Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.04 «ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: магистратура
Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Воронов А.Н. Рабочая программа дисциплины (модуля): Защищенные информационные системы. – Королев МО: «Технологический Университет», 2023.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н к.в.н., доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№5 от 11.04.2023г.			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, использовании организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующих создание и использование средств защиты информации, получение навыков в применении технологий обеспечения информационной безопасности объектов регионального уровня, а также в процессе управления информационной безопасностью защищаемых объектов.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Универсальные компетенции:

- УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Общепрофессиональные компетенции:

- ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

Основными задачами дисциплины являются:

1. ознакомление студентов с процессами анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества, разработка планов и программ проведения научных исследований и технических проектов, подготовка отдельных заданий для исполнителей и выполнение научных исследований по выбранной теме;
2. формирование у студентов способности самостоятельно организовывать работу коллектива исполнителей, принятию управленческих решений в условиях спектра мнений, определению порядка выполнения работ;
3. участие в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности, разработке проектов методических и нормативных документов, предложений и мероприятий по реализации разработанных проектов и программ;
4. формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.

- ОПК-1.3. Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении.

Необходимые умения:

- УК-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов.

- ОПК-1.2. Проектирует системы и подсистемы ИБ с учетом современных безопасных инструментальных технологий.

Необходимые знания:

- УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации.

- ОПК-1.1. Формирует актуальные модели угроз и нарушителей для современных информационных систем, учитывает их содержание при формировании требований технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина относится к обязательной части блока Б1. дсциплины (модули) основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01. «Информационная безопасность».

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах: “Основы информационной безопасности”, “Основы исследований информационной безопасности “.

Знания и компетенции, полученные при освоении дисциплины, «Защищенные информационные системы» являются базовыми при изучении следующих дисциплин: “Управление информационной безопасностью“, “Информационно-аналитические системы безопасности“, “Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем“ . прохождения практики (НИР),

государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

3.Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица 1

Виды занятий	**Всего часов**	**Семестр 1**	**Семестр …**	**Семестр …**	**Семестр …**
Общая трудоемкость	**108**	**108**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**54**	**54**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	16	16			
Другие виды контактной работы	**2**	**2**			
Практическая подготовка	**6**	**6**			
Самостоятельная работа	**52**	**52**			
Курсовые работы (проекты) *					
*Расчетно-графические работы**					
Контрольная работа *					
Текущий контроль знаний *	**Тест**	**Тест**			
Вид итогового контроля	**Экзамен**	**Экзамен**			

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Очное отделение				Практическая подго-товка	Код компетенций
	Лекции, час.	Практ. занятия, час	Лаборат. занятия, час.	Занятия в интер-активной форме		
1	2	3	4	5	6	7
Тема 1. Информационные технологии региона как объект информационной безопасности.	3	3	3	1	1	УК-1 ОПК-1-
Тема 2. Нормативно-правовые основы защиты информационных технологий региона	2	2	2	1	1	УК-1 ОПК-1
Тема 3. Защищённые информационные технологии в государственном и муниципальном управлении.	3	3	2	2	1	УК-1 ОПК- 1
Тема 4. Защищённые информационные технологии в управлении коммерческими структурами регио-на.	4	4	4	2	1	УК-1 ОПК-1
Тема 5. Организационно-технические методы защты информационных технологий региона.	4	4	4	2	2	УК-1 ОПК- 1
Итого:	**16**	**16**	**16**	**8**	**6**	

4.2. Содержание тем дисциплин

Тема 1. **Информационные технологии региона как объект информационной безопасности.**

Стратегический менеджмент, как система поведения предприятия на длительный период времени. Специфика информационного взаимодействия функциональных задач стратегического менеджмента. Информационные технологии стратегического менеджмента на предприятии. Реализация задач стратегического менеджмента с использованием специализированных компьютерных систем экономического и финансового моделирования. Информационные технологии решения задач финансового менеджмента и их основные процедуры. Основные принципы построения информационных систем управления персоналом в условиях корпоративных организаций.

Информационные технологии по использованию трудовых ресурсов и рабочего времени в корпоративных организациях.

Тема 2. Нормативно-правовые основы защиты информационных технологий региона.

Реализация теоретических и организационных принципов создания и функционирования информационных технологий в органах государственного и регионального управления. Информационно-вычислительные и ситуационные центры, их роль в государственном и региональном управлении. Особенности организации информационных технологий в муниципальном управлении. Информационное и технологическое обеспечение решения функциональных задач муниципального управления. Организация государственных информационных ресурсов России.

Тема 3. Защищённые информационные технологии в государственном и муниципальном управлении.

Необходимость обеспечения безопасности информационных технологий. Виды угроз безопасности информационных технологий и их характеристика. Формы атак на объекты информационных систем региона. Основные методы и средства защиты информации. Оценка безопасности информационных технологий, анализ угроз и каналов утечки информации. Анализ рисков и управление ими при использовании защищённых информационных технологий. Характеристика основных методов и средств построения систем информационной безопасности региона. Особенности защиты информации в корпоративных сетях.

Тема 4. Защищённые информационные технологии в управлении коммерческими структурами региона.

Организационные способы противодействия телефонному пиратству. Ограничение доступа к телефонным линиям связи. Основные рекомендации абонентам в случае обнаружения самовольного подключения. Характеристика современных пассивных устройств технического противодействия телефонному пиратству. Специализированные анализаторы телефонных линий связи. Краткий обзор зарубежных приборов для контроля состояния телефонных линий. Особенности активных устройств технического противодействия телефонному пиратству. Критерии оценки систем закрытия речи. Основные тенденции развития систем закрытия речи. Характеристика современных методов противодействия утечке компьютерной и аудиовидеоинформации.

Тема 5. Организационно-технические методы защиты информационных технологий региона.

Компьютерная безопасность региона. Решение задач безопасности речевой связи с помощью компьютерных информационных технологий. Представление речевых сигналов в виде графических образов. Компьютерные технологии безопасности связи на основе цифровой обработки изображений сонограмм. Технологии обеспечения безопасности на основе индивидуальных особенностей человека. Характеристика современных методов биометрической идентификации личности. Стеганографическая защита информации цифровыми водяными знаками. Характеристика современных систем цифровых водяных знаков. Обзор основных атак на системы цифровых водяных знаков.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю).

«Методические указания для обучающихся по освоению дисциплины (модуля)» представлены в Приложении 2 к настоящей РП.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине (модулю) «Теоретические основы компьютерной безопасности» приведена в Приложении 1 к настоящей РП.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1.Гагарина Л.Г., Федоров А.Р., Федоров П.А. Введение в архитектуру программного обеспечения: Учебное пособие - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 320 с. ISBN 978-5-8199-0649-1. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=542665

2.Астапчук В.А., Терещенко П.В. Архитектура корпоративных информационных систем – Новосиб.: НГТУ, 2015. - 75 с.: ISBN 978-5-7782-2698-2. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=546624

Дополнительная литература:

3.Царев Р.Ю., Прокопенко А.В., Князьков А.Н. Программные и аппаратные средства информатики - Краснояр.: СФУ, 2015. - 160 с. ISBN 978-5-7638-3187-0 / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=550017

4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. **http://www.gov.ru** - сервер органов государственной власти Российской Федерации.

2. **http://www.minfin.ru** - официальный сайт Министерства финансов Российской Федерации.
3. http://www.biblioclub.ru
4. http://znanium.com

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**
  1.Электронные ресурсы образовательной среды Университета.
  2. Информационно-справочные системы (Консультант+; Гарант).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7; программы эмуляции виртуальных машин (VM-vare, VM-box или др.); операционная система MS Windows Server 2003 или др. сетевая ОС.
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Лабораторные работы:

- компьютерная аудитория, оснащенная программно-аппаратными средствами защиты информации и аудита компьютерной безопасности, а также оснащенная специализированным оборудованием и контрольно-измерительной аппаратурой.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах академии с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.
Задания.

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

1. Изучить теоретическую часть Задания №1.
2. Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

3. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех

в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токо-

ведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб системы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

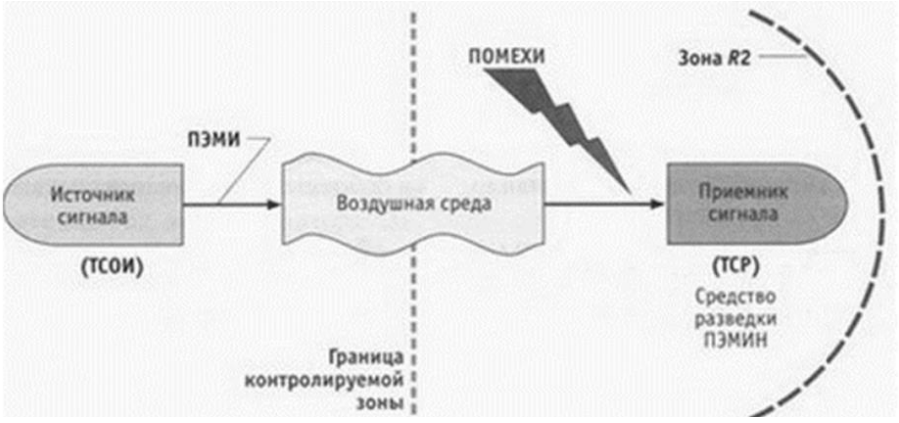

Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

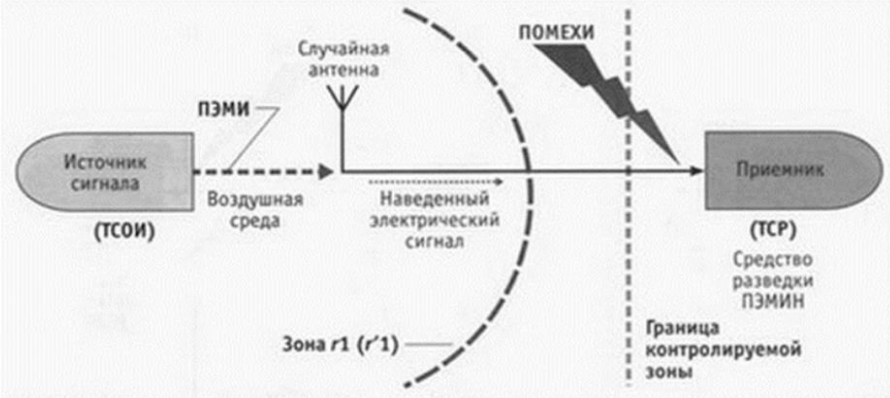

Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;
- зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;
- зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы

источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

1) Дайте определение специальным исследованиям в рамках данного учебного занятия.
2) Какие и сколько существует грифов секретности в рамках законодательства РФ?
3) Что такое зона r1(r’1) в ТЗИ?
4) Дайте определение ОТСС и ВТСС и в чем их различие?
5) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

1) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
2) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что бу-

дет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

4. Изучить теоретическую часть Задания №2.
5. Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

6. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной

частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до 4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	H-30	10 Гц – 30 МГц
Антенна электрическая дипольная	E-3000	30 МГц – 3000

активная		МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП преду-

сматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

1) Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.
2) Дайте определение измерительной площадки в рамках данного задания.
3) Сколько существует видов измерительных площадок (ИП) и в чем их различие?
4) На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?
5) Какой должен быть коэффициент калибровки у антенн?

Практические задания:

1) Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.

2) Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мнению, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции,, обучающийся должен:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-1 ОПК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	Тема 1. Информационные технологии (системы) региона как объект информационной безопасности. Тема 2. Нормативно-правовые основы защиты информационных технологий (систем) региона. Тема 3. Защищённые информационные технологии в государственном и муниципальном управлении.	УК-1.3 Использует методы системного и критического анализа, анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними. ОПК-1.3. Использует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности при формировании требований технического задания на создание автоматизированных систем в за-	- УК-1.2. Определяет уязвимости и угрозы информационной безопасности, необходимые для выявления и решения проблемной ситуации, планирует мероприятия и процессы по их устранению на основе системного и междисциплинарных подходов. - ОПК-1.2. Проектирует системы и подсистемы ИБ с учетом современных безопасных инструментальных технологий.	- УК-1.1. Ставит цель, определяет способы ее достижения, разрабатывает стратегию действия, принимает конкретные решения для ее реализации с учетом требований регуляторов в области защиты информации. ОПК-1.1. Формирует актуальные модели угроз и нарушителей для современных информационных систем, учитывает их содержание при формировании требований

				щищенном исполнении.		технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности.

Код компетенции	***Инструменты, оценивающие сформированность компетенции***	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-1 ОПК-1	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно.*** ***Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
УК-1 ОПК-1	Доклад	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сфор-***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин.

		мирована: • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
УК-1 ОПК-1	Письменное задание	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	1. Проводится в форме письменной работы 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа заявленной тематике (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
УК-1	Контрольная работа	***А) полностью***	1. Проводится устно в фор-

ОПК-1		***сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	ме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.
УК-1 ОПК-1	***Лабораторная работа***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	***1. Оформление в соответствии с требованиями (1 балл).*** ***2. Выбор методов измерений и вычислений (1 балл).*** ***3. Умение применять выбранные методы (1 балл).*** ***4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла).*** ***Максимальная оценка – 5 баллов.***

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Активные способы противодействия прослушиванию помещений по абонентским линиям связи.
2. Характеристика основных способов защиты абонентских телефонных линий связи от бесконтактного съёма информации.
3. Характеристика способов съёма акустической информации со стен и потолочных перекрытий охраняемых муниципальных объектов.
4. Характеристика способов съёма акустической информации с металлических труб и оконных стёкол охраняемых муниципальных объектов.
5. Характеристика способов съёма акустической информации в помещении по линии электросети охраняемых муниципальных объектов.
6. Характеристика пассивных способов противодействия прослушивания охраняемых помещений по абонентской линии связи.
7. Методика применения телефонолокационного способа съёма акустических сигналов в муниципальных защищаемых помещениях.

Примерная тематика реферата:

1. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях.
2. Основные компоненты охранной сигнализации при использовании различных датчиков.
3. Характеристика современных телевизионных средств охранной сигнализации.
4. Характеристика сетевых пассивных помехоподавляющих фильтров низких и высоких частот.
5. Методика обнаружения сигналов линейных сетевых закладок и особенности её применения.
6. Методика обнаружения оптических сигналов передатчиков ИК диапазона и особенности её применения.
7. Методика обнаружения активных прослушивающих устройств с помощью индикатора электромагнитного поля.

Примерная тематика письменного задания:

1. Эволюция возникновения и особенности развития научной теории современных
защищённых информационных систем и технологий.
2. Характеристика и основные направления развития современных защищённых коммуникационных технологий.
3. Обзор защищённых информационных технологий финансово-хозяйственной

деятельности региона и прогнозирования деятельности предприятий.
4. Анализ проблем использования защищённых информационных технологий в
глобальных компьютерных сетях и эволюция их развития при передаче данных.
5. Интегрированные защищённые информационные технологии в распределённых
системах обработки данных и особенности их применения в современных условиях обработки информации.
6. Концепция формирования защищённого информационного общества в Российской Федерации и в мире.
7. Характеристика основных мероприятий и проблем при реализации общегосударственной системы применения электронной цифровой подписи, как пространства PKI и пространства идентификации личности.
8. Методика оценки защищённости информационных систем и технологий с применением механизмов нечёткой логики и нейронных сетей.
9. Обзор применяемых перспективных информационных технологий и интеллектуальных систем в адаптивных моделях информационной безопасности регионов.
10. Характеристика комплекса показателей и инструментальных средств для оценки защищённых информационных ресурсов региона и безопасности иерархических систем.

Примерная тематика (контрольных заданий) задач для выполнения:

ЗАДАНИЕ № 1

Тема: Теоретические аспекты проведения специальных исследований (СИ) на предприятии

Цель работы.

Изучение основных принципов проведения специальных исследований на предприятии. Освоить структуру ведения общей теоретической части проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

7. Изучить теоретическую часть Задания №1.
8. Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

9. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Специальные исследования (специсследования, СИ) — комплекс действий, направленный на обнаружение потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Проведение специсследований определяет возможность считывания и перехвата сигнала специальными средствами разведки в рамках определённых границ (защищённость утечек по каналам ПЭМИН — побочные электромагнитные излучения и наводки).

Введем для большей ясности определения, связанные с основой ведения специсследований на предприятии. Технический канал утечки информации (ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается ценная информация.

Автоматизированная система (АС) – устройство или комплекс устройств, необходимых для передачи, хранения и обработки конфиденциальной информации, прошедшая процедуру аттестации в соответствии с законодательством РФ.

Контролируемая зона (КЗ) – пространство, в котором исключено неконтролируемое пребывание посторонних лиц или сотрудников, не имеющих

прямое отношение к данному пространству. Примерами могут послужить: периметр охраняемой территории; ограждающие конструкции охраняемого здания или охраняемой территории.

Информационный сигнал – электрические сигналы, акустические, электромагнитные и т.д., по параметрам которых можно раскрыть конфиденциальную информацию, передаваемую, хранимую или обрабатываемую в основных технических средствах и системах или обсуждаемая в защищенном исполнении.

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для обработки, хранения и передачи конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

Средства активной защиты информации по каналам ПЭМИН (САЗ) – технические средства формирования маскирующих электромагнитных помех в местах возможного съема защищаемой информации, прошедшие обязательную процедуру сертификации по линии ФСТЭК России.

Деятельность по технической защите конфиденциальной информации (ТЗКИ) – выполнение работ и (или) оказание услуг по ее защите:

– от несанкционированного доступа,

– от утечки по техническим каналам,

– от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

Важно! Данный вид деятельности является лицензируемым. Лицензирование деятельности по ТЗКИ осуществляет ФСТЭК России.

Побочные электромагнитные излучения и наводки (ПЭМИН) – электромагнитные поля, создаваемые в окружающем пространстве СВТ, специ-

ально для этого не предназначенными (в случае ПЭМИ) или наводки данных излучений на токоведущие конструкции, линии и подключенные к ним ТС.

Существует несколько видов проведения специсследований на определенные ТС. В данном случае это акустоэлектрическое преобразование (АЭП) и ПЭМИН. В случае АЭП исследуемое средство подвергается воздействию некоих акустических частот. Из этого обосновывается определенный вывод о возможности использования ТС на невозможности подверженности АЭП.

Как уже было указано в определениях, ПЭМИ создаются вокруг работающих технических средств, которые специально для данного излучения не создавались. То есть излучение от радиопередатчиков, мобильных телефонов – это не побочные излучения. А вот излучения при работе компьютера от монитора, принтера, накопителей информации являются побочными.

Если вспомнить физику, то вокруг проводника, по которому протекает электрический ток возникает электромагнитное поле. Если по данному проводнику передается какой-либо сигнал, то, следовательно, и электромагнитное поле тоже будет изменяться по тем же законам, что и сигнал, протекающий в линии. Таким образом, источником сигнала ПЭМИ являются все токоведущие линии в ТС, по которым в процессе работы передаются какие-либо сигналы.

Как известно электромагнитные поля могут распространяться на значительные расстояния и конструкции помещений тому не преграда. Скорость передачи данных и обработки информации в современных средствах вычислительной техники постоянно растет, а значит растут и частоты сигналов ПЭМИ. Частоты сигналов ПЭМИ могут начинаться от единиц кГц и заканчиваться единицами ГГц, а гармоники этих сигналов могут находиться еще выше по частоте.

Если вспомнить, что в проводнике, помещенном в электромагнитное поле, возникает электрический ток, то очевидно, что могут возникать наводки ПЭМИ на любые токоведущие элементы (систему отопления, короб си-

стемы вентиляции и т. д.), в том числе и любые линии и ТС, подключенные к ним, попадающие под действие данного электромагнитного поля.

Перехват этой информации можно осуществить путем анализа изменений параметров ПЭМИН с помощью специальных высокочувствительных радиоприемных устройств, оснащенных специализированными антеннами, пробниками напряжения, токосъемниками.

На (рис. 1) приведена физика утечки информации за счет ПЭМИ.

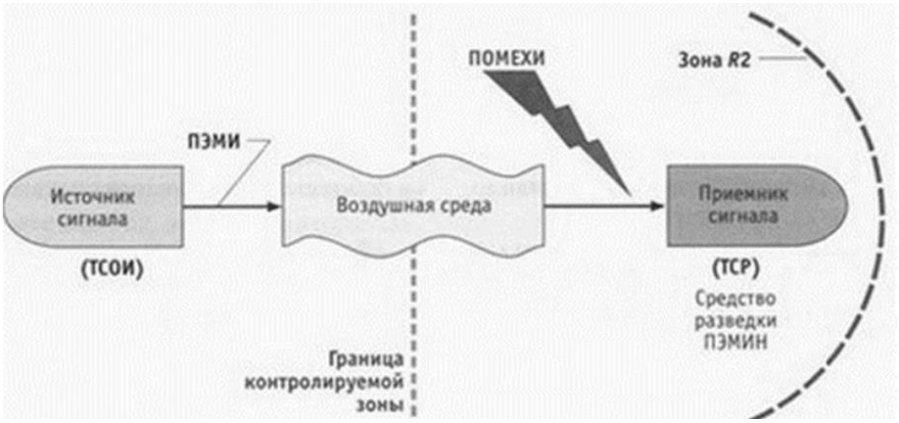

Рисунок 1. Схема ТКУИ за счет ПЭМИ

На (рис. 2) приведена физика утечки информации за счет ПЭМИН.

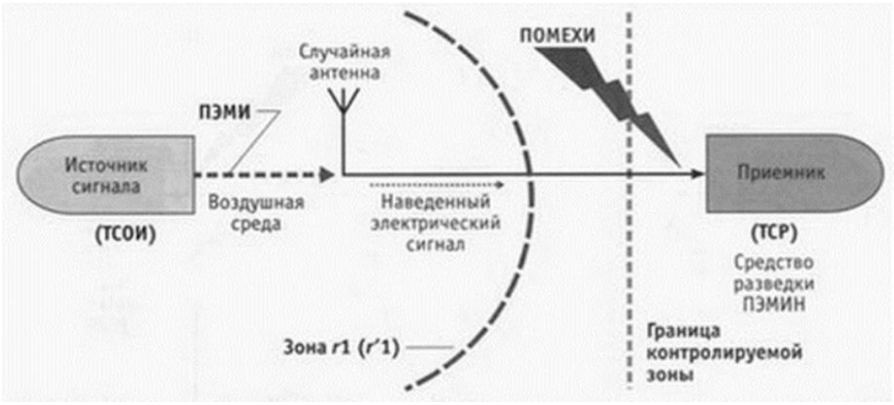

Рисунок 2. Схема ТКУИ за счет ПЭМИН

Поясним некоторые сокращения и термины на схемах:

- ТСОИ – технические средства обработки информации (все что попадает под определение ОТСС);
- ТСР–технические средства разведки;

• зона R2 – расстояние, на котором возможен перехват защищаемой информации за счет ПЭМИ;

• зона r1(r'1) – расстояние, наличие в пределах которого случайных антенн (токоведущие конструкции, линии и ТС) создает возможность утечки информации за счет наводок ПЭМИ.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенной случайной антенной может являться стационарный телефон, датчик пожарной сигнализации, громкоговоритель, подключенная к линии, выходящей за пределы КЗ.

Распределенные случайные антенным – антенны с распределенными параметрами. К ним можно отнести: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ.

Также разделяют саму информации по каналам АЭП и ПЭМИ на случай информативности. Информативные – сигналы с несущей, модулированной информативным сигналом. Примером могут послужить: сигнал от флэш-накопителя USB; VGA-интерфейс монитора; и т.д.

Неинформативные сигналы – сигналы, анализ которых не дает представления об обрабатываемой информации. Примеры: излучения от работы источников питания в узлах ТС; сигнал обработки режимов видеокартой; и т.д.

Важно! Всё приведенное выше относится к составной части по проведению работ, связанных с специальными исследованиями ОТСС и ВТСС. Однако это лишь малая часть того, что можно было бы изложить. Остальная теоретическая и прикладная часть изучается непосредственно работником предприятия в режимно секретном подразделении. Все методические материалы работ, связанных с проведением специальных исследований имеют грифы СЕКРЕТНО и СОВЕРШЕННО СЕКРЕТНО. Вышеизложенный материал является открытым и считается опорным в общих знаниях ТЗИ.

Практическая часть.

Вопросы для самопроверки:

6) Дайте определение специальным исследованиям в рамках данного учебного занятия.
7) Какие и сколько существует грифов секретности в рамках законодательства РФ?
8) Что такое зона r1(r’1) в ТЗИ?
9) Дайте определение ОТСС и ВТСС и в чем их различие?
10) На какие категории разбиваются случайные антенны в КЗ и в чем их разница? И на какие категории разбиваются информационные сигналы и в чем их разница?

Практические задания:

3) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.
4) В соответствии с (рис. 1) данного учебного задания, источником распространения сигнала ПЭМИ между техническим средством и техническим средством разведки является воздушная среда. Что будет если изменить воздушную среду на более плотную, а что, если перенести её в вакуум. Ответ обоснуйте.

Однажды, двое ученых задались очень интересной задачей, связанной с передачей информативного сигнала технического средства через канал ПЭМИ по очень интересной схеме. У них получилось и даже на современном этапе злоумышленники охотно придают значение данному средству получения заведомо важной для них информации. Двух ученых звали Маркус Кун и Росс Андерсон. При помощи сети Интернет, найдите информацию о данной процедуре получения информативного сигнала по каналу ПЭМИ и расскажите в общих чертах об этой технологии

ЗАДАНИЕ № 2

Тема: Теоретические основы средств измерения программно-аппаратных комплексов (ПАК) и альтернативной измерительной площадки (АИП)

Цель работы.

Изучение теоретической основы средств измерений сигналов. Освоить особенности поиска и идентификации сигналов при помощи альтернативной измерительной площадки.

Продолжительность занятия: полтора учебных часа.

Задания.

10. Изучить теоретическую часть Задания №2.
11. Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

12. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

В связи с тем, что многие организации, занимающиеся производством и распространением программно-аппаратных комплексов, предлагают на рынке целые линейки своих продуктов, отличающихся только аппаратной частью (анализаторы спектра) и соответственно ценой на данные товары в этой линейке. На рынке представлены программ- но-аппаратные комплексы следующих производителей, распространителей: «Навигатор ПхГ» – «НЕЛК», «Сигурд Мх» – «МАСКОМ», «Легенда» – «АВМ-СИСТЕМС». Стоит отметить, что все комплексы, рассматриваемые в данной работе, имеют сертификаты ФСТЭК России и метрологический сертификат соответствия на измерительное оборудование. Пример ПАК представлен на (рис. 1).

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

В полосе частот от 200 Гц до 30 МГц в комплект антенн должны входить магнитная и (или) электрическая антенны.

Для измерения магнитной составляющей электромагнитного поля, антенна должна быть: электрически экранированной рамочной антенной, имеющей такие размеры, чтобы ее рамка помещалась в квадрат со стороной не более 0,6 м, или ферритовая антенна длиной не более 0,5 м.

Допускаемая погрешность измерений напряженности магнитного поля (измеритель с магнитной антенной) не должна превышать 2,5 дБ.

Конструкция антенн (антенного штатива) должна обеспечивать возможность плавного изменения высоты расположения антенны над землей от 0,8 м до 1,25 м, а также возможность поворота магнитной и электрической антенн на 360° вокруг оси.

В полосе частот от 30 до 1000 МГц в комплект антенн должны входить одна или несколько электрических антенн одного из следующих типов:

а) линейный симметричный вибратор на полосу частот от 30 до 80 МГц, размер которого равен длине полуволнового симметричного вибратора

на частоте 80 МГц, и настраиваемый полуволновой симметричный вибратор в полосе частот от 80 до 1000 МГц, имеющий КСВН не более 2,5;

б) биконическая антенна, максимальный размер которой должен быть не более 1,35 м в полосе частот от 30 до 300 МГц и с КСВН не более 3,0, и биконическая антенна, максимальный размер которой – не более 0,5 м в полосе частот от 300 до 1000 МГц с КСВН не более 2,5;

в) широкополосная антенна, главный лепесток диаграммы направленности которой должен быть таким, чтобы в направлении непосредственного излучения от источника ПЭМИН и в направлении отраженного от земли луча разность коэффициентов усиления антенны не превышала бы 1 дБ, с КСВН не более 2,5.

Конструкция антенны (антенного штатива) должна обеспечивать возможность плавного изменения высоты центра симметрии над землей от 1 до 4 м и поворота вокруг горизонтальной оси на 180°, а также фиксированную ориентацию в трех взаимно ортогональных направлениях.

Допускаемая погрешность измерений напряженности электрического поля (измеритель с биконической, электрической антенной) не должна превышать 2,5 дБ на частотах до 1000 МГц.

Антенны должны иметь коэффициент калибровки, позволяющий измерять уровни полей. Рекомендуемый коэффициент калибровки антенн – не более 40 дБ. Погрешность коэффициента калибровки антенн должна быть не более 2 дБ.

Требования к анализатору.

Должен иметь несимметричный вход с номинальным значением сопротивления 50 Ом с коэффициентом стоячей волны по напряжению (КСВН) не более 2 при ослаблении входного аттенюатора 0 дБ и не более 1,2 при ослаблении входного аттенюатора 10 дБ и более.

Измерители совместно с первичными преобразователями должны обеспечивать измерения характеристик ПЭМИ в децибелах, относительно 1 мкВ, 1 мкА, 1 мкВ/м, 1 мкА/м, 1 мВт/м2.

Анализатор спектра должен быть программируемым, для дистанционного управления, т. е. должен обрабатывать команды, которые ему посылает ПЭВМ.

Должен иметь интерфейсы LAN или USB, или GPIB, или RS-232 для передачи данных с ПЭВМ на анализатор спектра и обратно.

Анализатор спектра должен иметь квазипиковый, пиковый и со среднеквадратичным отклонением детекторы.

Работать в полосе частот 9 кГц...1000 МГц.

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ, имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

Таблица 1. Перечень оборудования для проведения оценки защищенности по каналу ПЭМИН

Наименование средств измерения	Тип	Диапазон частот
Анализатор спектра	LIGNext1 NS-30A	10 кГц -3 ГГц
Антенна магнитная рамочная активная	Н-30	10 Гц – 30 МГц
Антенна электрическая дипольная активная	Е-3000	30 МГц – 3000 МГц
Антенна электрическая дипольная активная	Е-30	10 Гц – 30 МГц
Пробник напряжения	П-400	10 Гц – 300 МГц
Осциллограф	LeCroy Wavesurfer 62Xs	0 Гц – 600 МГц
Генератор сигналов	Г4-218	200 кГц-1 ГГц

Альтернативная измерительная площадка.

Временная методика оценки защищенности ОТСС, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации (КИ), описанная в «Сборнике временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам» предполагает собой поиск и измерение опасных сигналов непосредственно на объекте информатизации.

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная. Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

Стоячая волна (электромагнитная) – периодическое изменение амплитуды напряженности электрического и магнитного полей вдоль направления распространения, вызванное интерференцией, падающей и отраженной волн. Например, стоячая волна возникает при отражении волны от преград и неоднородностей в результате взаимодействия (интерференции), падающей и отражённой волн.

Присутствие такой волны во время проведения измерений однозначно приведёт к ошибке.

Измерительная площадка – площадка, отвечающая требованиям, обеспечивающим правильное измерение уровней индустриальных радиопомех (ИРП), излучаемых ТС в регламентированных условиях. Видов ИП предусматриваются два – «открытая измерительная площадка» и «альтернативная измерительная площадка». Поскольку строительство и эксплуатация открытой площадки весьма дорого, сосредоточимся на более дешёвом варианте – АИП. Разница между открытой ИП и АИП заключается в том, что последняя должна размещаться не в открытом пространстве, а в некотором помещении, в здании. При том физические характеристики АИП (прежде всего «затухание» электромагнитного поля) должны оставаться в пределах установленного допуска.

Важно! Перед вводом в эксплуатацию АИП оценивается минимум искажений, вносимых в распределение электромагнитного поля ограждающими конструкциями помещения, который можно допустить. Иными словами, оператор заранее знает о наличии и характере «стоячих волн» и о характеристиках закона затухания электромагнитного поля. Это позволяет получать информацию об «опасных» информативных сигналах корректнее, чем на ОИ, на котором абсолютно не исследована шумовая обстановка.

Практическая часть.

Вопросы для самопроверки:

6) Назовите весь перечень оборудования для проведения оценки защищенности по ПЭМИ.
7) Дайте определение измерительной площадки в рамках данного задания.
8) Сколько существует видов измерительных площадок (ИП) и в чем их различие?
9) На сколько метров минимально и максимально предполагается плавное размещение антенны по высоте?
10) Какой должен быть коэффициент калибровки у антенн?

Практические задания:

3) Как по Вашему мнению вы представляете себе открытую измерительную площадку и альтернативную? Опишите их. В чем их основное различие? Ответ обоснуйте.
4) Представьте, что Вы начинающий сотрудник предприятия ООО «НПП «ИБЦ». Начался ваш седьмой рабочий день. Вы в обычном распорядке, получив задание, идете включать лабораторное автоматизированное рабочее место и ПАК. Неожиданным образом узнаёте, что откалиброванная антенна начала давать сбой. Вы (без особой паники) начинаете искать пути решения. По Вашему мне-

нию, каковы основные три шага на пути решения этой проблемы? Ответ обоснуйте.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Защищённые информационные системы» являются текущая аттестация в виде контрольной работы и одна итоговая аттестация в виде экзамена в устной форме.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	Контрольная работа	УК-1 ОПК-1	3 вопроса	Контрольная работа проводится в письменной форме путём ответа на поставленные вопросы; время отведенное на процедуру - 90 минут	Результаты контрольной работы предоставляются в день проведения процедуры	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • знание основных научных теорий, изучаемых предметов; • правильные ответы на все поставленные вопросы контрольной работы. «**Хорошо**»: • знание основных понятий предмета; • представление об основных научных теориях,

						изучаемого предмета; • ответы на большинство поставленных вопросов контрольной работы. **«Удовлетвори-тельно»**: • демонстрирует частичные знания по темам дисциплин; • ответил не на все вопросы контрольной работы. «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплины; • незнание основных понятий предмета; ● не ответил на большинство вопросов контрольной работы.

Проводится в сроки, установленные графиком образовательного процесса	Экзамен	УК-1 ОПК-1	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на все вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на большинство вопросов билета **«Удовлетво-**

						ри-тельно»: • демонстрирует частичные знания по темам дисциплины; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • ответил не на все вопросы билета «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплины; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на большинствовопросов билета.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

4.1. Типовые вопросы, выносимые на контрольную работу

1. Какой вид входной информации используется на первом этапе системно-информационного подхода к преобразованию информации в стратегическом менеджменте?
2. Назовите и охарактеризуйте основные пакеты прикладных программ, реализующих задачи стратегического менеджмента на предприятии.
3. Охарактеризуйте типичные информационно-вычислительные системы, которые в настоящее время применяются для информационного обслуживания органов регионального управления.
4. Что понимается под компьютерной стегологией и чем она отличается от стеганографии?
5. Перечислите основные категории информационных ресурсов в России и какие государственные структуры осуществляют контроль за госресурсами?
6. Как делятся современные криптосистемы и в чём особенности их применения для передачи информации?
7. Что понимается под безопасностью информационных технологий, определение способов несанкционированного доступа к информации?
8. Охарактеризуйте основные задачи системы управления персоналом региона как объекта информационной безопасности.
9. Какие органы занимают ведущее место в информационном обслуживании органов госуправления на региональном и муниципальном уровне?
10. Охарактеризуйте современные способы визуального представления речевых сигналов в виде графических образов и их особенности применения?
11. В чём состоит идея речевой подписи и психоакустики, где они применяются?
12. Основные проблемы защиты интеллектуальной собственности и характеристика способов защиты авторского права на мультимедийные данные.

4.2. Типовые вопросы, выносимые на экзамен

1. Сущность стратегического менеджмента на предприятиях региона.

2. Функциональные задачи стратегического менеджмента и их реализация в условиях информационных технологий.
3. Какой вид входной информации используется на первом этапе преобразования информации стратегического менеджмента?
4. Информационные технологии стратегического менеджмента на предприятиях региона.
5. Основные пакеты прикладных программ, реализующих задачи стратегического менеджмента на предприятиях региона и их характеристика.
6. Программное обеспечение финансовых решений на предприятиях региона.
7. Информационные технологии решения задач финансового менеджмента.
8. Характеристика основных элементов управляющей подсистемы финансового менеджмента.
9. Комплекс задач финансового менеджмента и их особенности, виды информации, использующиеся, при решении этих задач.
10. Классификация программных средств финансового менеджмента, какие средства используются для решения задач финансового анализа?
11. Общие черты комплексных систем автоматизации управления финансово-хозяйственной деятельностью предприятий региона.
12. Особенности задач по оценке инвестиционных проектов и основные этапы их решения в регионе.
13. Основные особенности программных продуктов «Project Expert» и «Альт-Инвест» для решения задач финансового анализа и прогнозирования.
14. Общие технологические принципы решения задач управления персоналом в корпоративных организациях региона.
15. Основные подсистемы автоматизированной информационной системы управления персоналом и их характеристика.
16. Основные направления анализа информации в области управления персоналом на предприятиях региона.
17. Информационно-вычислительные и ситуационные центры в государственном и региональном управлении.
18. Информационные технологии решения функциональных задач в муниципальном управлении.
19. Государственные информационные ресурсы России и их характеристика.
20. Информационные ресурсы федеральных и региональных органов власти как объекты защиты информации.
21. Информационные ресурсы и технологии в сфере финансов и внешнеэкономической деятельности страны.
22. Информационные ресурсы отраслей материального производства, государственной системы статистики и социальной сферы, их особенности.
23. Основные виды угроз безопасности информационных систем и технологий, их характеристика.
24. Основные формы атак на объекты информационных систем региона и их особенности.
25. Анализ основных угроз и каналов утечки информации в регионе, их особенности.

26. Характеристика современных методов и средств защиты информационных технологий в регионе.
27. Основные методы и средства построения систем информационной безопасности региона, характеристика их структурных элементов.
28. Защита информации в корпоративных сетях управления региона.
29. Анализ возможных рисков применяемых информационных технологий и управление рисками.
30. Особенности стратегии защиты информации с использованием системного подхода, комплексных решений и принципа интеграции в защищённых информационных технологиях.
31. Организационные способы противодействия телефонному пиратству в регионе.
32. Ограничение доступа к телефонным линиям связи в регионе и основные рекомендации абонентам в случае обнаружения самовольного подключения.
33. Характеристика современных пассивных устройств технического противодействия телефонному пиратству.
34. Специализированные анализаторы телефонных линий связи в регионе и их характеристика.
35. Обзор характеристик основных зарубежных приборов для контроля состояния телефонных линий.
36. Особенности активных устройств технического противодействия телефонному пиратству.
37. Основные критерии оценки систем закрытия речи и передовые тенденции развития этих систем.
38. Характеристика современных методов противодействия утечке компьютерной и аудиовидеоинформации.
39. Особенности современных сканирующих приёмников и индикаторов поля.
40. Характеристики и примеры многофункциональных поисковых систем и устройств защиты.
41. Основные характеристики и примеры выжигателей закладных устройств, обнаружителей и подавителей диктофонов, других высокочастотных электронных устройств.
42. Характеристики и примеры современных систем виброакустического зашумления помещений и сетей.
43. Организация защиты объектов от встроенных и узконаправленных микрофонов.
44. Организация защиты объектов от лазерных прослушивающих устройств.
45. Характеристика и особенности современных нелинейных радиолокаторов.
46. Решение задач безопасности речевой связи региона с помощью компьютерных информационных технологий.
47. Особенности представления речевых сигналов в виде графических образов.
48. Компьютерные технологии безопасности связи региона на основе цифровой обработки изображений сонограмм.
49. Технологии обеспечения безопасности в регионе на основе индивидуальных особенностей человека.

50. Характеристика современных методов биометрической идентификации личности и их особенности.
51. Представление речевого сигнала сообщения в виде графических образов.
52. Реализация способов аудиомаркирования с помощью компьютерных технологий.
53. Основные рекомендации по практическому применению технологии «речевая подпись».
54. Стеганографическая защита информации цифровыми водяными знаками.
55. Характеристика современных систем цифровых водяных знаков и их особенности.
56. Характеристика и особенности основных атак на системы цифровых водяных знаков.
57. Особенности применения криптотехнологий в цифровом телевидении.
58. Основные рекомендации по практическому применению стеганографической технологии в цифровом телевидении.
59. Маркирование и защита интеллектуальной собственности в России.
60. Организация и методика экспресс-поиска устройств несанкционированного съёма информации.

Типовые вопросы, выносимые на экзамен (тестирование)

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

- Функции КСЗИ:
  создание механизмов защиты, сводящие до минимума возможность воздействия дестабилизирующих факторов на защищаемую информацию; непрерывное и оптимальное управление механизмами комплексной защиты
  обеспечение конфиденциальности, целостности, доступности информации
  обеспечение криптографической, программной и аппаратной защиты информации
  обеспечение защиты людей, материальных носителей, автоматизированных систем

- Требование безопасности повторного использования объектов противоречит:
  инкапсуляции
  наследованию
  полиморфизму

- Уровни модели OSI, по возрастанию:
  физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной

сетевой, канальный, транспортный, сеансовый, прикладной, представления, физический
прикладной, представления, физический, канальный, сетевой, транспортный, сеансовый
физический, сетевой, канальный, транспортный, сеансовый, представления, прикладной

- Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
запрет на чтение каких-либо файлов, кроме конфигурационных
запрет на изменение каких-либо файлов, кроме конфигурационных +
запрет на установление сетевых соединений

- Уровни модели TCP/IP, по возрастанию:
канальный, сетевой, транспортный, прикладной
транспортный, канальный, сетевой, прикладной
канальный, транспортный, сетевой, прикладной
прикладной, сетевой, транспортный, канальный

- К какому уровню модели TCP\IP относятся следующие протоколы HTTP, RTP, FTP, DNS:
прикладной
транспортный
сетевой
канальный

- В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
меры обеспечения целостности
административные меры
меры административного воздействия

- Что входит в функции систем мониторинга:
выявление состояния систем
установка отношений между объектами
установка соответствия правил и обязанностей
все варианты верны

- Какие существуют подходы по построению защищенных операционных систем применяемых в АС:
фрагментарный и комплексный
фрагментарный и операционный.
комплексный и позиционный.
системный и позиционный.

- Дублирование сообщений является угрозой:
доступности

конфиденциальности
целостности

- Какие существуют методы оценки качества КСИБ:
  метод оценки уязвимости Хоффмана +
  экспертная оценка +
  сигнатурный метод
  качественный метод.
- Самыми опасными источниками внутренних угроз являются:
  некомпетентные руководители
  обиженные сотрудники
  любопытные администраторы
- Для внедрения бомб чаще всего используются ошибки типа:
  отсутствие проверок кодов возврата
  переполнение буфера
  нарушение целостности транзакций
- В число целей политики безопасности верхнего уровня входят:
  решение сформировать или пересмотреть комплексную программу безопасности
  обеспечение базы для соблюдения законов и правил
  обеспечение конфиденциальности почтовых сообщений
- В число целей программы безопасности верхнего уровня входят:
  управление рисками
  определение ответственных за информационные сервисы
  определение мер наказания за нарушения политики безопасности
- Что означает обеспечение целостности баз данных.

  это соответствие информации базы данных её внутренней логике, структуре и заданным правилам. +
  это полное значение информации базы данных в котором действуют установленные правила
  это информация, работающая по установленной структуре базы данных.
  это логическая операция обеспечивающая полноту информации и соблюдающая условия того, что информация не будет изменена.
- В рамках программы безопасности нижнего уровня осуществляются:
  стратегическое планирование
  повседневное администрирование
  отслеживание слабых мест защиты +

- Политика безопасности строится на основе:
  общих представлений об ИС организации
  изучения политик родственных организаций
  анализа рисков

- В число целей политики безопасности верхнего уровня входят:
  формулировка административных решений по важнейшим аспектам реализации программы безопасности
  выбор методов аутентификации пользователей
  обеспечение базы для соблюдения законов и правил +

- Основные механизмы защиты применяемые в ОС:
  идентификации / аутентификации
  разграничения доступа
  аудита
  все перечисленные варианты верны

Приложение 2
Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: магистратура
Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

– дать обучающимся концептуальные знания и представления по современным защищённым информационным системам и технологиям, применяемым в регионе;

– выработать и закрепить у обучающихся базовые умения и навыки по практической организации и реализации современных защищённых технологий и информационных систем на типовых региональных информационных объектах с учётом современных международных и отечественных стандартов.

Задачи дисциплины:

– ознакомление обучающихся с процессами анализа фундаментальных и прикладных проблем информационной безопасности, основными информационными технологиями и информационными системами региона;

– изучение основных организационных и программно-технических мер по обеспечению информационной безопасности объектов региона, а также основных методов определения параметров, характеристик и условий применения защищённых информационных систем и технологий региона;

– формирование у обучающихся способности самостоятельно решать поставленные задачи в области применения защищённых информационных технологий и систем с помощью современных принципов, методов и сил в различных организационных структурах региона, по базовым направлениям и применительно к типовым информационным объектам.

2. Указания по проведению практических занятий

Тема 1. Государственные информационные ресурсы России как объект информационной безопасности.

Практическое занятие 1.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: групповая дискуссия

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки по анализу существующих информационных технологий (систем) региона как объектов информационной безопасности.

Основные положения темы занятия:

1. Реализация задач стратегического менеджмента с использованием специализированных компьютерных систем экономического и финансового моделирования.

2. Информационные технологии по использованию трудовых ресурсов и рабочего времени в корпоративных организациях.

Вопросы для обсуждения:

1. Информационные ресурсы библиотечной сети России.

2. Ресурсы государственной системы экономической и научно-технической
информации.

3. Российские ресурсы правовой информации.

4. Информационные ресурсы федеральных и региональных органов власти.

Продолжительность занятия – 3 ч.

Тема 2. Информационные ресурсы в различных областях экономической и социальной сферах деятельности государства как объекты информационной безопасности

Практическое занятие 2.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: беседа

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки по созданию и функционированию информационных систем (технологий) в органах государственного и регионального управления.

Основные положения темы занятия:

1. Информационные технологии решения задач финансового менеджмента и их основные процедуры.

2. Особенности организации функциональных задач и информационных технологий в муниципальном управлении.

Вопросы для обсуждения:

1. Информационные ресурсы в сфере финансов и внешнеэкономической
деятельности государства.

2. Информационные ресурсы отраслей материального производства.

3. Информационные ресурсы государственной системы статистики.

4. Информационные ресурсы социальной сферы.

Продолжительность занятия – 3 ч.

Тема 3. Основные понятия информационной безопасности региона и их характеристика.

Практическое занятие 3.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: групповая дискуссия

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки по определению видов угроз безопасности информационных систем и технологий, основным формам атак на объекты информационных систем региона.

Основные положения темы занятия:

1. Оценка безопасности информационных технологий, анализ угроз и каналов утечки информации.

2. Анализ рисков и управление ими при использовании защищённых информационных технологий.

Вопросы для обсуждения:

1. Классификация угроз безопасности информационным объектам региона.
2. Основные формы атак на объекты информационных систем и технологий.
3. Анализ угроз и каналов утечки информации на объектах региона.
4. Анализ рисков и управление ими при использовании защищённых инфомационных технологий.

Продолжительность занятия – 3 ч.

Тема 4. Основы защиты информации в корпоративных информационных технологиях управления.

Практическое занятие 4.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: практическая работа в группах.

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки по применению современных активных и пассивных устройств технического противодействия телефонному пиратству, а также по применению методов противодействия утечке компьютерной и аудиовидеоинформации.

Основные положения темы занятия:

1. Краткий обзор зарубежных и отечественных приборов для контроля состояния телефонных линий связи и других активных устройств технического противодействия телефонному пиратству.
2. Критерии оценки систем закрытия речи и основные тенденции их развития в корпоративных сетях управления региона.

Вопросы для обсуждения:

1. Создание системы защиты информации в корпоративной сети управления региона.
2. Основные этапы разработки систем защиты информационных систем и технологий региона и их характеристика.
3. Проблемы защиты интеллектуальной собственности в регионах России.
4. Основные направления совершенствования защищённых информационных технологий региона.

Продолжительность занятия – 3 ч.

Тема 5. Современные технологии противодействия утечке телефонных и компьютерных данных на информационных объектах региона.

Практическое занятие 5.

Вид практического занятия**:** смешанная форма практического занятия.

Образовательные технологии: групповая дискуссия

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки по компьютерным технологиям безопасности связи на основе цифровой обработки изображений и технологиям обеспечения безопасности на основе индивидуальных особенностей человека.

Основные положения темы занятия:

1. Характеристика современных методов биометрической идентификации личности.

2. Стеганографическая защита информации цифровыми водяными знаками и решение задач безопасности речевой связи с помощью современных компьютерных информационных технологий.

Вопросы для обсуждения:

1. Современные индикаторы поля и сканирующие приёмники.
2. Характеристика многофункциональных поисковых систем.
3. Выжигатели скрытых закладных устройств.
4. Обнаружители и подавители диктофонов и других высокочастотных электронных устройств.

Продолжительность занятия – 4 ч.

3. Указания по проведению лабораторного практикума

Цель проведения лабораторных работ – ознакомление обучаемых с комплексом показателей для оценки защищённости информационных систем (технологий) и программной средой, используемой для моделирования процессов оптимизации систем информационной безопасности региона.

Задачи выполнения лабораторных работ:

- определение положения механизмов защиты, включение которых в иерархию системы информационной безопасности региона повышает уровень защищённости информационных систем и технологий;
- мониторинг защищённости корпоративных информационных систем и технологий, базирующийся на решении оптимизационных задач на основе рейтинговых показателей, учитывающий разноплановые экспертные оценки, включая экономические;
- анализ существующих систем информационной безопасности региона на предмет определения эффективности их применения исходя из предполагаемых затрат на создание таких систем, их эксплуатацию и реализацию для предотвращения ущерба от выявленных и потенциальных угроз;
- формирование потенциальной структуры защищённых информационных систем и технологий, путём задания иерархии эшелонов и перечня механизмов защиты для нейтрализации требуемого поля угроз и предотвращённого ущерба;

- формирование динамической модели адаптивной защиты информационных систем и технологий региона для анализа последствий реализации угроз, приводящих к ущербу, близкому или превышающему допустимое для данного хозяйствующего субъекта значение.

Методика проведения лабораторных работ определяется моделью решаемых задач по обеспечению безопасности региональных информационных объектов и технологий, исследуемых обучаемыми на занятии по заданию преподавателя.

Средства выполнения лабораторных работ:

- программный комплекс “Project Expert”;
- программный комплекс «Альт – Инвест»;
- нелинейный локатор «NR-900-EM»;
- программный комплекс «Adobe Photoshop» с фильтром «Digimarc»

Этапы выполнения лабораторных работ:

1. Постановка задачи лабораторной работы.
2. Ознакомление обучаемых с содержанием и объёмом лабораторной работы.
3. Порядок выполнения лабораторной работы.
4. Регистрация результатов и оформление отчёта о лабораторной работе.
5. Заключительная часть лабораторной работы.

Тематика лабораторных работ и задания к ним

Лабораторная работа 1.

Тема: Технико-экономическое обоснование защищённой деятельности предприятий региона с помощью информационных технологий.

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем и технологий “Project Expert” и получение практических навыков в моделировании и оптимизации применения механизмов защиты в ходе осуществления мониторинга деятельности предприятий региона.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №1:

1. Ознакомиться с системой показателей для оценки информационной защищённости региональных объектов.

2. Запустить программу “Project Expert” и в интерактивном режиме сформировать перечень известных угроз, механизмов защиты и расставить их в иерархии эшелонов защиты для объектов региона.

3. Сформировать матрицы экспертных оценок «Механизмы защиты – Угрозы» и «Угрозы – Эшелоны защиты» для достоверности активации механизмов защиты.

4. Провести расчёт матрицы, определяющей распределение относительного потенциального ущерба по механизмам защиты и эшелонам безопасности на заданном множестве известных угроз.
5. Проанализировать активность системы информационной безопасности в разрезе использования конкретных механизмов защиты и эшелонов безопасности предприятий региона.
6. Действия пунктов 3-5 повторить для различных частот активизации угроз безопасности.
7. Сформировать рейтинговые показатели при использовании конкретных механизмов защиты и эшелонов информационной безопасности для указанных информационных объектов, а также показатели активности отдельных эшелонов и механизмов защиты.
8. Создать отчёт по лабораторной работе и сформулировать выводы.

Продолжительность практического занятия-4 часа

Лабораторная работа 2.

Тема: Экономическое обоснование инвестиционных проектов муниципаль ных предприятий с помощью защищённых информационных техно логий.

Цель занятия: Ознакомление с программным комплексом оценки защищённости инвестиционных проектов “Альт–Инвест” и получение практических навыков в моделировании и оптимизации применения механизмов защиты для деятельности муниципальных предприятий с учётом рисков и неопределённости внешней среды.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №2:

1. Ознакомиться с системой показателей для оценки защищённости инвестиционных проектов в деятельности муниципальных предприятий с учётом рисков и неопределённости внешней среды.
2. Запустить программу “Альт–Инвест” в интерактивном режиме, получить от преподавателя вариант многоуровневой системы защиты инвестиционных проектов муниципальных предприятий с индивидуальным распределением конкретных механизмов защиты по эшелонам региона.
3. Провести расчёт матрицы, определяющей распределение относительного ущерба по механизмам защиты и уровням адаптивной системы защищён ности инвестиционных проектов муниципальных предприятий на задан. ном множестве известных угроз.
4. Проанализировать активность адаптивной защиты в разрезе использования конкретных механизмов защиты и эшелонов безопасности инвестиционных проектов муниципальных предприятий.
5. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов безопасности инвестиционных проектов муниципальных предприятий.
6. Проанализировать существующую защищённость и сформулировать предложения по улучшению рейтинга системы защиты инвестиционных

проектов муниципального предприятия и всего регионального эшелона.
7. Создать отчёт по лабораторной работе и сформулировать выводы.
Продолжительность практического занятия-4 часа

Лабораторная работа 3.

Тема: Исследование технологий проведения поисковых мероприятий по выявлению электронных закладных устройств в информационных объектах региона.

Цель занятия: Изучение приёмов обнаружения нелинейных соединений полупроводниковых устройств с определением их типа независимо от их функционального состояния и получение практических навыков в работе с нелинейными радиолокаторами типа «NR-900-EM».

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №3:

1. Ознакомиться с предназначением, основными возможностями и порядком применения нелинейного радиолокатора «NR-900-EM» для поисковых мероприятий по выявлению электронных закладных устройств.
2. Определить отклик чистого полупроводника с помощью нелинейного локатора, провести поиск на минимальной и максимальной частоте.
3. Определить аудиоотклик сигнала с помощью головных телефонов, провести поиск на минимальной и максимальной частоте.
4. Определить ложное соединение (коррозионную нелинейность объекта) при одновременном интенсивном простукивании места расположения отражающего элемента деревянной палочкой (при этом коррозийный элемент, как правило, характеризуется хриплым нерегулярным звуком).
5. Определить максимальную дальность обнаружения выявленных объектов при различных уровнях излучения антенны.
6. Создать отчёт по лабораторной работе и сформулировать выводы.

Продолжительность практического занятия-4 часа

Лабораторная работа 4.

Тема: Исследование современных технологий противодействия утечке информации и защите авторских прав с помощью сокрытия аудиовидеоинформации в сообщениях и файлах мультимедийных продуктов.

Цель занятия: Изучение принципов компьютерной аудиовидеостеганографии, методов скрытия сообщений в аудиофайлах и получение практических навыков в работе со стеганографическими программными средствами защиты информации на примере программного комплекса «Adobe Photoshop» с фильтром «Digimarc».

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №4:

1. Ознакомиться с программными средствами стеганографической защиты авторских продуктов, доступ к которым должен иметь лишь определённый пользователем круг лиц.
2. Создать и скрыть текстовое сообщение и файл с диска в контейнер с ис-

пользованием технологии стеганографической защиты, позволяющей скрыть необходимую информацию в контейнере практически произвольного формата (BMP, JPEG, GIF, MP3), сохраняя при этом возможность чтения контейнера с помощью соответствующего формату файла программного средства.

3. Имена контейнеров и файлов с диска соответствуют Вашему порядковому номеру в списке группы. Скрываемое сообщение должно состоять из темы «Стеганография» и содержания, которым является любое четверостишие. Полученный результат сохранить в папку «Стегоконтейнера» под произвольным именем.
4. Извлечь и сохранить текстовое сообщение и файл.
5. Сравнить содержание скрытого и извлечённого сообщения, а также скрытый и извлечённый файлы.
6. Визуально сравнить исходный контейнер и стегоконтейнер, сравнить даты их создания и изменения, объёмы и свойства контейнера и стегоконтейнера, проанализировать результаты.
7. Результаты работы и итогового анализа сравнения поместить в Вашу папку на ПК.
8. Создать отчёт по лабораторной работе и сформулировать выводы.

Продолжительность практического занятия-4 часа

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	**Виды СРС**
2 семестр		
1	Информационные технологии региона как объект информационной безопасности.	**1.** Активные способы противодействия прослушиванию помещений по абонентским линиям связи. **2.** Характеристика основных способов защиты абонентских телефонных линий связи от бесконтактного съёма информации. **3.** Характеристика способов съёма акустической информации со стен и потолочных перекрытий охраняемых муниципальных объектов. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***
2	Нормативно-правовые основы защиты информационных технологий региона.	**1.** Характеристика способов съёма акустической информации с металлических труб и оконных стёкол охраняемых муниципальных объектов **2.** Характеристика способов съёма акустической информации в помещении по линии электро

		сети охраняемых муниципальных объектов. **3.** Характеристика пассивных способов проти водействия прослушивания охраняемых по мещений по абонентской линии связи. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***
3	Защищённые информационные технологии в государственном и муниципальном управлении.	1. Методика применения телефонолокационно го способа съёма акустических сигналов муниципальных защищаемых помещениях. 2. Характеристика основных устройств проти водействия съёму информации в муници пальных защищаемых помещениях. 3. Основные компоненты охранной сигнализации при использовании различных датчиков. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***
4	Защищённые информационные технологии в управлении коммерческими структурами региона.	1. Методика обнаружения сигналов линейных сетевых закладок и особенности её примене ния. 2. Методика обнаружения оптических сигнало передатчиков ИК диапазона и особенности е применения. 3. Методика обнаружения активных прослуши вающих устройств с помощью индикатора электромагнитного поля. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***
5	Организационно-технические методы защиты информационных технологий региона.	1. Реализация технологии речевой подписи (аудиомаркирования) сообщений с применением компьютерных технологий. 2. Практическое применение защитной технологии «речевая подпись» в современном мире. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***

Вопросы, выносимые на самостоятельное изучение:

1. Особенности шифрования данных псевдослучайными числами.
2. Основные методы шифрования информации и их характеристика.

3. Порядок применения поточных и блочных шифров, понятие криптографического протокола.
4. Криптографические системы с открытым ключом и их особенности применения.
5. Методы использования специальных свойств компьютерных форматов.
6. Философия использования электронной цифровой подписи и методы хеширования сообщений.
7. Методы использования избыточности аудио- и видеоинформации в компьютерной стеганографии.
8. Характеристика современных распространённых методов биометрической идентификации личности и особенности их применения.
9. Реализация технологии речевой подписи (аудиомаркирования) сообщений с применением компьютерных технологий.
10. Практическое применение защитной технологии «речевая подпись» в современном мире.

Примерные темы докладов

1. Активные способы противодействия прослушиванию помещений по абонентским линиям связи.
2. Характеристика основных способов защиты абонентских телефонных линий связи от бесконтактного съёма информации.
3. Характеристика способов съёма акустической информации со стен и потолочных перекрытий охраняемых муниципальных объектов.
4. Характеристика способов съёма акустической информации с металлических труб и оконных стёкол охраняемых муниципальных объектов.
5. Характеристика способов съёма акустической информации в помещении по линии электросети охраняемых муниципальных объектов.
6. Характеристика пассивных способов противодействия прослушивания охраняемых помещений по абонентской линии связи.
7. Методика применения телефонолокационного способа съёма акустических сигналов в муниципальных защищаемых помещениях.
8. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях.
9. Основные компоненты охранной сигнализации при использовании различных датчиков.
10. Характеристика современных телевизионных средств охранной сигнализации.
11. Характеристика сетевых пассивных помехоподавляющих фильтров низких и высоких частот.
12. Методика обнаружения сигналов линейных сетевых закладок и особенности её применения.
13. Методика обнаружения оптических сигналов передатчиков ИК диапазона и особенности её применения.

14. Методика обнаружения активных прослушивающих устройств с помощью индикатора электромагнитного поля.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. При определении целей и задач работы необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов и выводами.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. В процессе изложения материала необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы общие выводы по итогам исследования и рекомендации по применению работы.
7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.
8. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 20 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

необходимой для освоения дисциплины (модуля)

Основная литература:

1.Гагарина Л.Г., Федоров А.Р., Федоров П.А. Введение в архитектуру программного обеспечения: Учебное пособие - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 320 с. ISBN 978-5-8199-0649-1. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=542665

2.Астапчук В.А., Терещенко П.В. Архитектура корпоративных информационных систем – Новосиб.: НГТУ, 2015. - 75 с.: ISBN 978-5-7782-2698-2. / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=546624

Дополнительная литература:

3.Царев Р.Ю., Прокопенко А.В., Князьков А.Н. Программные и аппаратные средства информатики - Краснояр.: СФУ, 2015. - 160 с. ISBN 978-5-7638-3187-0 / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=550017

7.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. http://eup.ru/catalog/all-all.asp – **научно-образовательный портал;**
2. **www.wikIsec.ru** – Энциклопедия информационной безопасности. – Публикации, статьи;
3. **http://www.iso27000.ru/** - портал по управлению информационной безопасностью.
4. http://www.fsb.ru/ – **Официальный сайт Федеральной Службы Безопасности РФ;**
5. http://www.fstec.ru/ – **Официальный сайт Федеральной Службы по** Техническому Экспортному контролю РФ.

8.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.
- **Информационные справочные системы:**
  Электронные ресурсы образовательной среды Университета
  Информационно-справочные системы (Консультант+; Гарант).