МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Игнатова И.Г.
«__» _____ 2015 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки – 09.03.03 «Прикладная информатика»
Профиль – «Системы корпоративного управления»

2015 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательных программ:

Компетенции ОП	Компетенции/подкомпетенции, формируемые в дисциплине
Направление - **09.03.03 «Прикладная информатика»** Профиль – **«Системы корпоративного управления»**	
Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением ИКТ и с учетом основных требований информационной безопасности (ОПК-4).	Способность защищать обрабатываемую информацию от несанкционированного доступа и программно-математического воздействия (ОПК-4.2).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в базовую часть Блока 3 «Дисциплины (модули)» образовательной программы. Дисциплина изучается с применением дистанционных технологий.

Изучение дисциплины «Информационная безопасность» базируется на дисциплинах образовательной подготовки (ОП) бакалавриата по направлению подготовки 09.03.03 «Прикладная информатика» и профилю подготовки «Системы корпоративного управления»: «Электротехника», «Электроника», «Вычислительные системы, сети и телекоммуникации», «Операционные системы», «Базы данных», «Информатика», «Информационные системы и технологии».

Знания и практические навыки, полученные в результате изучения дисциплины, используются в дисциплинах «Проектирование информационных систем», «Практикум по администрированию баз данных», «Программная инженерия», в ходе учебной, производственной практиках и при подготовке ВКР.

В результате изучения дисциплины студент должен:

Знать:

место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

цели, задачи и направления защиты информации;

угрозы безопасности информации автоматизированных информационных систем и объектов информатизации;

основные нормативные правовые акты в области информационной безопасности и защиты информации;

способы и средства обеспечения информационной безопасности и защиты информации в автоматизированных информационных системах (АИС);

классы защищенности средств вычислительной техники (СВТ) и АИС от несанкционированного доступа (НСД) к информации и требования к показателям защищенности СВТ и АИС различных классов;

основные современные криптографические методы защиты информации, технологии электронной цифровой подписи;

основы проектирования АИС в защищенном исполнении;

порядок подготовки и проведения аудита информационной безопасности информационных систем;

организацию аттестации объектов информатизации и порядок ее проведения.

Уметь:

выявлять актуальные угрозы безопасности информации в корпоративных информационных системах;

обосновывать организационные и технические мероприятия по защите информации в корпоративных информационных системах;

осуществлять выбор функциональной структуры системы обеспечения безопасности информации корпоративной информационной системы;

разрабатывать основные документы политики информационной безопасности.

Владеть навыками:

оценки угроз безопасности информации в корпоративных информационных системах;

подбора, изучения и обобщения научно-технической литературы и нормативно-методических документов по вопросам защиты информации от несанкционированного доступа.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы				Самостоятельная работа, часы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Лабораторные работы	Практические занятия		
3		4	144				-	108	Экз. (36 часов)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	**Контактная работа, часы**			**Самостоятельная работа, часы**	**Формы текущего контроля**
	Лекции	**Лабораторные работы**	**Практические занятия**		
1. Угрозы безопасности информации и основные направления защиты информации				10	Компьютерный тест РК 1.
2. Защита информации от несанкционированного доступа				64	Компьютерный тест РК 1. Зачет по Лр 1–6.
3. Защита информации от утечки по техническим каналам				8	Компьютерный тест РК 2.
4. Организация и управление информационной безопасностью				26	Компьютерный тест РК 2. Зачет по Лр 7–8.

4.1. Лекционные занятия

Не предусмотрены

4.2. Практические занятия

Не предусмотрены

4.3. Лабораторные занятия

Не предусмотрены

4.4. Самостоятельная работа студентов

1. Самостоятельное изучение теоретического материала

Номер модуля дисциплины	Краткое содержание
1	**Информация – как объект защиты** Определение информации. Виды информации. Сведения, составляющие государственную тайну. Конфиденциальная информация. Объекты защиты: объекты информатизации, выделенные помещения, информационно-телекоммуникационные системы.
	Угрозы безопасности информации и задачи защиты информации Информационная безопасность предприятия (учреждения, объекта). Свойства информации: конфиденциальность, доступность, целостность. Безопасность информации (определение). Угрозы безопасности информации: утечка информации, неправомерное модификация (искажение, подмена), уничтожение информации, неправомерное блокирование доступа к ней. Виды утечки информации: разглашение сведений, хищение носителя информации, несанкционированный доступ к информации, перехват информации техническими средствами (утечка информации по техническим каналам). Источники угроз безопасности информации.
	Основные направления и задачи защиты информации Правовая защита информации. Техническая защита информации. Криптографическая защита информации. Физическая защита объектов информатизации. Основные задачи защиты информации. Государственная система защиты информации. Уголовная и административная ответственность за разглашение сведений ограниченного доступа и неправомерный доступ к информации.
2	
	Несанкционированный доступ к информации, обрабатываемой АС и СВТ Несанкционированный доступ к информации (НСД), обрабатываемой АС и СВТ. Классификация и характеристика способов НСД: физический; программно-аппаратный; программный. Модель нарушителя.
	Угрозы НСД к информации в АС с применением программных и программно-аппаратных средств Общая характеристика угроз НСД к информации в АС с применением программных и программно-аппаратных средств. Характеристика уязвимостей системного и прикладного программного обеспечения. Характеристика угроз безопасности информации, реализуемых с использованием протоколов межсетевого взаимодействия. Характеристика угроз программно-математических воздействий. Характеристика нетрадиционных информационных каналов.

Номер модуля дисциплины	Краткое содержание
	Способы защиты информации от НСД Защита информации от НСД. Защита информации от несанкционированного и непреднамеренного воздействия. Классификация способов защиты от НСД: физическая защита СВТ и носителей информации; идентификация и аутентификация пользователей и используемых компонентов обработки информации; разграничение доступа к информационным ресурсам; криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных); регистрация всех обращений к защищаемой информации. Способы идентификации и аутентификации: с использованием пароля; по биометрическим характеристикам человека (отпечатки пальцев, геометрия руки, голос, персональная роспись, структура сетчатки глаза, фотография и т.д.); по специальным устройствам (жетонам, картам, электронным ключам, кодовым устройствам и т.д.). Способы разграничения доступа: по уровням (кольцам) секретности; по специальным спискам; по так называемым матрицам полномочий; по специальным мандатам и т.д. Регистрация обращений к объектам доступа. DLP - системы.
	Защита информации от программно-математического воздействия Понятие вредоносного кода. Типы вредоносных программ. Способы проникновения вирусов на компьютер. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки. Классификация антивирусов. Антивирусная защита ПЭВМ. Антивирусная защита информационной системы и компьютерной сети.
	Криптографическая защита информации Основные понятия и определения в области криптографии. Основные современные криптографические методы защиты информации. Симметричные криптосистемы шифрования (ГОСТ 28147-89, DES т.п.). Асимметричные криптосистемы шифрования. Построение и использование хэш-функций. Технологии электронной цифровой подписи. Технологии распределения ключевой информации. Основы инфраструктуры открытых ключей (PKI). Жизненный цикл ключей и сертификатов. Модели доверия PKI.
	Основные требования по защите СВТ от НСД информации Показатели защищенности СВТ от несанкционированного доступа к информации. Требования к СВТ различных классов защищенности. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей (НДВ).

Номер модуля дисциплины	Краткое содержание
	Основные требования по защите АС от НСД к информации Классы защищенности АС от НСД к информации. Состав системы защиты информации от НСД (СЗИ НСД). Показатели классификации защищенности АС от НСД к информации. Требования к СЗИ НСД АС различных классов защищенности. Показатели защищенности межсетевых экранов от несанкционированного доступа к информации. Требования к межсетевым экранам различных классов защищенности.
3	
	Защита информации, обрабатываемой СВТ, от утечки по техническим каналам Классификация и характеристика технических каналов утечки информации, обрабатываемой СВТ. Способы и средства защиты объектов СВТ от утечки информации по техническим каналам.
	Защита выделенных помещений от утечки речевой информации по техническим каналам Классификация и характеристика технических каналов утечки речевой информации из выделенных помещений. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам.
4	
	Управление информационной безопасностью Организация управления информационной безопасностью. Политика информационной безопасности. Общие мероприятия по управлению информационной безопасностью.
	Документы по обеспечению информационной безопасности на объектах информатизации Документы политики информационной безопасности (модель угроз безопасности информации, концепция обеспечения безопасности информации, регламенты обеспечения безопасности информации, инструкции и другие организационно-распорядительные документы по вопросам обеспечения безопасности информации).
	Основы проектирования автоматизированных систем в защищенном исполнении Общие положения о порядке создания автоматизированных систем в защищенном исполнении. Общие и функциональные требования к автоматизированным системам в защищенном исполнении. Типовое содержание работ по защите информации на стадиях создания автоматизированных систем в защищенном исполнении. Особенности испытаний и применения автоматизированной системы в защищенном исполнении.

Номер модуля дисциплины	Краткое содержание
	Аудит информационной безопасности и аттестация объектов информатизации Аудит информационной безопасности. Виды аудита ИБ. Внешний аудит. Внутренний аудит. Цели и методы аудита. Порядок организации и проведения аудита ИБ. Аттестация объекта информатизации. Организация аттестации объектов информатизации. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Заключение аттестационной проверки объекта информатизации. Аттестат соответствия.

2. Дополнительные виды самостоятельной работы

Номер модуля дисциплины	Вид СРС
1-4	Изучение рекомендованной литературы.
1-2	**Подготовка в рубежному контролю РК 1:** Изучение материалов разделов №№ 1-10 и рекомендованной литературы.
3-4	**Подготовка в рубежному контролю РК 2:** Изучение материалов разделов №№ 11-16 и рекомендованной литературы.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, http://orioks.miet.ru/):

Материалы для изучения теории в рамках подготовки к лабораторным работам размещены в ОРИОКС: текст основных теоретических сведений, задания для СРС и критерии их оценивания, рекомендуемая литература в файле: «Методические указания для студентов по изучению дисциплины «Информационная безопасность».

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Основная литература

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: учеб. пособие для студентов вузов. Под ред. Зайцева

А.П. и Шелупанова А.А..– М.: Лань, 2012. – 616 с. (Гриф УМО по ИБ) . Электронный ресурс. Режим доступа - http://e.lanbook.com/books/element.php?pl1_id=5155.

2. Хорев, А.А. Техническая защита информации: учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А. А. Хорев. - М. : НПЦ "Аналитика", 2008. - 436 с. - 3000 экз. - ISBN 978-59901488-1-9 : 153-00
3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: [Учеб. пособие] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2012. - 592 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-94074-637-9.
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Текст] : [учеб. пособие] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2014. - 702 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-94074-768-0. 004.056(075.8) - Ш-228

Дополнительная литература

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с. - ISBN 5-93517-292-5. Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 5-93517-292-5.
2. Галатенко В.А. Стандарты информационной безопасности [Текст] : Курс лекций: Учеб. пособие / В. А. Галатенко ; Под ред. В.Б. Бетелина. - 2-е изд. - М. : Интернет-Университет Информационных технологий, 2012. - 264 с. - 2000 экз. - ISBN 978-5-9556-0053-6 : 262-51; 262-50.
3. Гришина Н.В. Комплексная система защиты информации на предприятии: учеб. пособие.- М.: Форум, 2011. - 240 с.
4. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учеб. пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с. - Доступ к электронной версии книги открыт на сайте http://e.lanbook.com/. - ISBN 978-5-9912-0147-6.
5. Мельников Д.А. Информационная безопасность открытых систем [Текст] : Учебник/ Д. А. Мельников. - М. : Флинта: Наука, 2013. - 448 с. - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7. 004.056(075.8) - М-482
6. Программно-аппаратная защита информации: учеб. пособие / П.Б. Хорев.- М.:Форум, 2012. – 352 с.

Периодические издания

1. Журнал «Специальная техника» (ВАК). Сайт журнала – http://ess.ru/index.htm;
2. Журнал «Специальная техника и связь» (ВАК). Сайт журнала – http://www.st-s.su/index.htm;
3. Журнал «Защита информации. Инсайд»; Сайт журнала – http://www.inside-zi.ru/
4. Журнал «Безопасность информационных технологий». Сайт журнала – сайт журнала http://www.pvti.ru/articles_14.htm.
5. Информационный бюллетень "Jet Info". Издатель: компания «Инфосистемы Джет». Сайт журнала – www.jetinfo.ru.
6. Бюро научно-технической информации «Техника для спецслужб». – http://www.bnti.ru/about.asp.
7. Журнал «Системы и сети». – http://systemseti.com/
8. Журнал «Information Security/Информационная безопасность». Издатель: компания «Гротек». – http://www.itsec.ru

7. ПЕРЕЧЕНЬ РЕСУРСОВ СЕТИ «ИНТЕРНЕТ»

1. ЭБС издательства Лань – http://e.lanbook.com/.
2. Научная электронная библиотека eLIBRARY.ru – http://elibrary.ru/.
3. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.
4. Раздел «Документы» сайта Федеральной службы по техническому и экспортному контролю (ФСТЭК России). - http://www.fstec.ru.

8. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1. Программное обеспечение, используемое для самостоятельной работы:
2. операционная система Microsoft Windows Server 7;
3. пакет офисных приложений Microsoft Office Std 2013 RUS OLP NL;
4. Корпоративная информационно-технологическая платформа ОРИОКС.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Освоение дисциплины предполагает наличие у студента компьютера с установленным программным обеспечением для просмотра образовательных ресурсов и подключенного к сети Интернет.

10. АКТИВНЫЕ И ИНТЕРАКТИВНЫЕ ФОРМЫ ПРОВЕДЕНИЯ ЗАНЯТИЙ

При обучении по дисциплине используются следующие интерактивные формы проведения занятий:

- ИФ1: обсуждение и разрешение сложных и дискуссионных вопросов и проблем: разбор конкретных ситуаций
- ИФ2: электронное тестирование
- ИФ3: интерактивное взаимодействие с преподавателем при выполнении домашних заданий через интернет-среду

№ п\п	Тип занятия или внеаудиторной работы	Вид и тематика (название) интерактивного занятия
1.	Самостоятельная работа	• ИФ1: обсуждение и разрешение сложных и дискуссионных вопросов и проблем: разбор конкретных ситуаций • ИФ2: электронное тестирование • ИФ3: интерактивное взаимодействие с преподавателем при выполнении домашних заданий через интернет-среду

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

№ п/п	Тип ФОС*	Код компетенции/ подкомпетенции	Перечень элементов ФОС
Направление - **09.03.03 «Прикладная информатика»** Профиль – **«Системы корпоративного управления»**			
1.	ФОС по подкомпетенции	Способность защищать обрабатываемую информацию от НСД к ней и программно-математического воздействия (ОПК-4.2).	Комплексное задание
2.	ФОС по элементам подкомпетенции	Способность защищать обрабатываемую информацию от НСД к ней и программно-математического воздействия (ОПК-4.2).	***Для оценки теоретического уровня*** Компьютерный тест (РК 1). Компьютерный тест (РК 2). Экзамен ***Для оценки практического уровня*** Комплексное задание

* *ФОС по компетенции; ФОС по подкомпетенции; ФОС по элементам компетенции*

Компетенция считается сформированной (базовый уровень), если по всем элементам ФОС студент получил положительные оценки.

12. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

12.1. Особенности организации процесса обучения

Особенность обучения по дистанционной технологии заключается в самостоятельном освоении дисциплины. В соответствии с графиком обучения, выданным перед началом обучения и имеющимся в ОРИОКС, выполняйте все учебные мероприятия.

В процессе изучения курса преподавателем проводятся ***консультационные занятия***. На консультациях студентам даются пояснения по трудноусваиваемым разделам дисциплины. Задать вопрос преподавателю можно по электронной почте или по Skype.

12.2. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется бальная накопительная система.

Структура и график контрольных мероприятий

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
10	Компьютерный тест (РК-1)	10	5
16	Компьютерный тест (РК-2)	10	5
12	***Комплексное задание №1***	***20***	***10***
16	***Комплексное задание №2***	***20***	***10***
17	***Экзамен***	***40***	***20***
	Накопленный рейтинг	**100**	**50**

Мониторинг успеваемости студентов проводится в течение семестра трижды: по итогам 1-8 учебных недель (9 неделя), 9 – 12 учебных недель (12 неделя), 13 – 16 (17-я неделя зачетная).

Текущая аттестация по дисциплине (итоговый контроль) осуществляется в виде **экзамена**.

Экзамен проводится строго по расписанию в специально отведенной для этого аудитории. На подготовку ответов на вопросы экзаменационных билетов студентам отводится не менее 30 минут.

Ответы экзаменующегося заслушиваются одним из экзаменаторов, который

выставляет оценку по каждому вопросу экзаменационного билета. При необходимости экзаменатор может задавать дополнительные и наводящие вопросы по тематике экзаменационного билета.

Общими критериями, определяющими оценку знаний по вопросу являются:

а) «отлично» (20 баллов) - наличие глубоких исчерпывающих знаний в объеме пройденного курса в соответствии с поставленными программой курса целями обучения, правильные уверенные действия по применению полученных знаний на практике, правильное и логически стройное изложение материала при ответе, наличие знаний по дополнительно рекомендованной литературы.

б) «хорошо» (15 баллов) - наличие твердых и достаточно полных знаний в объеме пройденного курса, незначительные ошибки при освещении заданных вопросов, правильные действия по применению знаний на практике, четкое изложение материала.

в) «удовлетворительно» (10 баллов) - наличие твердых знаний, изложение ответов с ошибками, уверенно исправляемых после дополнительных вопросов, правильные действия по применению знаний на практике.

г) «неудовлетворительно» (0 баллов) - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Считается, что студент успешно сдал экзамен, если он набрал за ответы на два вопроса не менее 20 баллов.

Максимальная сумма баллов итогового контроля составляет $R_{итог.max} = 40$ баллов.

Накопленный рейтинг $R_{нак}$ по дисциплине состоит из сумм рейтингов семестрового $R_{сем}$ и итогового контроля $R_{итог}$

$$R_{нак} = R_{сем} + R_{итог},$$

и является ***интегральным*** показателем, формируемым на основе достижений студента в ***течение обучения (семестровый период)*** и по итогам ***зачетно-экзаменационных испытаний.***

В экзаменационно-зачетную балльно-рейтинговую ведомость и зачетную книжку вносится не экзаменационная оценка по дисциплине, а ***итоговая 5-балльная оценка*** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учебной дисциплины.

Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	Оценка
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в экзаменационную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в экзаменационную ведомость.

Примерный перечень вопросов для экзамена:

Модуль 1:

1. Информация – как объект защиты. Определение информации. Виды информации.
2. Сведения, составляющие государственную тайну.
3. Конфиденциальная информация.
4. Объекты защиты: объекты информатизации, выделенные помещения, информационно-телекоммуникационные системы.
5. Угрозы безопасности информации и задачи защиты информации
6. Свойства информации: конфиденциальность, доступность, целостность. Безопасность информации (определение).
7. Угрозы безопасности информации: утечка информации, неправомерное модификация (искажение, подмена), уничтожение информации, неправомерное блокирование доступа к ней.
8. Виды утечки информации: разглашение сведений, хищение носителя информации, несанкционированный доступ к информации, перехват информации техническими средствами (утечка информации по техническим каналам).
9. Источники угроз безопасности информации.
10. Основные направления и задачи защиты информации: Правовая защита информации. Техническая защита информации. Криптографическая защита информации. Физическая защита объектов информатизации. Основные задачи защиты информации.
11. Государственная система защиты информации.
12. Уголовная и административная ответственность за разглашение сведений ограниченного доступа и неправомерный доступ к информации.
13. Органы системы лицензирования деятельности в области защиты информации.
14. Органы системы сертификации средств защиты информации.

15. Органы системы аттестации объектов защиты по требованиям безопасности информации.

Модуль 2:

1. Несанкционированный доступ к информации (НСД), обрабатываемой АС и СВТ.
2. Классификация и характеристика способов НСД: физический; программно-аппаратный; программный.
3. Модель нарушителя.
4. Угрозы НСД к информации в АС с применением программных и программно-аппаратных средств
5. Общая характеристика угроз НСД к информации в АС с применением программных и программно-аппаратных средств.
6. Характеристика уязвимостей системного и прикладного программного обеспечения.
7. Характеристика угроз безопасности информации, реализуемых с использованием протоколов межсетевого взаимодействия.
8. Характеристика угроз программно-математических воздействий.
9. Характеристика нетрадиционных информационных каналов.
10. Защита информации от НСД.
11. Защита информации от несанкционированного и непреднамеренного воздействия.
12. Классификация способов защиты от НСД: физическая защита СВТ и носителей информации; идентификация и аутентификация пользователей и используемых компонентов обработки информации; разграничение доступа к информационным ресурсам; криптографическое закрытие защищаемой информации, хранимой на носителях (архивация данных); регистрация всех обращений к защищаемой информации.
13. Способы идентификации и аутентификации: с использованием пароля; по биометрическим характеристикам человека (отпечатки пальцев, геометрия руки, голос, персональная роспись, структура сетчатки глаза, фотография и т.д.); по специальным устройствам (жетонам, картам, электронным ключам, кодовым устройствам и т.д.).
14. Способы разграничения доступа: по уровням (кольцам) секретности; по специальным спискам; по так называемым матрицам полномочий; по специальным мандатам.
15. Регистрация обращений к объектам доступа.
16. DLP – системы: назначение, состав и возможности по защите корпоративных информационных систем.

17. Понятие вредоносного кода. Типы вредоносных программ. Способы проникновения вирусов на компьютер. Признаки присутствия на компьютере вредоносных программ.

18. Методы защиты от вредоносных программ: сигнатурное и эвристическое сканирование, контроль целостности, мониторинг информационных потоков, изолированная программная среда, программные ловушки.

19. Классификация антивирусов. Антивирусная защита ПЭВМ. Антивирусная защита информационной системы и компьютерной сети.

20. Криптографическая защита информации. Основные понятия и определения в области криптографии.

21. Основные современные криптографические методы защиты информации. Симметричные криптосистемы шифрования (ГОСТ 28147-89, DES т.п.). Асимметричные криптосистемы шифрования.

22. Построение и использование хэш-функций.

23. Технологии электронной цифровой подписи.

24. Технологии распределения ключевой информации. Основы инфраструктуры открытых ключей (PKI). Жизненный цикл ключей и сертификатов. Модели доверия PKI.

25. Показатели защищенности СВТ от несанкционированного доступа к информации. Требования к СВТ различных классов защищенности.

26. Показатели защищенности автоматизированных систем, структура нормативного документа, классификация предмета требований, возможности использования автоматизированных систем различных классов для обработки сведений разной степени секретности.

27. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия недекларированных возможностей (НДВ).

28. Классы защищенности АС от НСД к информации. Состав системы защиты информации от НСД (СЗИ НСД).

29. Показатели классификации защищенности АС от НСД к информации. Требования к СЗИ НСД АС различных классов защищенности.

30. Показатели защищенности межсетевых экранов от несанкционированного доступа к информации. Требования к межсетевым экранам различных классов защищенности.

Модуль 3:

1. Объект информатизации (определение). Основные технические средства и системы (ОТСС, ТСПИ). Вспомогательные технические средства и системы (ВТСС).
2. Технический канал утечки информации (определение). Схема технического канала утечки информации
3. Классификация технических каналов утечки информации, обрабатываемых техническими средствами вычислительной техники (СВТ).
4. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений (электромагнитный ТКУИ).
5. Схема технического канала утечки информации, возникающего за счет наводок побочных электромагнитных излучений (электрический ТКУИ).
6. Классификация технических каналов утечки речевой информации и способов перехвата речевой информации.
7. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.
8. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.
9. Порядок специальной проверки выделенного помещения обследование выделенного помещения.

Модуль 4:

1. Политика информационной безопасности. Общие мероприятия по управлению информационной безопасностью.
2. Документы политики информационной безопасности (модель угроз безопасности информации, концепция обеспечения безопасности информации, регламенты обеспечения безопасности информации, инструкции и другие организационно-распорядительные документы по вопросам обеспечения безопасности информации).
3. Общие и функциональные требования к автоматизированным системам в защищенном исполнении.
4. Типовое содержание работ по защите информации на стадиях создания автоматизированных систем в защищенном исполнении.
5. Особенности испытаний и применения автоматизированной системы в защищенном исполнении.
6. Аудит информационной безопасности. Виды аудита ИБ.
7. Внешний аудит. Внутренний аудит ИБ.
8. Цели и методы аудита ИБ.

9. Порядок организации и проведения аудита ИБ.

10. Инструментальные средства аудита ИБ.

11. Аттестация объекта информатизации. Организация аттестации объектов информатизации.

12. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Заключение аттестационной проверки объекта информатизации. Аттестат соответствия.

Разработчик:

Доцент кафедры КИТиС
кандидат технических наук _____ / Соколова Н.Ю. /

Рабочая программа разработана на кафедре КИТиС
и утверждена на заседании кафедры «19» мая 2015 года, протокол № 9.

Заведующий кафедрой КИТиС
доктор технических наук, профессор _____ / Игнатова И.Г. /

Лист согласования

Рабочая программа согласована с УООП

Начальник УООП _____ /Никулина И.М./

ЛИСТ ИЗМЕНЕНИЙ, ВНОСИМЫХ В РАБОЧУЮ ПРОГРАММУ

№ п/п	Дата внесения изменения	Номер пункта	Суть изменения	Зав. кафедрой