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. Таюрский Д.А.

_____ "____" _____20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Технология построения защищенных автоматизированных систем Б1.В.ОД.9

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность автоматизированных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Акчурин А.Д. , Иванов К.В.

Рецензент(ы):

Хуторова О.Г.

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 624818

Казань
2018

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 К.В. , 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 " Б1.В.ОД.9 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к обязательным дисциплинам. 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:

В результате освоения дисциплины студент:

1. должен знать:

принципы и методы построения защищенных автоматизированных систем;

механизмы, используемые для защиты информации, циркулирующей в различных системах;

основные положения и особенности применения руководящих документов;

процессы, протекающие в ходе аттестации систем.

Жизненный цикл защищённых автоматизированных систем

2. должен уметь:

а) классифицировать защищаемую информацию по видам тайны и уровням конфиденциальности;

б) классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;

в) формировать комплекс мер по защите информации в АС и оценивать их эффективность на основе заданных требований по безопасности информации;

г) разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

3. должен владеть:

а) навыками создания АС в соответствии с ГОСТ 34.XXX;

б) навыками подготовки технического задания на разработку системы защиты информации

в) навыками подготовки системы к аттестации

4. должен демонстрировать способность и готовность:

- Интерпретировать данные полученные от заказчика;
- классифицировать АС по уровню защищенности;
-использовать 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. Теоретические основы построения защищённых автоматизированных систем	7	1	4	0	6	Устный опрос
2.	Тема 2. Аудит защищённой АС	7	2	2	0	4	Устный опрос
3.	Тема 3. Проектирование и развёртывание защищённых автоматизированных систем	7	3-4	2	0	10	Устный опрос
4.	Тема 4. Моделирование при разработке защищённых АС	7	5-7	4	0	12	Устный опрос
5.	Тема 5. Порядок аттестации автоматизированной системы.	7	8	2	0	0	Устный опрос
6.	Тема 6. Особенности построения систем защиты информации различного уровня конфиденциальности	7	9	4	0	4	Устный опрос
.	Тема . Итоговая форма контроля	7		0	0	0	Зачет

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
	Итого			18	0	36	

4.2 Содержание дисциплины

Тема 1. Теоретические основы построения защищённых автоматизированных систем

лекционное занятие (4 часа(ов)):

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.

лабораторная работа (6 часа(ов)):

Подготовка технического задания на Автоматизированную систему

Тема 2. Аудит защищённой АС

лекционное занятие (2 часа(ов)):

Аудит информационной безопасности корпоративной системы. Определение и классификации видов аудита. Назначение аудита. Последовательность действий в ходе аудита. Обзор методов аудита. Структура итогового отчёта. Определение и нормативное закрепление состава защищаемой информации

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. Проектирование и развёртывание защищённых автоматизированных систем

лекционное занятие (2 часа(ов)):

Проектирование и развёртывание защищённых корпоративных систем. Требования к содержанию документов по общесистемным решениям. Ведомость проекта. Пояснительная записка к проекту. Стандарты проектирования систем защиты информации.

лабораторная работа (10 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. Моделирование при разработке защищённых АС

лекционное занятие (4 часа(ов)):

Существующие точки зрения и подходы к моделированию. Модель нарушителя по РД Гостехкомиссии Классификация нарушителей в соответствии с документами ФСБ Классификация угроз безопасности в соответствии с ПП 1119 Альтернативные классификации угроз безопасности Классификации уязвимостей системы Этапы формирования модели угроз Создание модели защиты системы.

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 автоматизированной системы.

лекционное занятие (2 часа(ов)):

Нормативная база организации работ по аттестации объектов информатизации (ОИ) по требованиям без-опасности информации. Схема организации и проведения работ по аттестации ОИ. Функции организации-заявителя, ФСТЭК России и органов по аттестации ОИ. Содержание заявки на проведение аттестации ОИ. Исходные данные и документация, представляемые для проведения аттестации ОИ. Особенности исходных данных для различных типов аттестуемых ОИ. Методическое обеспечение и инструментальные средства для проведения аттестационных испытаний (общий обзор). Программа и методики аттестационных испытаний ОИ. Типовое содержание аттестационных испытаний ОИ. Основные факторы, определяющие содержание и объем аттестационных испытаний. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов. Ответственность за правильность аттестации и эксплуатации, аттестованных АС.

Тема 6. Особенности построения систем защиты информации различного уровня конфиденциальности

лекционное занятие (4 часа(ов)):

Особенности построения СЗИ для обработки информации, содержащей персональные данные. Особенности построения СЗИ для обработки информации в государственных учреждениях. Особенности построения СЗИ для обработки информации, содержащей коммерческую и служебную тайны. Особенности построения СЗИ для обработки информации, содержащей государственную тайну.

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. Теоретические основы построения защищённых автоматизированных систем	7	1	подготовка к устному опросу	6	устный опрос
2.	Тема 2. Аудит защищённой АС	7	2	подготовка к устному опросу	6	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
3.	Тема 3. Проектирование и развёртывание защищённых автоматизированных 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. Моделирование при разработке защищённых АС	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 автоматизированной системы.	7	8	подготовка к устному опросу	6	устный опрос
6.	Тема 6. Особенности построения систем защиты информации различного уровня конфиденциальности	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

7.1. Основная литература:

1. 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. - ISBN 978-5-9765-1272-6. - Режим доступа: http://znanium.com/bookread.php?book=453862

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

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

4. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2009. - 256 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-336-1, 2000 экз. - Режим доступа: http://znanium.com/bookread.php?book=165929

5. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-353-8, 1500 экз. - Режим доступа: http://znanium.com/bookread.php?book=169345

7.2. Дополнительная литература:

1. 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, 2000 экз. - Режим доступа: http://znanium.com/bookread.php?book=402686

2. Петровский В. И. Петровский В. В. Глова В. И. Комплексная защита информации на предприятии: методы и способы противодействия средствам технических разведок: учебное пособие. Казань [Изд-во Казанского государственного технического университета] 2012

3. 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

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 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность автоматизированных систем .

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

Рецензент(ы):
Хуторова О.Г. _____
"__" _____ 201 __ г.