МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

А1.В.ОД.3 «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА»

Направление подготовки

10.06.01 Информационная безопасность

Направленность (профиль):

Методы и системы защиты информации, информационная безопасность

Квалификация (степень) – Исследователь. Преподаватель-исследователь.

Форма обучения: очная, заочная

Пенза, 2014

Рабочая программа составлена в соответствии с ФГОС ВО по направлению 10.06.01 Информационная безопасность подготовки научно-педагогических кадров в аспирантуре (уровень подготовки кадров высшей квалификации)

Программу составил:
Фатеев А.Г., к.т.н, доцент _____
(Ф.И.О., должность, подпись)

Программа обсуждена на заседании кафедры «Информационная безопасность систем и технологий»
Протокол № 1 от «16» 09 2014 года
Зав. кафедрой ИБСТ _____ С.Л. Зефиров
(подпись, Ф.И.О.)

Программа согласована с деканом факультета приборостроения, информационных технологий и электроники
Декан факультета ПИТЭ _____ В.Д. Кревчик
(подпись, Ф.И.О., дата)

Программа одобрена методической комиссией факультета ПИТЭ
Протокол № 1 от «1» 10 20__ года
Председатель методической комиссии
факультета ПИТЭ _____ А.В. Задера
(подпись, Ф.И.О.)

Цели и задачи изучения дисциплины

Цель изучения дисциплины – формирование у аспирантов углубленных профессиональных знаний о методах и средствах защиты информации в условиях информационного противоборства.

Задачи дисциплины:

– изучить основные аспекты и модели информационного противоборства;

– изучить основные методы и средства защиты информации для информационных систем, находящихся в состоянии информационного конфликта;

– подготовить аспирантов к применению полученных знаний для анализа подсистемы информационной безопасности информационной системы и формирования модели управления информационной безопасностью объектов, находящихся в состоянии информационного конфликта.

2. Место дисциплины в структуре ОПОП аспирантуры

Дисциплина относится к обязательным дисциплинам вариативной части дисциплин, обеспечивающих подготовку аспирантов по направлению 10.06.01 «Информационная безопасность», направленность (профиль) «Методы и системы защиты информации, информационная безопасность». Изучение дисциплины базируется на следующих дисциплинах, формирующих определенные знания, умения и навыки: Информационная безопасность бизнеса и деятельности организации, Проблемы обеспечения информационной безопасности автоматизированных систем, Вычислительная техника и информационные технологии в профессиональной научной деятельности.

Основные положения дисциплины «Методы и средства защиты информации в условиях информационного противоборства» используются в следующих дисциплинах: Методы и системы защиты информации, информационная безопасность, Проблемы и методы защиты информации в телекоммуникационных системах специального назначения.

Также основные положения дисциплины могут быть использованы при прохождении практики по получению профессиональных умений и опыта профессиональной деятельности (научно-исследовательская практики), осуществлении научно-исследовательской деятельности и подготовки НКР (диссертации), при подготовке к государственному экзамену, подготовке научного доклада об основных результатах подготовленной НКР (диссертации).

3. Компетенции аспиранта, формируемые в результате освоения программы дисциплины

Изучение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки:

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ОПК-1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии	Знать: – основные методы защиты информации, применяемые для информационных систем, находящихся в состоянии информационного противоборства; – программные, программно-аппаратные средства и системы защиты информации и технические характеристики соответствующего

	теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	оборудования и программного обеспечения.
		Уметь: применять методы и средства защиты информации в информационных системах, находящихся в состоянии информационного конфликта.
		Владеть: навыками применения методов и средств защиты информации в информационных системах, находящихся в состоянии информационного конфликта.
ОПК-3	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	Знать: – методы, применяемые для контроля и оценки эффективности программных и программно-аппаратных средств защиты информации и оценки соответствия требованиям по ЗИ; – программно-аппаратные средства, применяемые для контроля и оценки эффективности средств защиты информации и оценки соответствия требованиям по ЗИ.
		Уметь: – применять методы контроля и оценки эффективности программных и программно-аппаратных средств защиты информации и оценки соответствия требованиям по ЗИ; – применять программно-аппаратные средства, применяемые для контроля и оценки эффективности средств защиты информации и оценки соответствия требованиям по ЗИ.
		Владеть: навыками контроля и оценки эффективности программных и программно-аппаратных средств защиты информации и оценки соответствия требованиям по ЗИ.
ПК-8	Способность анализировать проблемы обеспечения безопасности информации ограниченного доступа и применять методы защиты информации при ее обработке в информационных системах	Знать: – основные проблемы обеспечения безопасности информации ограниченного доступа, факторы и угрозы, влияющие на безопасность информации ограниченного доступа; – методы защиты информации, реализуемые программными, программно-аппаратными средствами и системами защиты информации; – программные, программно-аппаратные средства и системы защиты информации, применяемые для обеспечения безопасности информации ограниченного доступа.
		Уметь: – проводить анализ угроз и проблем обеспечения безопасности информации ограниченного доступа; – осуществлять сбор и анализ исходных данных, необходимых для выбора методов и средств защиты информации ограниченного доступа; – проводить сравнительный анализ

		программных, программно-аппаратных средств и систем защиты информации, применяемых для обеспечения безопасности информации ограниченного доступа.
		Владеть: – навыками выбора методов и средств защиты информации ограниченного доступа; – навыками применения программных, программно-аппаратных средств и систем защиты информации, применяемых для обеспечения безопасности информации ограниченного доступа.

4. Структура и содержание дисциплины

4.1. Структура дисциплины Методы и средства защиты информации в условиях информационного противоборства

4.1.1. Структура дисциплины для очной формы

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)							Формы текущего контроля успеваемости *(по неделям семестра)*	
				Аудиторная работа			Самостоятельная работа					
				Всего	Лекция	Практические занятия	Всего	Подготовка к аудиторным занятиям	Подготовка к практическим занятиям	Подготовка к экзамену	Проверка тестов	Оценка выполнения практических заданий в форме тестирования
1.	Раздел 1. Методы и средства информационного противоборства	5	1-2	2	2		8	4		4	9	
2.	Раздел 2. Методы ЗИ, реализуемые специальными СЗИ	5	3-12	20	10	10	60	20	20	20	9	
2.1	Тема 2.1. Методы ЗИ, реализуемые СЗИ от НСД	5	3-4	8	2	6	20	4	12	4	9	9
2.2	Тема 2.2. Методы ЗИ, реализуемые средствами защиты от вредоносного ПО	5	5-6	2	2		8	4		4	9	
2.3	Тема 2.3. Методы ЗИ, реализуемые СЗИ, обеспечивающими безопасное межсетевое взаимодействие	5	7-8	2	2		8	4		4	9	
2.4	Тема 2.4. Методы ЗИ, реализуемые средствами контроля и предотвращения утечек информации	5	9-10	6	2	4	16	4	8	4	16	9
2.5	Тема 2.5. Методы и средства,	5	11-12	2	2		8	4		4	16	

	применяемые для контроля и оценки эффективности функционирования СЗИ											
3.	Раздел 3. Защита информации в виртуальных инфраструктурах	5	13-16	8	4	4	24	8	8	8	16	16
3.1	Тема 3.1. Технологии и платформы виртуализации	5	13-14	6	2	4	16	4	8	4	16	16
3.2	Тема 3.2. Методы и средства ЗИ, применяемые для защиты ВИ	5	15-16	2	2		8	4		4	16	
4.	Раздел 4. Методы ЗИ, реализуемые в операционных системах	5	17-18	6	2	4	16	4	8	4	18	18
	Подготовка к экзамену	5								36		
	Общая трудоемкость, в часах	5	144	36	18	18	108	36	36		Промежуточная аттестация	
											Форма	Семестр
											Зачет	–
											Экзамен	5

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

4.1.2. Структура дисциплины для заочной формы

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости *(по неделям семестра)*
			Аудиторная работа		Самостоятельная работа			
			Всего	Лекция	Всего	Подготовка к аудиторным занятиям	Подготовка к экзамену	Проверка тестов
1.	Раздел 1. Методы и средства информационного противоборства	5	2	2	16	12	4	+
2.	Раздел 2. Методы ЗИ, реализуемые специальными СЗИ	5	5	5	80	60	20	+
2.1	Тема 2.1. Методы ЗИ, реализуемые СЗИ от НСД	5	1	1	16	12	4	+
2.2	Тема 2.2. Методы ЗИ, реализуемые средствами защиты от вредоносного ПО	5	1	1	16	12	4	+
2.3	Тема 2.3. Методы ЗИ, реализуемые СЗИ, обеспечивающими безопасное межсетевое взаимодействие	5	1	1	16	12	4	+
2.4	Тема 2.4. Методы ЗИ, реализуемые средствами контроля и предотвращения	5	1	1	16	12	4	+

	утечек информации							
2.5	Тема 2.5. Методы и средства, применяемые для контроля и оценки эффективности функционирования СЗИ	5	1	1	16	12	4	+
3	Раздел 3. Защита информации в виртуальных инфраструктурах	5	1	1	23	15	8	+
4	Раздел 4. Методы ЗИ, реализуемые в операционных системах	5	1	1	16	12	4	+
	Подготовка к экзамену	5					36	
	Общая трудоемкость, в часах	5	9	9	135	99		Промежуточная аттестация

Форма	Семестр
Зачет	–
Экзамен	5

4.2. Содержание дисциплины, очная форма обучения

Раздел 1. Основы теории информационного противоборства

Концепции и цели информационного противоборства. Модели и методы информационного противоборства. Информационная война. Информационное оружие. Средства, применяемые в качестве информационного оружия в информационном противоборстве.

Раздел 2. Методы ЗИ, реализуемые специальными СЗИ

Тема 2.1. Методы ЗИ, реализуемые СЗИ от НСД

Методы ограничения доступа и управления доступом. Замкнутая программная среда, управление доступом к устройствам, контроль целостности, контроль аппаратной конфигурации, регистрация событий безопасности, контроль работоспособности, дополнительные функции СЗИ.

Тема 2.2. Методы ЗИ, реализуемые средствами защиты от вредоносного ПО

Статическая и динамическая задачи защиты. Методы борьбы с воздействием вредоносного ПО. Защита от изменения и контроль целостности. Создание доверенной программной среды. Защита от изменения и контроль целостности.

Тема 2.3. Методы ЗИ, реализуемые СЗИ, обеспечивающими безопасное межсетевое взаимодействие

Трансляция сетевых адресов. Фильтрация сетевого трафика. Применение криптографических методов ЗИ. Управление доступом.

Тема 2.4. Методы ЗИ, реализуемые средствами контроля и предотвращения утечек информации

Контроль содержимого информации. Применение цифровых отпечатков. Лингвистические и статистические методы контроля. Контроль содержания графической информации.

Тема 2.5. Методы и средства, применяемые для контроля и оценки эффективности функционирования СЗИ

Методы контроля и оценки эффективности функционирования программных СЗИ. Программно-аппаратные средства, применяемые для контроля и оценки эффективности.

Раздел 3. Защита информации в виртуальных инфраструктурах

Тема 3.1. Технологии виртуализации

Виртуализация: термины и определения. Виды виртуализации, классификация видов виртуализации. Основные компоненты среды виртуализации. Основные платформы виртуализации.

Тема 3.2. Методы и средства ЗИ, применяемые для защиты ВИ

Методы защиты ВИ, реализуемые платформами виртуализации, встроенные механизмы безопасности. Специальные СЗИ, применяемые для защиты ВИ.

Раздел 4. Методы ЗИ, реализуемые в операционных системах

Механизмы обеспечения ИБ, реализованные в ОС общего назначения: идентификация и аутентификация, парольные системы, управление доступом, политики безопасности. Сертифицированные защищенные ОС. Механизмы обеспечения ИБ, реализованные в защищенных ОС.

4.3. Содержание дисциплины, заочная форма обучения

Раздел 1. Основы теории информационного противоборства

Концепции и цели информационного противоборства. Модели и методы информационного противоборства. Информационная война. Информационное оружие. Средства, применяемые в качестве информационного оружия в информационном противоборстве.

Раздел 2. Методы ЗИ, реализуемые специальными СЗИ

Тема 2.1. Методы ЗИ, реализуемые СЗИ от НСД

Методы ограничения доступа и управления доступом. Замкнутая программная

среда, управление доступом к устройствам, контроль целостности, контроль аппаратной конфигурации, регистрация событий безопасности, контроль работоспособности, дополнительные функции СЗИ.

Тема 2.2. Методы ЗИ, реализуемые средствами защиты от вредоносного ПО

Статическая и динамическая задачи защиты. Методы борьбы с воздействием вредоносного ПО. Защита от изменения и контроль целостности. Создание доверенной программной среды. Защита от изменения и контроль целостности.

Тема 2.3. Методы ЗИ, реализуемые СЗИ, обеспечивающими безопасное межсетевое взаимодействие

Трансляция сетевых адресов. Фильтрация сетевого трафика. Применение криптографических методов ЗИ. Управление доступом.

Тема 2.4. Методы ЗИ, реализуемые средствами контроля и предотвращения утечек информации

Контроль содержимого информации. Применение цифровых отпечатков. Лингвистические и статистические методы контроля. Контроль содержания графической информации.

Тема 2.5. Методы и средства, применяемые для контроля и оценки эффективности функционирования СЗИ

Методы контроля и оценки эффективности функционирования программных СЗИ. Программно-аппаратные средства, применяемые для контроля и оценки эффективности.

Раздел 3. Защита информации в виртуальных инфраструктурах

Виртуализация: термины и определения. Виды виртуализации, классификация видов виртуализации. Основные компоненты среды виртуализации. Основные платформы виртуализации. Методы защиты ВИ, реализуемые платформами виртуализации, встроенные механизмы безопасности. Специальные СЗИ, применяемые для защиты ВИ.

Раздел 4. Методы ЗИ, реализуемые в операционных системах

Механизмы обеспечения ИБ, реализованные в ОС общего назначения: идентификация и аутентификация, парольные системы, управление доступом, политики безопасности. Сертифицированные защищенные ОС. Механизмы обеспечения ИБ, реализованные в защищенных ОС.

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» и для реализации компетентностного подхода при изучении дисциплины предусматривается использование в учебном процессе активных и интерактивных форм проведения занятий.

Основными образовательными технологиями при освоении дисциплины являются лекции и практические занятия. Данные виды образовательных технологий относятся к аудиторной работе.

При изучении дисциплины предусматривается использование интерактивных методов и технологий формирования компетенций:

– лекций с применением мультимедийных технологий (18 часов);

– использование на практических занятиях индивидуальной работы и в малых группах с обсуждением результатов экспериментов в форме групповых дискуссий (36 часов);

– тестирования, включающего вопросы по материалам лекций и результатам выполнения практических заданий.

В целях реализации индивидуального подхода к обучению аспирантов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы с аспирантами в том числе в электронной образовательной среде с использованием соответствующего программного оборудования,

дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций.

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

6.1. План самостоятельной работы аспирантов

6.1.1 План самостоятельной работы аспирантов очной формы обучения

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-2	Раздел 1. Методы и средства информационного противоборства	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	8
3-12	Раздел 2. Методы ЗИ, реализуемые специальными СЗИ	Подготовка к аудиторным занятиям, Подготовка к практическим занятиям, Подготовка к экзамену	Проверка тестов, Оценка выполнения практических заданий в форме тестирования	См. раздел 7 РПУД	60
3-4	Тема 2.1. Методы ЗИ, реализуемые СЗИ от НСД	Подготовка к аудиторным занятиям, Подготовка к практическим занятиям, Подготовка к экзамену	Проверка тестов, Оценка выполнения практических заданий в форме тестирования	См. раздел 7 РПУД	20
5-6	Тема 2.2. Методы ЗИ, реализуемые средствами защиты от вредоносного ПО	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	8
7-8	Тема 2.3. Методы ЗИ, реализуемые СЗИ, обеспечивающим и безопасное межсетевое	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	8

	взаимодействие				
9-10	Тема 2.4. Методы ЗИ, реализуемые средствами контроля и предотвращения утечек информации	Подготовка к аудиторным занятиям, Подготовка к практическим занятиям, Подготовка к экзамену	Проверка тестов, Оценка выполнения практических заданий в форме тестирования	См. раздел 7 РПУД	16
11-12	Тема 2.5. Методы и средства, применяемые для контроля и оценки эффективности функционирования СЗИ	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	8
13-16	Раздел 3. Защита информации в виртуальных инфраструктурах	Подготовка к аудиторным занятиям, Подготовка к практическим занятиям, Подготовка к экзамену	Проверка тестов, Оценка выполнения практических заданий в форме тестирования	См. раздел 7 РПУД	24
13-14	Тема 3.1. Технологии и платформы виртуализации	Подготовка к аудиторным занятиям, Подготовка к практическим занятиям, Подготовка к экзамену	Проверка тестов, Оценка выполнения практических заданий в форме тестирования	См. раздел 7 РПУД	16
15-16	Тема 3.2. Методы и средства ЗИ, применяемые для защиты ВИ	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	8
17-18	Раздел 4. Методы ЗИ, реализуемые в операционных системах	Подготовка к аудиторным занятиям, Подготовка к практическим	Проверка тестов, Оценка выполнения практических	См. раздел 7 РПУД	16

		занятиям, Подготовка к экзамену	заданий в форме тестирования		

6.1.2 План самостоятельной работы аспирантов заочной формы обучения

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
	Раздел 1. Методы и средства информационного противоборства	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	16
	Раздел 2. Методы ЗИ, реализуемые специальными СЗИ	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	80
	Тема 2.1. Методы ЗИ, реализуемые СЗИ от НСД	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	16
	Тема 2.2. Методы ЗИ, реализуемые средствами защиты от вредоносного ПО	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	16
	Тема 2.3. Методы ЗИ, реализуемые СЗИ, обеспечивающим и безопасное межсетевое взаимодействие	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	16
	Тема 2.4. Методы ЗИ, реализуемые средствами контроля и предотвращения утечек информации	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	16
	Тема 2.5. Методы и средства,	Подготовка к	Проверка	См. раздел 7	16

	применяемые для контроля и оценки эффективности функционирования СЗИ	аудиторным занятиям, Подготовка к экзамену	тестов	РПУД	
	Раздел 3. Защита информации в виртуальных инфраструктурах	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	23
	Раздел 4. Методы ЗИ, реализуемые в операционных системах	Подготовка к аудиторным занятиям, Подготовка к экзамену	Проверка тестов	См. раздел 7 РПУД	16

6.2. Методические указания по организации самостоятельной работы аспирантов

При изучении дисциплины «Методы и средства защиты информации в условиях информационного противоборства» самостоятельная работа аспирантов направлена на расширение лекционного материала. Основные положения каждого раздела представляются лектором в ходе аудиторных занятий. Подготовка к аудиторным занятиям проводится с целью более углубленного изучения материала, тщательной проработки материала, подготовки к контрольному тестированию, а также с целью изучения теоретического материала для подготовки к выполнению практических заданий. При подготовке к экзамену используется материал лекционных занятий, а также используется основная и дополнительная литература, материалы, размещенные на Интернет-ресурсах, приведенных в разделе 7.

Предусмотрены контрольные тесты после изучения материалов разделов и отдельных тем лекционного материала. Также предусмотрены контрольные точки (на 9-ой и 15-ой неделях обучения) с выставлением баллов.

При организации **самостоятельной работы** используются технология поиска и сбора новой информации (работа на компьютере с целью поиска информации в базах данных, работа с учебной, справочной и научной литературой с целью подготовки к аудиторным занятиям: разделы 1-4 и темы 2.1 – 3.2, а также при подготовке к экзамену).

6.3. Материалы для проведения текущего и промежуточного контроля знаний

6.3.1 Материалы для проведения текущего и промежуточного контроля знаний аспирантов очной формы обучения

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий (проверка тестов, оценка выполнения практических	Разделы 1-4	ОПК-1, ОПК-3, ПК-8

	заданий в форме тестирования)		
2	Промежуточный (экзамен)	Разделы 1-4	ОПК-1, ОПК-3, ПК-8

6.3.2 Материалы для проведения текущего и промежуточного контроля знаний аспирантов заочной формы обучения

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий (проверка тестов)	Разделы 1-4	ОПК-1, ОПК-3, ПК-8
2	Промежуточный (экзамен)	Разделы 1-4	ОПК-1, ОПК-3, ПК-8

Текущий (рейтинговый) контроль проводится с использованием контрольного тестирования периодически вовремя лекционный занятий и лабораторных работ в соответствии с расписанием. Контроль должен охватывать всех студентов. Студенты, не явившиеся на контрольное занятие, проходят текущий контроль во внеурочное время.

Результаты текущего контроля должны оцениваться лектором дифференцированно и учитываться при проведении рубежного рейтингового контроля (контрольных точек) и промежуточной аттестации студентов.

При контрольном тестировании используются один тип вопросов – с единственным правильным ответом из множества вариантов.

Пример тестового вопроса для текущего контроля:

Какой компонент обеспечивает взаимодействие защитных подсистем в СЗИ Secret Net?

а) База данных
б) Диспетчер доступа
в) Подсистема контроля входа
г) Подсистема аппаратного контроля
д) Подсистема управления
е) Ядро СЗИ Secret Net
ж) Подсистема функционального контроля
и) Подсистема регистрации

Промежуточный контроль по окончании пятого семестра проводится в виде экзамена. На экзамен выносится два теоретических вопроса и задание.

Вопросы и задания к экзамену.

1 Основные принципы создания средств защиты информации

2 Концепция построения программно–аппаратных средств обеспечения информационной безопасности

3 Методы ограничения доступа и управления доступом. Идентификация и аутентификация. Парольные системы

4 Методы ограничения доступа и управления доступом. Дискреционное управление доступом

5 Методы ограничения доступа и управления доступом. Мандатное управление доступом

8 Методы ограничения доступа и управления доступом. Ролевое управление доступом

9 Структура и функции программно–аппаратных средств обеспечения информационной безопасности

10 Назначение, режимы функционирования, основные функции, состав устанавливаемых компонентов СЗИ от НСД Secret Net

11 Назначение, режимы функционирования, основные функции, состав устанавливаемых компонентов СЗИ от НСД Страж NT

12 Назначение, режимы функционирования, основные функции, состав устанавливаемых компонентов СЗИ от НСД Аккорд

13 Жизненный цикл компьютерных вирусов

14 Основные методы и средства защиты от вредоносных программ

15 Основные модели взаимодействия РПВ и прикладных программ

16 Основные классы программных закладок

17 Требования к СЗИ, обеспечивающим безопасное межсетевое взаимодействие. Типовые функции

18 СЗИ, обеспечивающие безопасное межсетевое взаимодействие

19 Общая характеристика систем контроля и предотвращения утечек информации. Контролируемые каналы утечки информации

20 Типовые функциональные возможности. Поиск защищаемой информации в ИС. Контроль действий пользователей. Мониторинг и защита агентов. Реакция на инциденты. Режимы функционирования

21 Типовые функциональные возможности. Интеграция со сторонними сервисами и средствами. Обеспечение производительности и отказоустойчивости. Хранение, ретроспективный анализ и отчётность

22 Типовые функциональные возможности. Анализ информации при контроле каналов передачи. Применяемые технологии

23 Типовые функциональные возможности. Анализ информации при контроле каналов передачи. Лингвистический анализ

24 Типовые функциональные возможности. Анализ информации при контроле каналов передачи. Статистические методы

25 Системы контроля и предотвращения утечек информации. Типовая структура. Основные компоненты

26 Системы контроля и предотвращения утечек информации. Концепция применения. Основные стадии применения

27 Испытания защищенных систем в соответствии с ГОСТ 34.603.

28 Виды испытаний программных СЗИ. Документы, оформляемые при проведении испытаний: программа и методика испытаний, протоколы испытаний

29 Общий подход к оценке эффективности программных СЗИ. Классификация СЗИ АС по способам реализации. Основные защитные механизмы, которые подвергаются оценке

30 Общий подход к оценке эффективности программных СЗИ. Задачи контроля эффективности

31 Определение технологии виртуализации. Классификация виртуализации. Аппаратная виртуализация

32 Классификация виртуализации. Программная виртуализация.

33 Структура виртуальной инфраструктуры. Гипервизор. Виртуальная машина. Основная и гостевая ОС. Система хранения данных.

34 Объекты виртуальной инфраструктуры, на которые может осуществляться воздействие. Проблемы обеспечения безопасности. Угрозы безопасности виртуальной инфраструктуры.

35 Платформа виртуализации Hyper-V. Гипервизор Hyper-V. Реализация Hyper-V.

36 Платформа виртуализации VMware. Гипервизор VMware. Реализация VMware.

37 Механизмы безопасности, реализованные в платформах виртуализации Hyper-V и VMware.

38 Программно-аппаратные средства обеспечения безопасности виртуальных инфраструктур

39 Защитные механизмы ОС. Процедуры идентификации, аутентификации и авторизации.

40 Защитные механизмы ОС. Управление доступом.

Формулировка вопроса для проверки уровня обученности УМЕТЬ

1 Дать характеристику основных принципов создания средств защиты информации и их применения

2 Пояснить применение концепции диспетчера доступа

3 Дать сравнительную характеристику основных подходов к разработке средств защиты информации

4 Пояснить применение концепций распространения прав доступа и дать их сравнительную характеристику

5 Описать способ контроля потоков данных, посредством применения основного правила разграничения доступа, применяемого в мандатном механизме управления доступом

6 Описать применение ролевого способа управления доступом

7 Указать основные документы, определяющие требования к структуре и функциям СЗИ

8 Описать порядок функционирования компонентов СЗИ от НСД Secret Net

9 Описать порядок функционирования компонентов СЗИ от НСД Страж NT

10 Описать порядок функционирования компонентов СЗИ от НСД Аккорд

11 Определить программы с потенциально опасными воздействиями и вредоносные программы

12 Определить особенности функционирования программ с потенциально опасными воздействиями и вредоносных программ

13 Описать типовые функциональные возможности СЗИ, обеспечивающих безопасное межсетевое взаимодействие

14 Описать особенности применения СЗИ, обеспечивающих безопасное межсетевое взаимодействие

15 Выполнить сравнительный анализ статистического и лингвистического методов анализа информации

16 Определить типовую структуру СКиПУИ

17 Пояснить реализацию метода контентного анализа, основанного на анализе форматов файлов

18 Пояснить реализацию метода контентного анализа, основанного на анализе ключевых слов

19 Пояснить реализацию метода контентного анализа, основанного на анализе регулярных выражений

20 Пояснить реализацию метода контентного анализа, основанного на анализе свойств файлов и составных правил

21 Определить содержание документов, оформляемых при испытаниях – программа и методика испытаний, протокол испытаний

22 Сформулировать основные задачи контроля эффективности программных СЗИ

23 Описать применение средств проведения проверок программных СЗИ для оценки эффективности их функционирования

24 Описать типовые действия при контроля эффективности программных СЗИ

25 Дать сравнительную характеристику технологии аппаратной и программной виртуализации

26 Дать сравнительную характеристику типов гипервизоров. Преимущества и недостатки

27 Описать особенности применения гостевой и основной ОС при использовании виртуальных машин (ВМ)

28 Сравнительная характеристика технологий и протоколов, применяемых в системах хранения данных

29 Охарактеризовать основные проблемы обеспечения ИБ виртуальных инфраструктур

30 Охарактеризовать основные угрозы ИБ виртуальных инфраструктур (ВМ, гипервизора, СХД) и их реализацию

31 Описать функциональные возможности платформы виртуализации Hyper-V и реализуемые технологии

32 Описать функциональные возможности платформы виртуализации VMware и реализуемые технологии

33 Описать механизмы безопасности, реализованные в платформах виртуализации Hyper-V и VMware.

34 Описать применение программно-аппаратных средств обеспечения безопасности виртуальных инфраструктур

Формулировка задания/задачи для проверки уровня обученности ВЛАДЕТЬ

1 Управление подсистемой регистрации событий СЗИ от НСД Secret Net: настройка параметров подсистемы, формирование перечня событий для регистрации

2 Управление подсистемой регистрации событий СЗИ от НСД Secret Net: формирование отчета по журналам регистрации событий, использование фильтрации и сортировки при формировании отчета

3 Управление подсистемой контроля входа пользователей СЗИ от НСД Secret Net: создание учетных записей пользователей с установкой параметров учетных записей

4 Управление подсистемой контроля входа пользователей СЗИ от НСД Secret Net: настройка парольной подсистемы

5 Управление подсистемой контроля входа пользователей СЗИ от НСД Secret Net: настройка механизма блокировок

6 Управление привилегиями пользователей СЗИ от НСД Secret Net

7 Настройка подсистемы управления подключением устройств и контроля аппаратной конфигурации

8 Настройка дискреционного управления доступом СЗИ от НСД Secret Net: настройка списка контроля доступа к файлам и каталогам, настройка наследования атрибутов

9 Настройка мандатного управления доступом СЗИ от НСД Secret Net: настройка категорий конфиденциальности

10 Настройка мандатного управления доступом СЗИ от НСД Secret Net: настройка атрибутов безопасности пользователей и привилегий

11 Настройка мандатного управления доступом СЗИ от НСД Secret Net: настройка атрибутов файлов и каталогов, наследования атрибутов

12 Настройка мандатного управления доступом СЗИ от НСД Secret Net: настройка и применение механизма контроля потоков данных

13 Настройка механизма контроля целостности СЗИ от НСД Secret Net: создание заданий контроля целостности и настройка параметров задания

14 Настройка механизма замкнутой программной среды СЗИ от НСД Secret Net: создание заданий замкнутой программной среды и настройка параметров задания

15 Создание модели данных СЗИ от НСД Secret Net

16 Настройка механизма замкнутой программной среды СЗИ от НСД Secret Net: использование методов автоматизации при создании заданий замкнутой программной среды

17 Настройка механизма управления доступом к устройствам с использованием дискреционного управления доступом

18 Настройка механизма управления доступом к устройствам с использованием мандатного управления доступом и контроля потоков

19 Настройка механизма контроля печати: настройка политики принтеров для разрешения печати с использованием дискреционного управления доступом

20 Использование функциональных возможностей ОС Windows, применяемых при администрировании СЗИ от НСД Secret Net

21 Настройка управления программным комплексом DeviceLock

22 Настройка разрешений на доступ к устройствам

23 Создание контентно-зависимых правил проверки содержимого для протоколов с использованием контентных групп

24 Настройка аудита и теневого копирования. Формирование отчетов DeviceLock Enterprise Server по журналу аудита

25 Сравнительный анализ технологий виртуализации. Дать сравнительную характеристику технологий программной виртуализации.

26 Проанализировать основные угрозы ИБ виртуальных инфраструктур и возможности их реализации.

27 Управление сервером виртуализации ОС Windows, с использованием команд оболочки Windows PowerShell.

28 Применение механизмов безопасности оболочки Windows PowerShell при управлении сервером виртуализации ОС Windows.

7. Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1. Основная литература

1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.

2. Семь безопасных информационных технологий [Электронный ресурс] : учеб. / А.В. Барабанов [и др.]. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: https://e.lanbook.com/book/97352. — Загл. с экрана.

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2017. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0.

4. Расторгуев С.П. Математические модели в информационном противоборстве. Экзистенциальная математика. – Электрон. дан. — М.: АНО ЦСОиП, 2014. – 260 с. – Режим доступа: csef.ru/media/articles/5310/5310.pdf. – Загл. с экрана.

7.2. Дополнительная литература

1. Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем [Электронный ресурс]: Учебное пособие/ Щеглов А.Ю.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2014.— 95 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=68667

2. Прокушев Я.Е. Программно-аппаратные средства защиты информации [Электронный ресурс]: Учебное пособие/ Прокушев Я.Е.— Электрон. текстовые данные.— СПб.: Интермедия, 2017.— 160 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=66799

3. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим

доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.

4. Леандро, К. Windows Server 2012 Hyper-V. Книга рецептов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2013. — 302 с. — Режим доступа: https://e.lanbook.com/book/58692. — Загл. с экрана.

5. Яковлев В.В. Технологии виртуализации и консолидации информационных ресурсов [Электронный ресурс]: Учебное пособие/ Яковлев В.В.— Электрон. текстовые данные.— М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2015.— 156 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=45322.

6. Лапонина О.Р. Межсетевое экранирование [Электронный ресурс]: Учебное пособие/ Лапонина О.Р.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 344 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=67391

7. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032. — Загл. с экрана.

8. Савельев А.О. Решения Microsoft для виртуализации ИТ-инфраструктуры предприятий [Электронный ресурс]/ Савельев А.О.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 284 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=52175

9. Лэнгоун, Д. Виртуализация настольных компьютеров с помощью VMware View 5. Полное руководство по планированию и проектированию решений на базе VMware View 5 [Электронный ресурс] : рук. / Д. Лэнгоун, А. Лейбовичи. — Электрон. дан. — Москва : ДМК Пресс, 2013. — 280 с. — Режим доступа: https://e.lanbook.com/book/69946. — Загл. с экрана.

7.3. Интернет-ресурсы

1. www.cnews.ru – ресурс, содержащий материалы об информационных технологиях и обеспечении ИБ
2. www.servernews.ru – информационные материалы о средствах ИТ и средствах обеспечения ИБ
3. www.fstec.ru – сайт ФСТЭК РФ
4. www.infosec.ru – группа компаний Информзащита
5. www.anti-malware.ru – аналитический центр Anti-Malware.ru
6. http://dlp-expert.ru – сайт, посвященный DLP-системам (системам контроля и предотвращения утечек информации)
7. https://www.vmware.com/ru/
8. https://www.microsoft.com/ru-ru/server-cloud/solutions/virtualization.aspx Hyper-V
9. http://technet.microsoft.com/ru-ru/library/hh831531.aspx Hyper-V
10. https://www.citrix.ru/products/xenserver/overview.html
11. http://propagandahistory.ru/

8. Материально-техническое обеспечение дисциплины (модуля)

Для освоения данной дисциплины необходимы:

– мультимедийные средства обучения (ноутбук, экран и проектор), используемые при проведении лекционных занятий;

– ПЭВМ с установленным средством виртуализации Virtual Box, подготовленными виртуальными машинами с установленными СЗИ (СЗИ от НСД Secret Net, СКиПУИ SecureTower, программным комплексом DeviceLock DLP Suite, межсетевым экраном TrustAccess), виртуальными машинами с установленными ОС (Windows Server 2012 R2, Windows 8,1, AstraLinux).

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов (страниц)		
			заменен-ных	новых	аннулиро-ванных
2015-2016	переутверждена Пр-л №1 от 3.09.2015	обновлен раздел 7	21	–	–
2016-2017	переутверждена Пр-л ~~от 1 от~~ 8.09.2016	обновлен раздел 7	20, 21	–	–
2017-2018	переутверждена Пр-л №1 от 31.08.2017	обновлен раздел 7	20, 21	–	–