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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.

подписано электронно-цифровой подписью

Программа дисциплины

Технология построения защищенных автоматизированных систем Б3.В.10

Направление подготовки: 090900.62 - Информационная безопасность
Профиль подготовки: Информационная безопасность автоматизированных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Иванов К.В.

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 699014

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) ассистент, к.н. Иванов К.В. Кафедра радиоастрономии Отделение радиофизики и информационных систем , KVIvanov@kpfu.ru

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) Б3.В10 "Технология построения защищенных автоматизированных систем" является необходимость дать теоретические знания по техническому проектированию и реализации систем защиты и практические навыки построения системы межсетевого экранирования, обнаружения вторжений, анализа сетевой безопасности, организации безопасной связи между отдельными сетями организации

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

Данная учебная дисциплина включена в раздел " Б3.В.10 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к вариативной части. Осваивается на 4 курсе, 7 семестр.

Дисциплина Б3.В10 "Технология построения защищенных автоматизированных систем"входит в цикл дисциплин "Профессиональный".

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-5 (общекультурные компетенции)	способность к кооперации с коллегами, работе в коллективе
ПК-5 (профессиональные компетенции)	способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации
ПК-6 (профессиональные компетенции)	способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-7 (профессиональные компетенции)	способность использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий
ПК-8 (профессиональные компетенции)	способность определить виды и формы информации, подтвержденной угрозами, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятий

В результате освоения дисциплины студент:

1. должен знать:

принципы и методы построения защищенных автоматизированных систем;

Жизненный цикл защищённых автоматизированных систем

2. должен уметь:

Принимать участие в работах по созданию и сопровождению СЗИ на всех этапах жизненного цикла АС

3. должен владеть:

Навыками аудита АС, проектирования СЗИ АС, подготовки АС к аттестации..

4. должен демонстрировать способность и готовность:

- Интерпретировать данные полученные от заказчика, а также классифицировать АС по уровню защищенности, используя нормативную документацию.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет 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	Практические занятия	Лабораторные работы	
1.	Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем	7	1	2	0	4	устный опрос
2.	Тема 2. Аудит информационной безопасности корпоративной системы.	7	2	2	0	4	устный опрос
3.	Тема 3. Техническое проектирование защищённых корпоративных систем	7	3-4	4	0	8	устный опрос
4.	Тема 4. Развёртывание защищённых корпоративных систем	7	5-7	6	0	12	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
5.	Тема 5. Порядок аттестации и сертификации корпоративной системы.	7	8	2	0	4	устный опрос
6.	Тема 6. Проблема эксплуатации защищённых АС, администрирование безопасности информации АС.	7	9	2	0	4	устный опрос
.	Тема . Итоговая форма контроля	7		0	0	0	зачет
	Итого			18	0	36	

4.2 Содержание дисциплины

Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем

лекционное занятие (2 часа(ов)):

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

лабораторная работа (4 часа(ов)):

Подготовка технического задания на Автоматизированную систему

Тема 2. Аудит информационной безопасности корпоративной системы.

лекционное занятие (2 часа(ов)):

Аудит информационной безопасности корпоративной системы. Определение и классификации видов аудита. Назначение аудита. Типовая методика аудита.

лабораторная работа (4 часа(ов)):

Изучение инструментальных средств проведения аудита ИБ Установка и использование Microsoft Baseline Security Analyzer Установка и использование сетевого сканера XSpider. Установка и использование сканера Nessus

Тема 3. Техническое проектирование защищённых корпоративных систем

лекционное занятие (4 часа(ов)):

Проектирование и развёртывание защищённых корпоративных систем. Используемое сетевое оборудование. Классификация сетевого оборудования. Техническое проектирование и реализация систем защиты АС. Основные подсистемы систем защиты информации, современное представление и реализация. Безопасность вычислительных сетей. Архитектура построения безопасных сетей Cisco SAFE.

лабораторная работа (8 часа(ов)):

Изучение настроек безопасности сетевого оборудования Обзор средств разграничения доступа на активном оборудовании Использование средств разграничения доступа на нескольких коммутаторах Создание и удаление виртуальных сетей на коммутаторе Catalyst 2950 Конфигурирование средств защиты, встроенных в Cisco IOS

Тема 4. Развёртывание защищённых корпоративных систем

лекционное занятие (6 часа(ов)):

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. Организация безопасной связи между отдельными сетями организации (VPN).

лабораторная работа (12 часа(ов)):

Изучение работы защищённой фермы терминальных серверов Настройка серверов контроллеров домена Настройка фермы терминальных серверов Настройка брокера терминального подключения Установка ПО СЗИ Secret Net на созданную конфигурацию

Тема 5. Порядок аттестации и сертификации корпоративной системы.

лекционное занятие (2 часа(ов)):

Порядок аттестации и сертификации корпоративной системы. Государственная система лицензирования и сертификации в области защиты информации. Виды деятельности, подлежащие лицензированию. Сертификация средств защиты информации.

лабораторная работа (4 часа(ов)):

Разработка шаблонов документов: 1) Программа и методика аттестационных испытаний объекта информатизации. 1) Предписание на эксплуатацию объекта ВТ. 2) Протоколы по оценке защищенности информации от утечки по каналам ПЭМИН. 3) Протокол оценки защищенности информации от утечки по каналу НСД. 4) Заключение по результатам аттестационных испытаний объекта информатизации. 5) Аттестат соответствия (при положительных выводах заключения по результатам аттестационных испытаний (п.5)). 6) Технический паспорт на АС (выделенное помещение).

Тема 6. Проблема эксплуатации защищённых АС, администрирование безопасности информации АС.

лекционное занятие (2 часа(ов)):

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), система удаленного администрирования средствами защиты информации (СУДАД)

лабораторная работа (4 часа(ов)):

Разработка шаблонов документов: 1) Описание технологического процесса обработки информации на АС. 2) Перечень защищаемых в АС ресурсов с документальным подтверждением степени конфиденциальности каждого ресурса. 3) Перечень проводимых работ на ПЭВМ. 4) Организационно-распорядительная документация (матрица доступа) разрешительной системы доступа персонала к защищаемым ресурсам АС. 5) Список лиц постоянно работающих в комнате с АС, а также лиц постоянно не работающих, но привлекаемых для различных работ. 6) Акт классификации АС. 7) Акт категорирования АС. 8) Инструкция пользователям АС. 9) Инструкция администратору безопасности информации. 10) Инструкция по антивирусной защите. 11) Инструкция по организации парольной защиты. 12) Инструкция по обеспечению режима секретности работ, проводимых на ПЭВМ. 13) Список лиц допущенных к работам на ПЭВМ. 14) Проект приказа о вводе в эксплуатацию аттестованной АС. 15) Проект приказа о назначении комиссии по категорированию и классификации АС.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем	7	1	подготовка к устному опросу	6	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
2.	Тема 2. Аудит информационной безопасности корпоративной системы.	7	2	подготовка к устному опросу	6	устный опрос
3.	Тема 3. Техническое проектирование защищённых корпоративных систем	7	3-4	Изучение нормативных документов: ГОСТ Р 50739-95 ?Средства вычислительной техники. Защита от несанк	4	устный опрос
				подготовка к устному опросу	6	устный опрос
4.	Тема 4. Развёртывание защищённых корпоративных систем	7	5-7	Изучение нормативных документов: ГОСТ 34.603-92 ?Информационная технология. Виды испытаний автомат	14	устный опрос
				подготовка к устному опросу	6	устный опрос
5.	Тема 5. Порядок аттестации и сертификации корпоративной системы.	7	8	подготовка к устному опросу	6	устный опрос
6.	Тема 6. Проблема эксплуатации защищённых АС, администрирование безопасности информации АС.	7	9	подготовка к устному опросу	6	устный опрос
	Итого				54	

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций читается на основе мультимедийных технологий. Компьютерный класс, позволяющий развёртывать на каждой ЭВМ не менее 2 виртуальных машин.

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

Тема 1. Техническое проектирование и реализация систем защиты корпоративных систем

устный опрос , примерные вопросы:

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

Тема 2. Аудит информационной безопасности корпоративной системы.

устный опрос , примерные вопросы:

Аудит информационной безопасности корпоративной системы. Определение и классификации видов аудита. Назначение аудита. Типовая методика аудита.

Тема 3. Техническое проектирование защищённых корпоративных систем

устный опрос, примерные вопросы:

Проектирование и развёртывание защищённых корпоративных систем. Используемое сетевое оборудование. Классификация сетевого оборудования. Техническое проектирование и реализация систем защиты АС. Основные подсистемы систем защиты информации, современное представление и реализация. Безопасность вычислительных сетей. Архитектура построения безопасных сетей Cisco SAFE.

устный опрос , примерные вопросы:

Проверка знания терминологии и определений, используемых в документации

Тема 4. Развёртывание защищённых корпоративных систем

устный опрос , примерные вопросы:

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. Организация безопасной связи между отдельными сетями организации (VPN).

устный опрос , примерные вопросы:

Проверка знания терминологии и определений, используемых в документации

Тема 5. Порядок аттестации и сертификации корпоративной системы.

устный опрос , примерные вопросы:

Порядок аттестации и сертификации корпоративной системы. Государственная система лицензирования и сертификации в области защиты информации. Виды деятельности, подлежащие лицензированию. Сертификация средств защиты информации.

Тема 6. Проблема эксплуатации защищённых АС, администрирование безопасности информации АС.

устный опрос , примерные вопросы:

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), система удаленного администрирования средствами защиты информации (СУДАД)

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Разработанный блок вопросов для компьютерной системы тестирования TCExam

7.1. Основная литература:

Аверченков, В. И. Разработка системы технической защиты информации [электронный ресурс] : учеб. пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. - 2-е изд., стереотип. - М. : ФЛИНТА, 2011. - 187 с. - http://znanium.com/bookread.php?book=453880

Поддержка принятия решений при проектировании систем защиты информации: Монография / В.В. Бухтояров, В.Г. Жуков, В.В. Золотарев. - М.: НИЦ ИНФРА-М, 2014. - 131 с. - http://znanium.com/bookread.php?book=445551

Гришина Н. В. Комплексная система защиты информации на предприятии: учеб.пособие / Н.В. Гришина. - М.: Форум, 2009. - 240 с.: http://znanium.com/bookread.php?book=175658

7.2. Дополнительная литература:

Расторгуев, С. П. Основы информационной безопасности. Серия: Высшее профессиональное образование / С.П. Расторгуев - Издательство: Академия, 2007.

Кузнецов И. Н. Кузнецов, И. Н. Бизнес-безопасность [Электронный ресурс] / И. Н. Кузнецов. - 3-е изд. - М.: Дашков и К, 2013. - 416 с.: http://znanium.com/bookread.php?book=430343

7.3. Интернет-ресурсы:

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

Робачевский А.М., Немнюгин С.А., Стесик О.Л. Операционная система Unix. - СПб.: БХВ-Петербург, 2005. - http://znanium.com/bookread.php?book=356894

Чекмарев, А. Н. Microsoft Windows Server 2008 / Алексей Чекмарев. ? СПб.: БХВ-Петербург, 2008. - http://znanium.com/bookread.php?book=350521

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Технология построения защищенных автоматизированных систем" предполагает использование следующего материально-технического обеспечения:

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.

Компьютерный класс, позволяющий развёртывать на каждой ЭВМ не менее 2 виртуальных машин.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 090900.62 "Информационная безопасность" и профилю подготовки Информационная безопасность автоматизированных систем .

Автор(ы):
Иванов К.В. _____
"__" _____ 201 __ г.

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