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.В.ДВ.03.03 «ОСНОВЫ УПРАВЛЕНИЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ (ООО «НОВО», НТЦ «ЗАРЯ»)»

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: Панцыр Р.Я. Рабочая программа дисциплины: Основы управления коорпоративной информационной безопасностью (ООО «НОВО», НТЦ «ЗАРЯ»). – Королев МО: «Технологический Университет», 2023

Рецензент: Журавлев С.И.

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 (модулю), соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины являются:

1. Формирование у обучаемых специализированной базы знаний по основным понятиям и умениям в области регионального комплексного аудита информационной безопасности;

2. Формирование организационно-технических навыков проведения комплексного аудита информационной безопасности в регионе (по базовым направлениям и типовым информационным объектам).

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

Профессиональные компетенции:

- ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.
- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.

Основными **задачами** дисциплины являются:

- раскрытие сущности, целей и содержание комплексного аудита информационной безопасности;
- выявление общих методологических основ комплексного аудита информационной безопасности региона;
- изучение нормативно-правовой базы комплексного аудита информационной безопасности типовых объектов региона;
- освоение методики комплексного аудита информационной безопасности (исполнительных органов государственной власти и органов местного самоуправления) региона;

- раскрытие основных положений по лицензированию деятельности по информационной безопасности организационных структур региона;
- изучение основ организации лицензирования деятельности, сертификации средств и систем информационной безопасности в регионе.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационнойзащите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.

- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

Необходимые знания:

- ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина **«Основы управления корпоративной информационной безопасностью» (ООО «НОВО», НТЦ «ЗАРЯ») Б1.В.ДВ.03.03** относится к дисциплинам по выбору части, формируемой участниками образовательных

отношений, блока 1 основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность»

Дисциплина базируется на ранее изученных дисциплинах: “Основы теории информационной безопасности»; «Специальные разделы физики»; «Теоретические основы компьютерной безопасности»; «Защищенные информационные системы» и компетенциях: УК-1, 2, 4; ОПК-1, 5.

Знания и компетенции, полученные при изучении дисциплины необходимы для написания магистерской диссертации.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр 3**	**Семестр** 8	**Семестр** …	**Семестр** …
Общая трудоемкость	72	72			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	46	46			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	**8**	**8**			
Практическая подготовка	**4**	**4**			
Другие виды контактной работы*	6	6			
Самостоятельная работа	26	26			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Текущий контроль знаний (7 - 8, 15 - 16 недели) – 2ч	нет	нет			
Вид итогового контроля	Зачет	Зачет			

* 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	Лекции, час.	Практ. занят., час.	Лабораторные занятия	Занят. в интеракт. форме, час.	Практическая погот овка ,час	Код компетенций
Раздел (модуль) 1. Теоретико-прикладные основы комплексного аудита информационной безопасности						
Тема 1. Основные положения по комплексному аудиту информационной безопасности	2	4	1	1	1	ПК-1.
Тема 2. Характеристика проблем и направлений аудита региональной информационной безопасности	2	4	1	1	1	ПК-1
Раздел (модуль) 2. Организация комплексного аудита информационной безопасности региональных объектов						
Тема 3. Нормативно-правовая база комплексного аудита информационной безопасности объектов региона	4	6	1	1	1	ПК-3
Тема 4. Методика комплексного аудита информационной безопасности объектов управления регионом	4	6	2	0.5	0.5	ПК-3
Тема 5. Лицензирование деятельности объектов и сертификация систем защиты в области региональной информационной безопасности	4	4	3	0.5	0.5	ПК-1,3
Итого:	**16**	**16**	**8**	**4**	**4**	

4.2. Содержание тем дисциплины

Тема 1. Основные положения по комплексному аудиту информационной безопасности

Предмет и задачи курса. Значение и место курса в подготовке магистров по информационной безопасности. Взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения контрольных мероприятий. Формы проверки знаний. Состав и методика самостоятельной работы студентов по изучению дисциплины.

Знания, умения, навыки и компетенции, которые должны быть получены студентами в результате изучения курса. Рекомендованная научная и учебная литература.

Определение, цели и задачи, возлагаемые на комплексный аудит информационной безопасности (ИБ) объектов региона. Привлекаемые силы для проведения регионального комплексного аудита ИБ. Сущность и этапы проведения комплексного аудита ИБ.

Тема 2. Характеристика направлений и проблемы комплексного аудита региональной информационной безопасности

Виды и характеристика основных направлений регионального комплексного аудита ИБ. Аудит ИБ исполнительных органов государственной власти и органов местного самоуправления субъектов региона, объектов финансовой и промышленной сферы, социальных объектов (с государственной и частной формой собственности) и других сфер.

Концептуальная модель комплексного аудита ИБ. Основные компоненты модели комплексного аудита (объекты, цели, масштабы, исполнители, требования, методы, алгоритмы).

Мониторинг информационной безопасности важнейших объектов региона как проблема дальнейшего развития процесса комплексного аудита.

Тема 3. Нормативно-правовая база комплексного аудита информационной безопасности органов управления регионом

Существующая система нормативно-правовых документов комплексного аудита в области информационной безопасности: законы РФ и подзаконные акты; постановления правительства РФ; руководящие документы ФСТЭК; Государственные и отраслевые стандарты; ведомственные приказы и распоряжения; лицензии и сертификаты.

Руководящие и нормативно-методические документы в области аудита информационной безопасности.

Государственные стандарты РФ в сфере обеспечения ИБ.

Тема 4. Методика комплексного аудита информационной безопасности объектов управления регионом

Назначение и цели комплексного аудита ИБ исполнительных органов государственной власти и органов местного самоуправления субъектов РФ.

Планирование и организация работ по комплексному аудиту ИБ. Этапы планирования аудита ИБ и их характеристика. План проведения аудита.

Существующие практические подходы проведения аудита ИБ: определения базового уровня обеспечения ИБ с жесткими и гибкими требованиями; активный аудит с целью выявления уязвимых мест (нарушений); по требованиям международных стандартов.

Базовая процедура комплексного аудита ИБ по требованиям СТР-К (ФСТЭК РФ): содержание, последовательность, отчетные документы и возможные результату аудита.

Тема 5. Лицензирование деятельности объектов и сертификация систем защиты в области региональной информационной безопасности

Общие положения по лицензированию и сертификации деятельности в области ИБ (региональный уровень). Правовая основа системы лицензирования, сертификации и аттестации объектов информатизации в РФ.

Характеристика процесса лицензирования деятельности организаций региона в области ИБ.

Понятие и содержание сертификации средств защиты информации на объектах ИБ региона.

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 проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Структура фонда оценочных средств проведения промежуточной аттестации обучающихся по дисциплине «Комплексная проверка информационной безопасности» приведена в Прил. 1. к настоящей РП.

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

Основная литература:

1. Основы управления информационной безопасностью. Учебное пособие для вузов/ А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия - Телеком, 2012.
2. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.

3. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.
4. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.
5. .Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Управление рисками информационной безопасности. Учебное пособие для вузов / Н. Г. Милославская. М. 10. Сенаторов, А. И. Толстой. - М: Горячая линия-Телеком, 2012.
2. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия-Телеком, 2012.
3. Анисимов А.А. Менеджмент в сфере информационной безопасности; Учебное пособие.- М.: БИНОМ. Лаборатория знаний,2012.
4. .Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.

8. 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. http://informika.ru/ – образовательный портал.
3. http://www.academy.it.ru/ – академия АЙТИ.
4. http://www.iso27000.ru/ - портал по управлению информационной безопасностью.
5. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2.

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

- **Перечень программного обеспечения: MS Office.**

- **Информационные справочные системы:**

1. Справочно-правовая система «Консультант плюс».
2. Электронные ресурсы образовательной среды Университета.

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;
- 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 университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети.

Задание.

ЗАДАНИЕ №1

«Федеральный закон

от 26 июля 2017 года №187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации»

Цель работы: Изучить нормативный акт в соответствии с содержанием

Представить отчетный материал.
Продолжительность занятия: 4 часа

ЗАДАНИЕ № 2

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 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 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.

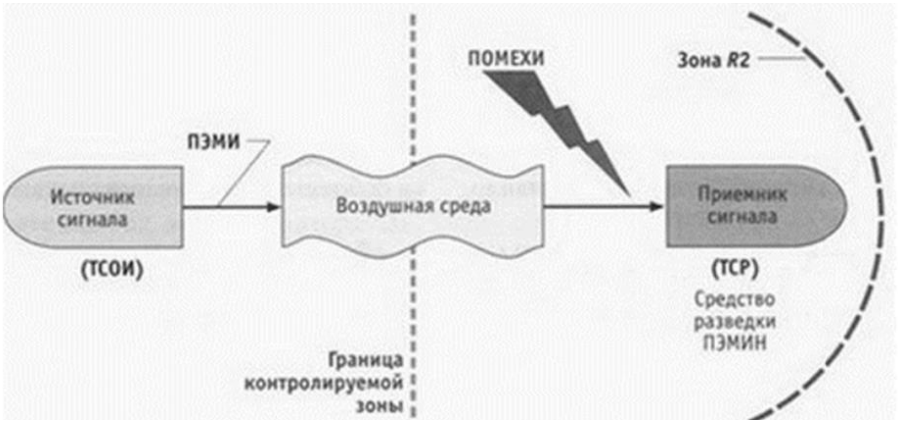


Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

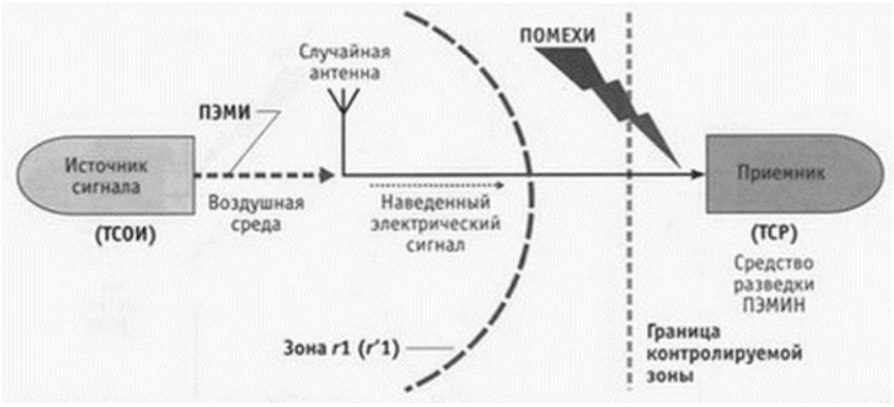


Рисунок 2. Схема ТКУИ за счет ПЭМИН

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 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 № 3

Тема: Определение ПЭМИ на примере информативного сигнала видеотракта

Цель работы.

Изучение теоретической основы измерений ПЭМИ на примере показателей информативного сигнала видеотракта. Изучение основных аспектов проведения специальных исследований.

Продолжительность занятия: полтора учебных часа.

Задания.

4. Изучить теоретическую часть Задания №3.
5. Выполнить практическую часть Задания №3:
   а) ответить на вопросы для самопроверки;
   б) выполнить практические задания.
6. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Одним из основных и, зачастую, самых мощных источников сигналов ПЭМИ является видеотракт. Конечно сигнал, который нас интересует, это сигнал интерфейса передачи видеосигнала, но все устройства видеотракта, включающие видеоконтроллер, соединительные кабели, KVM коммутаторы (для систем с несколькими устройствами отображения информации) и конечные устройства отображения (мониторы, прокторы, телевизоры) существенно влияют на уровень сигнала и направление его излучения, потому как выступают в качестве антенн.

Приведем список наиболее популярных видео-интерфейсов: аналоговый:

- VGA (несмотря на широкое развитие современных цифровых

интерфейсов имеет широкое распространение и еще долгое время будет эксплуатироваться на большинстве АС);

цифровые:

- DVI (бывает совмещен с VGA и применяются переходники VGADVI, в таком случае рассматривается как VGA);
- HDMI;
- DisplayPort.

Немного забегая вперед, для анализа интерфейса рассмотрим один из способов определения частот сигналов ПЭМИ – непосредственное подключение к линии передачи сигнала, путем использования специального

кабеля с выводами для подключения. Рассмотрение будем вести на примере VGA интерфейса в силу простоты сигнала, схожего с телевизионным, а также стабильности и понятности задания тестового режима. Не имеет значения к какому из проводов, передающих цвет (R, G или B) подключаться, так как при формировании тестового режима, обеспечивающего максимальную частоту следования импульсов, на экран монитора выводится статическая засветка пиксель белый, пиксель черный, пиксель белый и т. д. При формировании белой точки сигнал присутствует в проводе каждого из цветов (рис. 1).

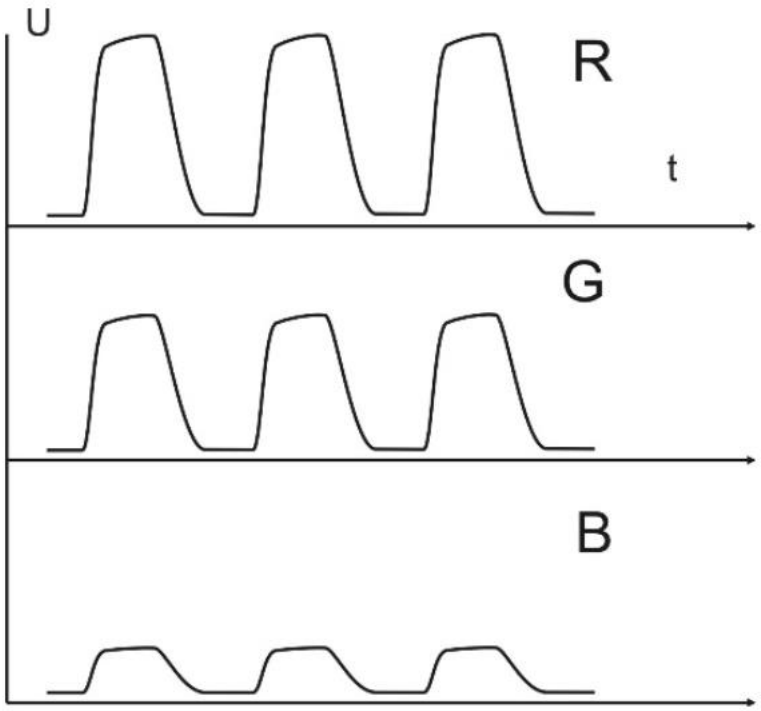
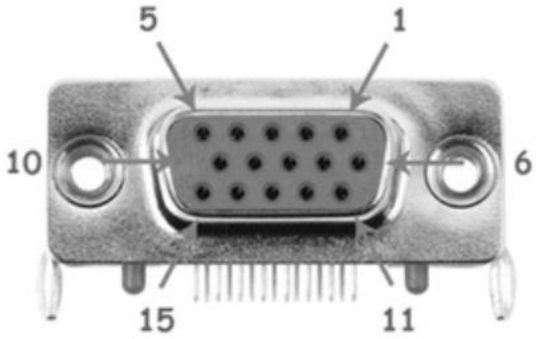


Рисунок 1. Осциллограммы сигналов в RGB интерфейсе

Распиновка разъема VGA информационного кабеля приведена на (рис. 2)



№	Наименование	Описание
1	RED	Красный сигнал
2	GREEN	Зеленый сигнал
3	BLUE	Синий сигнал
4	n/c	Не используется
5	GND	Земля
6	RED_RTN	Красный земля
7	GREEN_RTN	Зеленый земля
8	BLUE_RTN	Синий земля
9	VDC	+5В
10	GND	Земля
11	ID0	Идентификатор монитора
12	SDA	DDC / I2C data
13	HSYNC	Горизонтальная синхронизация
14	VSYNC	Вертикальная синхронизация
15	SCL	DDC / I2C clock

Рисунок 2. Распиновка разъема информационного кабеля VGA интерфейса

Кабель для данного вида исследований изготавливается специально и используется исключительно для определения частот сигналов ПЭМИ VGA интерфейса, измерения необходимо строго производить именно с тем кабелем, с которым будет эксплуатироваться АС. Структура сигнала представляется следующим образом.

С кадровой частотой (например, 60 Гц) следуют «пачки» импульсов, формирующих каждый кадр на экране монитора (рис. 3).

Кадровые «пачки» импульсов состоят в свою очередь из строчных последовательностей импульсов, каждая из которых задает сигнал для формирования строки на экране монитора (частота следования при разрешении 1024 × 768 в 768 чаще, чем кадровая, то есть около 46 кГц, рис. 4).

Строчные «пачки» импульсов состоят уже непосредственно из импульсов с переходами из 0 в 1, соответствующим тестовому режиму (пиксель белый, пиксель черный и т. д.).

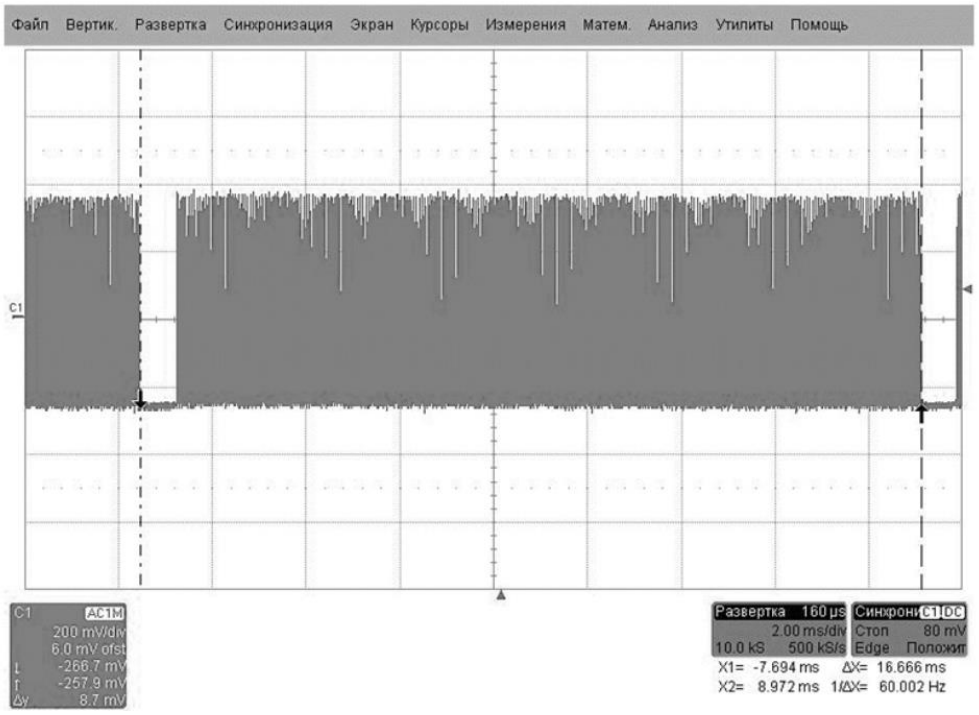


Рисунок 3. Кадровые видеоимпульсы

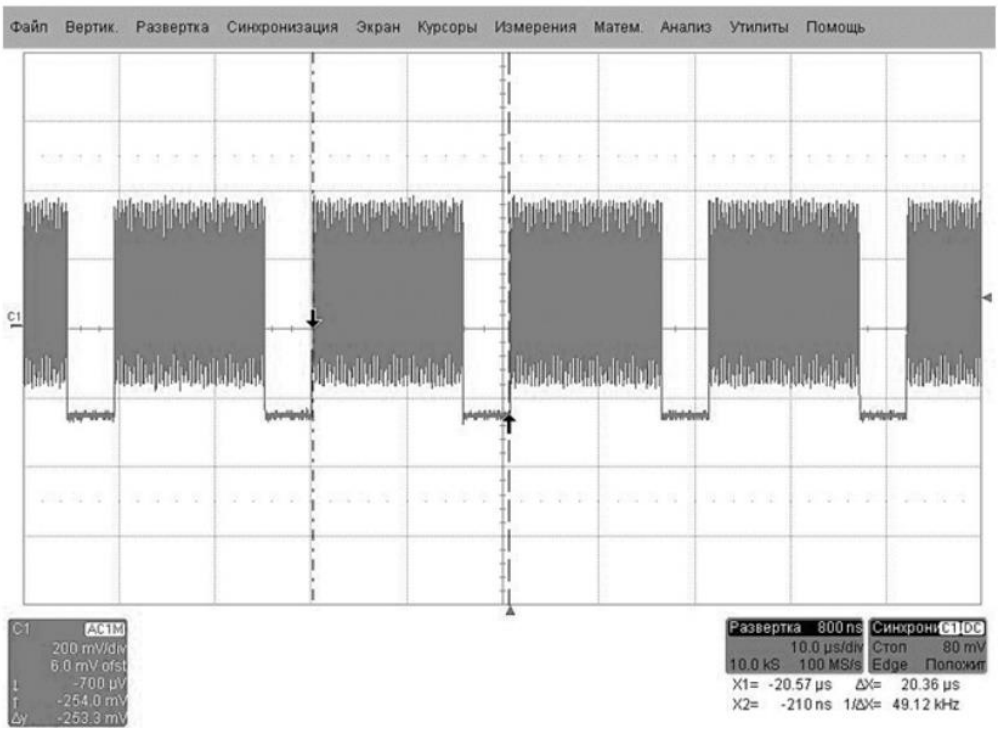


Рисунок 4. «Пачки» строчных видеоимпульсов

В результате, частота следования импульсов, задающих черные и белые пиксели и будет тактовой частотой (частотой первой гармоники) нашего сигнала ПЭМИ от видеотракта (в данном случае 32,5 МГц, можно также для уточнения применять режим БПФ). Следует отметить, что подобные кабели (с отводами для подключения осциллографа) используются только на этапе анализа сигналов, при измерениях необходимо в обязательном порядке применять кабели, с которыми в дальнейшем будет эксплуатироваться данная АС.

Сложнее дело обстоит с цифровыми видео интерфейсами, например, DVI, в основе которого лежит технология TMDS. Суть данной технологии заключается в том, что на каждый цвет приходится по две пары. Воздействие возможных помех будет производиться одинаково на оба провода, а, следовательно, их можно будет легко отфильтровать. Также в интерфейсе применяется технология минимизации количества переходов из «0» в «1» (и наоборот), что также сказывается на помехозащищенности интерфейса.

К сожалению, все это усложняет задачу для формирования тестового сигнала, который, наоборот, должен обеспечивать максимальную частоту следования импульсов в канале. У протокола TMDS есть одна особенность. Если длительное время передается сплошной поток «1», то в силу того, что кабель обладает определенной емкостью, спад уровня с «1» до «0» может произойти с задержкой, следовательно, произойдет потеря пакетов. Для того чтобы этого избежать, в таких ситуациях, протокол TMDS в конце каждых 8 битов добавляет бит DC-Balancing, который указывает на что, что следующие 8 битов будут инвертированы. В результате получаем последовательность импульсов с постоянными и стабильными переходами. Тактовая частота первой гармоники DVI интерфейса при данном тестовом режиме и стандартных разрешениях не выше 1600 × 1280 × 60 Гц лежит в пределах 130...170 МГц.

Интерфейсы HDMI и DisplayPort строятся также с применением технологии TMDS, но с увеличением скорости передачи данных, способ задания тестового режима остается такой же, только тактовые частоты будут гораздо выше, возможно даже за пределами исследуемого нами диапазона частот.

Практическая часть.

Вопросы для самопроверки:

1) Что такое видеоинтерфейс?
2) Какие интерфейсы есть у информационного кабеля для видео? Перечислите.
3) Чем отличаются кадровые «пачки» импульсов от строчных?
4) Какая частота приемлема для видео с интерфейсом VGA?
5) С каким видеоинтерфейсом больше всего возникает проблем при измерении?

Практические задания:

1) На Ваш взгляд, что нужно сделать при проведении измерений видеосигнала? Опишите начало измерений от получения технического средства для проведения исследований до передачи его обратно в комплект поставки. Для данного задания можете попросить помощи у Вашего преподавателя.
2) Как Вы считаете, что такое меандр информативного сигнала? Опишите это явление на примере информативного сигнала монитора с интерфейсом VGA.

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

ОСНОВЫ УПРАВЛЕНИЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТЬЮ

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 компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.	Тема:1-4	ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем	ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.	ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.
2.	ПК-3	Способен осуществлять анализ и систематизацию научно-технической	Тема:2,4	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулирова	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной

		информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.		развития, области научного знания и рынка труда. ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.	ть темы НИР и оказывать методическую помощь в их выполнении.	деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	***Инструменты, оценивающие сформированность компетенции***	***Этапы и показатель оценивания компетенции***	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
ПК-1,3	***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.***
ПК-1,3	Доклад	***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***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. 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 непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-1,3	Контрольная работа	***А) полностью сформирована (компетенция освоена***	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 -

		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***	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.
ПК-1,3	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	Например: 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 форме презентаций:

1. Нормативно-методологические основы комплексного аудита информационной безопасности.
2. Базовые положения по комплексному аудиту информационной безопасности предприятий (учреждений, организаций) региона.
3. Привлекаемые силы к проведению комплексного аудита ИБ объектов региона.
4. Принципы организации и методы проведения комплексного аудита ИБ.
5. Содержание комплексного аудита ИБ для выделенных помещений.
6. Основные этапы комплексного аудита ИБ объектов региона.
7. Подготовка к проведению комплексного аудита ИБ объектов региона.
8. Непосредственное проведению комплексного аудита ИБ объектов региона.
9. Оформление результатов проведения комплексного аудита ИБ объектов региона.
10. Основные направления проведения комплексного аудита ИБ объектов региона (общая характеристика).
11. Аттестация объектов информатизации по требованиям ИБ как направление комплексного аудита ИБ объектов региона.
12. Контроль защищенности информации ограниченного доступа как направление комплексного аудита ИБ объектов региона.
13. Спецобследование выделенных помещений как направление комплексного аудита ИБ объектов региона.
14. Спецобследование объектов вычислительной техники как направление комплексного аудита ИБ объектов региона.

15. Проектирование объектов в защищенном исполнении как направление комплексного аудита ИБ объектов региона.

16. Поставка, установка и наладка технических средств обработки и защиты информации как направление комплексного аудита ИБ объектов региона.

17. Организация комплексного аудита ИБ объектов региона.

18. Технические средства и системы комплексного аудита ИБ объектов региона.

19. Концептуальная модель комплексного аудита ИБ объектов региона.

20. Подготовка специалистов-аудиторов по комплексному аудиту ИБ объектов региона.

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

Формой контроля знаний по дисциплине «Основы управления корпоративной информационной безопасностью» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

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	тестирование	ПК-1 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51%***

						правильных ответов. Хорошо - от 70%. Отлично – от 90%
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1 ПК-3	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установленные графиком образовательного процесса	Зачет	ПК-1 ПК-3	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	***Критерии оценки:*** ***«Зачтено»:*** ***знание основных понятий предмета;*** ***умение использовать и применять полученные знания на практике;*** ***работа на семинарских занятиях;*** ***знание основных научных теорий, изучаемых предметов;*** ***ответ на вопросы билета.*** ***«Не зачтено»:*** ***демонстрирует частичные знания по темам дисциплин;*** ***незнание***

						основных понятий предмета; неумение использовать и применять полученные знания на практике; не работал на семинарских занятиях; не отвечает на вопросы.

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.

Типовые вопросы, выносимые на тестирование

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

1. Аудит информационной безопасности – это:

   оценка текущего состояния системы информационной безопасности

   проверка используемых компанией информационных систем, систем безопасности

   это проверка способности успешно противостоять угрозам

   специальная проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам

2. Анализ рисков включает в себя:

   набор адекватных контрмер осуществляется в ходе управления рисками

   анализ причинения ущерба и величины ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности

   выявление существующих рисков и оценку их величины

мероприятия по обследованию безопасности ИС, с целью определения того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите

3. Активный аудит – это:

   исследование средств для определения соответствия их решениям задач информационной безопасности

   исследование состояние системы сетевой защиты, использование которой помогает хакеру проникнуть в сети и нанести урон компании

   исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий).

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

5. Дублирование сообщений является угрозой:
   доступности
   конфиденциальности
   целостности

6. Самыми опасными источниками внутренних угроз являются:
   некомпетентные руководители
   обиженные сотрудники
   любопытные администраторы

7. Для внедрения бомб чаще всего используются ошибки типа:
   отсутствие проверок кодов возврата
   переполнение буфера
   нарушение целостности транзакций

8. 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

9. В число целей программы безопасности верхнего уровня входят:
   управление рисками

определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности

10. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование
повседневное администрирование
отслеживание слабых мест защиты

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

12. 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 +

Типовые вопросы, выносимые на звчет

1. Определение, цели и задачи, возлагаемые на комплексный аудит информационной безопасности (ИБ) объектов региона.

2. Привлекаемые силы для проведения регионального комплексного аудита ИБ.

3. Сущность и этапы проведения комплексного аудита ИБ.

4. Виды и характеристика основных направлений регионального комплексного аудита ИБ.

5. Аудит ИБ исполнительных органов государственной власти и органов местного самоуправления субъектов региона.

6. Концептуальная модель комплексного аудита ИБ. Основные компоненты модели комплексного аудита ИБ (объекты, цели, масштабы, исполнители, требования, методы, алгоритмы).

7. Мониторинг информационной безопасности важнейших объектов региона как проблема дальнейшего развития процесса комплексного аудита.

8. Существующая система нормативно-правовых документов комплексного аудита в области информационной безопасности: законы РФ и подзаконные акты; постановления правительства РФ.

9. Существующая система нормативно-правовых документов комплексного аудита в области информационной безопасности: руководящие документы ФСТЭК.

10. Существующая система нормативно-правовых документов комплексного аудита в области информационной безопасности: государственные и отраслевые стандарты.

11. Существующая система нормативно-правовых документов комплексного аудита в области информационной безопасности: ведомственные приказы и распоряжения; лицензии и сертификаты.

12. Руководящие и нормативно-методические документы в области аудита информационной безопасности: Государственные стандарты РФ в сфере обеспечения ИБ.

13. Нормативно-методические документы в области аудита информационной безопасности: международные стандарты в сфере обеспечения ИБ.

14. Назначение и цели комплексного аудита ИБ исполнительных органов государственной власти и органов местного самоуправления субъектов РФ.

15. Планирование и организация работ по комплексному аудиту ИБ.

16. Этапы планирования комплексного аудита ИБ и их характеристика.

17. План проведения комплексного аудита ИБ.

18. Существующие практические подходы проведения аудита ИБ: определения базового уровня обеспечения ИБ с жесткими и гибкими требованиями.

19. Существующие практические подходы проведения аудита ИБ: активный аудит с целью выявления уязвимых мест (нарушений).

20. Существующие практические подходы проведения аудита ИБ: по требованиям международных стандартов.

21. Базовая процедура комплексного аудита ИБ по требованиям СТР-К (ФСТЭК РФ): содержание аудита.

22. Базовая процедура комплексного аудита ИБ по требованиям СТР-К (ФСТЭК РФ): последовательность проведения аудита.

23. Базовая процедура комплексного аудита ИБ по требованиям СТР-К (ФСТЭК РФ): отчетные документы и возможные результату аудита.

25. Общие положения по лицензированию деятельности в области ИБ (региональный уровень).

26. Общие положения по сертификации систем и средств в области ИБ

27. Правовая основа системы лицензирования деятельности в области ИБ.

28. Правовая основа системы сертификации и аттестации объектов информатизации в РФ.

29. Характеристика процесса лицензирования деятельности в области ИБ организаций региона

30. Понятие и содержание сертификации средств защиты информации на объектах ИБ региона.

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ ОСНОВЫ УПРАВЛЕНИЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цели дисциплины:

1. Формирование у обучаемых специализированной базы знаний по основным понятиям и умениям в области регионального комплексного аудита информационной безопасности;

2. Формирование организационно-технических навыков проведения комплексного аудита информационной безопасности в регионе (по базовым направлениям и типовым информационным объектам).

Задачи дисциплины:

- раскрытие сущности, целей и содержание комплексного аудита информационной безопасности;
- выявление общих методологических основ комплексного аудита информационной безопасности региона;
- изучение нормативно-правовой базы комплексного аудита информационной безопасности типовых объектов региона;
- освоение методики комплексного аудита информационной безопасности (исполнительных органов государственной власти и органов местного самоуправления) региона;
- раскрытие основных положений по лицензированию деятельности по информационной безопасности организационных структур региона;
- изучение основ организации лицензирования деятельности, сертификации средств и систем информационной безопасности в регионе.

2. Указания по проведению практических (семинарских) занятий

Практическое занятие 1.

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

Образовательные технологии: *беседа*.

Тема: **Основные положения по комплексному аудиту информационной безопасности**

Практическое занятие 1

Учебные вопросы

1. Формулирование (определение) цели и обоснование задач, возлагаемых на комплексный аудит информационной безопасности (ИБ) типовых объектов региона.

2. Определение привлекаемые силы для проведения регионального комплексного аудита ИБ для типовых информационных объектов.

3. Обоснование содержания и этапов проведения комплексного аудита ИБ для типовых объектов региона.

4. Разработка плана проведения регионального комплексного аудита ИБ в финансовой (кредитно-финансовой и банковской) сфере.

Продолжительность занятия – ***3 ч.***

Практическое занятие 2.

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

Образовательные технологии: *групповая дискуссия.*

Тема: **Характеристика направлений и проблемы комплексного аудита региональной информационной безопасности**

Учебные вопросы

1. Критический анализ основных направлений регионального комплексного аудита ИБ.

2. Постановка задач на проведение аудита ИБ исполнительных органов государственной власти и органов местного самоуправления субъектов региона, объектов финансовой и промышленной сферы, социальных объектов (с государственной и частной формой собственности) и других сфер.

3. Моделирование комплексного аудита ИБ. Основные компоненты модели комплексного аудита (объекты, цели, масштабы, исполнители, требования, методы, алгоритмы).

4. Организация мониторинга информационной безопасности важнейших объектов региона как проблема дальнейшего развития процесса комплексного аудита

Продолжительность занятия – 3 ***ч.***

Практическое занятие 3.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *практическая работа в группах*.
Тема: **Нормативно-правовая база комплексного аудита информационной безопасности объектов региона**
Учебные вопросы

1. Анализ системы нормативно-правовых документов комплексного аудита в области информационной безопасности: законы РФ и подзаконные акты; постановления правительства РФ.

2. Критический анализ существующей система нормативно-правовых документов комплексного аудита в области информационной безопасности: руководящие документы ФСТЭК; Государственные и отраслевые стандарты; ведомственные приказы и распоряжения; лицензии и сертификаты.

3. Анализ нормативно-правовых документов по комплексному аудиту в области информационной безопасности: зарубежные и государственные стандарты РФ.

Продолжительность занятия – 3 ***ч.***

Практическое занятие 4.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии**:** ***групповая дискуссия.***
Тема: **Методика комплексного аудита информационной безопасности объектов управления регионом**

Форма занятия (интерактивная): групповой разбор конкретной ситуации.

Учебные вопросы

1. Формулирование назначения и цели комплексного аудита ИБ исполнительных органов государственной власти и органов местного самоуправления субъектов РФ.

2. Планирование и организация работ по комплексному аудиту ИБ. Этапы планирования аудита ИБ и их характеристика. План проведения аудита.

3. Анализ существующих практических подходов проведения аудита ИБ: определения базового уровня обеспечения ИБ с жесткими и гибкими требованиями; активный аудит с целью выявления уязвимых мест (нарушений); по требованиям международных стандартов.

4. Критический анализ базовой процедуры комплексного аудита ИБ по требованиям СТР-К (ФСТЭК РФ): содержание, последовательность, отчетные документы и возможные результату аудита.

Продолжительность занятия – 3 ***ч.***

Практическое занятие 5.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *беседа.*
Тема: **Лицензирование деятельности объектов и сертификация систем защиты в области региональной информационной безопасности**

Форма занятия (интерактивная): групповой разбор конкретной ситуации.

Учебные вопросы

1. Определения порядка лицензирования и сертификации деятельности в области ИБ (региональный уровень).

2. Обоснование правовой основа системы лицензирования, сертификации и аттестации объектов информатизации в РФ.

3. Целесообразный алгоритм процесса лицензирования деятельности организаций региона в области ИБ.

4. Целесообразный алгоритм процесс сертификации средств защиты информации на объектах ИБ региона.

Продолжительность занятия – 4 ***ч.***

3. Указания по проведению лабораторных работ.

Цель проведения лабораторных работ – ознакомление обучаемых:

- с методами и способами управления информационной безопасностью региона;
- с принципами построения системы управления информационной безопасности (СУИБ);
- с современными подходами к управлению информационной безопасностью (ИБ) региональных информационных объектов и направления их развития.

Задачи выполнения лабораторных работ:

- формирование основ подготовки магистров в области управления информационной безопасностью объектов региона;
- формирование подходов к выполнению самостоятельных исследований магистрами в области управления информационной безопасностью объектов региона, в частности, криптографических методов защиты информации в компьютерных системах и сетях.

Методика проведения лабораторных работ определяется моделью решаемых задач по управлению безопасностью региональными информационными объектами, исследуемых обучаемыми на занятии по заданию преподавателя.

Средства выполнения лабораторных работ:

- 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: **Основы оценки эффективности управления информационной безопасностью**

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем и технологий «Альт – Инвест» 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 за щищённости региональных объектов.

2. Запустить программу «Альт – Инвест» 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. Предложить рекомендации по управлению информационной безопасностью рассматриваемых объектов

9. Создать отчёт по лабораторной работе и сформулировать выводы.

Продолжительность практического занятия-2часа

Лабораторная работа 2.

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 – 2 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-2часа

Лабораторная работа 3.

Тема . Политика информационной безопасности отдельных региональных структур (объектов, процессов)

Понятие политики обеспечения информационной безопасности региона и политики информационной безопасности организаций (учреждений и предприятий). Причина выработки политики информационной безопасности. Основные требования и принципы, учитываемые при разработке и внедрении информационной безопасности. Содержание корпоративной и частных политик информационной безопасности.

Жизненный цикл политик информационной безопасности: разработка; внедрение; применение и аннулирование. Ответственность за исполнение политики информационной безопасности.

Продолжительность практического занятия-4часа

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих региональных проблем по обеспечению информационной безопасности;

2) привить навыки самостоятельного решения нестандартных исследовательских задач в области информационной безопасности региона.

Примерные темы докладов

1. Основные направления деятельности в области аудита безопасности информации.
2. Активный аудит ИБ.
3. Экспертный аудит ИБ,
4. Аудит ИБ на соответствие стандартам.
5. Аудит выделенных помещений.
6. Оценивание результатов аудита и самооценки информационной безопасности.
7. Риск - ориентированная интерпретация полученных оценок информационной безопасности.
8. Особенности аудита информационной безопасности организаций банковской системы Российской Федерации.
9. Аудит управления непрерывностью бизнеса и восстановления после сбоев информационных систием.
10. Особенности аудита информационной безопасности организаций, использующих аутсорсинг.
11. Этапы непосредственного проведения аудита ИБ.
12. Аудит ИБ федеральных информационных систем.
13. Самооценка безопасности для систем информационных технологий.
14. Метрики безопасности для систем информационных технологий.
15. Отечественные законы и стандарты по основам аудита ИБ.

4. Указания по проведению самостоятельной работы студентов

№ п/п	*Наименование блока (раздела) дисциплины*	*Виды СРС*
		4 семестр
1	Тема 1. Основные положения по комплексному аудиту информационной безопасности	***Создание доклада с презентацией.*** 1. Основные направления деятельности в области аудита безопасности информации. 2. Активный аудит ИБ. 3. Экспертный аудит ИБ, ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***
2	Тема 2. Характеристика направлений и проблемы комплексного аудита региональной информационной безопасности	***Создание доклада с презентацией.*** *Примерная тематика работы:* 4. Аудит ИБ на соответствие стандартам. 5. Аудит выделенных помещений. 6. Оценивание результатов аудита и самооценки информационной безопасности.
3	Тема 3. Нормативно-правовая база комплексного аудита информационной безопасности органов управления регионом	***Создание доклада с презентацией.*** 7. Риск - ориентированная интерпретация полученных оценок информационной безопасности. 8. Особенности аудита информационной безопасности организаций банковской системы Российской Федерации. 9. Аудит управления непрерывностью бизнеса и восстановления после сбоев информационных систем. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***
4	Тема 4. Методика комплексного аудита информационной безопасности объектов управления регионом	***Создание доклада с презентацией.*** 12. Аудит ИБ федеральных информационных систем. 13. Самооценка безопасности для систем информационных технологий. 14. Метрики безопасности для систем информационных технологий. 15. Отечественные законы и стандарты по основам аудита ИБ. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

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 исследования 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.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению.

Объём контрольной работы – … страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

Тематика контрольных работ

1. Нормативно-методологические основы комплексного аудита информационной безопасности.
2. Базовые положения по комплексному аудиту информационной безопасности предприятий (учреждений, организаций) региона.
3. Привлекаемые силы к проведению комплексного аудита ИБ объектов региона.
4. Принципы организации и методы проведения комплексного аудита ИБ.
5. Содержание комплексного аудита ИБ для выделенных помещений.
6. Основные этапы комплексного аудита ИБ объектов региона.

7. Подготовка к проведению комплексного аудита ИБ объектов региона.

8. Непосредственное проведению комплексного аудита ИБ объектов региона.

9. Оформление результатов проведения комплексного аудита ИБ объектов региона.

10. Основные направления проведения комплексного аудита ИБ объектов региона (общая характеристика).

11. Аттестация объектов информатизации по требованиям ИБ как направление комплексного аудита ИБ объектов региона.

12. Контроль защищенности информации ограниченного доступа как направление комплексного аудита ИБ объектов региона.

13. Спецобследование выделенных помещений как направление комплексного аудита ИБ объектов региона.

14. Спецобследование объектов вычислительной техники как направление комплексного аудита ИБ объектов региона.

15. Проектирование объектов в защищенном исполнении как направление комплексного аудита ИБ объектов региона.

16. Поставка, установка и наладка технических средств обработки и защиты информации как направление комплексного аудита ИБ объектов региона.

17. Организация комплексного аудита ИБ объектов региона.

18. Технические средства и системы комплексного аудита ИБ объектов региона.

19. Концептуальная модель комплексного аудита ИБ объектов региона.

20. Подготовка специалистов-аудиторов по комплексному аудиту ИБ объектов региона.

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

Основная литература:

1. Основы управления информационной безопасностью. Учебное пособие для вузов/ А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия - Телеком, 2012.
2. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.
3. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.
4. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.
5. .Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Управление рисками информационной безопасности. Учебное пособие для вузов / Н. Г. Милославская. М. 10. Сенаторов, А. И. Толстой. - М: Горячая линия-Телеком, 2012.
2. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия-Телеком, 2012.
3. Анисимов А.А. Менеджмент в сфере информационной безопасности; Учебное пособие.- М.: БИНОМ. Лаборатория знаний,2012.
4. .Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.

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. **http://informika.ru/ – образовательный портал.**
3. **www.wikIsec.ru - Энциклопедия информационной безопасности.**

Публикации, статьи.

4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. **http://www.academy.it.ru/ – академия АЙТИ.**
7. **http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации**
8. **http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.**
9. **http://www.fsb.ru/ - Официальный сайт Федеральной службы Безопасности**
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Университета;
2. Информационные системы (консультант+; Гарант)