.-P., Dallot, L. (2010). Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Mathematics in Computer Science, 3 (2), 129–140. doi: https://doi.org/10.1007/s11786-009-0015-8

22. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P. S. L. M. (2013). MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. 2013 IEEE International Symposium on Information Theory. doi: https://doi.org/10.1109/isit.2013.6620590

23. Bernstein, D. J., Buchmann, J., Dahmen, E. (Eds.) (2009). Post-Quantum Cryptography. Springer, 246. doi: https://doi.org/10.1007/978-3-540-88702-7

24. Courtois, N. T., Finiasz, M., Sendrier, N. (2001). How to Achieve a McEliece-Based Digital Signature Scheme. Lecture Notes in Computer Science, 157–174. doi: https://doi.org/10.1007/3-540-45682-1_10

25. Faugere, J.-C., Gauthier-Umana, V., Otmani, A., Perret, L., Tillich, J.-P. (2011). A distinguisher for high rate McEliece cryptosystems. 2011 IEEE Information Theory Workshop. doi: https://doi.org/10.1109/itw.2011.6089437

26. Gaborit, P. (2005). Shorter keys for code based cryptography. In International Workshop on Coding and Cryptography – WCC'2005, 81–91.

27. Heyse, S., von Maurich, I., Güneysu, T. (2013). Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices.

Lecture Notes in Computer Science, 273–292. doi: https://doi.org/10.1007/978-3-642-40349-1_16

28. Baldi, M., Bianchi, M., Chiaraluce, F. (2013). Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. IET Information Security, 7 (3), 212–220. doi: https://doi.org/10.1049/iet-ifs.2012.0127

29. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903

30. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: https://doi.org/10.15587/1729-4061.2016.86175

31. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: https://doi.org/10.15587/978-617-7319-31-2

32. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. doi: https://doi.org/10.15587/1729-4061.2017.108461

33. Сидельников, В. М. (2002). Криптография и теория кодирования. Материалы конференции: Московский университет и развитие криптографии в России. М.: МГУ.

34. Ranjitha, C. R., Thomas, J., Chithra, K. R. (2016). A brief study on LDPC codes. International Journal of Engineering Research and General Science, 4 (2), 612–618. URL: http://pnrsolution.org/Datacenter/Vol4/Issue2/85.pdf

35. Broul´ım, J. (2018). LDPC codes - new methodologies. University of West Bohemia, 127. URL: https://cds.cern.ch/record/2730008/files/CERN-THESIS-2018-479.pdf

36. Zhu, H., Pu, L., Xu, H., Zhang, B. (2018). Construction of Quasi-Cyclic LDPC Codes Based on Fundamental Theorem of Arithmetic. Wireless Communications and Mobile Computing, 2018, 1–9. doi: https://doi.org/10.1155/2018/5264724

37. Singh, H. (2020). Code based Cryptography: Classic McEliece. arxiv.org. doi: https://doi.org/10.48550/arXiv.1907.12754

38. Chen, P.-J., Chou, T., Deshpande, S., Lahr, N., Niederhagen, R., Szefer, J., Wang, W. (2022). Complete and Improved FPGA Implementation of Classic McEliece. Cryptology ePrint Archive: Report 2022/412. URL: https://eprint.iacr.org/2022/412

39. Liva, G., Song, S., Lan, L., Zhang, Y., Lin, S., Ryan, W. E. (2017). Design of LDPC Codes: A Survey and New Results. Journal of Communications Software and Systems, 2 (3), 191. doi: https://doi.org/10.24138/jcomss.v2i3.283

40. Richardson, T. J., Urbanke, R. L. (2001). Efficient encoding of low-density parity-check codes. IEEE Transactions on Information Theory, 47 (2), 638–656. doi: https://doi.org/10.1109/18.910579

41. Chandrasetty, V. A., Aziz, S. M. (2011). FPGA Implementation of a LDPC Decoder using a Reduced Complexity Message Passing Algorithm. Journal of Networks, 6 (1). doi: https://doi.org/10.4304/jnw.6.1.36-45

42. Wang, Y. (2008). Generalized constructions, decoding and implementation of LDPC codes. University of Hawaii at Manoa. URL: https://scholarspace.manoa.hawaii.edu/bitstream/10125/20577/Ph.D._AC1.H3_5085_r.pdf

43. Sarvaghad-Moghaddam, M., Ullah, W., Jayakody, D. N. K., Affes, S. (2020). A New Construction of High Performance LDPC Matrices for Mobile Networks. Sensors, 20 (8), 2300. doi: https://doi.org/10.3390/s20082300

44. Hübner, C., Merz, H., Hansemann, T. (2009). Gebäudeautomation. Kommunikationssysteme mit EIB/KNX, LON und BACnet. Hanser. doi: https://doi.org/10.3139/9783446422636

45. 2CKA001473B8668. KNX Technical Manual. Busch-Presence detector KNX / Busch-Watchdog Sky KNX (2017). Busch-Jaeger Elektro GmbH, 198. URL: https://library.e.abb.com/public/ddedcbf7ab704705affb179ca91e0fa2/2CKA001473B8668_Prasenzmelder_6131_03_ABB_EN.pdf

46. Technical documentation on KNX devices (2006). ABB.

47. KNX Handbook Version 1.1 Revision 1 (2004). Konnex Association.

48. ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual. Busch-Watchdog Sky KNX (2016). Busch-Jaeger Elektro GmbH, 648.

49. ABB GPG Building Automation Webinar ABB i-bus® KNX Basics and Products (2016). ABB, 86. URL: https://library.e.abb.com/public/d26bd890d3ef476fbc3a59a2fdca6116/Webinar%20ABB%20i-bus%20KNX%20-%20KNX%20Basics%20and%20Products.pdf

50. Manual for KNX Planning (2017). Siemens Switzerland Ltd, 100.

51. Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation (2010). Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 116.

52. Kottapalli, N. (2011). Diameter and LTE Evolved Packet System. Corporate Headquarters, 10. URL: http://go.radisys.com/rs/radisys/images/paper-lte-diameter-eps.pdf

53. Ventura, H. (2002). Diameter - Next generation's AAA protocol. Institutionen för Systemteknik, 66. URL: https://www.diva-portal.org/smash/get/diva2:18347/FULLTEXT01.pdf

54. Vinay Kumar, S. B., Harihar, M. N. (2012). Diameter-Based Protocol in the IP Multimedia Subsystem. International Journal of Soft Computing and Engineering (IJSCE), 1 (6), 266–269. URL: https://www.ijsce.org/portfolio-item/F0320121611/

55. Qanbari, S., Mahdizadeh, S., Rahimzadeh, R., Behinaein, N., Dustdar, S. (2016). Diameter of Things (DoT): A Protocol for Real-Time Telemetry of IoT Applica-

tions. Lecture Notes in Computer Science, 207–222. doi: https://doi.org/10.1007/978-3-319-43177-2_14

56. Tschofenig, H. (2019). Diameter: new generation AAA protocol – design, practice, and applications. John Wiley & Sons, Inc. doi: https://doi.org/10.1002/9781118875889

57. Угрозы безопасности ядра пакетной сети 4G (2017). URL: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/

58. Уязвимости протокола Diameter в сетях 4G (2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/

59. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et. al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. doi: https://doi.org/10.15587/1729-4061.2021.233533

60. Yevseiev, S., Pohasii, S., Khvostenko, V. (2021). Development of a protocol for a closed mobile internet channel based on post-quantum algorithms. Information Processing Systems, 3 (166), 35–40. doi: https://doi.org/10.30748/soi.2021.166.03