

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский

_____» _____ 20__ г.

подписано электронно-цифровой подписью

Программа дисциплины

Программно-аппаратные методы защиты информации Б1.В.03

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2019

Автор(ы): Акчурин А.Д., Иванов Константин Васильевич

Рецензент(ы): Шерстюков О.Н.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Акчурин А. Д.

Протокол заседания кафедры No ____ от " ____ " _____ 20__ г.

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК No ____ от " ____ " _____ 20__ г.

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы
2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
 - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
 - 4.2. Содержание дисциплины
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
 - 6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения
 - 6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания
 - 6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы
 - 6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)
 - 7.1. Основная литература
 - 7.2. Дополнительная литература
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

Программу дисциплины разработал(а)(и) заведующий кафедрой, к.н. (доцент) Акчурин А.Д. (Кафедра радиоастрономии, Отделение радиофизики и информационных систем), Adel.Akchurin@kpfu.ru ; Иванов Константин Васильевич

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Выпускник, освоивший дисциплину, должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-10	способностью проводить аттестацию объектов информатизации по требованиям безопасности информации
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности

Выпускник, освоивший дисциплину:

Должен знать:

принципы работы и организацию современных средств защиты информации;
функции и задачи, стоящие перед администраторами безопасности

Должен уметь:

Администрировать средства защиты информации, встроенные в современные операционные системы, обеспечивающие дополнительный функционал для СВТ, а также сетевые средства защиты информации.

Должен владеть:

Навыками аргументированного выбора механизмов защиты информации, используемых при построении системы защиты информации Автоматизированных систем.

Должен демонстрировать способность и готовность:

- Применять программно-технические способы и средства для обеспечения информационной безопасности объекта.

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Данная учебная дисциплина включена в раздел "Б1.В.03 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Математические методы и программные технологии защиты информации)" и относится к вариативной части.

Осваивается на 1 курсе в 1 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 16 часа(ов), в том числе лекции - 0 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 16 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 56 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 1 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	

Тема 1. Техническое

проектирование и реализация систем защиты корпоративных систем.

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.	1	0	0	4	14
3.	Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.	1	0	0	4	14
4.	Тема 4. Построение подсистемы антивирусной защиты.	1	0	0	2	2
5.	Тема 5. Использование добавочных средств защиты.	1	0	0	2	2
6.	Тема 6. Построение системы межсетевого экранирования.	1	0	0	2	14
7.	Тема 7. Средства защиты информации активного сетевого оборудования.	1	0	0	1	6
	Итого		0	0	16	56

4.2 Содержание дисциплины

Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем.

- Жизненный цикл защищённой корпоративной АС
- Функции администратора безопасности и инструменты их реализации
- Средства борьбы с несанкционированным доступом (НСД) к информационным ресурсам.
- Системы комплексного администрирования безопасности: система комплексного администрирования безопасности (СКАД).

Тема 2. Операционная система (ОС) Linux и её подсистема безопасности.

Возможности комплекса средств защиты (КСЗ) ОС семейства Linux

- Подсистема разграничения доступа
- Подсистема регистрации и учёта
- Подсистема обеспечения целостности
- Криптографическая подсистема
- Интерфейс администратора безопасности

Пересборка ядра ОС Вывод системы из нестабильного состояния: поиск и устранение источника неполадок в дисковой подсистеме ОС семейства Linux; поиск и устранение источника неполадок в сетевой подсистеме ОС семейства Linux; поиск и устранение источника неполадок в распределении виртуальной памяти ОС семейства Linux; поиск и устранение источника неполадок в распределении ресурсов центрально-го процессора ОС семейства Linux.

Тема 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности.

Возможности КСЗ ОС семейства Windows

- Подсистема разграничения доступа
- Подсистема регистрации и учёта
- Подсистема обеспечения целостности
- Криптографическая подсистема
- Интерфейс администратора безопасности

Вывод системы из нестабильного состояния: по-иск и устранение источника неполадок в дисковой подсистеме ОС Windows; поиск и устранение источника неполадок в сетевой подсистеме ОС Windows; поиск и устранение источника неполадок в распределении виртуальной памяти ОС Windows; поиск и устранение источника неполадок в распределении ресурсов центрального процессора ОС Windows.

Тема 4. Построение подсистемы антивирусной защиты.

Классификация вредоносного программного обеспечения (ПО). Обзор существующих методов и средств антивирусной защиты. Стратегии антивирусной защиты. Создание системы контроля целостности файлов в дополнение в применяемый в операционной системе. Настройка алгоритмов своевременного обнаружения нарушения целостности.

Тема 5. Использование добавочных средств защиты.

Создание системы многофакторной идентификации и аутентификации. Стратегии резервного копирования. Создание зашифрованных носителей. Использование зашифрованных каналов связи. Использование защищенных удаленных подключений. Создание защищенных сетей. Классификация решений VPN. Установка и настройка VPN.

Тема 6. Построение системы межсетевого экранирования.

Компоненты корпоративной сети, определяющие уровень безопасности Межсетевое экранирование. Обзор и классификация межсетевых экранов. Проблема эксплуатации защищенных АС, администрирование безопасности информации. Построение системы обнаружения вторжений, построение системы анализа сетевой безопасности, построение системы кодирования информации, передаваемой по открытым каналам связи.

Тема 7. Средства защиты информации активного сетевого оборудования.

Используемое сетевое оборудование. Его классификация. Архитектура построения безопасных сетей передачи данных. Средства обеспечения безопасности корпоративных сетей. Основные защитные механизмы и примеры их реализации: построение защиты сетевых средств и сервисов, построение системы межсетевого экранирования.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301).

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений".

Положение от 29 декабря 2018 г. № 0.1.1.67-08/328 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет".

Положение № 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет".

Положение № 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет".

Регламент № 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет".

Регламент № 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет".

Регламент № 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет".

6. Фонд оценочных средств по дисциплине (модулю)

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 1			
	Текущий контроль		
1	Лабораторные работы	ПК-2 , ПК-10	1. Техническое проектирование и реализация систем защиты корпоративных систем. 2. Операционная система (ОС) Linux и её подсистема безопасности. 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности. 4. Построение подсистемы антивирусной защиты. 5. Использование добавочных средств защиты. 6. Построение системы межсетевого экранирования. 7. Средства защиты информации активного сетевого оборудования.
2	Контрольная работа	ПК-2 , ПК-10	1. Техническое проектирование и реализация систем защиты корпоративных систем. 2. Операционная система (ОС) Linux и её подсистема безопасности. 3. Семейство операционных систем (ОС) MS Windows и их подсистемы безопасности. 4. Построение подсистемы антивирусной защиты. 5. Использование добавочных средств защиты. 6. Построение системы межсетевого экранирования. 7. Средства защиты информации активного сетевого оборудования.
	Зачет	ПК-10, ПК-2	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Семестр 1					
Текущий контроль					
Лабораторные работы	Оборудование и методы использованы правильно. Проявлена превосходная теоретическая подготовка. Необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям.	Оборудование и методы использованы в основном правильно. Проявлена хорошая теоретическая подготовка. Необходимые навыки и умения в основном освоены. Результат лабораторной работы в основном соответствует её целям.	Оборудование и методы частично использованы правильно. Проявлена удовлетворительная теоретическая подготовка. Необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям.	Оборудование и методы использованы неправильно. Проявлена неудовлетворительная теоретическая подготовка. Необходимые навыки и умения не освоены. Результат лабораторной работы не соответствует её целям.	1
Контрольная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	2
	Зачтено		Не зачтено		

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Зачет	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных программой дисциплины.		Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.		

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Семестр 1

Текущий контроль

1. Лабораторные работы

Темы 1, 2, 3, 4, 5, 6, 7

Темы 4, 5, 6, 7, 8, 9, 10

Лабораторная работа ♦1 Изучение требований к классам защищенности средств защиты информации.

Ознакомиться с руководящими документами. Выписать полный перечень требований к классу СБТ, указанному преподавателем

Лабораторная работа ♦2 Анализ классов и семейств требований 2 части РД ИСО 15408.

Ознакомиться с руководящими документами и ГОСТ. Выписать полный перечень семейств требований для каждой подсистемы ИБ

Лабораторная работа ♦3 Анализ требований к 4 классу антивирусного ПО

Ознакомиться с руководящими документами. Для антивирусного продукта, указанного преподавателем описать все реализованные механизмы и их соответствие требованиям РД

Лабораторная работа ♦4 Изучение КСЗ ОС семейства Windows

Настройка механизмов защиты информации, реализованных в ОС

Лабораторная работа ♦5 Изучение КСЗ ОС семейства Linux

Настройка механизмов защиты информации, реализованных в ОС

Лабораторная работа ♦6 Изучение механизмов работы межсетевых экранов и сканеров уязвимостей.

Настройка механизмов защиты информации, реализованных в МЭ. Проверка корректности настроек при помощи сканера уязвимостей.

Лабораторная работа ♦7 Изучение механизмов работы виртуальных частных сетей

Установка и настройка VPN-туннеля

Лабораторная работа ♦8 Изучение ГОСТ 19.XXX.

Оформить техническое задание по ГОСТ на разработку программы, содержащей механизмы защиты информации, по указанию преподавателя

Лабораторная работа ♦9 Подготовка к сертификации программного обеспечения

Оформить заявку на сертификацию программы, разработанной по ТЗ из работы по теме 8, и все необходимые приложения к ней

2. Контрольная работа

Темы 1, 2, 3, 4, 5, 6, 7

Вопросы к контрольной работе: 1. Подсистема управления доступом. Особенности реализации в различных ОС и в активном сетевом оборудовании 2. Подсистема регистрации и учёта событий. Особенности реализации в различных ОС и в активном сетевом оборудовании 3. Криптографическая подсистема. Особенности реализации в различных ОС и в активном сетевом оборудовании 4. Подсистема обеспечения целостности. Особенности реализации в различных ОС 5. Межсетевые экраны. Определение и классификация. 6 Особенности построения виртуальных частных сетей. VPN и SSL. 7. Списки контроля доступа. 8 Виртуальные локальные сети.

Зачет

Вопросы к зачету:

1. Построение подсистемы антивирусной защиты.

2. Межсетевые экраны. определение, назначение, классификации.

3. Обзор инструментальных средств анализа защищенности АС.

4. Средства защиты информации. активного сетевого оборудования.

5. Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации

6. Организационная поддержка мер защиты. Отраслевые стандарты

7. Пакет руководящих документов Гостехкомиссии России
8. ISO 15408. Единые критерии
9. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности
10. Документы ФСТЭК России, разработанные на базе ISO 15408
11. Подсистема управления доступом
12. Подсистема обеспечения целостности
13. Подсистема регистрации и учёта событий
14. Криптографическая подсистема
15. КСЗ ОС семейства Windows. Подсистема управления доступом
16. КСЗ ОС семейства Windows. Подсистема обеспечения целостности
17. КСЗ ОС семейства Windows. Подсистема регистрации и учёта событий.
18. КСЗ ОС семейства Windows. Криптографическая подсистема
19. КСЗ ОС Linux. Подсистема управления доступом.
20. КСЗ ОС Linux. Подсистема обеспечения целостности
21. КСЗ ОС Linux. Подсистема регистрации и учёта событий.
22. КСЗ ОС Linux. Криптографическая подсистема.
23. Применение средств защиты в активном сетевом оборудовании, и при построении защищённых сетей.
24. Построение системы межсетевого экранирования .
25. Построение системы обнаружения вторжений.
26. Понятие сертификации. Основные участники сертификации.
27. Схемы сертификационных испытаний. Инспекционный контроль.
28. Порядок проведения сертификационных испытаний.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

56 баллов и более - "зачтено".

55 баллов и менее - "не зачтено".

Для экзамена:

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Семестр 1			
Текущий контроль			
Лабораторные работы	В аудитории, оснащённой соответствующим оборудованием, обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области.	1	40
Контрольная работа	Контрольная работа проводится в часы аудиторной работы. Обучающиеся получают задания для проверки усвоения пройденного материала. Работа выполняется в письменном виде и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	2	10
Зачет	Зачёт нацелен на комплексную проверку освоения дисциплины. Обучающийся получает вопрос (вопросы) либо задание (задания) и время на подготовку. Зачёт проводится в устной, письменной или компьютерной форме. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература:

Хорев П. Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с. - (Высшее образование). ISBN 978-5-00091-004-7 - Режим доступа: <http://znanium.com/bookread2.php?book=489084>

Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9 - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785991203289.html>

Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Режим доступа: <http://znanium.com/bookread2.php?book=463061>

7.2. Дополнительная литература:

Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс]: учеб. пособие - Электрон. дан. - СПб. : Лань, 2017. - 324 с. - Режим доступа: <http://e.lanbook.com/book/90153>

Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. - Режим доступа: <http://znanium.com/bookread.php?book=474838>

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Аверченков В И Рытов М. Ю. Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. 3-е изд., стереотип. М. : ФЛИНТА, 2011. - <http://znanium.com/bookread.php?book=453862>

Бабаш А. В. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - <http://znanium.com/bookread.php?book=405000>

Кузнецов И. Н. Кузнецов, И. Н. Бизнес-безопасность [Электронный ресурс] / И. Н. Кузнецов. - 3-е изд. - М.: Дашков и К, 2013. - <http://znanium.com/bookread.php?book=430343>

Партыка Т. Л. Попов И. И. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - <http://znanium.com/catalog.php?bookinfo=167284>

Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - <http://znanium.com/bookread.php?book=169345>

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лабораторные работы	<p>Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе выполнения лабораторных работ, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения. По каждой лабораторной работе преподавателю должен быть представлен отчет следующей структуры: 1. Отчет должен иметь заголовок со следующей информацией ? фамилия и.о. студента, ? группа, ? тема лабораторной работы (название) ? Содержание , включающее в себя как минимум названия упражнений, включенных в отчет(подряд или выборочно, если это необходимо). Если упражнение одно, название можно не включать. 2. Отчет по каждому упражнению составляется в следующей последовательности. 2.1. Постановка задачи: ? формулировка задания к упражнению лабораторной работы; ? цель (задание выполняется ради наблюдения некоторого эффекта, изучения типичной особенности; задание моделирует распространенную на практике ситуацию и т.п.). В данном пункте проверяется понимание студента, какой результат ожидается получить, зачем ему получаемый результат, где его можно применить. также фиксируются ожидания студента; ? какие средства используются; если формулировка оставляет свободу выбора каких-либо методов или параметров, произвести и обосновать этот выбор. 2.2. Начальная ситуация (подчеркнуть, что будет создано, изменено, дополнено или удалено в ходе выполнения задания) - если применимо. 2.3. Выполнение задания: ? алгоритм выполнения задания и пояснения к его шагам; ? какие проблемы возникли и как они были решены ? какие результаты достигнуты (подтвердить листингами/снимками экрана, выделить основной момент). 3. При написании отчета следует стремиться к сжато, но четкому изложению. Руководствуйтесь критерием: отчет должен быть понятен читателю, не знакомому с заданием, но являющемуся достаточным специалистом в этой области. 4. Отчет, идентичный целиком или фрагментами ранее поступившему отчету другого студента, независимо от того, совместно или отдельно выполнялась работа, при выставлении рейтингов в расчёт не принимается и наказывается дополнительным вопросом/заданием на зачёте. 5. Больше требований к оформлению отчета и стилю изложения нет. В то же время отчет, не соответствующий требованиям пп. 1-4, оценивается с существенным штрафом(до 50% баллов). 6. Отчеты по заданиям выполняются в электронном виде, в одном из форматов winword-DOC, RTF, ODT. По каждой теме рекомендуется составлять один отчет, охватывающий все задания темы.</p>
самостоятельная работа	<p>Важнейшим этапом практического занятия является самостоятельная работа обучающихся. В зависимости от конкретной темы занятия обучающиеся самостоятельно выполняют контрольные задания. Во время разбора контролируется качество выполнения самостоятельной работы и сформированных навыков и умений. Преподаватель индивидуально оценивает выполнение целей практического занятия. Самостоятельная (внеаудиторная) работа обучающихся складывается из нескольких разделов: 1. Теоретическая самоподготовка обучающихся по учебным темам, входящим в примерный тематический учебный план. 3. Знакомство с дополнительной учебной литературой и другими учебными методическими материалами, закрепляющими некоторые практические навыки обучающихся.</p>

Вид работ	Методические рекомендации
контрольная работа	<p>Цель выполнения работы: - научить студентов самостоятельно пользоваться учебной и нормативной литературой; - дать возможность приобрести умения и навыки излагать материал по конкретным вопросам; - документально установить уровень знания пройденного материала. Контрольные задания составляются преподавателем таким образом, чтобы можно было проверить знания основных разделов. Работа разрабатывается в одном или нескольких вариантах (в зависимости от вида работы, дисциплины, формы обучения и т.д.). Возможны индивидуальные задания каждому студенту. В каждом варианте содержится несколько заданий: теоретические вопросы, задачи, практические задания. Распределение вариантов работ осуществляется преподавателем. При выполнении работы следует придерживаться следующих правил: <input type="checkbox"/> подобрать необходимую литературу; <input type="checkbox"/> составить развернутый план работы; <input type="checkbox"/> затем изложить теоретическую часть вопроса (не допускается дословное переписывание текстов из брошюр, статей, учебников); <input type="checkbox"/> привести практические примеры, используя конкретный материал (с приложением материала и поименным источником печати); <input type="checkbox"/> решить предложенные практические задания; <input type="checkbox"/> оформить работу; <input type="checkbox"/> сдать (выслать) ее на проверку преподавателю. Работа должна быть выполнена грамотно и аккуратно, четко и разборчиво, без помарок и зачёркиваний, запрещается произвольно сокращать слова (кроме общепринятых сокращений). На проверку не принимаются работы: <input type="checkbox"/> выполненные не по своему варианту; <input type="checkbox"/> выполненные небрежно и неразборчиво.</p> <p>Критерии качества работы</p> <ol style="list-style-type: none"> 1. Правильное раскрытие содержания основных вопросов темы, правильное решение задач. 2. Самостоятельность суждений, творческий подход, научное обоснование раскрываемой проблемы. 3. Правильность использования цитат (если цитата приводится дословно, то надо взять ее в кавычки и указать источник с указанием фамилии автора, названия произведения, места и города издания, тома, части, параграфа, страницы).

Вид работ	Методические рекомендации
зачет	<p>Подготовка к зачёту.</p> <p>При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки.</p> <p>Конспекты. В начале подготовки в первый день: прочитайте свои конспекты с лекционным материалом, постарайтесь его понять, но не старайтесь запомнить. Результат для вас: общее обзорное представление обо всем данном учебном курсе.</p> <p>Помните, что лекции следует читать 2 раза - в начале вашей подготовки к зачёту и в конце - перед зачётом. Итак, вечером накануне повторно перечитайте(или хотя бы пролистайте) свои конспекты лекций. Важнейшие определения стремитесь запомнить. Результат: обзорное запоминание важнейших положений данного курса. Вы будете меньше путаться при ответе на экзамене</p> <p>Дополнительная литература. По списку вопросов подберите соответствующие разделы литературы, чтобы знать ответы на эти вопросы. Книги более полно и развернуто объясняют то, что очень кратко было записано в ваших конспектах. Помните, что некоторые нюансы не освещаются на лекциях и вы должны их подготовить самостоятельно по литературе или лабораторным работам. Результат: более полное знание учебного материала курса, заполнение тех пробелов, которые неизбежно бывают в лекциях.</p> <p>Лабораторные работы. Пересмотрите свои отчёты и разберитесь во всех выполненных работах. Здесь тоже могут встретиться полезные определения и выводы. Считается, что студент на практических занятиях должен получить подтверждения тем теоретическим положениям, которые излагаются в лекциях. Результат: умение доказать теоретические положения конкретными фактами.</p> <p>Вопросы к зачёту. Просмотрите вопросы и попробуйте дать определения всем важнейшим понятиям, о которых там спрашивается. Если не получается дать определение, то найдите его и выучите. С него-то вам и надо будет начинать свой ответ на экзамене.</p> <p>Трудные вопросы. В последний день перед зачётом пересмотрите список вопросов и убедитесь, что на большинство из них вы уже можете дать ответ. Дополнительно перечитайте учебный материал по самым сложным и 'страшным' для вас вопросам.</p> <p>Погружение. В материал каждой учебной дисциплины при подготовке к зачёту следует 'погружаться'. Это означает, что при подготовке не надо заниматься ничем другим, ничем посторонним. Отвлекаться можно только на отдых. А всё остальное время - учить, учить, учить...</p> <p>Высшее образование требует именно такой способности: способности к погружению в предмет и к усвоению больших объёмов знаний за относительно короткий срок.</p> <p>Учите основное</p> <p>Необходимо также выучить все определения по предложенной литературе, которые могут встретиться на контрольной работе, чтобы потом, в процессе подготовки не пришлось вспоминать, что значит тот или иной термин. В итоге, ко дню контрольной работы нужно подойти, держа в своей памяти примерный ход ответов по всем темам, рекомендованным к ознакомлению и основную теоретическую базу, требуемую для успешного решения.</p> <p>Не засиживайтесь за лекциями в последнюю ночь перед контрольной работой или зачётом - толку будет мало. Материал запомнится плохо и наутро голова будет забита несвязанными отрывками конспектов. В ночь перед работой нужно хорошо выспаться и отдохнуть, успокоить себя и не волноваться во что бы то ни стало.</p>

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Освоение дисциплины "Программно-аппаратные методы защиты информации" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows Professional 7 Russian

Пакет офисного программного обеспечения Microsoft Office 2010 Professional Plus Russian

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Освоение дисциплины "Программно-аппаратные методы защиты информации" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Специализированная лаборатория оснащена оборудованием, необходимым для проведения лабораторных работ, практических занятий и самостоятельной работы по отдельным дисциплинам, а также практик и научно-исследовательской работы обучающихся. Лаборатория рассчитана на одновременную работу обучающихся академической группы либо подгруппы. Занятия проводятся под руководством сотрудника университета, контролирующего выполнение видов учебной работы и соблюдение правил техники безопасности. Качественный и количественный состав оборудования и расходных материалов определяется спецификой образовательных программ.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.04.01 "Информационная безопасность" и магистерской программе Математические методы и программные технологии защиты информации .