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)

Б.1.О.06 «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТЬЮ»

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: Соляной В.Н. Рабочая программа дисциплины (модуля): Управление информационной безопасностью. – Королев МО: «Технологический Университет», 2023

Рецензент: **Сухотерин А.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.			

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

Целью изучения дисциплины является:

1. Дать студентам концептуальные знания основ управления информационной безопасностью для региональных информационных объектов с учетом современных требований теории по защите информации;
2. Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий менеджмента информационной безопасности на типовых региональных информационных объектах с учетом современных международных и отечественных стандартов.

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

Универсальные компетенции:

- УК-2: Способен управлять проектом на всех этапах его жизненного цикла.
- ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

Основными **задачами** дисциплины являются:

- Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- УК-2.3 Формулирует, на основе поставленной проблемы проектную задачу и способы ее решения через реализацию проектного управления, разрабатывает и реализует проекты.
- 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-2.2. Разрабатывает тактико-технические требования, техническое задание по реализации проекта в рамках обозначенной проблемы, определяет целевые этапы, основные направления работ, объясняет цели и формулирует задачи, связанные с подготовкой и реализацией проекта.

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

Необходимые знания:

- УК-2.1. Разрабатывает план реализации проекта с использованием инструментов планирования и управляет проектом, оценивает потребности в ресурсах, осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта и оценивает эффективность проекта.
- 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 в структуре ОПОП ВО

Дисциплина «Управление информационной безопасностью» Б1.О.06 относится к обязательной части блока 1 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“, “ Информационная безопасность автоматизированных систем” и на дисциплинах, изученных ранее в магистратуре: “Экономика и управление”, “Защищенные информационные системы”, «Теория игр и исследование операций», «Теоретические основы компьютерной безопасности» и компетенции УК-1, 2; ОПК-1, 3,5; ПК-2;3.

Знания и компетенции, полученные при освоении дисциплины «Управление информационной безопасностью», являются базовыми при дальнейшем изучении всех дисциплин профессионального цикла (обязательной и вариативной частей) прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 3 зачетных единицы, 108 часов.

Таблица1

Виды занятий	Всего часов	Семестр 3	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**72**	**72**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**38**	**38**			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	8	8			
Лабораторные работы (ЛР)	8	8			
Другие виды контактной работы	**6**	**6**			
Практическая подготовка	**4**	**4**			
Самостоятельная работа	**34**	**34**			
Курсовые работы (проекты)	**-**	**-**			
Расчетно-графические работы	**-**	**-**			
Контрольная работа, домашнее задание	**+**	**+**			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	-	-			
Вид итогового контроля	Зачет с оценкой	Зачет с оценкой			

* 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. Очное	Практические занятия, час Очное	Лабораторные работы	Практическая подготовка	Занятия в интерактивной форме, час	Код компетенций
Седьмой семестр Раздел 1. Концептуально-теоретические основы управления информационной безопасностью						
Тема 1. Базовые основы процессов и систем управления информационной безопасностью	4	2	2	1	1	УК-2
Тема 2. Политика информационной безопасности региона и отдельных региональных структур (объектов, процессов)	4	2	2	1	1	УК-2
Раздел 2. Прикладные аспекты управления информационной безопасностью						
Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью	4	2	2	1	2	УК-2 ОПК-1
Тема 4. Основы оценки эффективности управления информационной безопасностью	4	2	2	1	2	УК-2 ОПК-1
Итого:	16	8	8	4	6	

4.2. Содержание тем дисциплины

Раздел 1. Концептуально-теоретические основы управления информационной безопасностью

Тема 1. Базовые основы систем и процессов управления информационной безопасностью

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 и умения студентов, которые должны быть получены в результате изучения курса. Рекомендованная научная и учебная литература.

Характеристика базовой терминологии в области управления информационной безопасностью: сущность управления; управление как процесс; системный подход к управлению; процессный подход к управлению; циклическая модель улучшения процессов управления; системы управления информационной безопасностью.

Стандартизация систем и процессов управления информационной безопасностью: международные и российские стандарты; особенности стандартов банковской системы РФ.

Тема 2. 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.

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью

Особенности организации управления информационной безопасностью региона: корпоративных структур, отдельных организаций и их информационно- телекоммуникационных технологий.

Организация реагирования на чрезвычайные ситуации (инциденты). Управления информационными рисками. Аудит (мониторинг) состояния информационной безопасности региона. Стратегии построения и внедрения управленческих процессов и систем управления информационной безопасностью в целом.

Система управления информационной безопасностью: область действия; документальное обеспечение; политика системы управления и поддержка системы управления со стороны руководства. Основы кадрового обеспечения управления информационной безопасностью. Департамент информационной безопасности региона.

Технические аспекты управления информационной безопасностью. Администрирование информационных систем управления информационной безопасностью. Защита систем управления информационной безопасностью региона.

Страхование информационных рисков: основы методологии и рынок страховых услуг. Методические основы экономики информационной безопасности

Тема 4. Основы оценки эффективности управления информационной безопасностью

Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью: международные и российские стандарты.

Характеристики типовых процессов проверки систем управления информационной безопасности: виды проверок, мониторинг, самооценка, внутренний и внешний аудит, инструментальные средства.

Практическая оценка деятельности по управлению информационной безопасности: результативность (эффективность), метрики и измерения, модели зрелости процессов систем управления информационной безопасностью.

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины (модуля» «Управление информационной безопасностью»представлены в Приложении 2 к настоящей программе

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Управление информационной безопасностью» приведена в Приложении 1 к настоящей программе.

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

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.

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

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

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

- **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;
- 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 (спец. исследования, 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.

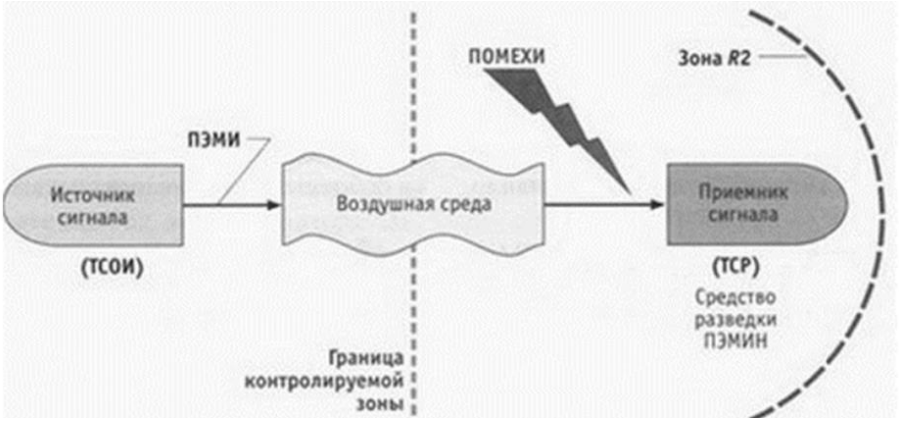


Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

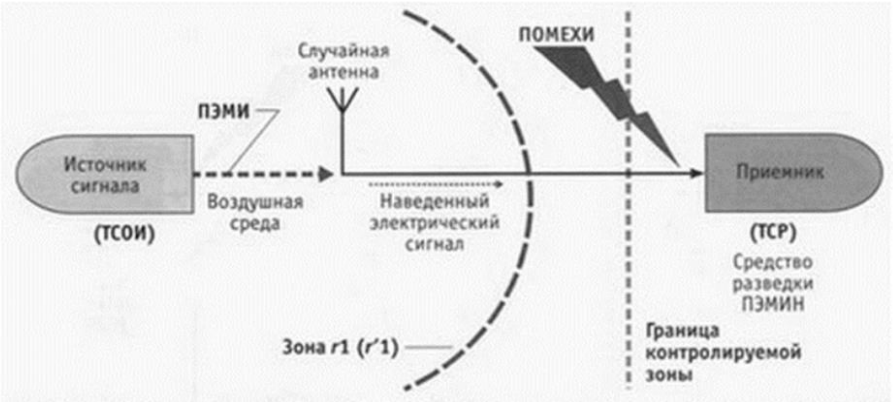


Рисунок 2. Схема ТКУИ за счет ПЭМИН

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).

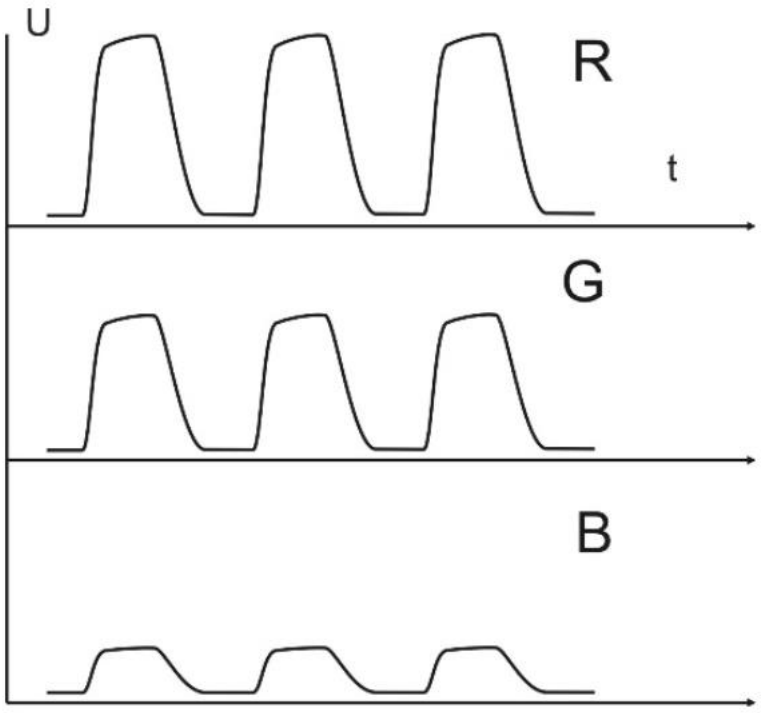
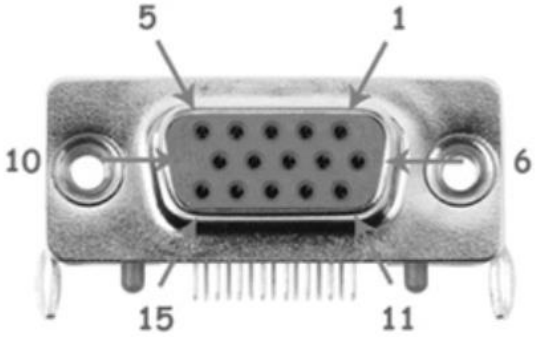


Рисунок 1. Осциллограммы сигналов в RGB интерфейсе

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.).

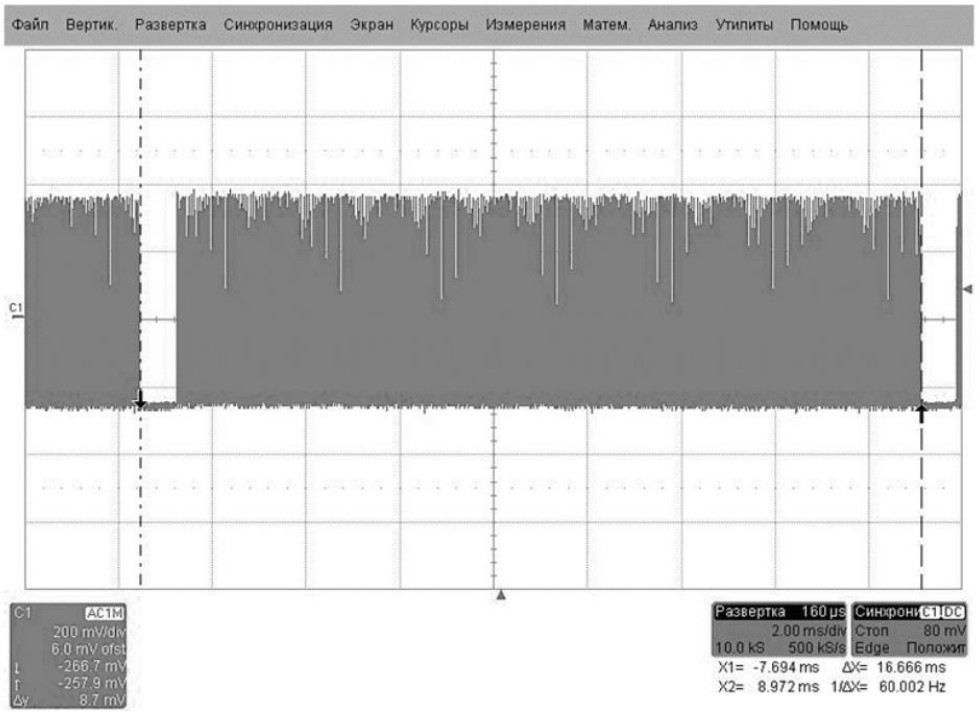


Рисунок 3. Кадровые видеоимпульсы

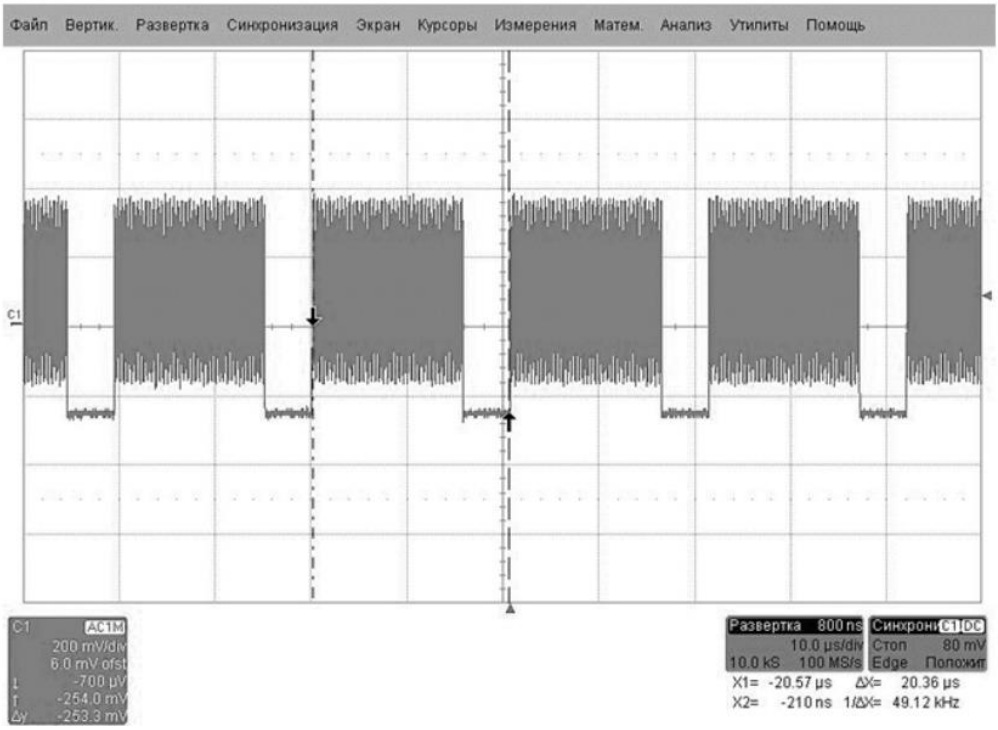


Рисунок 4. «Пачки» строчных видеоимпульсов

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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТЬЮ

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.	УК-2	Способен управлять проектом на всех этапах его жизненного цикла.	Тема:1-4	- УК-2.3 Формулирует, на основе поставленной проблемы проектную задачу и способы ее решения через реализацию проектного управления, разрабатывает и реализует проекты.	- УК-2.2. Разрабатывает тактико-технические требования, техническое задание по реализации проекта в рамках обозначенной проблемы, определяет целевые этапы, основные направления работ, объясняет цели и формулирует задачи, связанные с подготовкой и реализацией проекта.	- УК-2.1. Разрабатывает план реализации проекта с использованием инструментов планирования и управляет проектом, оценивает потребности в ресурсах, осуществляет мониторинг хода реализации проекта, корректирует отклонения, вносит дополнительные изменения в план реализации проекта и оценивает эффективность проекта.
2.	ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического	Тема:1-4	- ОПК-1.3. Использует основы отечественных и зарубежных стандартов в области обеспечения информационной	ОПК-1.2. Проектирует системы и подсистемы ИБ с учетом современных безопасных инструментальных технологий.	- ОПК-1.1. Формирует актуальные модели угроз и нарушителей для современных информационных систем, учитывает их содержание при формировании требований

		задания на ее создание.		безопасности при формировании требований технического задания на создание автоматизированных систем в защищенном исполнении.		технического задания, умеет разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности.

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***
УК—2 ОПК-1	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.
УК-2 ОПК-1	Выполнение Контрольной работы	***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. Проводится устно в форме 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-2 ОПК-1	Лабораторная работа	А) полностью сформирована (компетенция освоена на высоком уровне) – 5 баллов Б) частично сформирована: • компетенция освоена на продвинутом уровне – 4 балла; • компетенция освоена на базовом уровне – 3 балла; В) не сформирована (компетенция не сформирована) – 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. Ведущие мировые разведки и их деятельность в России.
2. Основы обеспечения безопасности информации в компьютерных системах.
3. Информационная безопасность современной России: угрозы и их отражения.
4. Информационные войны в современном мире.
2. Компьютерная преступность в экономических областях.
3. Мир XXI века: информационное противоборство.
4. Компьютерные вирусы в современных информационных системах.
5. Информационные угрозы современным экономическим объектам.
6. Информатизация России и проблема защиты информации.
7. Безопасность информации в коммерческой деятельности.

8. Разведки России – исторический аспект.
9. Мировой информационный терроризм.
10. Этика защиты информации.
11. Становление и развитие промышленного шпионажа.

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

Формой контроля знаний по дисциплине «Управление информационной безопасностью региона» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета с оценкой

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	УК-2 ОПК-1	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	УК-2 ОПК-1	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 с оценкой		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: «**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 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

						вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических 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.

4.1. 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. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции
   наследованию
   полиморфизму

2. 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

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

4. Дублирование сообщений является угрозой:
   доступности
   конфиденциальности
   целостности

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

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

7. 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

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

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

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

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

11. 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

1.2. Типовые вопросы, выносимые на зачет с оценкой

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения
17. Правовые аспекты построения СУИБ организации.

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ 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

Цель дисциплины:

- Дать студентам концептуальные знания основ управления информационной безопасностью для региональных информационных объектов с учетом современных требований теории по защите информации;
- Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий менеджмента информационной безопасности на типовых региональных информационных объектах с учетом современных международных и отечественных стандартов.

Задачи дисциплины:

- Ознакомление обучаемых с основными методами управления.
- Изучение правовых, организационных и программно-технических мер обеспечения информационной безопасности.
- Формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем
- Формирование требований к системе управления ИБ конкретного объекта
- Обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации
- Проектирование системы управления ИБ конкретного объекта.

2. Указания по проведению практических занятий

Раздел 1. Концептуально-теоретические основы управления информационной безопасностью

Тема 1. Базовые основы систем и процессов управления информационной безопасностью

Практическое занятие 1.

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

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки систем и процессов управления информационной безопасностью

Учебные вопросы:

- Управление информационной безопасностью. Комплексная система управления информационной безопасностью.
- Основные определения и критерии классификации угроз. Основные угрозы доступности.
- Основные угрозы целостности.
- Основные угрозы конфиденциальности.
- Источники угроз.
- Продолжительность практического занятия-2часа

Тема 2. Политика информационной безопасности отдельных структур (объектов, процессов)
Практическое занятие 2.

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 о политике безопасности отдельных структур

Учебные вопросы:

- Определение политики информационной безопасности
- Принципы политики безопасности
- Виды политики безопасности
- Политики безопасности для
- Уровни политики безопасности
- Продолжительность практического занятия-2часа

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью
Практическое занятие 3.

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

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в организационно-кадровых и технических аспектах управления информационной безопасностью

Учебные вопросы:

- Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии.
- Нормативные акты предприятия по информационной безопасности.
- Формы правовой защиты информации на предприятии.

- Продолжительность практического занятия-2часа

Тема 4. Основы оценки эффективности управления информационной безопасностью

Практическое занятие 4.

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

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

- Метод оценки рисков на основе модели информационных потоков.
- Расчет рисков по угрозе конфиденциальность.
- Расчет рисков по угрозе целостность.
- Методы оценивания информационных рисков.
- Табличные методы оценки рисков.
- Разделение рисков на приемлемые и неприемлемые.
- Продолжительность практического занятия-2часа

3. Указания по проведению лабораторного практикума

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

3. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных аппаратных средств вычислительной техники;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
2 семестр		
1	**Базовые основы систем и процессов управления информационной безопасностью**	1. Вредоносные программы и антивирусные программные средства. 2. Методы программно-аппаратной защиты информации. 3. Аттестация объектов информатизации. 19. Виды защиты информации. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***
2	**Политика информационной безопасности отдельных структур (объектов, процессов)**	1. Системы защиты информации. 2. Модели разграничения доступа. 3. Криптографические стандарты и их использование в информационных системах. ***Подготовка рефератов, письменная работа,***

		самостоятельное изучение тем.
3	**Организационно-кадровые и технические аспекты управления информационной безопасностью**	1. Способы и средства защиты информации от утечки по техническим каналам. 2. Принципы организации информационных систем в соответствии с требованиями по защите информации. 3. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
4	**Основы оценки эффективности управления информационной безопасностью**	1. Основные нормативные правовые акты в области информационной безопасности и защиты информации. 2. Отечественные и зарубежные стандарты в области компьютерной безопасности. 3. Принципы и методы организационной защиты информации. ***Подготовка рефератов, письменная работа, самостоятельное изучение тем.***

Вопросы, выносимые на самостоятельное изучение:

для очной формы обучения:

1 Место информационной безопасности в системе национальной безопасности.

2. Современная концепция информационной безопасности.

3. Цели и концептуальные основы защиты информации.

4. Критерии, условия и принципы отнесения информации к защищаемой.

5. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

6. Понятие и структура угроз защищаемой информации.

7. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.

8. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.

9. Виды уязвимости информации и формы ее проявления.

10. Каналы и методы несанкционированного доступа к конфиденциальной информации.

11. Модель нарушителя.

12. Модель угроз.

13. Критерии оценки безопасности информационных технологий.

14. Методы защиты информации от несанкционированного доступа.

15. Риски информационной безопасности.

Примерные темы докладов

1. Вредоносные программы и антивирусные программные средства.
2. Методы программно-аппаратной защиты информации.
3. Аттестация объектов информатизации. 19. Виды защиты информации.
4. Системы защиты информации.
5. Модели разграничения доступа.
6. Криптографические стандарты и их использование в информационных системах.
7. Способы и средства защиты информации от утечки по техническим каналам.
8. Принципы организации информационных систем в соответствии с требованиями по защите информации.
9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.
13. Лицензирование и сертификация в области защиты информации.
14. Комплексные системы защиты информации.

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. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

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»

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

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. Электронные ресурсы образовательной среды Университета
2. Информационные системы (консультант+; Гарант)