

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

УДК

АНДРИЯНОВ  
Павел Александрович

Организация дистанционного обучения на основе защищенной  
ведомственной информационной сети

**АВТОРЕФЕРАТ**

магистерской диссертации на соискание степени  
магистра техники и технологии

по специальности 1-45 81 01 «Инфокоммуникационные системы и сети»

Научный руководитель  
канд.техн.наук, доцент  
Саломатин С.Б.

Минск 2018

## ВВЕДЕНИЕ

В силу индивидуальности ряда проблем, сложившихся подходов, наличия технических и технологических апробированных решений большинство организаций создают свое информационное пространство, зачастую используя несовместимые подходы, что влечет за собой дополнительные затраты на разработку собственных систем при отсутствии гарантий достижения поставленных целей. Данные проблемы обусловлены широтой спектра решаемых задач, частой несовместимостью используемых платформ, техническим несовершенством, недокументированностью решений, отсутствием четкой политики со стороны управляющих и контролирующих организаций и т.д.

Опыт создания и функционирования современных ведомственных инфокоммуникационных систем подтвердил экономическую и техническую целесообразность формирования сетей данного типа на базе арендованных магистральных линий передачи и создания на их основе систем передачи данных (далее – информационная сеть).

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

Характерной особенностью ПТК информационных сетей является то, что в них интегрированы процессы ввода-вывода, защиты от ошибок, формирования и анализа сигналов. Кроме того, они выполняют и другие, не связанные с передачей данных, функции, такие как поиск и формирование файловых данных, компрессия и декомпрессия, защита от НСД и др.

В настоящее время крайне актуальна задача развития и эффективного использования информационно – технической ресурсной базы каждого органа государственного управления по направлению информационных технологий. Потребность решения этой задачи в Республике Беларусь постоянно подчёркивается в документах органов власти и управления, в которых особая роль отводится развитию и совершенствованию «электронного правительства» – комплексной системы государственного управления на основе электронных средств обработки, передачи и распространения информации в сочетании с организационными изменениями и новыми методами для улучшения услуг государственного секторов.

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.

## **ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ**

### **Актуальность темы исследования**

В данной работе рассмотрены современные решения применения ведомственных информационных сетей. Данные сети исследуются как средства обеспечения функционирования информационных систем и ресурсов, а также как средства обеспечения предоставления услуг по переподготовке и повышению квалификации сотрудников закрытых ведомств. Данные структуры представляют собой организации, в которых строго ограничен доступ к глобальной информационной сети Интернет, а также обрабатывается информация ограниченного распространения по сетям передачи данных.

Создание и последующая интеграция в составе информационной образовательной среды программной платформы дистанционного обучения образовательного учреждения в настоящее время лимитируются отсутствием продуктивных научно-методических подходов к решению задач комплексного обеспечения корпоративной и сетевой безопасности.

Методам обработки и защиты данных в информационных системах посвящены многочисленные работы авторов: В.А. Балыбердина, В.А. Герасименко, А.А. Малюка, В.Д. Киселёва, В.В. Кульбы, А.Г. Мамиконова, Л.Дж. Хоффмана, Б.Дж. Уолкера и др. В этих исследованиях получили развитие теоретические положения и методы обеспечения информационной безопасности в системах управления в сферах науки, производства и бизнеса. Значительно меньше внимания уделялось обеспечению информационной безопасности в области образования, где используемые подходы к защите конфиденциальной информации отличаются многообразием и противоречивостью. В частности, остаются мало изученными вопросы создания и исследования защищенной сетевой инфраструктуры высшего профессионального образования.

Решение данной задачи является особенно актуальным и новым для военных учебных заведений в Республике Беларусь, так как внедрение дистанционного обучения исследуется в рамках ограниченного доступа к глобальной информационной сети Интернет.

Таким образом, актуальной является научно-техническая проблема разработки и теоретического обоснования технологических основ создания и развития защищенного сегмента информационной сети организации на основе различных подходов к интеграции, объединяющих информационные системы и ресурсы в единую систему.

### **Степень разработанности проблемы**

Исследование влияния дистанционного обучения рассмотрено в работах Смоликовой, Т. М., Жучкова В.М., Кораблева А.В. и других авторов. Изучение использования технологий дистанционного обучения в странах СНГ представлено в работах Батаева, А.В., Готской, И.Б.

Изучена законодательная база Республики Беларусь и стран СНГ, а именно: Модельный закон о дистанционном обучении в государствах-участниках СНГ, Концепция информатизации системы образования Республики Беларусь на период до 2020 года, Образовательный стандарт Республики Беларусь «Переподготовка руководящих работников и специалистов, имеющих высшее образование».

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. Малюка.

В области защиты информации изучена и применена в работе нормативно-правовая база Республики Беларусь.

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.

### **Цель и задачи исследования**

Целью исследования является, разработка механизмов расчета, необходимых для реализации программно-аппаратной платформы системы дистанционного обучения, разработка технического задания на создание защищенного сегмента информационной сети, создание защищенного сегмента ведомственной информационной сети, создание стенда в рамках настройки программно-аппаратного комплекса «Шлюз безопасности» с учётом разработки руководства пользователя.

Для выполнения поставленной цели в работе были сформулированы следующие задачи:

1. Анализ существующих подходов к созданию дистанционной образовательной среды организации с точки зрения использования ее в закрытых информационных сетях, с целью выявления недостатков и возможных подходов к решению проблемы;

2. Проанализировать тенденции развития инфокоммуникационной инфраструктуры образовательных учреждений и оценить требования к обеспечению защиты её ресурсов;

3. Описание структуры защиты ведомственной информационной сети на основе программного комплекса «Шлюз безопасности» для обеспечения сетевой безопасности ведомственной сети любой топологии;

4. Реализация алгоритма параллельной обработки сетевого трафика 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. Построить теоретическую модель организации центра дистанционного обучения с использованием процедур в области информационной безопасности на основе методов авторизации в системе дистанционного обучения.

**К объектам исследования относятся:** защищенная ведомственная информационная сеть на основе средств защиты информации, система дистанционного обучения и методы её интеграции.

**Предметом** работы является модель организации дистанционного обучения, обеспечивающая оптимальную эффективность получения образования закрытой ведомственной информационной сети.

**Область исследования.** Содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-45 81 01 «Инфокоммуникационные системы и сети».

#### **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, изучения технологий дистанционного обучения.

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

Оценка применения технологий дистанционного образования в органах государственного управления и коммерческом секторе проводилась на основе литературных источников, интернет изданий и аналитических платформ сети Интернет.

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

#### **Основные положения, выносимые на защиту**

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

2. Алгоритм параллельной обработки сетевого трафика 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.

3. Внедрение дистанционной образовательной среды организации с точки зрения использования ее в закрытых информационных сетях.

4. Теоретическая модель организации центра дистанционного обучения с использованием процедур в области информационной безопасности на основе алгоритмов авторизации в системе дистанционного обучения.

**Теоретическая значимость** диссертации заключается в том, что в ней предложен подход к выбору программной платформы системы дистанционного обучения и способов её применения 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; при обучении и повышении квалификации специалистов в области создания сложных информационных систем на основе порталных технологий.

#### **Апробация и внедрение результатов исследования**

Результаты исследования были неоднократно представлены на научных конференциях в УО «Белорусский государственный университет информатики и радиоэлектроники», и международно-технической конференции на базе Резекненской технологической академии г. Резекне, Республика Латвия.

Также результаты внедрения подтверждены актом внедрения результатов научно-исследовательской работы в государственном учреждении образования «Институт пограничной службы Республики Беларусь».

### **Публикации**

Основные положения работы и результаты диссертации изложены в трех опубликованных работах общим объемом 14,0 п.л. (авторский объем 5,0 п.л.).

**Структура и объем работы.** Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трёх глав и заключения, библиографического списка и приложений. Общий объем диссертации – 78 страниц. Работа содержит 3 таблицы, 17 рисунков. Библиографический список включает 25 наименований.

## **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 исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В первой главе рассматриваются существующие средства организации учебного процесса с использованием дистанционных технологий. Отечественный и зарубежный опыт внедрения дистанционных технологий их рейтинг и качественные характеристики.

Во второй главе приведен анализ и изучены проблемные вопросы обеспечения информационной безопасности функционирования ведомственной информационной сети.

В **третьей главе** представлены результаты созданного сегмента ведомственной информационной сети, с применением технологии виртуальных защищенных туннелей VPN на основе программно-аппаратного шлюза безопасности.

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. Проведен анализ существующих подходов к созданию дистанционной образовательной среды организации с точки зрения использования ее в закрытых информационных сетях, с целью выявления недостатков и возможных подходов к решению проблемы;

2. Проанализированы тенденции развития инфокоммуникационной инфраструктуры образовательных учреждений и оценены требования к обеспечению защиты её 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 трафика 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. Построена теоретическая модель организации центра дистанционного обучения с использованием процедур в области информационной безопасности на основе алгоритмов авторизации в системе дистанционного обучения.

В практической части диссертации были решены следующие задачи:

1. Разработка технического решения на создание защищенного сегмента ведомственной информационной сети, определяющего содержание и условия работы технических средств защиты, информационной сети и систем во взаимодействии с программной платформой системы дистанционного обучения.

2. Разработаны критерии расчёта возможности использования различных информационно – технических систем, с последующим выбором программной платформы системы дистанционного обучения.

3. Создан сегмент ведомственной 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 ПК «Шлюз безопасности». Раскрыта структурно-функциональная схема ПК «Шлюз безопасности» со всеми элементами взаимодействующих между собой функциональных подсистем.

Все указанные задачи были решены, цели достигнуты.



Достаточно значимой составляющей внедрения инноваций в любой процесс является оценка рисков, но этот вопрос (в силу его объемности и необходимости более углубленного изучения) не рассматривался в рамках магистерской работы и может быть решен в будущем в рамках, например, магистерского исследования другого магистранта или в рамках кандидатской диссертации.

#### СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Andriyanov, P. Use of modern educational technologies in field of military education. Distance learning – problems and decision / P. Andriyanov // Journal of internal security and civil defence sciences. – 2016. – Vol. 1 (6).

2-А. Андриянов, П. А. Особенности использования шлюзов безопасности в ведомственной вычислительной сети / П. А. Андриянов // Материалы конференций БГУИР. – 2017. – С. 96–97.

3-А. Андриянов, П. А. Внутриведомственная сеть как средство обеспечения безопасности информации в системе дистанционного обучения военнослужащих / П. А. Андриянов // Сб. АПС КНБ Респ. Казахстан. – 2017. – С. 338–341.