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.О.43 Программно-аппаратные средства защиты информации

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 05.03.2024, протокол № 5

8. Учебный год:

2027-2028

9.Цели и задачи учебной дисциплины:

изучение основ технологий реализации и применения программных и программно-аппаратных систем защиты информации (СЗИ) в компьютерных сетях, инфокоммуникационных и операционных системах; приобретение навыков управления системами обеспечения информационной безопасности на основе данных технологий СЗИ

10. Место учебной дисциплины в структуре ООП:

дисциплина обязательной части (Б1.О), входные знания в области курсов: «Аппаратные средства вычислительной техники», «Методы и средства криптографической защиты информации», «Сети и системы передачи информации».

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-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.1 знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	знать: состав и фукнкционирование ПАСЗИ средств
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ОПК-10.2 умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	уметь: конфигурировать ПАСЗИ инфраструктуры и конечных систем
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1 знает принципы формирования политики информационной безопасности в информационных системах;	знать: принципы формирования политик безопасности для компьютерной инфраструктуры организации
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.2 знает принципы организации информационных систем в соответствии с требованиями по защите информации;	знать: принципы формирования процедур безопасности для заданных политик

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.5 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	уметь: проектировать систему защиты с использование ПАСЗИ
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.6 умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	уметь: формировать и анализировать показатели защищенности
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.8 умеет оценивать информационные риски в автоматизированных системах;	уметь: составлять план управления рисками
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.4 владеет навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации	владеть: навыками разветывания и настройки ПАСЗИ
ОПК-1.2 Способен администрировать средства защиты информации в компбютерных системах и сетях;	ОПК-1.2.5 знает принципы функционирования программных средств криптографической защиты информации	знать: архитектуру, функции и способы внедрения в инфраструктуру КЗИ

12. Объем дисциплины в зачетных единицах/час:

4/144

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 7	Всего
Аудиторные занятия	68	68
Лекционные занятия	34	34
Практические занятия		0
Лабораторные занятия	34	34
Самостоятельная работа	40	40
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	Введение, основные определения и понятия.	Основные определения и понятия в области аппаратно-программных СЗИ. Классификации СЗИ. Классические системы защиты ОС. Проблемы производительности СЗИ.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
2	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Windows.	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Windows. Домены и доверие. Политики и шаблоны безопасности. NAP-технологии. Антивирусные технологии. Обеспечение комплексной ИБ АРМ.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Linux.	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС GNU/Linux. Концепция и реализация SELinux.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
4	Методы и системы аутентификации, авторизации и учета.	Основные способы проверки подлинности субъектов. AAA-серверы.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
5	Инфраструктура открытых ключей и соответствующие стандарты.	Основы PKI. Сертификаты с цифровыми подписями. Стандарт X.509. Стандарты PKCS.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
6	Карты памяти и смарт-карты.	Виды смарт-карт и карт памяти. ПО смарт-карт. Жизненные циклы карт. Практика программирования и применения смарт-карт.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
7	Технологии обеспечения информационной безопасности (ИБ) в компьютерных сетях и инфокоммуникационных системах.	Классификация угроз, атак. Идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности. .	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
8	Межсетевые экраны	Виды межсетевых экранов. DPI, IDS, IPS.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
9	Виртуальные частные сети. Виртуальные защищённые сети.	Технологии и виды виртуальных частных сетей и виртуальных защищённых сетей. Состав и требования к инфраструктуре.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
10	Аппаратная реализация компонентов СЗИ, крипто-шлюзы.	Различные архитектуры аппаратной части СЗИ. Проблемы производительности и существующие решения.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
2	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Windows. (лаб.)	Развертывание АРМ с использованием Secret Net Studio: полномочное управление доступои, журналы аудита, контроль устройств, замкнутая среда.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
4	Методы и системы аутентификации, авторизации и учета. (лаб.)	Развертывание RADIUS-сервера и централизованной проверки подлинности для VPN-серверов.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
5	Инфраструктура открытых ключей и соответствующие стандарты. (лаб.)	Формирование многоуровневой инфраструктуры PKI. Выпуск сертификатов для подписи ПО.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
6	Карты памяти и смарт-карты. (лаб.)	Сформировать необходимую для смарт-карт инфраструктуру PKI. Выпустить требуемые шаблоны, сформировать политики для выполнения входа в систему только с помощью смарт-карт. Запрограммировать смарт-карту и продемонстрировать работу политики требования смарт-карты для входа.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
6	Технологии обеспечения информационной безопасности (ИБ) в компьютерных сетях и инфокоммуникационных системах. (лаб.)	Сканеры, NMAP. Решение XSpider.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
3	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Linux. (лаб.)	Выполнение, согласно требованиям, развертывания политик SELinux.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
8	Межсетевые экраны (лаб.)	Развертывание системы DPI с использованием D-Link DFL-260 и Cisco ASA5505	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
9	Виртуальные частные сети. Виртуальные защищённые сети. (лаб.)	Развертывание виртуальных защищенных сетей ViPNet.	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795
10	Аппаратная реализация компонентов СЗИ, крипто-шлюзы. (лаб.)	Выполнение типовых задач, связанных с применением криптошлюзов (на примере АПКШ Континент).	ЭУМК «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Введение, основные определения и понятия.	2	0	2	2	6
2	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Windows.	4	0	4	2	10

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
3	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Linux.	2	0	4	2	8
4	Методы и системы аутентификации, авторизации и учета.	2	0	2	2	6
5	Инфраструктура открытых ключей и соответствующие стандарты.	4	0	2	4	10
6	Карты памяти и смарт-карты.	2	0	2	4	8
7	Технологии обеспечения информационной безопасности (ИБ) в компьютерных сетях и инфокоммуникационных системах.	4	0	2	4	10
8	Межсетевые экраны	4	0	4	6	14
9	Виртуальные частные сети. Виртуальные защищённые сети.	4	0	4	8	16
10	Аппаратная реализация компонентов СЗИ, крипто-шлюзы.	6	0	8	6	20
		34	0	34	40	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. 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.
3	Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770 (дата обращения: 23.05.2023).

б) дополнительная литература:

№ п/п	Источник
1	*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*
2	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).
3	Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 23.05.2023). – Библиогр.: с. 190. – ISBN 978-5-8265-1737-6. – Текст : электронный.

в) информационные электронно-образовательные ресурсы:

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

№ п/п	Источник
2	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
3	Электронный ресурс «Программно-аппаратные средства защиты информации», https://edu.vsu.ru/course/view.php?id=3795

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
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-библиотечная система «Университетская библиотека online», http://biblioclub.ru

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. Бесконтактные и контактные карты памяти и смарт-карты.

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

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

10. ПО XSpider на 16 хостов.

11. ПО VipNet и ПАК 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				
2				
3				
4				
5				
6	1-3	ОПК-10	ОПК-10.1	лаб.1, К.Р.1
7	4-10	ОПК-10	ОПК-10.2	лаб.2-5,8-10, К.Р.2
8	7	ОПК-12	ОПК-12.1	лаб.1, К.Р.1
9	7	ОПК-12	ОПК-12.2	лаб.1, К.Р.1
10				
11				
12	7	ОПК-12	ОПК-12.5	лаб.1, К.Р.1
13	6	ОПК-12	ОПК-12.6	лаб.6, К.Р.3
14				
15	7	ОПК-12	ОПК-12.8	лаб.1, К.Р.1
16				
17	4-6	ОПК-1.2	ОПК-1.2.4	лаб.3-5, К.Р.2
18	8-10	ОПК-1.2	ОПК-1.2.5	лаб.8-10, К.Р.3

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 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. 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?

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. 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.
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.
5. Смарт-карты.
6. RFID и смарт-карты.

№	Лабораторные задания (подробное описание, а также необходимое ПО, конфигурационные файлы, скрипты и пояснения находятся на серверах \\FS\Library, edu.vsu.ru)
1	Проект мультифилиальной сети
2	Развертывание АРМ с использованием Secret Net Studio: полномочное управление доступои, журналы аудита, контроль устройств, замкнутая среда.
3	Развертывание RADIUS-сервера и централизованной проверки подлинности для VPN-серверов.
4	Формирование многоуровневой инфраструктуры PKI. Выпуск сертификатов для подписи ПО.

5	Сформировать необходимую для смарт-карт инфраструктуру PKI. Выпустить требуемые шаблоны, сформировать политики для выполнения входа в систему только с помощью смарт-карт. Запрограммировать смарт-карту и продемонстрировать работу политики требования смарт-карты для входа.
6	Сканеры, NMAP. Решение XSpider.
7	Выполнение, согласно требованиям, проектирования и развертывание политик SELinux.
8	Развертывание системы DPI с использованием D-Link DFL-260, Cisco ASA5505, ViPNet IDS
9	Развертывание виртуальных защищенных сетей ViPNet ОАО ИнфоТеКС.
10	Выполнение типовых задач, связанных с применением криптошлюзов (на примере АПКШ Континент).

Оценка остаточных знаний

ОПК-10

Задания закрытого типа

1. 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
2. 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
3. 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
4. Компоненты VPN (как системы удаленного доступа) могут включать:
    A. NYS
    B. YP
    C. AAA
    D. WPA
    E. AIA
5. 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

6. 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
7. 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
8. Выберите вид топологии сетевых экранов,
   A. Централизованная
   B. Бастион
   C. Распределенная
   D. Активная
   E. Пассивная
9. Выберите вид топологии сетевых экранов,
   A. Централизованная
   B. Спина-к-спине
   C. Распределенная
   D. Активная
   E. Пассивная
10. Выберите вид топологии сетевых экранов,
   A. Централизованная
   B. Трехногая
   C. Распределенная
   D. Активная
   E. Пассивная

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-12

Задания закрытого типа

1. Формируется новая защищенная сеть с использованием АПКШ Континент. Последовательность действий по включению в сеть ЦУС включает в себя.
   A. передать ключевую информацию на носителе из АПКШ в ПУ ЦУС

   B. выполнить инициализацию ЦУС на стороне ПУ ЦУС
   C. передать ключевую информацию на носителе из ПУ ЦУС в АПКШ
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. 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
5. 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
6. 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
7. 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
8. 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?

ОПК-1.2

Задания закрытого типа

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. формирование дистрибутива ключей
   B. работа с УКЦ
   C. Работа с Деловой Почтой
   D. Установка Координатора

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. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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

10. Назовите типы удостоверяющего центра (CA – Certification Authority), с точки зрения PKI-иерархии
    A. Standalone, Enterprise
    B. Root, Subordinate
    C. Public
    D. Private

Задания открытого типа

1. Интерфейс низкого уровня, используемый со смарт-картами называется(APDU, PC/SC или CryptoAPI):
2. Интерфейс высокого уровня криптографических функций, используемый в том числи и со смарт-картами называется(APDU, PC/SC или CryptoAPI):

Задание с развёрнутым ответом

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

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	Классификации СЗИ. Классические системы защиты ОС. Проблемы производительности СЗИ.
2	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Windows. Домены и доверие.
3	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Windows. Политики и шаблоны безопасности.
4	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Windows. NAP-технологии. Антивирусные технологии.
5	Особенности и тенденции развития подсистем, связанных с информационной безопасностью ОС Linux.
6	Концепция и реализация SELinux.

7	Основные способы проверки подлинности субъектов.
8	AAA-серверы.
9	Основы PKI. Сертификаты с цифровыми подписями.
10	Стандарт X.509. Стандарты PKCS. Виды смарт-карт и карт памяти. Жизненные циклы карт.
11	Обеспечение ИБ АРМ: полномочное управление доступои, аудит, контроль устройств, замкнутая среда.
12	Классификация угроз, атак.
13	Идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности.
14	Аудит и Pen-тестирование. Сканеры, NMAP. Решение XSpider.
15	Виды межсетевых экранов. DPI, IDS, IPS.
16	Технологии и виды виртуальных частных сетей и виртуальных защищённых сетей. Состав и требования к инфраструктуре. На примере решения VipNet.
17	Технологии и виды виртуальных частных сетей и виртуальных защищённых сетей. Состав и требования к инфраструктуре. На примере решения АКПШ Континент.
18	Различные архитектуры аппаратной части СЗИ. Проблемы производительности и существующие решения.