Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

 10.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.03.01 Информационная безопасность интранет-сетей

1. **Код и наименование направления подготовки/специальности:**

09.04.02 Информационные системы и технологии

2. **Профиль подготовки/специализация:**

Цифровые технологии в жизненном цикле изделий

3. **Квалификация (степень) выпускника:**

Магистратура

4. **Форма обучения:**

Заочная

5. **Кафедра, отвечающая за реализацию дисциплины:**

Кафедра информационных систем

6. **Составители программы:**

Коваль Андрей Сергеевич, koval@cs.vsu.ru, ст.преп, факультет компьютерных наук, кафедра информационных систем

7. Рекомендована:

рекомендована НМС ФКН 05.03.2024, протокол № 5

8. Учебный год:

2024-2025

9.Цели и задачи учебной дисциплины:

изучение студентами методологии проектирования и реализации системы защиты информации, с учетом угроз, характерных для современных интранет-сетей. Ставятся задачи: на лекционных занятиях познакомить студентов с основами технологий обеспечения информационной безопасности (ИБ) и рассмотреть использование этих технологий для построения систем ИБ, снижающих риски, характерные для корпоративных сетей.

Студенты, после успешного прохождения курса могут проектировать и реализовывать системы защиты интранет сетей с учетом характерных для них угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с использованием аппаратных решений.

10. Место учебной дисциплины в структуре ООП:

дисциплина вариативной части цикла (Б1.В). Входные знания: «Иностранный язык в профессиональной сфере», «Введение в программирование». Требуются знания в области инфокоммуникационных систем и сетей уровня бакалавра.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-4 Способен выполнять проектирование структур данных и баз данных	ПК-4.1 Умеет применять методы и средства проектирования программного обеспечения, структур данных, баз данных	знать: типовое использование технологий обеспечения информационной безопасности для построения систем ИБ, снижающих риски, характерные для корпоративных сетей; уметь: применять методы и средства проектирования систем защиты интранет-сетей с учетом характерных для них угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с использованием аппаратных решений; реализовывать системы защиты интранет-сетей;

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 1	Всего
Аудиторные занятия	12	12
Лекционные занятия	6	6
Практические занятия		0
Лабораторные занятия	6	6
Самостоятельная работа	92	92
Курсовая работа		0
Промежуточная аттестация	4	4
Часы на контроль	4	4
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности	Интранет сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
2	Сети IPv4, IPv6 и технология IPSec	IPSec – технология для сетей, построенных на IPv4 и IPv6.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
3	Технологии виртуальных частных сетей	VPN технологии: задачи, основные типы, способы реализации.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
4	RADIUS. Сетевой карантин	NAS-серверы. Централизация аутентификации на основе RADIUS. Отказоустойчивость RADIUS.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
5	Инфраструктураоткрытых ключей.Смарт-карты.	Инфраструктура открытых ключей. Различные архитектуры доверия. Проблемы развертывания и многоуровневые PKI решения. Многофакторная аутентификация, смарт-карты	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
6	Безопасность хранения и обработки данных в ОС хостов	Безопасность хранения данных. Шифрация данных масштаба файлов, файловых систем, носителей. Безопасность ОС в корпоративной сети: шаблоны и эталоны безопасности, системы обновлений.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения.	Безопасность сетевых устройств 2 уровня с ОС IOS. Безопасность сетевых устройств 3 уровня с ОС IOS. TACACS, RADIUS – решения для сетевого оборудования.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
8	Аппаратная реализация IPSec, VPN.	Реализация IPSec в ОС IOS. Реализация VPN в ОС IOS.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Аппаратная реализация межсетевых экранов, IDS, IPS.	Обеспечение ИБ интранет сетей - как задача управления рисками. Стратегии управления рисками, технологии внедрения управления рисками. Проектирование модульной инфраструктуры интранет сетей на основе типовых решений (проект CISCO SAFE).	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2	Сети IPv4, IPv6 и технология IPSec (лаб.)	Создание IPSec соединения между серверами Windows с сертификационной аутентификацией	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
3	Технологии виртуальных частных сетей (лаб.)	Развертывание RAS сервера в Windows и настройка VPN подключения с использованием PPTP.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
4	RADIUS. Сетевой карантин (лаб.)	Установка RADIUS сервера IAS и политик доступа для VPN клиентов. NPS. NAP.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
5	Инфраструктура открытых ключей. Смарт-карты. (лаб.)	Развертывание 2-уровневой PKI на компьютерах под управлением Windows Server. Создание сертификационных шаблонов для автовыпуска сертификатов. Создание субъекта, уполномоченного выпускать сертификаты для смарт-карты. Резервное копирование в PKI. Создание DRA и KRA.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения. (лаб.)	Обеспечение безопасности коммутаторов с ОС IOS. Обеспечение безопасности коммутаторов 3 уровня и маршрутизаторов с ОС IOS. Настройка TACACS, RADIUS для централизованной аутентификации.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
8	Аппаратная реализация IPSec, VPN. (лаб.)	Реализация IPSec в ОС IOS занятие 1, 2. Реализация VPN в ОС IOS с помощью SDM. Реализация VPN в ОС IOS в командном интерфейсе.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Аппаратная реализация межсетевых экранов, IDS, IPS. (лаб.)	Аппаратная реализация межсетевых экранов на основе пакетной фильтрации. Аппаратная реализация зональных межсетевых экранов на основе классификаторов трафика. Аппаратная реализация IPS (IOS).	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности	0	0	0	4	4
2	Сети IPv4, IPv6 и технология IPSec	2	0	2	6	10
3	Технологии виртуальных частных сетей	2	0	2	6	10
4	RADIUS. Сетевой карантин	0	0	0	8	8

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
5	Инфраструктура открытых ключей. Смарт карты.	2	0	2	14	18
6	Безопасность хранения и обработки данных в ОС хостов	0	0	0	15	15
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения.	0	0	0	18	18
8	Аппаратная реализация IPSec, VPN.	0	0	0	18	18
9	Аппаратная реализация межсетевых экранов, IDS, IPS.	0	0	0	3	3
		6	0	6	92	104

14. Методические указания для обучающихся по освоению дисциплины

Дисциплина требует работы с файлами-презентациями лекций и соответствующими главами рекомендованной основной литературы, а также, обязательного выполнения всех лабораторных заданий в компьютерном классе. Самостоятельная подготовка к лабораторным занятиям не требуется, т.к. необходимые рекомендации даются в аудитории, где выполняются лабораторные работы.

Самостоятельная работа проводится в компьютерных классах ФКН с использованием методических материалов расположенных на учебно-методическом сервере ФКН "\\fs.cs.vsu.ru\Library” и на сервере Moodle ВГУ edu.vsu.ru и выполнением задач конфигурирования виртуализированной ИС. Во время самостоятельной работы студенты используют электронно-библиотечные системы, доступные на портале Зональной Библиотеки ВГУ по адресу www.lib.vsu.ru. Часть заданий может быть выполнена вне аудиторий на домашнем компьютере, после копирования методических указаний и необходимого ПО с учебно-методического сервера ФКН.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	Булычёв, Г. Г. Программно-аппаратные средства защиты информации : учебно методическое пособие / Г. Г. Булычёв. — Москва : РТУ МИРЭА, 2022 — Часть 1 — 2022. — 203 с. — ISBN 978-5-7339-1652-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310781 (дата обращения: 23.05.2023).
2	Булычёв, Г. Г. Программно-аппаратные средства защиты информации : учебно методическое пособие / Г. Г. Булычёв. — Москва : РТУ МИРЭА, 2022 — Часть 2 — 2022. — 177 с. — ISBN 978-5-7339-1653-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/310784 (дата обращения: 23.05.2023). — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
1	Основы работы в программе CISCO PACKET TRACER : учебно-методическое пособие / составители Г. В. Абрамов [и др.]. — Воронеж : ВГУ, 2017. — 31 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154795 (дата обращения: 23.05.2023).
2	Нестеров, С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : практическое пособие / С.А. Нестеров. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2009. – 233 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book&id=234529
3	Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов : [16+] / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 224 с. — Университетская библиотека онлайн : электронно библиотечная система. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=93351

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Библиотека ВГУ, http://www.lib.vsu.ru
2	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
3	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
2	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

1. Технологии виртуализации:
Среда виртуализации Oracle/Sun Virtual Box
2. Электронно-библиотечная системы «Университетская библиотека online» (http://biblioclub.ru) и «Лань» (http://lanbook.com)
3. Образовательный портал Moodle (сервер Moodle ВГУ)
4. Серверные и клиентские ОС Microsoft.
5. Операционная система GNU/Linux (дистрибутив CentOS)

18. Материально-техническое обеспечение дисциплины:

1. Лекционная аудитория, оснащенная видеопроектором.
2. Компьютерный класс для проведения лабораторных занятий, оснащенный программным обеспечением VirtualBox. Объем свободной после загрузки ОС оперативной памяти на рабочее место не менее 4 ГБ (требуется для виртуальных машин).

3. Лаборатории программно-аппаратных средств обеспечения информационной безопасности (ауд.303п), включающая аппаратно-программные СЗИ: смарт-карты, RFID-токены и карты, карт-ридеры; аппаратные IPS, IDS, VPN системы; развернутая виртуальная сетевая инфраструктура для выполнения лабораторных работ с аппаратными сетевыми экранами и VPN. Учебно-методический комплекс "Программно-аппаратная защита сетей с защитой от НСД" ОАО "ИнфоТеКС". АПКШ «Континент».
4. Лаборатория безопасности компьютерных сетей (ауд. 384), включающая коммутаторы и маршрутизаторы CISCO, аппаратный межсетевой экран, программный анализатор сетевого трафика WireShark. Программный симулятор, для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	1-9	ПК-4	ПК-4.1	Контрольные работы 1-3. Практические задания №1-8
2				

Промежуточная аттестация

Форма контроля - Зачет с оценкой

Оценочные средства для промежуточной аттестации

Письменная контрольная работа. Одно из лабораторных заданий

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Технология проведения:

Текущая аттестация проводится в формах письменных (или в электронном виде на сайте edu.vsu.ru) контрольных работ по лекциям и лабораторных заданий. Оценки за вопросы каждой контрольной работы суммируются и сумма затем нормируется к 50-балльному значению. Каждая лабораторная работа оценивается как выполненная или невыполненная согласно критериям в её описании на edu.vsu.ru. В конце семестра вычисляется средняя оценка за все контрольные работы и лабораторные задания. Эта оценка является оценкой за работу студента в течение всего семестра и используется для расчета итоговой оценки по предмету (см. раздел 20.2).

Соотношение показателей, критериев и шкалы оценивания результатов обучения

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Верные ответы на все вопросы контрольной работы. Все критерии выполнения и работоспособности в лабораторных заданиях - удовлетворены.	Повышенный уровень	Отлично
Верные ответы на большую часть вопросов контрольной работы. Большая часть критериев выполнения и работоспособности в лабораторных заданиях - удовлетворена.	Базовый уровень	Хорошо
Верные ответы на наиболее важные части вопросов контрольной работы. Базовая часть критериев выполнения и работоспособности в лабораторных заданиях - удовлетворена.	Пороговый уровень	Удовлетворительно
Нет или крайне мало верных ответов на наиболее важные части вопросов контрольной работы. Базовая часть критериев выполнения и работоспособности в лабораторных заданиях – не удовлетворена.	-	Неудовлетворительно

Формирование оценок:

При оценивании результатов текущей аттестации используется количественная шкала оценок. Упомянутая выше 50-балльная средняя оценка определяет уровень сформированности компетенций и влияет на итоговую оценку (см. раздел 20.2).

Перечень вопросов контрольных работ

К.Р. 1

1. Как возникает пара ключей при создании сертификата в PKI и где хранится закрытый, а где открытый ключи?
2. Для чего используется протокол AH в IPsec? Что такое SA, main-mode (основной режим) quick-mode (оперативный режим)? Какие три вида аутентификации конечных систем обычно поддерживаются в реализациях IPsec? Когда (в каких сценариях) какой используется?
3. В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС

выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие уровни/вида шифрования будут задействованы при посылки пользователем зашифрованного письма на этот АП, какие соответствующие ключи потребуются для расшифрования сообщения, где эти ключи находятся (кому принадлежат/доступны)?
4. Для чего используются фильтры IPsec? Какие последствия применения IPsec без фильтров или с грубыми фильтрами (например, теми, что установлены по-умолчанию на виртуальных машинах лабораторных занятий этого курса)?
5. Какова специфика работы IPsec при использовании NAT (как решаются проблемы и в какой степени их вообще возможно решить)?
6. В ходе конфигурирования VIPnet на рабочем месте администратора с помошью ЦУС выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие ключи должны быть переданы на АП, как они связаны между собой и каково назначение каждого?
7. Меры обеспечения информационной безопасности для инфраструктуры PKI: что и как следует защищать в PKI инфраструктуре (так же опишите месторасположение критических элементов PKI, которые требуют защиты)?
8. Какие существуют методы восстановления закрытых ключей, как можно решить проблему их потери, какие инструменты для этого потребуются?

K.P. 2

1. В ходе конфигурирования VIPnet на рабочем месте администратора с помошью ЦУС выполнена адресная администрация сети и добавлен новый пользователь. Какие ключи должны быть переданы пользователю, как они связаны между собой и каково назначение каждого?
2. Для чего необходима иерархия удостоверяющих центров, почему недостаточно одного? В каких случаях создание иерархии оправдано? Что такое кросс-сертификация? Что такое публичный и частный УЦ, когда используются?
3. Что такое KRA, как создается и работает? Какие уязвимости в PKI появляются при работе RA и как их можно закрыть, хотя бы частично?
4. В ходе конфигурирования ViPNet на рабочем месте администратора потребовалолсь добавить еще один "Абонентский Пункт" для администрации нового района города. Опишите последовательность действий администратора ViPNet (схематично, но по шагам) для введения этого АП (компьютер уже закуплен).
5. Какие требования к IP-сети предъявляют обычно VPN-технологии? Почему современные реализации VPN часто используют транспорт 443/TCP?
6. Назовите типы и роли CA. Что принимают во внимание при проектировании иерархии PKI?
7. Не заработал АПКШ в роли криптошлюза: в ПУ ЦУС статус "не включен".Вы решили проверить доступность АПКШ со стороны компьютера администратора командой ping. Команда показала таймауты от IP-адреса криптошлюза. Говорит ли это о том, что компьютер Администратора и криптошлюз в данный момент не обмениваются пакетами? В какой последовательности Вы бы искали причину по которой АПКШ "не включен" в ПУ ЦУС и каковы возможные причины этого?
8. В каких сценариях целесообразно использовать транспортный, а в каких - туннельный режим IPSec?
9. Опишите жизненный цикл закрытого ключа: где происходит его формирование, где он может храниться, куда может перемещаться/передаваться.

K.P.

1. В ходе лабораторных вы создавали VPN-подключение PPTP и аналогичное по функционалу

L3VPN решение с применением АПКШ Континент. Как отличается скорости развертывания этих решений для создания защищенной сети с очень большим количеством рабочих мест (точек подключения к VPN)? Объясните почему одно из решений потребует значительно большего времени и усилий. Опишите по шагам последовательность действий по развертыванию PPTP и СД-Континент решений.

2. Как проверить работу криптокоммутаторов, расположенных в филиалах (опишите последовательность действий)?
3. Какие существуют методы восстановления закрытых ключей, как можно решить проблему их потери, какие инструменты для этого потребуются? Приведите пример реакции на потерю секретного ключа от сертификата пользователя, например, в результате повреждения профиля, где он хранился (пользователь зашифровал множество файлов этим ключом).
4. В ходе конфигурирования в ПУ ЦУС был создан новый криптошлюз для администрации нового района города. Опишите последовательность действий администратора (схематично, но по шагам) по дальнейшей настройке этого криптошлюза.
5. Опишите жизненный цикл сертификата от момента его создания. Как именно создается сертификат, в какой последовательности. Как в этом процессе участвует CA? Инструменты/утилиты для выпуска сертификатов. Как пользователи PKI получают доступ к сертификату УЦ? Как пользователи PKI получают доступ к списку отзыва УЦ?
6. Какова специфика работа VPN при использовании NAT (как решаются проблемы и какие)?
7. Формируется новая защищенная сеть с использованием АПКШ Континент. Опишите последовательность действий по включению в сеть КШ с ЦУС. Чем решение КШ ЦУС отличается от ЦУС ViPNet?

Перечень лабораторных заданий

N	Задачи лабораторной работы
1	Создание IPSec соединения между серверами Windows с сертификационной аутентификацией
2	Развертывание RAS-сервера в Windows и настройка VPN подключения с использованием PPTP.
3	Установка RADIUS-сервера IAS и политик доступа для VPN-клиентов. NPS. NAP.
4	Развертывание 2-уровневой PKI на компьютерах под управлением Windows Server. Создание сертификационных шаблонов для автовыпуска сертификатов. Создание субъекта, уполномоченного выпускать сертификаты для смарт-карты. Резервное копирование в PKI. Создание DRA и KRA.
5	Развертывание EFS. Шифрация BitLocker Drive. Применение эталонных шаблонов безопасности к серверной и клиентской ОС (Windows 2003, XP). Создание инфраструктуры WSUS в лабораторной сети.
6	Обеспечение безопасности коммутаторов с ОС IOS. Обеспечение безопасности коммутаторов 3 уровня и маршрутизаторов с ОС IOS. Настройка TACACS, RADIUS для централизованной аутентификации.
7	Реализация IPSec в ОС IOS занятие 1, 2. Реализация VPN в ОС IOS с помощью SDM. Реализация VPN в ОС IOS в командном интерфейсе.

8	Аппаратная реализация межсетевых экранов на основе пакетной фильтрации. Аппаратная реализация зональных межсетевых экранов на основе классификаторов трафика. Аппаратная реализация IPS (IOS).

Оценка остаточных знаний

ПК-5

Задания закрытого типа

1. Не заработал АПКШ в роли криптошлюза: в ПУ ЦУС статус "не включен", таблица arp после команды ping содержит MAC-адрес АПКШ. Возможные причины такого статуса?
   A. неверная IP-конфигурация компьютера управления или АПКШ
   B. несоответствие ключевой информации АПКШ и ПУ ЦУС
   C. отсутствие правил, разрешающих прохождение пакетов для ping
   D. неисправности физического подключения компьютера с ПУ ЦУС или АПКШ к сети
2. Не заработал АПКШ в роли криптошлюза: в ПУ ЦУС статус "не включен", таблица arp показывает отсутствие ответа о MAC-адресе от АПКШ. Возможные причины такого статуса?
   A. неверная IP-конфигурация компьютера управления или АПКШ
   B. несоответствие ключевой информации АПКШ и ПУ ЦУС
   C. отсутствие правил, разрешающих прохождение пакетов для ping
   D. неисправности физического подключения компьютера с ПУ ЦУС или АПКШ к сети
3. Как возникает пара ключей при создании сертификата в PKI ?
   A. генерируется на стороне клиента
   B. генерируется на стороне удостоверяющего центра
   C. генерируется на стороне корневого удостоверяющего центра
   D. генерируется на стороне CRL
   E. генерируется на стороне AIA
4. Где может формироваться пара ключей при создании сертификата в PKI ?
   A. на смарт-карте
   B. на стороне удостоверяющего центра
   C. на стороне корневого удостоверяющего центра
   D. на стороне CRL
   E. на стороне AIA
5. В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие ключи должны быть переданы на АП?
   A. ключи обмена коллективов, ключи защиты ключей обмена, ключи связи с ЦУС
   B. ключи защиты ключей обмена, действующий персональный ключ, ключи подписи
   C. ключи обмена коллективов, действующий персональный ключ, ключи подписи
   D. ключи обмена коллективов, ключи защиты ключей обмена, действующий персональный ключ
   E. ключи обмена коллективов, ключи защиты ключей обмена, ключи подписи
   F. действующий персональный ключ, ключи подписи
6. В ходе конфигурирования VIPnet на рабочем месте администратора с помощьюЦУС выполнена адресная администрация сети и добавлен новый пользователь. Какие ключи должны быть переданы пользователю?
   A. ключи обмена коллективов, ключи защиты ключей обмена, ключи связи с ЦУС
   B. ключи защиты ключей обмена, действующий персональный ключ, ключи подписи
   C. ключи обмена коллективов, действующий персональный ключ, ключи подписи

D. ключи обмена коллективов, ключи защиты ключей обмена, действующий персональный ключ
E. ключи обмена коллективов, ключи защиты ключей обмена, ключи подписи
F. действующий персональный ключ, ключи подписи

7. Какие уязвимости в PKI появляются при использовании KRA?
   A. передача открытого ключа через сеть
   B. передача закрытого ключа через сеть
   C. передача ключевой пары через сеть
   D. генерация ключевой пары не на стороне клиента
8. Какие уязвимости в PKI появляются при использовании KRA?
   A. передача открытого ключа через сеть
   B. хранение закрытого ключа не на стороне клиента
   C. передача ключевой пары через сеть
   D. генерация ключевой пары не на стороне клиента
   E. хранение открытого ключа не на стороне клиента
9. Компоненты VPN (как системы удаленного доступа) обязательно доолжны включать:
   A. NAS
   B. DHCP
   C. AAA
   D. ADDS
   E. Kerberos
10. Компоненты VPN (как системы удаленного доступа) могут включать:
    A. NYS
    B. YP
    C. AAA
    D. WPA
    E. AIA

Задания открытого типа

1. Вы ищете неисправность IPsec (неверная конфигурация, IPsec - не работает). Для этого включили захват всего трафика через интерфейс и инициировали передачу данных. Выключив захват, пакеты какого протокола вы увидите первыми, если фаза IKE начала работу?
2. Вы ищете неисправность IPsec (неверная конфигурация, IPsec - не работает). Для этого включили захват всего трафика через интерфейс и инициировали передачу данных. Выключив захват, UDP-дейтаграммы с каким номером порта вы увидите первыми, если фаза IKE начала работу?
3. Самый быстрый вариант проверки CRL (в публичных сетях) требует вариант опубликования (HTTP, HTTPS, OCSP, CIFS/SMB, FTP):
4. Из трех основных свойств информации: целостности, доступности и конфиденциальности, протокол AH в IPsec применяется для обеспечения свойства

Задание с развёрнутым ответом

1. Что такое L2 VPN? Опишите сценарии, при которых возникает необходимость в реализации этой технологии.

2. В чем отличия транспортного от туннельного режима IPSec? В каких сценариях целесообразно использовать каждый режим?

20.2 Промежуточная аттестация

Технология проведения:

Промежуточная аттестация проводится в форме письменной контрольной работы при обязательном условии выполнения в течение семестра всех лабораторных заданий и с учетом полученных текущих оценок. Оценки за вопросы контрольной работы суммируются, сумма нормируется к 50-балльному значению.

Требования к выполнению заданий, шкалы и критерии оценивания

При оценивании результатов промежуточной аттестации используется количественная шкала оценок. Согласно положению о балльно-рейтинговой системе обучения, 50-балльная оценка за итоговую контрольную работу складывается с оценкой, полученной по итогам аттестаций. Полученное 100-балльное значение определяет уровень сформированности компетенций и итоговую оценку (согласно положению о балльно-рейтинговой системе обучения):

оценка «отлично» – 90...100 баллов

оценка «хорошо» – 70...89 баллов

оценка «удовлетворительно» – 50...69 баллов

оценка «неудовлетворительно» – 0...49 баллов

Перечень вопросов к итоговой контрольной работе

№	Вопросы контрольной работы
1	Что такое IPsec, какие задачи решает, в чем отличие и/или несоответствие термину VPN? Как настроить IPsec, что такое фильтры, политики IPsec? Какие средства служат для отладки IPsec? Какие уже готовые политики IPsec предконфигурированы на ОС семейства Windows?
2	Опишите жизненный цикл сертификата от момента его создания. Как именно создается сертификат, в какой последовательности. Как в этом процессе участвует CA? Инструменты/утилиты для выпуска сертификатов.
3	Меры обеспечения информационной безопасности для инфраструктуры PKI.
4	Что такое удостоверяющий центр (CA – Certification Authority)? Назовите типы и роли CA. Что такое иерархия CA, что принимают во внимание при проектировании этой иерархии?
5	Что такое транспортный режим и туннельный режим IPsec? Для чего используется протокол IKE в IPsec? Для чего используются фильтры IPsec?
6	Что такое WSUS, какие задачи решает, из каких компонентов состоит? MBSA – основные режимы и возможности.
7	Для чего используются протоколы ESP AH в IPsec? Какие проблемы могут возникать у IPsec при использовании NAT?
8	Что такое VPN, перечислите компоненты VPN. Какие существуют технологии реализации VPN, какие требования к IP-сети предъявляет каждая технология?
9	Для чего используется протокол IKE в IPsec? Что такое SA, main-mode (основной режим) quick-mode (оперативный режим)? Какие три вида аутентификации конечных систем обычно поддерживаются в реализациях IPsec? Когда какой используется?
10	Что такое сетевой экран уровня «приложения», в чем отличие от сетевого экрана «пакетный фильтр»? Что такое unsolicited трафик и чем отличаются файерволы statefull и stateless? Как размещены по отношению к корпоративной сети сетевые экраны, опишите основные архитектуры

11	Что такое EFS, какие задачи решает, из каких компонентов состоит? Как технически реализована возможность расшифровки файла другими пользователями, перечислите условия, в которых это возможно?