Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.75

ЛОДИС
Артем Викторович

УДОСТОВЕРЯЮЩИЙ ЦЕНТР СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОЙ СЕТИ ПРЕДПРИЯТИЯ

Автореферат
на соискание степени магистра
по специальности 1–45 80 01 Системы и сети инфокоммуникаций

_____

Научный руководитель
кандидат технических наук, доцент
САЛОМАТИН Сергей Борисович

_____

Минск 2022

ВВЕДЕНИЕ

В настоящее время особо актуальна задача развития и эффективного использования инфокоммуникационной ресурсной базы каждого органа государственного управления. В век бурного развития именно инфокомуникаций наша страна не может оставаться в стороне от необходимости решения этой задачи, тем более что в законодательных и распорядительных документах органов власти и управления подчеркивается и указывается необходимость по дальнейшему развитию «электронного правительства» –системы государственного управления, основанной на автоматизации управленческих процессов в масштабах страны.

При внедрении систем электронного документооборота на предприятии и присоединении к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь необходимо организовать и четко отладить функционирование сети передачи данных.

Ведомственная информационная сеть предназначена для решения следующих основных задач:

– обеспечение обмена информацией и организация доступа пользователей к информационным и вычислительным ресурсам;

– совершенствование системы управления;

– создание условий для внедрения новых информационных технологий в основные направления деятельности подчиненных подразделений;

– интегрирование информационных и вычислительных ресурсов на основе Intranet-технологий в единую сеть;

– поддержание обмена информацией между пользователями информационной сети с предоставлением стандартного набора услуг для IP-сетей.

Современные информационные сети представляют собой программно-технические комплексы, созданные на основе компьютеров, серверов, высокоскоростных сетевых устройств и каналов связи, в которых формирование и анализ сигналов выполняется как на аппаратном, так и на программном уровнях.

Как правило у самого предприятия нет собственных ресурсов сети связи и необходимые канальные ресурсы арендуются из сети связи общего пользования у региональных и национальных операторов связи

В целях обеспечения безопасности при сопряжении собственных сетей связи с сетями связи общего пользования должны быть использованы

решения, обеспечивающие изоляцию адресных пространств отдельных сетей в составе собственных сетей связи и передаваемых потоков трафика от тех сегментов и потоков, которые обслуживаются в сетях связи общего пользования оператором связи.

Вопросы защиты от несанкционированного доступа к ведомственной сети предприятия, а также информации передаваемой и хранящейся в ней должны являться одними из приоритетных при организации сети.

В данной работе рассмотрены современные решения применения ведомственных информационных сетей специального назначения, а также присоединение к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь. Данные сети исследуются как средства обеспечения функционирования информационных систем и ресурсов, а также как средства обеспечения информационной безопасности при издании, распространении и хранении сертификатов открытых ключей проверки электронной цифровой подписи в закрытых ведомствах. Данные ведомства представляют собой организации, в которых строго ограничен доступ к глобальной информационной сети Интернет, а также на оборудовании обрабатывается и по сетям передачи данных передается информация ограниченного распространения.

Решение данной задачи является актуальным и новым для государственных и военизированных структур в Республике Беларусь, так как внедрение электронного документооборота и присоединение к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь исследуется в рамках ограниченного доступа к глобальной информационной сети Интернет.

Задачи исследовательской составляющей диссертации:

1 Провести оценку вариантов использования систем электронного документооборота по их соответствию задачам организации и по соответствию законодательству Республики Беларусь.

2 Обосновать необходимость создания регистрационного центра предприятия как элемента Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг и обеспечение функционирования в распределенной информационной сети.

3 Раскрыть основные проблемы обеспечения безопасности функционирования информационных систем и сетей специального назначения.

В практической части диссертации решить следующие задачи:

1 Разработать техническое решение на создание защищенного сегмента ведомственной информационной сети, определяющего содержание и условия работы технических средств защиты, информационной сети и систем во взаимодействии с Республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг.

2 Создать облик ведомственной защищенной информационной сети в соответствии с законодательством Республики Беларусь в области защиты информации, с элементами защиты канала передачи данных, на основе технологии виртуальных защищенных туннелей VPN IPsec и применением программно-аппаратных комплексов (далее – ПАК) «Шлюз безопасности». Раскрыть структурно-функциональную схему ПАК «Шлюз безопасности» со всеми элементами взаимодействующих между собой функциональных подсистем.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Задачи развития и эффективного использования инфокоммуникационной ресурсной базы органов государственного управления во время бурного развития информационных технологийособенно актуальны.

Одними из приоритетных вопросов при организации сети являются вопросы защиты от несанкционированного доступа к ведомственной сети предприятия, а также информации передаваемой и хранящейся в ней.

Присоединение к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь является необходимостью государственных предприятий, в целях развития и присоединения к политике «электронного правительства».

Тема исследования является актуальной и новой для государственных и военизированных структур в Республике Беларусь, так как присоединение к политике применения сертификатов Республиканского удостоверяющего

центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь исследуется в рамках ограниченного доступа к глобальной информационной сети Интернет.

Степень разработанности проблемы

Исследования развития электронного документооборота и издания, распространения и хранения сертификатов открытых ключей проверки электронной цифровой подписи рассмотрены в работах Дрыганова В.А., Завидова Б.Д., Леонова А.П., Полещука М.И. и других авторов.

Изучена законодательная база Республики Беларусь, а именно: Закон Республики Беларусь от 10.11.2008 г. № 455-З «Об информации, информатизации и защите информации» (в ред. Закона Республики Беларусь от 24.05.2021г. №111-З), Закон Республики Беларусь от 28.12.2009 г. № 113-З «Об электронном документе и электронной цифровой подписи» (в ред. Закона Республики Беларусьот 08.11.2018 г. №143-З), Постановление Совета безопасности Республики Беларусь от 18.03.2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь».

Область использования распределенных информационных сетей в коммерческих и ведомственных сетях рассмотрена в работах Буренина А.Н., Легкова К.Е., Косякова М.С., В.А. Балыбердина, В.А. Герасименко, А.А. и др.

Одним из недостатков, представленных в современной литературе, является неполное рассмотрение опыта применения способов защиты информационных ведомственных сетей на основе программно-аппаратных средств защиты, а также этапов создания политики информационной безопасности. Предложенное исследование направлено на устранение некоторых недостатков на основе опыта внедрения сегмента ведомственной защищенной информационной сети.

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 «Обеспечение безопасности человека, общества, государства» приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь № 156 от 7 мая 2020 г. «О приоритетных направлениях научной, научно-технической и инновационной деятельности на 2021–2025 годы». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью исследования является разработка технического решения на создание защищенного сегмента информационной сети, и присоединение к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, для последующего внедрения систем электронного документооборота на предприятиии обеспечении информационной безопасности при издании, распространении и хранении сертификатов открытых ключей проверки электронной цифровой подписи, создание стенда в рамках настройки программно-аппаратного комплекса «Шлюз безопасности» с учетом разработки руководства пользователя.

Для выполнения поставленной цели в работе были сформулированы следующие задачи:

1 Анализ существующих подходов к созданию систем электронного документооборота на предприятии с точки зрения использования ее в закрытых информационных сетях,с целью выявления недостатков и выработке возможных подходов к решению проблемы.

2 Проанализировать особенности присоединения к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

3 Изучение тенденций развития инфокоммуникационной инфраструктуры закрытых государственных учреждений и оценить требования к обеспечению защиты ее ресурсов.

4 Описать структуру защиты ведомственной информационной сети на основе программного комплекса «Шлюз безопасности» для обеспечения сетевой безопасности ведомственной сети любой топологии.

5 Реализация алгоритмов параллельной обработки сетевого траффика между различными узлами сети и защиты трафика самого шлюза безопасности на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP, в целях обеспечения производительности СКЗИ.

6 Построение модели регистрационного центра предприятия с использованием процедур в области информационной безопасности.

Объект исследования

Закрытая ведомственная информационная сеть на основе средств защиты информации.

Предмет исследования

Модель регистрационного центра предприятия, обеспечивающая оптимальную эффективность присоединенияк политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь.

Теоретическая и методологическая основа исследования

В основу диссертации легли результаты известных исследований отечественных и зарубежных авторов в области защиты информации, безопасности инфокоммуникационных систем и сетей специального назначения.

Для получения теоретических результатов исследования применялись модели использования сетей специального назначения в различных сферах деятельности государственного назначения.

Оценка применения технологий,предоставляемых регистрационным центром присоединенным к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, в органах госуправления и коммерческом секторе, проводилась на основе литературных источников, интернет-изданий и аналитических платформ сети Интернет.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Разработка модели сегмента защищенной ведомственной информационной сети на основе программно-технических средств защиты. Предложена модель, описывающая процессы создания и развития ведомственной сети, отличительной особенностью которой является функционирование ее в условиях ограниченного доступа к глобальной информационной сети Интернет.

Личный вклад соискателя ученой степени

Содержание диссертации отображает личный вклад автора. Он заключается в научном обосновании использования в целях обеспечения

криптографической защиты информации сети предприятия программно-аппаратных комплексов «Шлюз безопасности», постановке и проведении экспериментов по исследованию характеристик данного аппаратного комплекса, настройке функционирования в требуемом режиме, оценке эффективности работы оборудования в ведомственной сети предприятия, обработке и анализе полученных результатов, формулировке выводов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем кандидатом технических наук, доцентом С.Б. Саломатиным.

Апробация диссертации и информации об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 57-й научной конференции аспирантов, магистрантов и студентов БГУИР, г. Минск,на Республиканской научно-практической конференции «Обеспечение пограничной безопасности Республики Беларусь: направления развития всестороннего обеспечения» ГУО «ИПС РБ»31марта 2021 г., г. Минск.

С практической точки зрения результаты исследований использованы в июле-августе 2021 г. при развертывании удостоверяющего центра Государственного пограничного комитета Республики Беларусь (далее – Госпогранкомитет) и удаленных постов регистрации в территориальных органах пограничной службы Республики Беларусь и присоединении Госпогранкомитетак политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь с аккредитацией удостоверяющего центра Национальным центром электронных услуг Республики Беларусь.

Опубликование результатов диссертации

Основные положения работы и результаты диссертации изложены в 2 опубликованных работах, представленных в материалах Республиканской заочной научно-практической конференцииГУО «ИПС РБ» и 57 научно-технической конференцииБГУИР. Общий объем публикаций 8 страниц.

Основные положения диссертации, выносимые на защиту

1 Ведомственная защищенная сеть на основе программно-технического комплекса «Шлюз безопасности». Модель сегментаVPN сети.

2 Алгоритм параллельной обработки сетевого траффика между различными узлами сети и защиты трафика самого шлюза безопасности на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP.

3 Требования, предъявляемые для создания регистрационного центра предприятия как элемента Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг и обеспечение функционирования в распределенной информационной сети.

4 Модель регистрационного центра предприятия и облик ведомственной защищенной информационной сети в соответствии с законодательством Республики Беларусь в области защиты информации, с элементами защиты канала передачи данных, на основе технологии виртуальных защищенных туннелей VPN IPsec и применением ПАК «Шлюз безопасности».

Теоретическая значимость диссертации заключается в том, что в ней предложен подход к присоединению к политике применения сертификатов Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь способ реализации удостоверяющего центра предприятия в различных информационных сетях. Раскрыт один из способов защиты канала передачи данных информационной сети на основе программного комплекса «Шлюз безопасности».

Практическая значимость результатов работы заключается в разработанных подходах, моделях и методах, составляющих основу защищенной информационной сети. Они могут быть использованы: при проектировании и разработке элементов информационной сети; при интеграции разрозненных информационных сетей и информационных ресурсов в единую ведомственную сеть; при построении сложных систем, обладающих схожим функционалом, и систем, обеспечивающих автоматизацию деятельности организации.

Структура и объем работы

Диссертация состоит из общей характеристики работы, введения, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложения.

Общий объем диссертационной работы составляет91 страницу,из них 59 страницы текста, 11 рисунков на 5 страницах, список использованных

библиографических источников (25 наименований на 2 страницах), список публикаций автора по теме диссертации (2 наименования на 1 странице), 1 приложение на 14 страницах,графический материал на 7 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Лодиса А.В. «Удостоверяющий центр системы защиты информации в распределенной сети предприятия» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 04.06.2022 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 87,24 %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассмотрено современное состояние проблемы функционирования современных ведомственных инфокоммуникационных систем, определены основные направления исследований, а также дается обоснование актуальности темы диссертационной работы.

В общей характеристике работы сформулированы ее цель и задачи, показана связь с научными программами и проектами, даны сведения об объекте и предмете исследования, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В первомразделерассмотрены принципы и задачи, решаемые электронным документооборотом, основные факторы, влияющие на решение о выборе системы электронного документооборота, общая классификация и обзор основных систем. Рассмотрено понятие электронной цифровой подписи и порядок ее получения, необходимость создания регистрационного центра на предприятии как элемента Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг.

Во второй главеприведен анализ и изучены проблемные вопросы обеспечения информационной безопасности в области функционирования ведомственной информационной сети. Определена теоретическая и правовая основа по созданию надежной ведомственной защищенной информационной сети, которая определяется как информационная система специального назначения.

В третьей главе раскрыта структура защиты ведомственной информационной сети на основе программно-аппаратного комплекса. Создан регистрационный центр предприятия и сегмент ведомственной информационной сети, с применением технологии виртуальных защищенных туннелей VPN на основе программно-аппаратного шлюза безопасности. Реализован алгоритм параллельной обработки сетевого траффика между различными узлами сети.

В приложении приведены результаты настройки построения VPN туннеля между шлюзом безопасности и рабочим местом администратора для удаленной настройки шлюза.

ЗАКЛЮЧЕНИЕ

В начале работы были названы задачи исследовательской составляющей диссертации, по каждой из которых получены результаты:

1 Проведена оценка вариантов использования систем электронного документооборота по их соответствию задачам организации и по соответствию законодательству Республики Беларусь.

2 Проанализированы тенденции развития инфокоммуникационной инфраструктуры организаций и оценены требования к обеспечению защиты ее ресурсов.

3 Раскрыта структура защиты ведомственной информационной сети на основе программного комплекса «Шлюз безопасности» для обеспечения сетевой безопасности ведомственной сети любой топологии.

4 Реализован алгоритм параллельной обработки сетевого траффика между различными узлами сети и защиты трафика самого шлюза безопасности на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP, в целях обеспечения производительности средств СКЗИ.

5 Обоснована необходимость создания регистрационного центра предприятия как элемента Республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг и обеспечение функционирования в распределенной информационной сети.

В практической части диссертации были решены следующие задачи:

1 Разработано техническое решение на создание защищенного сегмента ведомственной информационной сети, определяющее содержание и условия

работы технических средств защиты, информационной сети и систем во взаимодействии с Республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь Национального центра электронных услуг.

2 Создан облик ведомственной защищенной информационной сети в соответствии с законодательством Республики Беларусь в области защиты информации, с элементами защиты канала передачи данных, на основе технологии виртуальных защищенных туннелей VPN IPsec и применением ПАК «Шлюз безопасности». Раскрыта структурно-функциональная схема ПАК «Шлюз безопасности» со всеми элементами взаимодействующими между собой функциональными подсистемами.

Все указанные задачи были решены, цели достигнуты.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А.Лодис,А.В. Удостоверяющий центр системы защиты информации в распределенной сети предприятия / ЛодисА.В., Саломатин С.Б. // 57-я научная конференция аспирантов, магистрантов и студентов БГУИР : тезисы докладов 57-ой научной конференции аспирантов, магистрантов и студентов БГУИР. Минск, 19-23 апреля 2021 г. / редкол. : В.Ю. Цветков [и др.]. – Минск : БГУИР, 2021. – С. 64–66.

2–А.Лодис,А.В. Система защиты информации на основе доверия в динамической сенсорной сети / ЛодисА.В., Саломатин С.Б.//Республиканская заочная научно-практическая конференция «Обеспечение пограничной безопасности Республики Беларусь: направления развития всестороннего обеспечения». Минск, 31 марта 2021 г. / редкол. :В.П. Вишневская [и др.]. – Минск: ИПС РБ, 2021. – С. 51–55.