МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Институт физики

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Программно-аппаратные средства информационной безопасности Б1.В.ДВ.7

Направление подготовки: 09.03.04 - Программная инженерия
Профиль подготовки: Технология проектирования аппаратно-программных информационных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Тептин Г.М. , Иванов Константин Васильевич

Рецензент(ы):

Акчурин А.Д.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Акчурин А. Д.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института физики:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 6120819

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (профессор) Тептин Г.М. Кафедра радиоастрономии Отделение радиофизики и информационных систем , Guerman.Teptin@kpfu.ru ; Иванов Константин Васильевич

1. Цели освоения дисциплины

-принципы работы и организацию современных аппаратных средств защиты информации;

-функции и задачи, стоящие перед администраторами безопасности.

-администрировать аппаратные средства защиты информации, дополняющие механизмы защиты операционных систем, обеспечивающие дополнительный функционал для СВТ, а также сетевые средства защиты информации

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

Данная учебная дисциплина включена в раздел "Б1.В.ДВ.7 Дисциплины (модули)" основной образовательной программы 09.03.04 Программная инженерия и относится к дисциплинам по выбору. Осваивается на 3, 4 курсах, 6, 7 семестры.

программы 09.03.04 'Программная инженерия 'Программно-аппаратные средства информационной безопасности' относится к дисциплинам Б1.В.ДВ.7

Осваивается на 4 курсе в 6-7 семестре.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-4 (профессиональные компетенции)	способность осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий
ПК-16 (профессиональные компетенции)	способностью формализовать предметную область программного проекта и разработать спецификации для компонентов программного продукта
ПК-5 (профессиональные компетенции)	владением стандартами и моделями жизненного цикла
ПК-6 (профессиональные компетенции)	владением классическими концепциями и моделями менеджмента в управлении проектами
ПК-8 (профессиональные компетенции)	владением основами групповой динамики, психологии и профессионального поведения, специфичных для программной инженерии
ПК-21 (профессиональные компетенции)	владением навыками чтения, понимания и выделения главной идеи прочитанного исходного кода, документации
ПК-22 (профессиональные компетенции)	способностью создавать программные интерфейсы

В результате освоения дисциплины студент:

1. 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.

2. 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

3. 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.

4. 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.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 8 зачетных(ые) единиц(ы) 288 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 6 семестре; экзамен в 7 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
1.	Тема 1. введение в предметную область.	7		2	0	0	
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	
3.	Тема 3. Теоретические основы реализации механизмов защиты информации	7		4	0	0	
4.	Тема 4. Организационные основы реализации механизмов защиты информации/ Нормативно-правовые документы, регламентирующие применение программно-аппаратных методов и средств ЗИ.	7		4	0	2	
5.	Тема 5. Механизмы защиты, реализуемые на основе программных продуктов фирмы Microsoft	7		4	0	2	
6.	Тема 6. Механизмы защиты, реализуемые на базе ОС семейства Linux	7		2	0	4	
7.	Тема 7. Средства защиты информации, реализованные в активном сетевом оборудовании	7		4	0	4	
8.	Тема 8. Средства защиты информации, реализованные в прикладном программном обеспечении	7		4	0	0	
9.	Тема 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР).	7		4	0	4	
10.	Тема 10. Сертификация средств защиты информации.	7		4	0	2	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
11.	Тема 11. Методы обеспечения безопасности систем	6		4	0	0	Контрольная работа
12.	Тема 12. Нормативная документация, используемая при создании и эксплуатации аппаратных средств защиты.	6		8	0	10	Контрольная работа
13.	Тема 13. Загрузка ОС и использование BIOS/UEFI в качестве средства создания замкнутой среды	6		8	0	8	
14.	Тема 14. Электронные замки и аппаратно-программные модули доверенной загрузки	6		8	0	10	
15.	Тема 15. Механизмы защиты информации, используемые в активном сетевом оборудовании	6		8	0	8	
.	Тема . Итоговая форма контроля	6		0	0	0	Экзамен
.	Тема . Итоговая форма контроля	7		0	0	0	Экзамен
	Итого			72	0	54	

4.2 Содержание дисциплины

Тема 1. Введение в предметную область.

лекционное занятие (2 часа(ов)):

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.

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

лекционное занятие (4 часа(ов)):

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.

Тема 3. Теоретические основы реализации механизмов защиты информации

лекционное занятие (4 часа(ов)):

Основные теоретические положения защиты информации. Подсистема управления доступом. Подсистема обеспечения целостности. 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.

лекционное занятие (4 часа(ов)):

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.

лабораторная работа (2 часа(ов)):

Документы ФСТЭК России, разработанные на базе ISO 15408.

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

лекционное занятие (4 часа(ов)):

Возможности КСЗ ОС семейства Windows. Подсистема управления доступом. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. Интерфейс администратора безопасности.

лабораторная работа (2 часа(ов)):

Возможности КСЗ ОС семейства Windows. Подсистема управления доступом. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. Интерфейс администратора безопасности.

Тема 6. Механизмы защиты, реализуемые на базе ОС семейства Linux

лекционное занятие (2 часа(ов)):

Возможности комплекса средств защиты (КСЗ) ОС. Подсистема управления доступом. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. Интерфейс администратора безопасности.

лабораторная работа (4 часа(ов)):

Интерфейс администратора безопасности.

Тема 7. Средства защиты информации, реализованные в активном сетевом оборудовании

лекционное занятие (4 часа(ов)):

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.

лабораторная работа (4 часа(ов)):

Основные защитные механизмы

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

лекционное занятие (4 часа(ов)):

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).

лекционное занятие (4 часа(ов)):

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

лабораторная работа (4 часа(ов)):

Порядок выполнения ОКР.

Тема 10. Сертификация средств защиты информации.

лекционное занятие (4 часа(ов)):

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.

лабораторная работа (2 часа(ов)):

Основные системы обязательной сертификации средств защиты информации

Тема 11. Методы обеспечения безопасности систем

лекционное занятие (4 часа(ов)):

Основные теоретические положения защиты информации. Подсистема управления доступом. Подсистема обеспечения целостности. Подсистема регистрации и учёта событий. Криптографическая под-система.

Тема 12. Нормативная документация, используемая при создании и эксплуатации аппаратных средств защиты.

лекционное занятие (8 часа(ов)):

Пакет руководящих документов Гостехкомиссии России. ISO 15408. Единые критерии. Особенности ISO 15408 по сравнению с другими стан-дартами в области безопасности. Документы ФСТЭК России, разработанные на базе ISO 15408.

лабораторная работа (10 часа(ов)):

Документы ФСТЭК России, разработанные на базе ISO 15408.

Тема 13. Загрузка ОС и использование BIOS/UEFI в качестве средства создания замкнутой среды

лекционное занятие (8 часа(ов)):

Порядок начальной загрузки системы. Штатные средства замыкания среды. Общие сведения о работе BIOS/UEFI . Описание алгоритма функционирования ЭЗ с проверкой целостности программной среды. Понятие АПМДЗ.

лабораторная работа (8 часа(ов)):

Описание алгоритма функционирования ЭЗ с проверкой целостности программной среды. Понятие АПМДЗ.

Тема 14. Электронные замки и аппаратно-программные модули доверенной загрузки

лекционное занятие (8 часа(ов)):

Аппаратные средства защиты от несанкционированного входа. Функция временной блокировки компьютера Механизмы управления доступом и защиты ресурсов. Механизм избирательного управления доступом. Механизм полномочного управления доступом. Механизм замкнутой программной среды. Механизмы контроля и регистрации.

лабораторная работа (10 часа(ов)):

Функция временной блокировки компьютера Механизмы управления доступом и защиты ресурсов.

Тема 15. Механизмы защиты информации, используемые в активном сетевом оборудовании

лекционное занятие (8 часа(ов)):

Используемое сетевое оборудование. Его классификация. Архитектура построения без-опасных сетей. Средства обеспечения безопасности корпоративных сетей. Основные за-щитные механизмы и примеры их реализации: построение защиты сетевых средств, построение системы межсетевого экранирования.

лабораторная работа (8 часа(ов)):

Средства обеспечения безопасности корпоративных сетей. Основные за-щитные механизмы и примеры их реализации: построение защиты сетевых средств, построение системы межсетевого экранирования.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
1.	Тема 1. введение в предметную область.	7		подготовка к отчету	2	отчет
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		подготовка к отчету	4	отчет

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
3.	Тема 3. Теоретические основы реализации механизмов защиты информации	7		подготовка к отчету	6	отчет
4.	Тема 4. Организационные основы реализации механизмов защиты информации/ Нормативно-правовые документы, регламентирующие применение программно-аппаратных методов и средств ЗИ.	7		подготовка к отчету	12	отчет
5.	Тема 5. Механизмы защиты, реализуемые на основе программных продуктов фирмы Microsoft	7		подготовка к отчету	5	отчет
6.	Тема 6. Механизмы защиты, реализуемые на базе ОС семейства Linux	7		подготовка к отчету	5	отчет
7.	Тема 7. Средства защиты информации, реализованные в активном сетевом оборудовании	7		подготовка к отчету	5	отчет
8.	Тема 8. Средства защиты информации, реализованные в прикладном программном обеспечении	7		подготовка к отчету	5	отчет

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
9.	Тема 9. Разработка средств защиты, реализуемых на программно-аппаратном уровне на примере выполнения опытно-конструкторской работы(ОКР).	7		подготовка к отчету	8	отчет
10.	Тема 10. Сертификация средств защиты информации.	7		подготовка к отчету	2	отчет
11.	Тема 11. Методы обеспечения безопасности систем	6		подготовка к контрольной работе	2	Контроль-ная работа
12.	Тема 12. Нормативная документация, используемая при создании и эксплуатации аппаратных средств защиты.	6		подготовка к контрольной работе	2	Контроль-ная работа
13.	Тема 13. Загрузка ОС и использование BIOS/UEFI в качестве средства создания замкнутой среды	6		подготовка к отчету	4	отчет
14.	Тема 14. Электронные замки и аппаратно-программные модули доверенной загрузки	6		подготовка к отчету	4	отчет

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
15.	Тема 15. Механизмы защиты информации, используемые в активном сетевом оборудовании	6		подготовка к отчету	6	отчет
	Итого				72	

5. Образовательные технологии, включая интерактивные формы обучения

Освоение дисциплины 'Программно-аппаратные средства информационной безопасности' 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

Браузер Google Chrome

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.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. введение в предметную область.

отчет , примерные вопросы:

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.

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

отчет , примерные вопросы:

Проблемы проектирования и реализации защищенных АС. Синтез КСЗ и его этапы.

Тема 3. Теоретические основы реализации механизмов защиты информации

отчет , примерные вопросы:

Основные теоретические положения защиты информации. Подсистема управления доступом. Подсистема обеспечения целостности. 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.

отчет , примерные вопросы:

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 защиты. 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

отчет , примерные вопросы:

Возможности КСЗ ОС семейства Windows. Подсистема управления доступом. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. Интерфейс администратора безопасности.

Тема 6. Механизмы защиты, реализуемые на базе ОС семейства Linux

отчет , примерные вопросы:

Возможности комплекса средств защиты (КСЗ) ОС. Подсистема управления доступом. Подсистема регистрации и учёта. Подсистема обеспечения целостности. Криптографическая подсистема. Интерфейс администратора безопасности.

Тема 7. Средства защиты информации, реализованные в активном сетевом оборудовании

отчет , примерные вопросы:

Используемое сетевое оборудование. Его классификация. Архитектура построения безопасных 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 безопасности, построение системы кодирования информации, передаваемой по открытым каналам связи.

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

отчет , примерные вопросы:

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).

отчет , примерные вопросы:

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.

отчет, примерные вопросы:

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 требуемого класса защищенности и уровня контроля отсутствия недекларированных возможностей. Сертификация на соответствие техническим условиям. Особенности сертификации средств защиты конфиденциальной 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.

Тема 11. Методы обеспечения безопасности систем

Контрольная работа , примерные вопросы:

Основные теоретические положения защиты информации. Подсистема управления доступом. Подсистема обеспечения целостности. Подсистема регистрации и учёта событий. Криптографическая под-система.

Тема 12. Нормативная документация, используемая при создании и эксплуатации аппаратных средств защиты.

Контрольная работа , примерные вопросы:

Пакет руководящих документов Гостехкомиссии России. ISO 15408. Единые критерии. Особенности ISO 15408 по сравнению с другими стан-дартами в области безопасности. Документы ФСТЭК России, разработанные на базе ISO 15408.

Тема 13. Загрузка ОС и использование BIOS/UEFI в качестве средства создания замкнутой среды

отчет , примерные вопросы:

Порядок начальной загрузки системы. Штатные средства замыкания среды. Общие сведения о работе BIOS/UEFI . Описание алгоритма функционирования ЭЗ с проверкой целостности программной среды. Понятие АПМДЗ.

Тема 14. Электронные замки и аппаратно-программные модули доверенной загрузки

отчет , примерные вопросы:

Аппаратные средства защиты от несанкционированного входа. Функция временной блокировки компьютера. Механизмы управления доступом и защиты ресурсов. Механизм избирательного управления доступом. Механизм полномочного управления доступом. Механизм замкнутой программной среды. Механизмы контроля и регистрации.

Тема 15. Механизмы защиты информации, используемые в активном сетевом оборудовании

отчет , примерные вопросы:

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, построение системы межсетевого экранирования.

Итоговая форма контроля

экзамен (в 6 семестре)

Итоговая форма контроля

экзамен (в 7 семестре)

Примерные вопросы к экзамену:

Вопросы к экзамену:

Пакет руководящих документов Гостехкомиссии России
1. Особенности ISO 15408 по сравнению с другими стандартами в области безопасности
2. Документы ФСТЭК России, разработанные на базе ISO 15408
3. Подсистема управления доступом
4. Подсистема обеспечения целостности
5. Подсистема регистрации и учёта событий
6. Криптографическая подсистема
7. Средства защиты информации активного сетевого оборудования
8. Профили защиты АПМДЗ
9. Структура государственных органов, осуществляющих контроль за выполнением требований по защите информации
10. Организационная поддержка мер защиты. Отраслевые стандарты

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.

7.1. Основная литература:

Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. Режим доступа: http://znanium.com/bookread.php?book=405000

Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5. Режим доступа: http://znanium.com/bookread.php?book=423927

Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: http://znanium.com/bookread.php?book=169345

7.2. Дополнительная литература:

Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4 - http://znanium.com/catalog.php?bookinfo=402686

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. - 184 с. :http://znanium.com/bookread.php?book=453862

7.3. Интернет-ресурсы:

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

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

Хорев П. Б. Программно-аппаратная защита информации: учебное пособие - http://znanium.com/bookread.php?book=169345

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Программно-аппаратные средства информационной безопасности" 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. 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, УМК, 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 профессионального образования (ФГОС ВПО) нового поколения.

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 Cre i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audi, 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.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 09.03.04 "Программная инженерия" и профилю подготовки Технология проектирования аппаратно-программных информационных систем .

Автор(ы):
Тептин Г.М. _____
Иванов Константин Васильевич _____
"__" _____ 201 __ г.

Рецензент(ы):
Акчурин А.Д. _____
"__" _____ 201 __ г.