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 средства защиты информации Б1.Б.8

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
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

Программу дисциплины разработал(а)(и) доцент, 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
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

Выпускник, освоивший дисциплину:

Должен знать:

принципы работы и организацию современных средств защиты информации;

основные подходы к созданию программно-аппаратных 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 средств защиты СВТ, а также сетевые средства защиты информации;

- осуществлять поиск уязвимостей механизмов защиты, реализованных в программном и аппаратном обеспечении;

- выбирать и устанавливать аппаратные средства защиты информации и соответствующее программное обеспечение

Должен владеть:

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

-навыками внедрения и эксплуатации современных средств программно-аппаратной защиты информации;

- навыками во внедрении, адаптации и настройке механизмов защиты прикладных ИС.

Должен демонстрировать способность и готовность:

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

осуществлять аргументированный выбор средств защиты информации;

использовать встроенные в программное и аппаратное обеспечение механизмы защиты информации.

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

Данная учебная дисциплина включена в раздел "Б1.Б.8 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к базовой (общепрофессиональной) части.
Осваивается на 4 курсе в 7 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 5 зачетных(ые) единиц(ы) на 180 часа(ов).

Контактная работа - 90 часа(ов), в том числе лекции - 54 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 54 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 7 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	
1.	Тема 1. введение в предметную область.	7	2	0	0	2
2.	Тема 2. Техническое проектирование и реализация комплексов средств защиты информации. Обзор подходов к созданию средств защиты информации. Проблемы проектирования и реализации механизмов защиты	7	4	0	0	4
3.	Тема 3. Теоретические основы реализации механизмов защиты информации	7	10	0	0	6
4.	Тема 4. Организационные основы реализации механизмов защиты информации/ Нормативно-правовые документы, регламентирующие применение программно-аппаратных методов и средств ЗИ.	7	8	0	10	12
5.	Тема 5. Механизмы защиты, реализуемые на основе программных продуктов фирмы Microsoft	7	4	0	6	5
6.	Тема 6. Механизмы защиты, реализуемые на базе ОС семейства Linux	7	2	0	6	5
7.	Тема 7. Средства защиты информации, реализованные в активном сетевом оборудовании	7	6	0	6	5
8.	Тема 8. Средства защиты информации, реализованные в прикладном программном обеспечении	7	4	0	0	5
9.	Тема 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР).	7	10	0	6	8
10.	Тема 10. Сертификация средств защиты информации.	7	4	0	2	2
	Итого		54	0	36	54

4.2 Содержание дисциплины

Тема 1. введение в предметную область.

Место программно-аппаратных методов и средств в комплексных системах защиты информации.Основные термины и определения. Структура и состав систем защиты информации и комплексов средств защиты. Законы РФ "О государствен-ной тайне", "Об информации, информатизации и защите информации". Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации. Органи-зационная поддержка мер за-щиты. Отраслевые стандар-ты. Пакет руководящих до-кументов Гостехкомиссии России. ISO 15408. Единые критерии. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности. Документы ФСТЭК России, разработан-ные на базе ISO 15408.

Тема 2. Техническое проектирование и реализация комплексов средств защиты информации. Обзор подходов к созданию средств защиты информации. Проблемы проектирования и реализации механизмов защиты

Техническое проектирование и реализация комплексов средств защиты. Жизненный цикл корпоративный системы. Обзор подходов к созданию комплексов средств защиты. Проблемы проектирования и реализации защищенных АС. Синтез КСЗ и его этапы.

Основные термины и определения. Техническое проектирование и реализация систем защиты. Жизненный цикл системы. Обзор подходов к созданию защищённых автоматизированных систем (АС). Проблемы проектирования и реализации защищенных АС. Синтез АС и его этапы.

Организационно-правовые аспекты защиты информации в АС.

Тема 3. Теоретические основы реализации механизмов защиты информации

Основные теоретические положения защиты информации. Подсистема управления доступом.Идентификация и аутентификация. Формальные модели и политики управления доступом. Подсистема обеспечения целостности. Контроль целостности. Антивирусная защиты. Резервное копирование. Подсистема регистрации и учёта событий. Криптографическая подсистема.

Тема 4. Организационные основы реализации механизмов защиты информации/ Нормативно-правовые документы, регламентирующие применение программно-аппаратных методов и средств ЗИ.

Законы РФ ?О государственной тайне?, ?Об информации, информатизации и защите информации?. Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации. Организационная поддержка мер за-щиты. Отраслевые стандарты. Пакет руководящих документов Гостехкомиссии России. ISO 15408. Единые критерии. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности. Документы ФСТЭК России, разработанные на базе ISO 15408.

Тема 5. Механизмы защиты, реализуемые на основе программных продуктов фирмы Microsoft

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 се-тевой 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 6. Механизмы защиты, реализуемые на базе ОС семейства Linux

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 Вы-вод системы из нестабильного состояния: по-иск и устранение источника неполадок в дисковой подсистеме ОС семейства Linux; поиск и устранение источника неполадок в сетевой под-системе 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 7. Средства защиты информации, реализованные в активном сетевом оборудовании

Используемое сетевое оборудование. Его классификация. Архитектура построения без-опасных сетей. Средства обеспечения безопасности корпоративных сетей. Основные защитные механизмы и примеры их реализации: построение защиты сетевых средств и сервисов, построение системы межсетевого экранирования, построение системы обнаружения вторжений, построение системы анализа сетевой без-опасности, построение системы кодирования информации, передаваемой по открытым каналам связи.

Тема 8. Средства защиты информации, реализованные в прикладном программном обеспечении

Возможности реализации средств защиты на прикладном уровне. Использование API и библиотек. Использование системных вызовов. Реализация собственных библиотек. При-меры реализации механизмов защиты на прикладном уровне. Стандарты разработки ПО. Понятие о Единой Системе Программной Документации. Стадии разработки программного обеспечения. Виды программ и программных документов. Техническое задание, требования к содержанию и оформлению. Пояснительная записка. Требования к содержанию и оформлению. Описание применения. Требования к содержанию и оформлению. Описание про-граммы.

Тема 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР).

Порядок выполнения ОКР. Этап разработки эскизного проекта. Этап разработки технического проекта. Этап разработки рабочей конструкторской документации для изготовления опытного образца. Этап изготовления опытного образца и проведения предварительных испытаний. Этап проведения государственных испытаний опытного образца (межведомственных испытаний опытного образца). Этап утверждения рабочей конструкторской документации для организации промышленного (серийного) производства. Требования к порядку разработки рабочей конструкторской документации

Тема 10. Сертификация средств защиты информации.

Понятие сертификации. Основные участники сертификации: федеральный орган, аккредитованный орган, испытательная лаборатория, заявитель. Основные системы обязательной сертификации средств защиты информации: системы ФСТЭК России, Минобороны России, ФСБ России. Добровольные системы сертификации средств защиты информации. Схемы сертификационных испытаний. Инспекционный контроль. Выбор требу-емого класса защищенности и уровня контроля отсутствия недекларированных возможно-стей. Сертификация на соот-ветствие техническим услови-ям. Особенности сертификации средств защиты конфиденци-альной информации и средств защиты персональных данных. Требования к заявке на проведение сертификационных испытаний и к техническим условиям. Структура требований руководящего документа Гостехкомиссии России по НДВ. Порядок проведения испытаний для каждого из уровней контроля отсутствия недекларированных возможностей.

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 7			
	Текущий контроль		
1	Лабораторные работы	ОПК-7 , ПК-1 , ОПК-4	4. Организационные основы реализации механизмов защиты информации/ Нормативно-правовые документы, регламентирующие применение программно-аппаратных методов и средств ЗИ. 5. Механизмы защиты, реализуемые на основе программных продуктов фирмы Microsoft 6. Механизмы защиты, реализуемые на базе ОС семейства Linux 7. Средства защиты информации, реализованные в активном сетевом оборудовании 8. Средства защиты информации, реализованные в прикладном программном обеспечении 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР). 10. Сертификация средств защиты информации.
2	Письменная работа	ОПК-4 , ОПК-7 , ПК-1	1. введение в предметную область. 2. Техническое проектирование и реализация комплексов средств защиты информации. Обзор подходов к созданию средств защиты информации. Проблемы проектирования и реализации механизмов защиты 3. Теоретические основы реализации механизмов защиты информации
3	Письменная работа	ОПК-4 , ОПК-7 , ПК-1	7. Средства защиты информации, реализованные в активном сетевом оборудовании 8. Средства защиты информации, реализованные в прикладном программном обеспечении 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР).
	Экзамен	ОПК-4, ОПК-7, ПК-1	

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 7					
Текущий контроль					

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
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
Письменная 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 серьёзные 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 3
Экзамен	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	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 7

Текущий контроль

1. Лабораторные работы

Темы 4, 5, 6, 7, 8, 9, 10

Лабораторная работа №1 Изучение требований к классам защищённости средств защиты информации. Ознакомиться с руководящими документами. Выписать полный перечень требований к классу СВТ, 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 уяз-вимостей.

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. Письменная работа

Темы 1, 2, 3

1. Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации
2. Организационная поддержка мер защиты. Отраслевые стандарты
3. Пакет руководящих документов Гостехкомиссии России
4. ISO 15408. Единые критерии
5. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности
6. Документы ФСТЭК России, разработанные на базе ISO 15408

Подсистема управления доступом

8. Подсистема обеспечения целостности
9. Подсистема регистрации и учёта событий
10. Криптографическая подсистема

3. Письменная работа

Темы 7, 8, 9

1. Стадии разработки программного обеспечения.
2. Виды программ и программных документов.
3. Техническое задание, требования к содержанию и оформлению.
4. Пояснительная записка. Требования к содержанию и оформлению.
5. Описание применения. Требования к содержанию и оформлению
6. Описание программы
7. Порядок выполнения ОКР
8. Требования к порядку разработки рабочей конструкторской документации
9. Понятие сертификации. Основные участники сертификации.
10. Схемы сертификационных испытаний. Инспекционный контроль.
11. Порядок проведения испытаний.

Экзамен

Вопросы к экзамену:

1. Построение подсистемы антивирусной защиты.
2. Межсетевые экраны. определение, назначение, классификации.
3. Обзор инструментальных средств анализа защищённости 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 7			
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	30
Письменная работа	Обучающиеся получают задание по освещению определённых теоретических вопросов или решению задач. Работа выполняется письменно и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	2 3	10 10
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. 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:

1. 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. - Режим доступа: http://znanium.com/bookread2.php?book=489084

2. Безопасность и управление доступом в информационных системах:Учебное пособие / А.В. Васильков, И.А.Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. - Режим доступа: http://znanium.com/bookread2.php?book=405313

3. 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:

1.Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] : учеб. Пособие - Электрон. Дан. -СПб. : Лань, 2017. - 324 с. - Режим доступа: https://e.lanbook.com/book/90153

2. Партыка Т. Л. Информационная безопасность [Электронный ресурс]:Учебное пособие /Т.Л. Партыка, И.И.Попов. - 5-е изд., перераб. И доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432с. - Режим доступа:http://znanium.com/bookread2.php?book=420047

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

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет-портал по информационной безопасности - http://all-ib.ru/

Сайт федеральной службы по техническому и экспортному контролю - www.fstec.ru

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

Вид работ	Методические рекомендации
лекции	Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Вид работ	Методические рекомендации
лабораторные работы	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 отчёт 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 сжатому, 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 раздельно 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. 7. Имя файла отчета: name_labN_course.ext где name - фамилия студента латинскими буквами, N - номер темы, course - аббревиатура курса, ext - расширение файла (doc, txt, rtf), например: 'ivanov_lab2_ПАСЗИ.doc';
самостоя-тельная работа	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.

Вид работ	Методические рекомендации
письменная работа	Цель выполнения работы: - научить студентов самостоятельно пользоваться учебной и нормативной литературной; - 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: подобрать необходимую литературу; составить развернутый план работы; затем изложить теоретическую часть вопроса (не допускается дословное переписывание текстов из брошюр, статей, учебников); привести практические примеры, используя конкретный материал (с приложением материала и поименным источником печати); решить предложенные практические задания; оформить работу; 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: выполненные не по своему варианту; выполненные небрежно и неразборчиво. Критерии качества работы 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).
экзамен	лекционным материалом, постарайтесь его понять, но не старайтесь запомнить. Результат для вас: общее обзорное представление обо всём данном учебном курсе. Помните, что лекции следует читать 2 раза - в начале вашей подготовки к экзамену и в конце - перед экзаменом. 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 Дополнительная литература. По списку вопросов подберите соответствующие разделы литературы, чтобы знать ответы на эти вопросы. Книги более полно и развёрнуто 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. 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. Вопросы. 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. Трудные вопросы. В последний день перед экзаменом 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. 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... Высшее образование требует именно такой способности: способности к погружению в предмет и к усвоению больших объёмов знаний за относительно короткий срок.

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 средства 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.

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

Освоение дисциплины "Программно-аппаратные средства 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 оборудованием 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 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .