Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.725.5

КУДРЯШОВ

Роман Викторович

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СТРУКТУРЕ ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ

Автореферат

диссертации на соискание степени магистра

по специальности 7-06-0611-06 «Системы и сети инфокоммуникаций (углубленное высшее образование)»

_____

Научный руководитель

кандидат технических наук,
доцент Мищенко В.Н.

_____

Минск 2026

ВВЕДЕНИЕ

В современных условиях цифровой трансформации государства и расширения использования информационно-коммуникационных технологий существенным образом возрастает значение информационной безопасности в деятельности государственных учреждений. Республика Беларусь последовательно развивает электронное государственное управление, внедряет государственные информационные системы и сервисы электронного взаимодействия, расширяет электронный документооборот и межведомственный обмен данными. Указанные процессы сопровождаются ростом объёма обрабатываемой информации, включая персональные данные граждан, служебную информацию ограниченного распространения, сведения государственных реестров и иные ресурсы, критичные для выполнения управленческих функций.

Одновременно с ростом цифровизации возрастает и уровень угроз информационной безопасности. Внешние и внутренние нарушители способны воздействовать как на конечные информационные системы, так и на каналы связи, применяя атаки перехвата и подмены трафика, атаки типа «человек посередине» (MITM), повтор сообщений (replay), навязывание ослабленных параметров криптографической защиты (downgrade), а также эксплуатацию ошибок конфигурации (misconfiguration). Нарушение конфиденциальности и целостности данных при межведомственном обмене или при удалённом доступе способно привести к существенным правовым, финансовым и репутационным последствиям: компрометации персональных данных граждан, искажению записей в информационных ресурсах, остановке предоставления государственных услуг и снижению доверия к электронным механизмам управления.

В отличие от коммерческих организаций, государственные учреждения функционируют в условиях повышенного нормативного регулирования и обязательности соблюдения требований защиты информации. В Республике Беларусь правовые основы обращения и защиты информации определяются

законом «Об информации, информатизации и защите информации», а обработка персональных данных регламентируется законом «О защите персональных данных». Отдельный блок требований связан с техническим регулированием и подтверждением соответствия средств защиты информации, включая требования технического регламента ТР 2013/027/BY, а также процедур допуска и применения сертифицированных решений. Значимую роль в части контроля и ведения соответствующих реестров играет Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ). Практическим следствием указанных требований является необходимость использования в государственном секторе только таких средств защиты информации, которые имеют подтверждённый статус соответствия, определённую область применения и нормативную допустимость использования.

В этих условиях особую значимость приобретают средства криптографической защиты информации (СКЗИ). Они являются ключевыми компонентами обеспечения информационной безопасности при передаче данных по потенциально не защищённым каналам связи и позволяют реализовать необходимые свойства защищённого обмена: конфиденциальность, целостность, аутентичность участников соединения и доказательность действий (в том числе посредством механизмов инфраструктуры открытых ключей – PKI). Для государственных учреждений СКЗИ играют системообразующую роль, поскольку обеспечивают безопасное функционирование межведомственного взаимодействия, защищённого удалённого доступа, взаимодействия территориально распределённых подразделений, обмена сообщениями между государственными информационными системами и сервисами.

Таким образом, актуальность выбранной темы определяется совокупностью факторов: ростом цифровизации государственного управления, увеличением масштаба и критичности обрабатываемых данных, усложнением моделей угроз, обязательностью применения сертифицированных средств защиты информации, а также потребностью в формировании обоснованных

требований к СКЗИ и демонстрации практических механизмов защиты каналов связи.

Целью диссертационной работы является разработка и обоснование требований к средствам криптографической защиты информации для защиты каналов связи в государственных учреждениях Республики Беларусь, а также создание и экспериментальная проверка прототипа СКЗИ, реализующего защищённый канал связи с учётом актуальных угроз и эксплуатационных требований государственного сектора.

Для достижения поставленной цели в работе решаются следующие задачи:

Провести анализ теоретических и нормативно-правовых основ обеспечения информационной безопасности в государственных учреждениях Республики Беларусь.

Выполнить классификацию информации, подлежащей защите в государственном учреждении, и определить требования к защите данных различных категорий.

Проанализировать актуальные угрозы информационной безопасности, характерные для государственного сектора, с акцентом на угрозы в каналах связи.

Сформировать модель нарушителя и модель угроз для защищаемых каналов связи, определить наиболее критичные сценарии атак (MITM, replay, downgrade, misconfiguration и др.).

Выполнить оценку рисков с применением матрицы «вероятность × ущерб» и сформировать реестр ключевых рисков.

На основе результатов анализа угроз и рисков обосновать требования к СКЗИ (функциональные, криптографические, эксплуатационные, требования аудита и управляемости).

Определить критерии выбора СКЗИ для государственных учреждений с учётом нормативно-сертификационных требований (ОАЦ, ТР 2013/027/BY) и практики эксплуатации.

Разработать архитектуру прототипа СКЗИ, реализующего защищённый канал связи (клиент–сервер / шлюз–шлюз) с использованием взаимной аутентификации по сертификатам (mTLS/PKI).

Реализовать основные модули прототипа, включая управление криптографической политикой, защиту от replay, аудит и журналирование.

Провести демонстрационные испытания прототипа, включая моделирование атак MITM/replay/downgrade, оформить результаты тестирования (тест-кейсы, логи, примеры «пакетов»).

Объектом исследования является система обеспечения информационной безопасности государственных учреждений Республики Беларусь в части защиты данных при передаче по каналам связи в условиях функционирования государственных информационных систем и межведомственного электронного взаимодействия.

Предметом исследования являются методы и средства криптографической защиты информации, применяемые для защиты каналов связи (VPN/TLS/mTLS/IPsec и др.), а также архитектурные и эксплуатационные принципы построения СКЗИ с учётом требований нормативного регулирования и актуальных моделей угроз.

В работе используются следующие методы исследования: анализ нормативных и методических источников по защите информации; системный анализ и декомпозиция объекта защиты; методы построения модели нарушителя и модели угроз (CIA/STRIDE); риск-ориентированный подход к оценке угроз; экспертная оценка рисков на основе матрицы 5×5; проектирование модульной архитектуры прототипа защищённого канала; экспериментальное тестирование и анализ журналов безопасности.

Научная новизна работы состоит в формализации совокупности требований к СКЗИ для государственного учреждения Республики Беларусь на основе взаимосвязи «угроза → риск → меры снижения → требование» с выделением критических факторов защиты каналов связи (сертификатная взаимная аутентификация, контроль статуса сертификатов, централизованная

криптографическая политика, противодействие replay/downgrade, аудит и управляемость).

Практическая значимость диссертационной работы заключается в том, что сформированные требования и критерии выбора СКЗИ могут быть применены при проектировании и внедрении систем защиты каналов связи в государственных учреждениях Республики Беларусь, а разработанный прототип может использоваться как демонстрационная и учебно-методическая основа для проверки решений и подготовки специалистов по информационной безопасности.

Структура и объём работы. Диссертация состоит из введения, трёх глав, заключения, списка использованных источников и приложений. В первой главе рассмотрены теоретико-нормативные основы обеспечения информационной безопасности государственных учреждений и место СКЗИ в системе государственного управления. Во второй главе выполнены анализ угроз и рисков, построены модель нарушителя и модель угроз для защищаемых каналов связи, сформированы требования и критерии выбора СКЗИ с учётом государственных требований. В третьей главе разработана архитектура и реализован прототип СКЗИ для защиты каналов связи, проведены демонстрационные испытания, включая имитацию атак MITM/replay/downgrade, представлены результаты тестирования и анализ журналов безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель исследования. анализ угроз и рисков для каналов связи государственного учреждения Республики Беларусь, обоснование требований к средствам криптографической защиты информации для защиты каналов связи и разработка прототипа СКЗИ, реализующего защищённый обмен с использованием инфраструктуры открытых ключей и механизмов аудита.

Объект исследования. система обеспечения информационной безопасности государственных учреждений Республики Беларусь в части защиты данных при передаче по каналам связи в условиях функционирования

государственных информационных систем и межведомственного электронного взаимодействия.

Предмет исследования. методы и средства криптографической защиты информации, применяемые для защиты каналов связи (VPN/TLS/mTLS/IPsec и др.), а также архитектурные и эксплуатационные принципы построения СКЗИ с учётом требований нормативного регулирования и актуальных моделей угроз.

Научная новизна работы. формализации совокупности требований к СКЗИ для государственного учреждения Республики Беларусь на основе взаимосвязи «угроза → риск → меры снижения → требование» с выделением критических факторов защиты каналов связи (сертификатная взаимная аутентификация, контроль статуса сертификатов, централизованная криптографическая политика, противодействие replay/downgrade, аудит и управляемость).

Практическая значимость. сформированные требования и критерии выбора СКЗИ могут быть применены при проектировании и внедрении систем защиты каналов связи в государственных учреждениях Республики Беларусь, а разработанный прототип может использоваться как демонстрационная и учебно-методическая основа для проверки решений и подготовки специалистов по информационной безопасности.

Личный вклад соискателя ученой степени. Содержание диссертации отображает личный вклад автора, который заключается в научном обосновании требований к СКЗИ, разработке и апробации архитектурно-программного прототипа защищённого канала связи, проведении экспериментального исследования его характеристик и формулировке итоговых выводов.

Апробация диссертации и информация об использовании ее результатов. Результаты работы апробированы в рамках выполнения научно-исследовательской работы и практической реализации прототипа, обсуждения промежуточных результатов на консультациях и научных семинарах кафедры, а также экспериментального тестирования прототипа.

Опубликование результатов диссертации. По результатам исследований, были опубликованы статья «Риск – ориентированное формирование требований к СКЗИ для защиты каналов связи госучреждений Республики Беларусь» стр. 154-155 и статья «Прототип скзи для защиты каналов связи госучреждений: архитектура, криптополитика и тестирование устойчивости к mitm/replay/downgrade» стр. 156-157 в части 2 «Международного научного журнал «Академик» (г. Астана)» выпуск 15.12.2025. (ссылка на журнал: https://journal-academic.com/f/mezhdunarodnyj_nauchnyj_zhurnal_akademik_1512_chast_ 2.pdf).

Структура и объем диссертации. Диссертационная работа состоит из перечня условных обозначений, общей характеристики работы, введения, трех глав с выводами по каждой главе, заключения, списка использованных источников и приложений. Общий объем диссертационной работы составляет 107 страниц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационной работы, сформулированы цель и задачи исследования, определены объект и предмет исследования, приведены научная новизна и практическая значимость полученных результатов.

В первой главе рассмотрены теоретико-нормативные основы обеспечения информационной безопасности государственных учреждений Республики Беларусь. Выполнена классификация информации и требований к ее защите, проанализированы актуальные внешние и внутренние угрозы, а также

нормативно-правовое регулирование и организационно-технические меры защиты информации.

Во второй главе выполнены анализ угроз и рисков для защищаемых каналов связи государственного учреждения. Построены модель нарушителя и модель угроз (включая MITM, replay, downgrade и misconfiguration). Проведена оценка рисков с применением матрицы 5×5 «вероятность × ущерб», сформирован реестр ключевых рисков. На основе результатов анализа обоснованы требования к СКЗИ: функциональные, криптографические (криптографическая политика), требования к PKI и управлению ключами, эксплуатационные требования, требования к журналированию и аудиту, надежности и соответствию государственным требованиям и сертификации. Сформированы критерии выбора СКЗИ для государственного учреждения.

В третьей главе разработана архитектура прототипа СКЗИ для защиты каналов связи и реализованы основные модули: защищённый канал на базе TLS/mTLS, модуль PKI и идентификации, модуль криптографической политики, модуль защиты от повторов (Replay Protection), модуль журналирования и аудита (Audit & Logging). Представлен демонстрационный сценарий работы и результаты тестирования прототипа, включая имитацию атак MITM/replay/downgrade.

ЗАКЛЮЧЕНИЕ

В результате выполнения диссертационной работы выполнен анализ теоретико-нормативных основ обеспечения информационной безопасности государственных учреждений Республики Беларусь, построена модель угроз и проведена оценка рисков для защищаемых каналов связи. Обоснован комплекс требований к СКЗИ по схеме «угроза → риск → требование», сформированы критерии выбора СКЗИ с учётом нормативно-сертификационных ограничений. Разработана модульная архитектура и реализован прототип СКЗИ,

обеспечивающий защищённый обмен на основе TLS/mTLS и PKI, защиту от replay/downgrade и событийное журналирование. Проведенные испытания подтвердили устойчивость прототипа к ключевым угрозам защищаемого канала связи.