Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

 03.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.50 Безопасность компьютерных сетей

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

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 03.05.2023, протокол № 7

8. Учебный год:

2026-2027

9.Цели и задачи учебной дисциплины:

изучение студентами методологии проектирования и реализации мер обеспечения информационной безопасности (ИБ) компьютерных сетей, с учетом угроз, характерных для современных инфокоммуникационных систем и сетей. Ставятся задачи: на лекционных занятиях познакомить студентов с основами технологий обеспечения ИБ компьютерных сетей, на лабораторных занятиях выработать навыки применения этих технологий в рамках общей методологии снижения рисков характерных, прежде всего, для корпоративных сетей.

10. Место учебной дисциплины в структуре ООП:

Дисциплина обязательной части (Б1.О). Для успешного освоения дисциплины необходимы входные знания в области "основ информационной безопасности", "сетей и систем передачи информации",

"операционных систем".

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
ОПК-1.1 Способен разрабатывать и реализовывать полики управления доступом в компьютерных системах;	ОПК-1.1.6 умеет использовать криптографические протоколы, применяемые в компьютерных сетях	уметь: планировать и устанавливать инфраструктуры открытых ключей, VPN-решения
ОПК-1.1 Способен разрабатывать и реализовывать полики управления доступом в компьютерных системах;	ОПК-1.1.7 владеет настройкой программных и аппаратных средств построения компьютерных сетей, в том числе использующих криптографическую защиту информации	владеть: методами обеспечения защиты данных на этапе передачи в IP-сетях
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.1 знает виды политик управления доступом и информационными потоками в компьютерных сетях	зхнать: полномочную и дискреционную политики доступом
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.2 умеет настраивать правила обработки пакетов в компьютерных сетях	уметь: конфигурировать сетевые экраны 2-7 уровней
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.3 владеет навыками управления средствами межсетевого экранирования в компьютерных сетях	владеть: методами выбора типов и топологий сетевого экранирования
ОПК-1.1 Способен разрабатывать и реализовывать полики управления доступом в компьютерных системах;	ОПК-1.1.5 знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы	знать: принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой,Контрольная работа

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 8	Всего
Аудиторные занятия	72	72
Лекционные занятия	36	36
Практические занятия		0
Лабораторные занятия	36	36
Самостоятельная работа	36	36
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Общие принципы проектирования современных компьютерных сетей.	Общие принципы проектирования современных компьютерных сетей. Известные модели построения сетей. Модель корпоративной сети CISCO. Проектирование на основе шаблонов.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
2	Проектирование защищенных сетей.	Идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для случаев возможных нарушений безопасности. Стандарты в области управления безопасностью сетей и систем на их основе.	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
3	Технология IPSec.	Технология IPSec и сопутствующие протоколы. Практическое конфигурирование и поиск неисправностей IPSec-инфраструктуры.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
4	Технологии виртуальных частных сетей. Виртуальные защищенные сети.	Технологии VPN и сопутствующие протоколы. Практическое конфигурирование и поиск неисправностей VPN-инфраструктуры. Виртуальные защищенные сети в решения ИнфоТеКС и Код Безопасности	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
5	RADIUS.	Централизация проверки подлинности. Используемые средства. Конфигурирование и управление централизованной системой AAA.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
6	Сетевой карантин.	Понятие и реализация сетевого карантина. Практическое конфигурирования карантина с различными видами «принуждения»: DHCP, IPsec, VPN.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
7	Инфраструктура открытых ключей.	Основы PKI. Сертификаты с цифровыми подписями. Стандарт X.509. Стандарты PKCS.	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	Аудит и Pen-тестирование.	Аудит ИБ Информационных Систем. Pen-тестирование. Упреждающие меры. Honeypot.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Безопасность хранения и обработки данных в ОС хостов.	Проблема защиты данных хостов. Файловые системы с шифрацией. Ограничение выполнения кода. Политики безопасности ОС.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
10	Безопасность сетевых устройств 2 и 3 уровней.	Известные уязвимости 2 и 3 уровней. Управление безопасностью на уровне доступа (port security). Основанная на политиках маршрутизация.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
11	Аппаратная реализация IPSec, VPN.	Проблемы производительности криптошлюзов, известные решения.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
12	Контекстный анализ трафика, DPI.	Контекстный анализ трафика, DPI. Аппаратная реализация межсетевых экранов, IDS, IPS.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
3	Технология IPSec. (лаб.)	Реализация IPSec взаимодействия между двумя конечными системами.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
4	Технологии виртуальных частных сетей. Виртуальные защищенные сети. (лаб.)	Формирование VPN-сети с использованием распределенной проверки подлинности.	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
5	RADIUS. (лаб.)	Формирование VPN-сети с использованием централизованной проверки подлинности на AAA-сервере (RADIUS).	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
6	Сетевой карантин. (лаб.)	Сетевой карантин NAP/NPS.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
7	Инфраструктура открытых ключей. (лаб.)	Создание корпоративной иерархической системы PKI.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
7	Инфраструктура открытых ключей. (лаб.)	Внедрение PKI на основе отечественных криптоалгоритмов.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
8	Аудит и Pen-тестирование. (лаб.)	Аудит и Pen-тестирование. Honeypot.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Безопасность хранения и обработки данных в ОС хостов. (лаб.)	Защита данных конечных систем (EFS).	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Безопасность хранения и обработки данных в ОС хостов. (лаб.)	Ограничение выполнения ПО в конечных системах. Secret Net Studio	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Безопасность хранения и обработки данных в ОС хостов. (лаб.)	Распределенное и централизованное управление обновлениями с помощью WSUS.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
10	Безопасность сетевых устройств 2 и 3 уровней. (лаб.)	Сетевые экраны и типовые архитектуры на их основе.	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
10	Безопасность сетевых устройств 2 и 3 уровней. (лаб.)	Обеспечение ИБ на 2 уровне корпоративных сетей.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
11	Аппаратная реализация IPSec, VPN. (лаб.)	Аппаратные средства IPSec и VPN. АПКШ Континент. Знакомство с ViPNet.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
12	Контекстный анализ трафика, DPI. (лаб.)	ViPNet IDS. Snort.	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	Общие принципы проектирования современных компьютерных сетей.	2		0	2	4
2	Проектирование защищенных сетей.	2		4	2	8
3	Технология IPSec.	4		4	3	11
4	Технологии виртуальных частных сетей. Виртуальные защищенные сети.	4		2	2	8
5	RADIUS.	2		2	4	8
6	Сетевой карантин.	2		2	2	6

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
7	Инфраструктура открытых ключей.	4		4	5	13
8	Смарт-карты.	2		2	2	6
9	Безопасность хранения и обработки данных в ОС хостов.	2		2	4	8
10	Безопасность сетевых устройств 2 и 3 уровней.	4		2	4	10
11	Аппаратная реализация IPSec, VPN.	6		8	2	16
12	Контекстный анализ трафика, DPI.	2		4	4	10
		36	0	36	36	108

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. Большая 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	Мэйволд, Э. Безопасность сетей : учебное пособие : [16+] / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 23.05.2023). – Текст : электронный.
2	Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие : [16+] / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 23.05.2023). – Библиогр. в кн. – Текст : электронный.

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).

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	Электронный университет ВГУ, http://edu.vsu.ru

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

- Среда виртуализации KVM/libvirt

2. Электронно-библиотечные системы «Университетская библиотека online» (http://biblioclub.ru), «Лань» (http://lanbook.com)

3. Образовательный портал Moodle (сервер Moodle ВГУ)

4. Серверные и клиентские ОС Microsoft.

5. Операционная система GNU/Linux (дистрибутив CentOS).

6. Аппаратные сетевые экраны D-Link, CISCO.

7. АПКШ Континент IPC-25 в исполнении ЦУС и КШ компании «ООО Код Безопасности»

8. ПО Secret Net Studio компании «ООО Код Безопасности»

9. ПО VipNet и ПАК, IDS компании ОАО ИнфоТеКС.

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 8 ГБ (требуется для виртуальных машин).

3. Лаборатория программно-аппаратных средств обеспечения информационной безопасности (ауд. 303п), включающая аппаратно-программные СЗИ, в т.ч. решения VipNet, Континент, SNS, D-Link, CISCO.

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	4-8	ОПК-1.1	ОПК-1.1.6	Лаб.3-5 , К.Р.1
2	9,10	ОПК-1.1	ОПК-1.1.7	Лаб.7,9 , К.Р.2
3	1-2,9	ОПК-1.2	ОПК-1.2.1	Лаб.2,6 , К.Р.1
4	8	ОПК-1.2	ОПК-1.2.2	Лаб.8 , К.Р.2
5	11,12	ОПК-1.2	ОПК-1.2.3	Лаб.10 , К.Р.3
6	3,11,12	ОПК-1.1	ОПК-1.1.5	Лаб.1, 11,12 , К.Р.3

Промежуточная аттестация

Форма контроля - Зачет с оценкой,Контрольная работа

Оценочные средства для промежуточной аттестации

Контрольная работы. Все лабораторные задания.

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).

Вопросы к итоговой контрольной работе 1

1. Почему для port-security чаще используют MAC, а не более надежный 802.1x . Опишите что нужно, для конфигурирования (по шагам) первого и второго варианта и, если есть, возможные сценарии преодоления этих способов защиты.
2. В ходе конфигурирования VIPnet на рабочем месте администратора с помошью 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).
3. 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?
4. Активное и пассивное тестирование IP-сети. Реализование в Nmap метода исследования IP-узлов.

Вопросы к итоговой контрольной работе 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. Как проверить работу криптокоммутаторов, расположенных в филиалах? В чем отличие от L3VPN решения с использованием криптокоммутаторов?
3. В ходе лабораторных вы создавали VPN-подключение PPTP и аналогичное по функционалу L3VPN решение от Кода Безопасности 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.
4. В ходе конфигурирования ViPNet на рабочем месте администратора потребовалось 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. Контексная фильтрация трафика.
6. Преимущества и недостатки МСЭ с 5-элементным кортежем (5-tuple).

Вопросы к итоговой контрольной работе 3

1. 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)?
2. Какова специфика работы IPsec при использовании NAT (как решаются проблемы и в какой степени их вообще возможно решить)?
3. В каких сценариях целесообразно использовать транспортный, а в каких - туннельный режим IPSec?
4. Опишите жизненный цикл закрытого ключа: где происходит его формирование, где он может храниться, куда может перемещаться/передаваться.

Перечень лабораторных заданий

	Лабораторные задания (подробное описание, а также необходимое ПО, конфигурационные файлы, скрипты и пояснения находятся на серверах \\FS\Library, edu.vsu.ru)
1	Реализация IPSec взаимодействия между двумя конечными системами.
2	Формирование VPN-сети с использованием централизованной проверки подлинности на AAA-сервере (RADIUS).Сетевой карантин
3	Создание корпоративной иерархической системы PKI.
4	Защита данных конечных систем (EFS). Ограничение выполнения ПО в конечных системах. Secret Net Studio
5	Сетевые экраны и типовые архитектуры на их основе. ViPNet-IDS. Snort.
6	Обеспечение ИБ на 2 уровне корпоративных сетей. APR. Port Security.

7	Аппаратные средства IPSec и VPN. Аппаратные сетевые экраны: IPS/IDS (CISCO ASA, D-Link DFL)
8	Honeypot.
9	Pen-тестирование. Xspider.

Оценка остаточных знаний

ОПК-1.1

Задания закрытого типа

1. 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
2. В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС 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
3. Компоненты VPN (как системы удаленного доступа) могут включать:
    A. NYS
    B. YP
    C. AAA
    D. WPA
    E. AIA
4. Какие существуют методы восстановления закрытых ключей, например, в случае их повреждения?
    A. агент восстановления ключей
    B. экспорт
    C. агент восстановления данных
    D. шаблон сертификата
    E. отзыв сертификата
5. Как проверить работу криптокоммутаторов, расположенных в филиалах?
    A. ping на узел внутри одной IP-сети; узел должен находиться в другом филиале
    B. ping на узел IP-сети другого филиала
    C. ping на узел внутри одной IP-сети; узел должен находиться в том же филиале
6. Выберите вид топологии сетевых экранов,
    A. Централизованная
    B. Бастион
    C. Распределенная
    D. Активная
    E. Пассивная

7. Выберите вид топологии сетевых экранов,
    A. Централизованная
    B. Спина-к-спине
    C. Распределенная
    D. Активная
    E. Пассивная
8. Выберите вид топологии сетевых экранов,
    A. Централизованная
    B. Трехногая
    C. Распределенная
    D. Активная
    E. Пассивная
9. Что необходимо сделать в первую очередь, при потере секретного ключа от сертификата пользователя, используемого для проверки подлинности.
    1. добавить серийный номер сертификата в CRL
    2. добавить серийный номер сертификата в AIA
    3. добавить отпечаток сертификата в CRL
    4. восстановить из архива сохраненный предварительно ключ
    5. обратиться к KRA для восстановления
10. В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие уровни/виды шифрования будут задействованы при посылки пользователем зашифрованного письма на этот АП?
    A. на прикладном уровне
    B. на сетевом уровне
    C. на транспортном уровне
    D. на сетевом и транспортном уровнях
    E. на прикладном и транспортном уровнях
    F. на сетевом и канальном уровнях
    G. на канальном уровне

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. Самый быстрый вариант проверки CRL (в публичных сетях) требует вариант опубликования (HTTP, HTTPS, OCSP, CIFS/SMB, FTP):

Задание с развёрнутым ответом

1. Что представляет собой технологическое решение Microsoft "шаблоны сертификатов"? Какими инструментами с ними работают и для чего они используются? (вспомните лабораторные)

ОПК-1.2

Задания закрытого типа

1. Формируется новая защищенная сеть с использованием АПКШ Континент. Последовательность действий по включению в сеть ЦУС включает в себя.

2. Назовите тип(ы) УЦ, приемлемые для получения сертификатов для смарткарт пользователей VPN.
    A. Standalone, Enterprise
    B. Root, Subordinate
    C. Public
    D. Private
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. Какие уязвимости в PKI появляются при использовании KRA?
    A. генерация ключевой пары не на стороне клиента
    B. передача ключевой пары через сеть
    C. передача закрытого ключа через сеть
    D. передача открытого ключа через сеть
5. Какие частично закрыть уязвимости в PKI, которые появляются при использовании KRA?
    A. постоянно не хранить закрытый ключ на стороне базы KRA.
    B. никогда не помещать закрытый ключ на стороне базы KRA
    C. не осуществлять передачу закрытого ключа через сеть.
6. Какие частично закрыть уязвимости в PKI, которые появляются при использовании KRA?
    A. удалить или деактивировать шаблон сертификата KRA
    B. не выпускать сертификат KRA
    C. не формировать пару ключей и сертификат KRA
7. Компоненты VPN (как системы удаленного доступа) обязательно доолжны включать:
    A. NAS
    B. DHCP
    C. AAA
    D. ADDS
    E. Kerberos
9. Какие существуют методы восстановления закрытых ключей, например, в случае их повреждения?
    A. импорт
    B. экспорт
    C. агент восстановления данных
    D. шаблон сертификата
    E. отзыв сертификата
10. Какие существуют методы восстановления закрытых ключей, например, в случае их повреждения?
    A. kra
    B. экспорт
    C. агент восстановления данных
    D. шаблон сертификата
    E. отзыв сертификата

Задания открытого типа

1. Из трех основных свойств информации: целостности, доступности и конфиденциальности,

протокол AH в IPsec применяется для обеспечения свойства

2. Из трех основных свойств информации: целостности, доступности и конфиденциальности, протокол ESP в IPsec применяется для обеспечения свойства:

Задание с развёрнутым ответом

1. 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

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? Что такое Zero-Day уязвимость?
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?
12	Что такое DPI, применимость IPS и IDS решений? Сетевой нейтралитет и особенности применения DPI в корпоративных сетях.
13	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)
14	Как проверить работу криптокоммутаторов, расположенных в филиалах? В чем отличие от L3VPN решения с использованием криптокоммутаторов?
15	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?