МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.42 Основы построения защищенных компьютерных сетей

1. Код и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки / специализация / магистерская программа:
Безопасность компьютерных систем и сетей
Математические методы защиты информации

3. Квалификация (степень) выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кибербезопасности информационных систем

6. Составители программы: Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована: НМС факультета ПММ, протокол № 5 от 22.03.2024

_____
отметки о продлении вносятся вручную)

8. Учебный год: 2027/2028 **Семестр(ы): 8**

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:

изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;

раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

10. Место учебной дисциплины в структуре ООП:

обязательная часть блока Б1.Для успешного освоения дисциплины необходимы входные знания в области "сетей и систем передачи информации", "компьютерных сетей", "операционных систем", "методов и средств криптографической защиты информации", "криптографических протоколов".

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-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.11 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	владеть: методом отладки групповых политик в режимах "результата" и "моделирования
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты	ОПК-9.9 умеет формулироватьи настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем;	уметь: разрабатывать политики и процедуры безопасности в области компьютерных сетей

информации от утечки по техническим каналам, сетей и систем передачи информации;	ОПК-9.11 Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных	знать: методологию проектирования СЗИ на основе анализа рисков
	ОПК-9.12 знает общие и специфические угрозы безопасности операционных систем и систем управлениябаз данных;	знать: классификациюугроз в контексте проектирования СЗИ
ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.10 умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем	уметь: разрабатывать политики и процедуры безопасности в области компьютерных сетей
ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования;	ОПК-15.7 владеет навыками администрирования компьютерных сетей;	владеть: навыками управления сетевым оборудованием
	ОПК-15.8 владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением;	владеть: навыками управления сетевым оборудованием и сетевыми ОС
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;	ОПК-16.1 знает средства и методы хранения и передачи аутентификационной информации в компьютерных системах и сетях;	знать: технологии удаленного доступа с использованием распределенной и централизованной проверками подлинности
	ОПК-16.2 знает механизмы реализации атак в сетях TCP/IP;	знать: типовые уязвимости 2 и 3 уровней
	ОПК-16.3 знает основные протоколы идентификации и аутентификации абонентов сети;	знать: методы проверки подлинности при удаленном доступе и с использованием AAA
	ОПК-16.4 знает защитные механизмы и средства обеспечения сетевой безопасности;	знать: принцип и реализации сетевого карантина

ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;	ОПК-16.5 знает средства и методы предотвращения и обнаружения вторжений;	знать: основы технологий DPI/IPS/IDS
	ОПК-16.6 умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;	уметь: конфигурировать групповые политики, связанные с реализацией процедур безопасности в ОС
	ОПК-16.7 умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях;	уметь: конфигурировать сетевые экраны типа "пакетный фильтр"; систему ViPNet IDS
	ОПК-16.8 умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;	уметь: создавать и конфигурировать защищенные сети на основе технологий VipNet, Континент, IPsec/VPN
	ОПК-16.9 владеет навыками настройки межсетевых экранов;	владеть: навыками конфигурирования L2-L7 экранов
	ОПК-16.10 владеет методиками анализа сетевоготрафика;	владеть: навыками перехвата и анализа сетевого трафика

12. Объем дисциплины в зачетных единицах/час:

4/144

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 8	Всего
Аудиторные занятия	56	56
Лекционные занятия	28	28
Практические занятия		0
Лабораторные занятия	28	28
Самостоятельная работа	52	52
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	144	144

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 корпоративнойсети CISCO. Проектирование на основе шаблонов.	https://edu.vsu.ru/course/
2	Проектирование защищенных сетей.	Идентификация угроз, анализ рисков, созданиесистемы противодействия, разработка ответных мер для случаев возможных нарушений безопасности. Стандарты в области управления безопасностью сетей исистем на их основе.	https://edu.vsu.ru/course/
3	Технология IPSec.	Технология IPSec и сопутствующие протоколы. Практическое конфигурирование и поиск неисправностей IPSec-инфраструктуры.	https://edu.vsu.ru/course/
4	Технологии виртуальных частных сетей. Виртуальные защищенные сети.	Технологии VPN и сопутствующие протоколы. Практическое конфигурирование и поиск неисправностейVPN-инфраструктуры.Виртуальные защищенные сети в решения ИнфоТеКС и Код Безопасности	https://edu.vsu.ru/course/
5	RADIUS.	Централизация проверки подлинности. Используемые средства. Конфигурирование и управление централизованной системой AAA.	https://edu.vsu.ru/course/
6	Сетевой карантин.	Понятие и реализация сетевого карантина. Практическое конфигурирования карантина с различнымивидами «принуждения»:DHCP, IPsec, VPN.	https://edu.vsu.ru/course/
7	Инфраструктура открытых ключей.	Основы PKI. Сертификаты с цифровыми подписями. Стандарт X.509. Стандарты PKCS.	https://edu.vsu.ru/course/

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
8	Смарт-карты.	Виды смарт-карт и карт памяти. ПО смарт-карт. Жизненные циклы карт. Практика программирования и применения смарт-карт.	https://edu.vsu.ru/course/
9	Безопасность хранения и обработки данных в ОС хостов.	Проблема защитыданных хостов. Файловые системы с шифрацией. Ограничение выполнения кода. Политики безопасностиОС.	https://edu.vsu.ru/course/
10	Безопасность сетевых устройств 2 и 3уровней.	Известные уязвимости 2 и 3 уровней. Управление безопасностью на уровне доступа (port security). Основанная на политиках маршрутизация.	https://edu.vsu.ru/course/
11	Аппаратная реализацияIPSec, VPN.	Проблемы производительности криптошлюзов, известные решения.	https://edu.vsu.ru/course/
12	Контекстный анализ трафика, DPI.	Контекстный анализ трафика, DPI. Аппаратная реализациямежсетевых экранов, IDS, IPS.	https://edu.vsu.ru/course/
3	Технология IPSec. (лаб.)	Реализация IPSec взаимодействия между двумя конечными системами.	https://edu.vsu.ru/course/
4	Технологии виртуальных частных сетей. Виртуальные защищенные сети. (лаб.)	Формирование VPN-сетис использованием распределенной проверки подлинности.	https://edu.vsu.ru/course/

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).	https://edu.vsu.ru/course/
6	Сетевой карантин. (лаб.)	Сетевой карантин NAP/NPS.	https://edu.vsu.ru/course/
7	Инфраструктура открытых ключей. (лаб.)	Создание корпоративной иерархической системы PKI.	https://edu.vsu.ru/course/
7	Инфраструктура открытых ключей. (лаб.)	Внедрение PKI на основеотечественных криптоалгоритмов.	https://edu.vsu.ru/course/
8	Смарт-карты. (лаб.)	Смарткарты и PKI.	https://edu.vsu.ru/course/
9	Безопасностьхранения и обработки данных в ОС хостов. (лаб.)	Защита данных конечных систем (EFS).	https://edu.vsu.ru/course/
9	Безопасностьхранения и обработки данных в ОС хостов. (лаб.)	Ограничение выполнения ПО в конечных системах.Secret Net Studio	https://edu.vsu.ru/course/
9	Безопасностьхранения и обработки данных в ОС хостов. (лаб.)	Распределенное и централизованноеуправление обновлениями с помощью WSUS.	https://edu.vsu.ru/course/
10	Безопасность сетевых устройств 2 и 3уровней. (лаб.)	Сетевые экраны и типовые архитектуры наих основе.	https://edu.vsu.ru/course/

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
10	Безопасность сетевых устройств 2 и 3уровней. (лаб.)	Обеспечение ИБ на 2 уровне корпоративных сетей.	https://edu.vsu.ru/course/
11	Аппаратная реализация IPSec, VPN. (лаб.)	Аппаратные средстваIPSec и VPN. АПКШ Континент. Знакомство cViPNet,	https://edu.vsu.ru/course/
12	Контекстный анализ трафика, DPI. (лаб.)	ViPNet IDS.	https://edu.vsu.ru/course/

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	1	7
5	RADIUS.	2		2	4	8
6	Сетевой карантин.	1		1	4	6

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
7	Инфраструктура открытых ключей.	2		2	6	10
8	Смарт-карты.	1		1	4	6
9	Безопасность хранения и обработки данных в ОС хостов.	2		2	8	12
10	Безопасность сетевых устройств 2 и 3 уровней.	4		2	4	10
11	Аппаратная реализация IPSec, VPN.	2		4	10	16
12	Контекстный анализ трафика, DPI.	2		4	4	10
		28	0	28	52	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 ПММ и на сервере Moodle ВГУ moodle.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.

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

№ п/п	Источник
1	*Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник : [16+] / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book&id=499170*
2	*Шаньгин, В. Ф. Информационная безопасность : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2014. — 702 с. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/50578*

б) дополнительная литература:

№ п/п	Источник
1	*Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/3032*
2	*Томаси, У. Электронные системы связи : практическое пособие / У. Томаси ; пер. Н.Л. Бирюков. – Москва : РИЦ Техносфера, 2007. – 1360 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book&id=135422*
3	*Хабракен, Д. Маршрутизаторы Cisco. Практическое применение : учебник / Д. Хабракен. — Москва : ДМК Пресс, 2008. — 320 с. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/1076*
4	*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*
5	*Жикун Чен, Технология Java Card ™ для смарт-карт: Архитектура и руководство программиста. Пер с англ. / Жикун Чен ; пер. И. Морозов ; пер. с англ. под ред. М. Смирнова, А. Гласман. – Москва : РИЦ Техносфера, 2008. – 342 с. : табл., схем. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=135425*

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Библиотека ВГУ, http://www.lib.vsu.ru

№ п/п	Источник
2	Электронный университет ВГУ, http://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
2	Электронный ресурс «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795

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 компании ОАО ИнфоТеКС.

18. Материально-техническое обеспечение дисциплины (см.файл МТО):

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).

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 длятекущей аттестации
1	9	ОПК-8 *Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей*	ОПК-8.11 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	Лаб.9
2	1,2	ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.9 Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем.	Лаб.1
3	2	ОПК-9	ОПК-9.11 Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных.	Лаб.2
4	2	ОПК-9	ОПК-9.12 Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных.	Лаб.2,8

5	1,2	ОПК-11 *Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации*	ОПК-11.10 Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.	Лаб.1
6	3	ОПК-15 *Способен администрировать компьютерные сети и контролировать корректность их функционирования*	ОПК-15.7 Владеет навыками администрирования компьютерных сетей.	Лаб.1,7
7	3,4	ОПК-15	ОПК-15.8 Владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением.	Лаб.1,6
8	4,5	ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	ОПК-16.1 Знает средства и методы хранения и передачи аутентификационной информации в компьютерных системах и сетях.	Лаб.3,4
9	10	ОПК-16	ОПК-16.2 Знает механизмы реализации атак в сетях TCP/IP.	Лаб.13
10	5	ОПК-16	ОПК-16.3 Знает основные протоколы идентификации и аутентификации абонентов сети.	Лаб.4
11	6	ОПК-16	ОПК-16.4 Знает защитные механизмы и средства обеспечения сетевой безопасности.	Лаб.5

12	12	ОПК-16	ОПК-16.5 Знает средства и методы предотвращения и обнаружения вторжений.	Лаб.15
13	9	ОПК-16	ОПК-16.6 Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе	Лаб.9
14	12	ОПК-16	ОПК-16.7 Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях.	Лаб.15
15	7-11	ОПК-16	ОПК-16.8 Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Лаб.16,17,10,14
16	10,12	ОПК-16	ОПК-16.9 Владеет навыками настройки межсетевых экранов	Лаб.15,11
17	3, 10	ОПК-16	ОПК-16.10 Владеет методиками анализа сетевого трафика	Лаб.1,13

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Письменная контрольная работа. Все лабораторные задания курса.

20. Типовые оценочные средства и методические материалы, определяющие процедурыоценивания

20.1 Текущий контроль успеваемости

Перечень вопросов для контрольных работ

1	Реализация IPSec взаимодействия между двумя конечными системами.
2	Проект мультифилиальной сети
3	Формирование VPN-сети с использованием распределенной проверки подлинности.
4	Формирование VPN-сети с использованием централизованной проверки подлинности на AAA-сервере (RADIUS).
5	Сетевой карантин.
6	Создание корпоративной иерархической системы PKI.
7	Внедрение PKI на основе отечественных криптоалгоритмов.
8	Смарткарты и PKI.
9	Защита данных конечных систем (EFS).
10	Ограничение выполнения ПО в конечных системах. Secret Net Studio
11	Распределенное и централизованное управление обновлениями.
12	Сетевые экраны и типовые архитектуры на их основе.
13	Обеспечение ИБ на 2 уровне корпоративных сетей. APR.
14	Аппаратные средства IPSec и VPN.
15	Аппаратные сетевые экраны: IPS/IDS (CISCO ASA, D-Link DFL, ViPNet-IDS)
16	ViPNet Custom
17	АПКШ Континент.

20.2 Промежуточная аттестация

Перечень вопросов к экзамену

№	Вопросы контрольной работы: 2 вопроса в билете.
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 готовыеполитики IPsec предконфигурированы на ОС семейства Windows?
2	Опишите жизненный цикл сертификата от момента его создания. Как именно создается сертификат, вкакой 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 прииспользовании 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 реализованавозможность 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 потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. Опишите последовательность действийадминистратора 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?

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

1) закрытые задания (тестовые, средний уровень сложности):

1. Компоненты VPN (как системы удаленного доступа) обязательно должны включать:
   A) NAS
   B) DHCP
   C) AAA
   D) ADDS
   E) Kerberos
2. Что необходимо сделать в первую очередь, при потере секретного ключа от сертификата пользователя, используемого для проверки подлинности.
   A) добавить серийный номер сертификата в CRL
   B) добавить серийный номер сертификата в AIA
   C) добавить отпечаток сертификата в CRL
   D) восстановить из архива сохраненный предварительно ключ
   E) обратиться к KRA для восстановления
3. Что такое удостоверяющий центр (CA – Certification Authority)?
   A) сервер, который подписывает данные субъекта и его открытый ключ
   B) сервер, который подписывает данные субъекта и его закрытый ключ
   C) сервер, который подписывает открытый ключ субъекта
   D) сервер, который подписывает закрытый ключ субъекта
   E) сервер, который подписывает данные субъекта
4. Назовите типы удостоверяющего центра (CA – Certification Authority), с точки зрения функциональности и поддержки сетевых протоколов
   A) Standalone, Enterprise
   B) Root, Subordinate
   C) Public
   D) Private

Ответы к тестовым заданиям

N	Ответ
1	A
2	A
3	A
4	A

2) открытые задания (тестовые, средний уровень сложности):

1. В чем отличие и/или несоответствие IPsec термину VPN? Какие средства служат для отладки IPsec вообще и конкретно в ОС Windows? Какая роль политик IPsec, почему "демо" политики MS Windows, которые содержат фильтры ALL-IP ALL-ICMP и включают ESP не могут быть в большинстве реальных корпоративных сетей использованы?

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы. Ответ не содержит грубых ошибок. 1 балл
Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

2. Что такое PKI, какие задачи решает? Из каких компонентов состоит?

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы. Ответ не содержит грубых ошибок. 1 балл
Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;

1) закрытые задания (тестовые, средний уровень сложности):

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. 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
3. В ходе конфигурирования ViPNet администратору потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. В последовательности действий администратора ViPNet для введения этого АП (компьютер уже закуплен) обязательно будет следующий шаг:
   A) работа с ЦУС
   B) работа с УКЦ
   C) Работа с Деловой Почтой
   D) Установка Координатора
4. В ходе конфигурирования ViPNet администратору потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. В последовательности действий администратора ViPNet для введения этого АП (компьютер уже закуплен) обязательно будет следующий шаг:
   A) формирование дистрибутива ключей
   B) работа с УКЦ
   C) Работа с Деловой Почтой
   D) Установка Координатора
5. Как проверить работу криптокоммутаторов, расположенных в филиалах?
   A) ping на узел внутри одного сегмента, но находящегося в другом филиале
   B) ping на узел внутри одного сегмента, находящегося в том же филиале
   C) ping на узел в другом сегменте, находящийся в том же филиале
   D) ping на узел в другом сегменте, находящийся в другом филиале
6. 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)?.
   A) развёртывание СД на АПКШ Континент медленнее
   B) развёртывание СД наАПКШ Континент быстрее
7. 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 и сетевом уровнях
   B) на прикладном уровне
   C) на сетевом уровне
   D) на транспортном уровне
   E) на сетевом и транспортном уровнях
   F) на прикладном и транспортном уровнях
   G) на сетевом и канальном уровнях
   H) на канальном уровне

Ответы к тестовым заданиям

N	Ответ

1	B
2	A
3	A
4	A
5	A
6	A
7	A

2) открытые задания (тестовые, средний уровень сложности):

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

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы, не приводятся сценарии. Ответ не содержит грубых ошибок. 1 балл
Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

2. В чем состоят задачи обновления ПО? Что такое Zero-Day уязвимость? Что такое эксплойт и что такое уязвимость, в чем различие? Какие тенденции существуют во времени появления уязвимостей, эксплойтов, обновлений?

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы, не приводятся сценарии. Ответ не содержит грубых ошибок. 1 балл
Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

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

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы, указаны не все функции шаблонов. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы, не приводит инструменты работы с шаблонами. Ответ не содержит грубых ошибок. 1 балл
Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

1) открытые задания (тестовые, средний уровень сложности):

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

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы, сценарий использования не очень убедителен. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы, не приводятся сценарии. Ответ не содержит грубых ошибок. 1 балл
Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

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?

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы, не приводятся сценарии-случаи. Ответ не содержит грубых ошибок. 1 балл

Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

3. 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.

Критерии оценивания – шкала оценок в баллах
Обучающийся отвечает на все вопросы и подвопросы. 3 балла
Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла
Обучающийся отвечает не на все вопросы и подвопросы, не приводятся инструменты. Ответ не содержит грубых ошибок. 1 балл
Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования;
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

1) закрытые задания (тестовые, средний уровень сложности):

1. В ходе конфигурирования ViPNet администратору потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. В последовательности действий администратора ViPNet для введения этого АП (компьютер уже закуплен) обязательно будет следующий шаг:
   A) копирование на АП дистрибутива ключей
   B) работа с УКЦ
   C) Работа с Деловой Почтой
   D) копирование на АП ключей пользователя
2. 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
3. В ходе лабораторных вы создавали VPN-подключение PPTP и аналогичное по функционалу L3VPN решение от Кода Безопасности с применением АПКШ Континент. Каким образом передаётся конфигурация клиента СД АПКШ Континент ?
   A) через групповую политику
   B) передаётся набор параметров: адрес, имя пользователя и т.д.
   C) передается файл с параметрами конфигурации
4. В ходе конфигурирования ViPNet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация локальной сети ViPNet и добавлено новое рабочее место (АП). Какие ключи потребуются (без учёта ключей защиты ключей) для обработки входящего зашифрованного сообщения на этот новый АП?
   A) ключи ЭП, ключи АП
   B) ключи ЭП, ключи АП, ключи пользователя
   C) ключи ЭП, ключи АП, межсетевой мастер-ключ
   D) ключи АП, ключи пользователя
   E) ключи ЭП, ключи пользователя
5. Формируется новая защищенная сеть с использованием АПКШ Континент. Последовательность действий по включению в сеть ЦУС включает в себя.
   A) выполнить инициализацию ЦУС на стороне АПКШ
   B) выполнить инициализацию ЦУС на стороне ПУ ЦУС
   C) передать ключевую информацию на носителе из ПУ ЦУС в АПКШ
6. Назовите типы удостоверяющего центра (CA – Certification Authority), с точки зрения PKI-иерархии
   A) Standalone, Enterprise
   B) Root, Subordinate
   C) Public
   D) Private

Ответы к тестовым заданиям

7	A
8	A
9	C
10	A
11	A
12	B

2) открытые задания (тестовые, средний уровень сложности):

4. Что такое CRL? Какие существуют варианты опубликования CRL?

Критерии оценивания – шкала оценок в баллах

Обучающийся отвечает на все вопросы и подвопросы. 3 балла

Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла

Обучающийся отвечает не на все вопросы и подвопросы, не приводятся сценарии для вариантов. Ответ не содержит грубых ошибок. 1 балл

Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

5. Что такое транспортный режим и туннельный режим IPSec? В каких сценариях обычно используется каждый? На примере компании с несколькими филиалами опишите алгоритм выбора режимов в каждом филиале и штаб-квартире.

Критерии оценивания – шкала оценок в баллах

Обучающийся отвечает на все вопросы и подвопросы. 3 балла

Обучающийся отвечает на все вопросы и подвопросы. Допускаются незначительные неточности. 2 балла

Обучающийся отвечает не на все вопросы и подвопросы, не приводятся сценарии. Ответ не содержит грубых ошибок. 1 балл

Ответ отсутствует, либо содержит грубые ошибки или неточности. 0 баллов

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).