Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Борисов Дмитрий Николаевич

Кафедра информационных систем

 21.04.2021

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 информационный систем

7. Рекомендована:

Научно-методическим советом ФКН, протокол НМС №5 от 10.03.2021

8. Учебный год:

2024-2025

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. Аудит и Pen-тестирование.	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 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. 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	*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*
2	*Мытник, К. Я. Смарт-карты и информационная безопасность / К. Я. Мытник, С. П. Панасенко ; под редакцией В. Ф. Шаньгина. — Москва : ДМК Пресс, 2018. — 516 с. — Лань : электронно-библиотечная система. — Режим доступа : https://e.lanbook.com/book/116128*

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	*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*

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Библиотека ВГУ, http://www.lib.vsu.ru
2	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
3	Электронный 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
7	4-10	ОПК-10	ОПК-10.2	лаб.2-5,8-10
8	7	ОПК-12	ОПК-12.1	лаб.1

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
9	7	ОПК-12	ОПК-12.2	лаб.1
10				
11				
12	7	ОПК-12	ОПК-12.5	лаб.1
13	6	ОПК-12	ОПК-12.6	лаб.6
14				
15	7	ОПК-12	ОПК-12.8	лаб.1
16				
17	4-6	ОПК-1.2	ОПК-1.2.4	лаб.3-5
18	8-10	ОПК-1.2	ОПК-1.2.5	лаб.8-10

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

№	Лабораторные задания (подробное описание, а также необходимое ПО, конфигурационные файлы, скрипты и пояснения находятся на серверах \\FS\Library, moodle.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).

20.2 Промежуточная аттестация

№	**Перечень вопросов к экзамену**
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.