Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

28.02.2022

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

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

1. Код и наименование направления подготовки/специальности:

09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализация:

Анализ и синтез информационных систем

3. Квалификация (степень) выпускника:

Магистратура

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:

протокол НМС № 3 от 25.02.2022

8. Учебный год:

2022-2023

9.Цели и задачи учебной дисциплины:

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

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

10. Место учебной дисциплины в структуре ООП:

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

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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПКВ-14 Способен проектировать архитектуру программного средства	ПКВ-14.2 Умеет определять способы взаимодействия между программными подсистемами программного средства	знать: типовое использование технологий обеспечения информационной безопасности для построения систем ИБ, снижающих риски, характерные для корпоративных сетей; уметь: проектировать системы защиты интранет-сетей с учетом характерных для них угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с использованием аппаратных решений; реализовывать системы защиты интранет-сетей; владеть: методами анализа состояния защищенности интранет-сети; средствами администрирования систем ИБ интранет-сетей;

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет с оценкой

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 1	Всего
Аудиторные занятия	54	54
Лекционные занятия	18	18
Практические занятия		0
Лабораторные занятия	36	36
Самостоятельная работа	54	54
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	Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности	Интранет сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
2	Сети IPv4, IPv6 и технология IPSec	IPSec – технология для сетей, построенных на IPv4 и IPv6.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
3	Технологии виртуальных частных сетей	VPN технологии: задачи, основные типы, способы реализации.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
4	RADIUS. Сетевой карантин	NAS-серверы. Централизация аутентификации на основе RADIUS. Отказоустойчивость RADIUS.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
5	Инфраструктура открытых ключей. Смарт-карты.	Инфраструктура открытых ключей. Различные архитектуры доверия. Проблемы развертывания и многоуровневые PKI-решения. Многофакторная аутентификация, смарт-карты.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
6	Безопасность хранения и обработки данных в ОС хостов	Безопасность хранения данных. Шифрация данных масштаба файлов, файловых систем, носителей. Безопасность ОС в корпоративной сети: шаблоны и эталоны безопасности, системы обновлений.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения.	Безопасность сетевых устройств 2 уровня с ОС IOS. Безопасность сетевых устройств 3 уровня с ОС IOS. TACACS, RADIUS – решения для сетевого оборудования.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
8	Аппаратная реализация IPSec, VPN.	Реализация IPSec в ОС IOS. Реализация VPN в ОС IOS.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Аппаратная реализация межсетевых экранов, IDS, IPS.	Обеспечение ИБ интранет сетей - как задача управления рисками. Стратегии управления рисками, технологии внедрения управления рисками. Проектирование модульной инфраструктуры интранет сетей на основе типовых решений (проект CISCO SAFE).	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
2	Сети IPv4, IPv6 и технология IPSec (лаб.)	Создание IPSec соединения между серверами Windows с сертификационной аутентификацией	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3	Технологии виртуальных частных сетей (лаб.)	Развертывание RAS-сервера в Windows и настройка VPN подключения с использованием PPTP.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
4	RADIUS. Сетевой карантин (лаб.)	Установка RADIUS-сервера IAS и политик доступа для VPN-клиентов. NPS. NAP.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
5	Инфраструктура открытых ключей. Смарт-карты. (лаб.)	Развертывание 2-уровневой PKI на компьютерах под управлением Windows Server. Создание сертификационных шаблонов для автовыпуска сертификатов. Создание субъекта, уполномоченного выпускать сертификаты для смарт-карты. Резервное копирование в PKI. Создание DRA и KRA.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
6	Безопасность хранения и обработки данных в ОС хостов (лаб.)	Развертывание EFS. Шифрация BitLocker Drive. Применение эталонных шаблонов безопасности к серверной и клиентской ОС (Windows 2003, XP). Создание инфраструктуры WSUS в лабораторной сети.	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
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения. (лаб.)	Обеспечение безопасности коммутаторов с ОС IOS. Обеспечение безопасности коммутаторов 3 уровня и маршрутизаторов с ОС IOS. Настройка TACACS, RADIUS для централизованной аутентификации.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
8	Аппаратная реализация IPSec, VPN. (лаб.)	Реализация IPSec в ОС IOS занятие 1, 2. Реализация VPN в ОС IOS с помощью SDM. Реализация VPN в ОС IOS в командном интерфейсе.	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995
9	Аппаратная реализация межсетевых экранов, IDS, IPS. (лаб.)	Аппаратная реализация межсетевых экранов на основе пакетной фильтрации. Аппаратная реализация зональных межсетевых экранов на основе классификаторов трафика. Аппаратная реализация IPS (IOS).	ЭУМК «Информационная безопасность интранет-сетей», https://edu.vsu.ru/course/view.php?id=2995

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности	2			2	4
2	Сети IPv4, IPv6 и технология IPSec	2		4	4	10
3	Технологии виртуальных частных сетей	2		4	4	10
4	RADIUS. Сетевой карантин	2		2	4	8
5	Инфраструктура открытых ключей. Смарт-карты.	2		6	10	18
6	Безопасность хранения и обработки данных в ОС хостов	1		6	8	15
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения.	2		6	10	18
8	Аппаратная реализация IPSec, VPN.	2		6	10	18
9	Аппаратная реализация межсетевых экранов, IDS, IPS.	3		2	2	7

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
		18	0	36	54	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 moodle.vsu.ru, 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	*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	*Семь безопасных информационных технологий : учебник / А. В. Барабанов, А. В. Дорофеев, А. С. Марков, В. Л. Цирлов ; под редакцией А. С. Маркова. — Москва : ДМК Пресс, 2017. — 224 с. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/97352*

б) дополнительная литература:

№ п/п	Источник
1	*Петренко, С.А. Аудит безопасности Intranet : учебное пособие / С.А. Петренко, А.А. Петренко. – Москва : ДМК Пресс, 2010. – 387 с. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/1113*
2	*Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях : учебное пособие. – Москва : ДМК Пресс, 2012. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/3032*

№ п/п	Источник
3	*Нестеров, С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : практическое пособие / С.А. Нестеров. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2009. – 233 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book&id=234529*
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	*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*

в) информационные электронно-образовательные ресурсы:

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

16. Перечень учебно-методического обеспечения для самостоятельной работы

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

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

1. Технологии виртуализации:

Среда виртуализации Oracle/Sun Virtual Box

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

3. Образовательный портал Moodle (сервер Moodle ВГУ)

4. Серверные и клиентские ОС Microsoft.

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

18. Материально-техническое обеспечение дисциплины:

1. Лекционная аудитория, оснащенная видеопроектором.

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

3. Лаборатории программно-аппаратных средств обеспечения информационной безопасности (ауд. 303п), включающая аппаратно-программные СЗИ: смарт-карты, RFID-токены и карты, карт-ридеры; аппаратные IPS, IDS, VPN системы; развернутая виртуальная сетевая инфраструктура для выполнения лабораторных работ с аппаратными сетевыми экранами и VPN. Учебно-методический комплекс "Программно-аппаратная защита сетей с защитой от НСД" ОАО "ИнфоТеКС". АПКШ «Континент».

4. Лаборатория безопасности компьютерных сетей (ауд. 384), включающая коммутаторы и маршрутизаторы CISCO, аппаратный межсетевой экран, программный анализатор сетевого трафика WireShark. Программный симулятор, для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	1-9	ПКВ-14	ПКВ-14.2	Практические задания №1-8

Промежуточная аттестация

Форма контроля - Зачет с оценкой

Оценочные средства для промежуточной аттестации

Письменная контрольная работа. Одно из лабораторных заданий

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Перечень лабораторных заданий

N	Задачи лабораторной работы
1	Создание IPSec соединения между серверами Windows с сертификационной аутентификацией
2	Развертывание RAS-сервера в Windows и настройка VPN подключения с использованием PPTP.
3	Установка RADIUS-сервера IAS и политик доступа для VPN-клиентов. NPS. NAP.

4	Развертывание 2-уровневой PKI на компьютерах под управлением Windows Server. Создание сертификационных шаблонов для автовыпуска сертификатов. Создание субъекта, уполномоченного выпускать сертификаты для смарт-карты. Резервное копирование в PKI. Создание DRA и KRA.
5	Развертывание EFS. Шифрация BitLocker Drive. Применение эталонных шаблонов безопасности к серверной и клиентской ОС (Windows 2003, XP). Создание инфраструктуры WSUS в лабораторной сети.
6	Обеспечение безопасности коммутаторов с ОС IOS. Обеспечение безопасности коммутаторов 3 уровня и маршрутизаторов с ОС IOS. Настройка TACACS, RADIUS для централизованной аутентификации.
7	Реализация IPSec в ОС IOS занятие 1, 2. Реализация VPN в ОС IOS с помощью SDM. Реализация VPN в ОС IOS в командном интерфейсе.
8	Аппаратная реализация межсетевых экранов на основе пакетной фильтрации. Аппаратная реализация зональных межсетевых экранов на основе классификаторов трафика. Аппаратная реализация IPS (IOS).

20.2 Промежуточная аттестация

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

10	Что такое сетевой экран уровня «приложения», в чем отличие от сетевого экрана «пакетный фильтр»? Что такое unsolicited трафик и чем отличаются файерволы statefull и stateless? Как размещены по отношению к корпоративной сети сетевые экраны, опишите основные архитектуры
11	Что такое EFS, какие задачи решает, из каких компонентов состоит? Как технически реализована возможность расшифровки файла другими пользователями, перечислите условия, в которых это возможно?