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.05 «ЭКСПЕРТНЫЕ СИСТЕМЫ КОМПЛЕКСНОЙ ОЦЕНКИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ»

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: Смирнова П.В. Рабочая программа дисциплины (модуля): Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем. – Королев МО: «Технологический Университет», 2023

Рецензент: В.Н. Соляной

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	№9 от 29.03.2023г			

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

Рабочая программа рекомендована на заседании УМС:

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

2

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

Целью изучения дисциплины является:

Формирование у обучаемых концептуальных и методологических основ в области теории обеспечения информационной безопасности в процессе развития современного информационного общества на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Освоение студентами теоретических основ, технологий и механизмов оценки систем.

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.

Профессиональные компетенции:

- ПК-2: Способен разрабатывать проектные решения по развитию автоматизированных ИАС в защищенном исполнении.

Основными задачами дисциплины являются:

1. раскрытие сущности, целей и содержание основ теории информационной безопасности и методологии защиты информации в автоматизированных телекоммуникационных системах;
2. определение общих методологических подходов построения экспертных систем оценки безопасности (ЭСКОБ) в автоматизированных телекоммуникационных системах;
3. освоение методических подходов установления состава защищаемой информации и выявления объектов защиты в автоматизированных телекоммуникационных системах;
4. выявление целесообразных методов комплексной оценки безопасности актуальных информационных угроз и опасных нарушителей в автоматизированных телекоммуникационных системах;
5. овладение методами оценки уязвимости защищаемой информации в автоматизированных телекоммуникационных системах;
6. определение методов выявления параметров и структуры систем защиты информации;

7. освоение методов разработки ЭСКОБ и целесообразности их использования для анализа состояния безопасности автоматизированных телекоммуникационных систем;

8. раскрытие методов управления ЭСКОБ;

9. определение методологических подходов оценки эффективности использования ЭСКОБ для оценки комплексной безопасности информации в автоматизированных телекоммуникационных системах и др.

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.

- ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.

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.

- ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.

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.

- ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина “Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем” относится к вариативной части основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина “Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем” базируется на одновременно изучаемых дисциплинах: «Специальные разделы математики»; «Специальные разделы физики»; «Современная философия и методология науки»; «Защищенные информационные системы» и компетенциях: УК-1, 2, 4; ПК-1; ОПК-1 .

Знания и компетенции, полученные при освоении дисциплины “Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем”, являются базовыми при дальнейшем изучении дисциплин профессионального цикла «Концептуальное проектирование технологий обеспечения информационной безопасности», «Организационно-правовые механизмы обеспечения информационной безопасности», «Информационно-аналитические системы безопасности» и выполнении выпускной квалификационной работы магистра.

3.Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр**
		Второй
Общая трудоемкость	**180**	**180**
Аудиторные занятия	**94**	**94**
Лекции (Л)	16	16
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	8	8
Другие виды контактной работы*	48	48
Практическая подготовка	**6**	**6**
Самостоятельная работа	**80**	**80**
Расчетно-графические работы	**-**	**-**
Курсовая работа	**+**	**+**
Текущий контроль знаний (7-8, 15-16 неделя)	**-**	**-**
Вид итогового контроля	**Экзамен**	**Экзамен**

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

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практ. занят., час.	Лаб. работы час	Занятия в интерактивной форме, час	Практическая погото вка ,час	Код компетенций
Раздел (модуль) 1. Интеллектуальные информационные системы (ИИС). Назначение, классификация ЭСКОБ и использование для комплексной оценки безопасности автоматизированных телекоммуникационных систем						
Тема 1. Введение. Современные проблемы информационной безопасности. ИИС и их возможности для комплексной оценки безопасности	2	2	1	1	0.5	УК-2 ПК-2
Тема 2. Классификация ИИС по решаемым задачам, по типу ЭВМ по степени интеграции с другими программами	2	2	1	1	0.5	УК-2 ПК-2
Тема3.ЭСОБ. Архитектура и составные части экспертных систем	2	2	2	1	1	УК-2 ПК-2
Тема 4. Организация базы знаний ЭСОБ. Формы представления знаний	2	3	1	1	1	УК-2 ПК-2
Раздел 2. Проектирование, тестирование и развитие ЭСКОБ автоматизированных телекоммуникационных систем						
Тема 5.	2	2	1	1	0.1	УК-2

Составные части базы знаний: база фактов и база правил. Языки представления знаний. Предметное, декларативная и процедурная форма представления знаний. Семантические сети, фреймы, продукционная модель, основанная на правилах.						ПК-2
Тема 6. Этапы проектирования ЭСКОБ. Участники процесса проектирования	3	3	1	1	1	УК-2 ПК-2
Тема 7. Тестирование и развитие ЭСКОБ	3	2	1	2	1	УК-2 ПК-2
Итого:	**16**	**16**	**8**	**8**	**6**	

4.2. Содержание тем дисциплины

Тема 1. Введение.

Прикладные информационные системы. Состояние и перспективы рынка ИИС. Виды интеллектуальных систем. Отличия ИИС и экспертных систем (ЭС) от других программных средств.

Тема 2. Классификация ИИС по решаемым задачам, по типу ЭВМ по степени интеграции с другими программами

Интерпретация данных – традиционная задача для ЭС. Диагностика – процесс соотнесения объекта с некоторым классом объектов. Мониторинг – Непрерывная интерпретация данных в реальном масштабе времени и сигнализация о выходе тех или иных параметров за допустимые пределы. Проектирование – подготовка спецификаций по созданию «объектов» с заранее определенными свойствами. Прогнозирование, Планирование. Обучение. Управление. Поддержка принятия решений.

Тема 3. Экспертные системы. Архитектура и составные части экспертных систем комплексной оценки безопасности автоматизированных телекоммуникационных систем

Экспертные – системы сложные программные комплексы, аккумулирующие знания специалистов в конкретных предметных областях и тиражирующие этот эмпирический опыт для консультаций менее квалифицированных пользователей. Обобщенная структура ЭСКОБ. База знаний – ядро ЭСКОБ, совокупность знаний предметной области, записанная на машинных носителях в форме, понятной эксперту и пользователю. Механизм вывода. Вывод на знаниях. Машина вывода. Механизмы приобретения и объяснения знаний. Интеллектуальный интерфейс.

Тема 4. Организация базы знаний ЭСОБ. Формы представления знаний

Составные части базы знаний: база фактов и база правил. Языки представления знаний.

Предметное (фактуальное) и проблемное (операционное) представление знаний. Декларативная и процедурная форма представления знаний. Семантические сети – ориентированный граф, вершины которого – понятия, а дуги – отношения между ними.

Фреймы – структура знаний для восприятия пространственных сцен. Продукционная модель – модель, основанная на правилах.

Тема 5. Методы представления знаний. Методы рассуждения в ИИС. Нечеткий вывод знаний.

Формальные логические модели. Описание предметной области в виде аксиом. Эвристические методы рассуждений. Рассуждения на основе. Дедукции, индукции и аналогии.

Тема 6. Этапы проектирования ЭСКОБ. Участники процесса проектирования

Идентификация, концептуализация, формализация, реализация, тестирование, опытная эксплуатация. Участники процесса проектирования: эксперты, инженеры по знаниям, конечные пользователи.

Тема 7. Тестирование и развитие ИИС

Тестирование и развитие ЭСКОБ автоматизированных телекоммуникационных систем.

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

1. «Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2. (

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

Структура фонда оценочных средств проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы.

Основная литература:

1.Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103198 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
2.Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256274 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
3.Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171525 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
4.Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223223 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223304 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.
6.Малышева Е.Н. Экспертные системы/Издательство**:** КемГУКИ (Кемеровский государственный университет культуры и искусств), 2010.
Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7

7.Информационные технологии и системы: Учебное пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 352 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0376-6
8.Экспертные системы САПР: учебное пособие / А.Л. Ездаков. - М.: ИД ФОРУМ, 2012. - 160 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0398-8
9.Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2004.

10.Квашнина Г. А. Донозологический мониторинг комплексной оценки управления адаптивного состояния субъекта в условиях экстремальной ситуации: монография / Г. А. Квашнина, Я. О. Мун. Воронеж: ВГТУ, 2008. 150 с.

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. 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;**
11. http://www.minfin.ru **- Официальный сайт Министерства финансов Российской Федерации;**
12. http://www.gov.ru **- Официальный сервер органов государственной власти Российской Федерации;**
13. http://www.fsb.ru/ **- Официальный сайт Федеральной Службы Безопасности;**

14. 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 (модуля), приведены в Приложении 2 к настоящей рабочей программе.

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

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

- **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; программы эмуляции виртуальных машин (VM-vare, VM-box или др.); операционная система MS Windows Server 2003 или др. сетевая ОС.
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Практические занятия целесообразно проводить в специализированной учебной лаборатории кафедры информационной безопасности с использованием имеющихся технических средств:

1. Имитатор многофункциональный ИМФ-2;
2. Многофункциональный комплекс радиоконтроля «Омега»;
3. Измеритель шума и вибраций ВШВ-003-М3;

4. Поисковый приемник радиосигналов «Скорпион».
5. Селективные микровольтметры;

Анализатор спектра;

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.

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

ЭКСПЕРТНЫЕ СИСТЕМЫ КОМПЛЕКСНОЙ ОЦЕНКИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Направление подготовки: 10.04.01 - Информационная безопасность

Программа подготовки: магистратура

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:1-7	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.	ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности	Тема:1-7	ПК-2.3. Разрабатывать проекты документов по созданию защищенных технологий с оформлением технических заданий на проектирование, осуществлять непосредственную разработку проектных решений по ИБ и оценку их эффективности в автоматизированной ИАС.	ПК-2.2. Проводить предпроектное обследование с выбором перспективной технологии защиты автоматизированной ИАД с разработкой проектной документации и комплексной оценкой эффективности применения автоматизированной ИАС.	ПК-2.1. Знать нормативную базу создания и эксплуатации защищенных функциональных и обеспечивающих подсистем, методы проектирования, критерии и показатели эффективности автоматизированной ИАС.

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

Код компетенции	*Инструменты, оценивающие сформированность компетенции*	*Показатель оценивания компетенции*	***Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания***
УК-2 ПК-2	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 ПК-2	Контрольная работа	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	1. 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	***Лабораторная***	***А) полностью***	***1. Оформление в соответствии с***

ПК-2	***работа***	***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***	***требованиями (1 балл).*** ***2. Выбор методов измерений и вычислений (1 балл).*** ***3. Умение применять выбранные методы (1 балл).*** ***4. Анализ и выводы, отражающие суть изучаемого явления с указанием конкретных результатов (2 балла).*** ***Максимальная оценка – 5 баллов.***

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

Примерная тематика докладов в презентационной форме:

1. 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.
5. Компьютерная преступность в экономических областях.
6. Мир XXI века: информационное противоборство.
7. Компьютерные вирусы в современных информационных системах.
8. Информационные угрозы современным экономическим объектам.
9. Информатизация России и проблема защиты информации.
10. Безопасность информации в коммерческой деятельности.
11. Разведки России – исторический аспект.
12. Мировой информационный терроризм.
13. Этика защиты информации.
14. Становление и развитие промышленного шпионажа.
15. Язык описания знаний.
16. Семиотическая модель поля знаний.
17. Извлечение знаний из данных.
18. Когнитивные системы.
19. Соотношение понятий «данные» и «знания».
20. Машинное обучение на примерах.
21. Нейросеть и ее структура.
22. Правила моделирования естественных нейронов искусственными.

23. Структура ЭСС нейросетевых вычислений.
24. Назначение и функция отдельных блоков.
25. Общая схема выполнения генетического алгоритма.
26. Идентификация, концептуализация, формализация, реализация, тестирование, опытная эксплуатация.
27. Участники процесса проектирования: эксперты, инженеры по знаниям, конечные пользователи.

Примерная тематика (контрольных заданий) задач для выполнения:

ЗАДАНИЕ № 1

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

Цель работы.

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

Продолжительность занятия: полтора учебных часа.

Задания.

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.

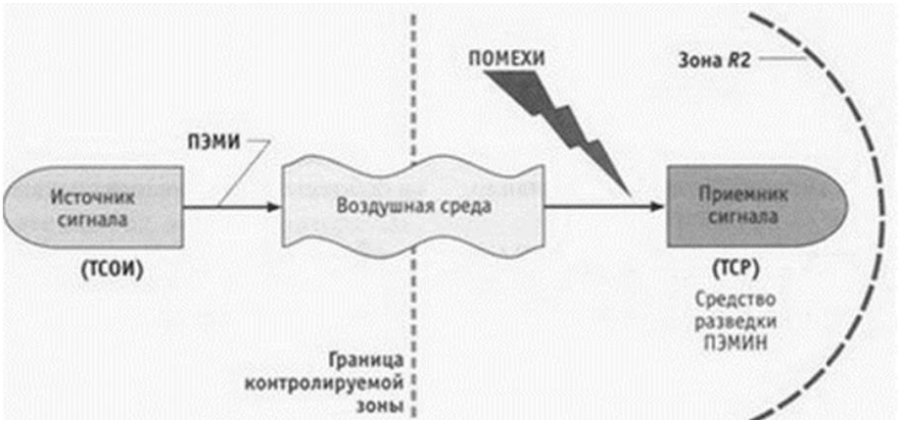

Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

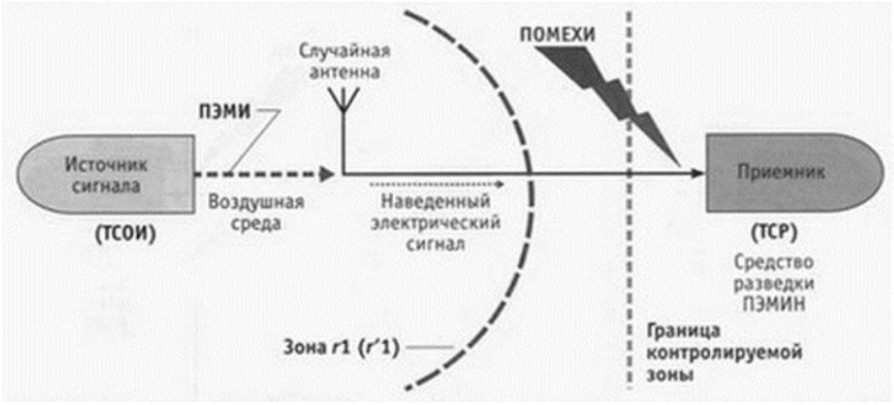

Рисунок 2. Схема ТКУИ за счет ПЭМИН

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

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

Формой контроля знаний по дисциплине «Экспертные системы комплексной оценки безопасности автоматизированных и телекоммуникационных систем» 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
Согласно графика учебного процесса	тестирование	УК-2 ПК-2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно графика учебного процесса	тестирование	УК-2 ПК-2	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно графика учебного процесса	Экзамен	УК-2 ПК-2	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 20 минут на каждого студента	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на практике; 3. работа на практических занятиях; 4. знание основных научных

						теорий, изучаемых предметов; 5. 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 экзамен (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 +

4.2.Типовые вопросы, выносимые на экзамен

1.Прикладные информационные системы. Состояние и перспективы рынка ИИС.

2.Виды интеллектуальных систем.

3.Отличия ИИС и экспертных систем (ЭС) от других программных средств.

4.Интерпретация данных – традиционная задача для ЭС.

5.Диагностика – процесс соотнесения объекта с некоторым классом объектов.
6.Мониторинг – Непрерывная интерпретация данных в реальном масштабе времени и сигнализация о выходе тех или иных параметров за допустимые пределы.
7.Проектирование – подготовка спецификаций по созданию «объектов» с заранее определенными свойствами.
8.Прогнозирование, Планирование. Обучение. Управление. Поддержка принятия решений.
9.ЭСКОБ – системы сложные программные комплексы, аккумулирующие знания специалистов в конкретных предметных областях и тиражирующие этот эмпирический опыт для консультаций менее квалифицированных пользователей.
10.Обобщенная структура ЭС.
11База знаний – ядро ЭС, совокупность знаний предметной области, записанная на машинных носителях в форме, понятной эксперту и пользователю.
12.Механизм вывода.
13.Вывод на знаниях.
14.Машина вывода.
15.Механизмы приобретения и объяснения знаний.
16.Интеллектуальный интерфейс.
17.Составные части базы знаний: база фактов и база правил.
18.Языки представления знаний.
19.Предметное (фактуальное) и проблемное (операционное) представление знаний.
20.Декларативная и процедурная форма представления знаний.
21.Семантические сети – ориентированный граф, вершины которого – понятия, а дуги – отношения между ними.
22.Фреймы – структура знаний для восприятия пространственных сцен.
23.Продукционная модель – модель, основанная на правилах.
24.Формальные логические модели.
25.Описание предметной области в виде аксиом.
26.Эвристические методы рассуждений. Рассуждения на основе дедукции, индукции и аналогии.
27..Нечеткий вывод знаний.
28.Применение статистических методов для интеллектуальной компьютерной обработки текстов. Немонотонность вывода.

29.Статические ЭС и области их применения. Динамические ЭС и области их применения (системы реального времени).
30.Приобретение знаний. Поле знаний.
31.Язык описания знаний.
32.Семиотическая модель поля знаний.
33.Извлечение знаний из данных.
34.Когнитивные системы.
35. Соотношение понятий «данные» и «знания».
36Машинное обучение на примерах.
37.Нейросеть и ее структура.
38.Правила моделирования естественных нейронов искусственными.
39.Структура ЭСС нейросетевых вычислений.
40.Назначение и функция отдельных блоков.
41.Общая схема выполнения генетического алгоритма.
42.Идентификация, концептуализация, формализация, реализация, тестирование, опытная эксплуатация.
43.Участники процесса проектирования: эксперты, инженеры по знаниям, конечные пользователи.

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

ЭКСПЕРТНЫЕ СИСТЕМЫ КОМПЛЕКСНОЙ ОЦЕНКИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Направление подготовки: 10.04.01 - Информационная безопасность

Программа подготовки: Магистратура

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

Целью изучения дисциплины является формирование у обучаемых концептуальных и методологических основ в области теории обеспечения информационной безопасности в процессе развития современного информационного общества на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Задачи дисциплины:

- раскрытие сущности, целей и содержание основ теории информационной безопасности и методологии защиты информации в автоматизированных телекоммуникационных системах;
- определение общих методологических подходов построения экспертных систем оценки безопасности (ЭСКОБ) в автоматизированных телекоммуникационных системах;
- освоение методических подходов установления состава защищаемой информации и выявления объектов защиты в автоматизированных телекоммуникационных системах;
- выявление целесообразных методов комплексной оценки безопасности актуальных информационных угроз и опасных нарушителей в автоматизированных телекоммуникационных системах;
- овладение методами оценки уязвимости защищаемой информации в автоматизированных телекоммуникационных системах;
- определение методов выявления параметров и структуры систем защиты информации;
- освоение методов разработки ЭСКОБ и целесообразности их использования для анализа состояния безопасности автоматизированных телекоммуникационных систем;
- раскрытие методов управления ЭСКОБ;
- определение методологических подходов оценки эффективности использования ЭСКОБ для оценки комплексной безопасности информации в автоматизированных телекоммуникационных системах и др.

2. Указания по проведению практических занятий

Тема 1. Введение

Прикладные информационные системы. Состояние и перспективы рынка ИИС. Виды интеллектуальных систем. Отличия ИИС и экспертных систем (ЭС) от других программных средств.

Практическое занятие 2.

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

Образовательные технологии: *групповая дискуссия.*

Учебные вопросы:

- Определение понятия “Интеллектуальная система”.
- Обеспечение работы ИИС
- Виды интеллектуальных систем.
- Отличия ИИС и экспертных систем (ЭС) от других программных средств.
- Продолжительность практического занятия-2 часа

Тема 2. Классификация ИИС по решаемым задачам, по типу ЭВМ по степени интеграции с другими программами

Практическое занятие 2.

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

Образовательные технологии: *беседа.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки о классификации ИИС по различным признакам.

Учебные вопросы:

- Классификация задач, решаемых ИИС.
- Экспертные системы (собственно экспертные системы (ЭС), интерактивные баннеры (web + ЭС)).
- Вопросно-ответные системы (в некоторых источниках «системы общения»).
- Интеллектуальные поисковики (например, система Старт).
- Виртуальные собеседники.
- Виртуальные цифровые помощники
- Продолжительность практического занятия-2 часа

.

Тема 3. Экспертные системы. Архитектура и составные части экспертных систем комплексной оценки безопасности автоматизированных телекоммуникационных систем

Практическое занятие 3.

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 об архитектуре и составных компонентах экспертных систем комплексной оценки безопасности автоматизированных телекоммуникационных систем

Учебные вопросы:

- Состав и структура ЭС
- Назначение базы знаний (ядра ЭСКОБ)
- Механизм вывода.
- Вывод на знаниях.
- Машина вывода.
- Механизмы приобретения и объяснения знаний.
- Принцип работы интеллектуального интерфейса.
- Продолжительность практического занятия-2 часа

Тема 4. Организация базы знаний ЭСОБ. Формы представления знаний

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 по организации базы знаний ЭСОБ информационных систем, о формах представления знаний.

Учебные вопросы:

- Составные части базы знаний
- Языки представления знаний.
- Предметное и проблемное представление знаний.
- Декларативная и процедурная форма представления знаний.
- Семантические сети
- Фреймы
- Продукционная

- Продолжительность практического занятия-2 часа
-

Тема 5. Методы представления знаний. Методы рассуждения в ИИС. Нечеткий вывод знаний.

Практическое занятие 5.

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

Образовательные технологии*: беседа.*

Тема и содержание практического занятия:

Цель работы: получить практические знания и навыки о формальных логических моделях, об эвристических методах рассуждений, о дедукции, индукции, аналогии и о нечетком выводе знаний.

Учебные вопросы:

- Методы представления знаний.
- Методы рассуждения в ИИС.
- Нечеткий вывод знаний
- Раздел математики “Нечёткая логика”, его использование в ЭСОБ.
- Продолжительность практического занятия-4 часа

Тема 6. Этапы проектирования ЭСКОБ. Участники процесса проектирования

Практическое занятие 6.

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

Образовательные технологии: *групповая дискуссия.*

Тема и содержание практического занятия:

Цель работы: получить практические знания и навыки об этапах проектирования ЭСКОБ информационных телекоммуникационных систем.

Учебные вопросы:

- Этапы проектирования ЭСКОБ
- Идентификация

- Концептуализация
- Формализация
- Реализация
- Тестирование
- Опытная эксплуатация.
- Участники процесса проектирования: эксперты, инженеры по знаниям, конечные пользователи и их функции.
- Продолжительность практического занятия-4 часа

1. Указания по проведению лабораторного практикума

Цель и задачи выполнения лабораторных работ: Определение порядка и последовательности действий по обоснованию предложений руководителю по результатам анализа и прогноза по заданной ситуации.

Методика *определяется моделью соответствующей задачи, решаемой обучающимся на занятии по заданию преподавателя)* и средства *для* выполнения лабораторных работ: общее *программное обеспечение*

Этапы выполнения лабораторных работ *(Постановка задачи лабораторной работы. Ознакомление обучающегося с содержанием и объемом лабораторной работы. Порядок выполнения лабораторной работы. Регистрация результатов и оформление отчета о лабораторной работе. Заключительная часть лабораторной работы).*

Тематика лабораторных работ и задания к ним *(тематика лабораторных работ должна соответствовать рабочей программе дисциплины).*

Лабораторная работа № 1.
Тема: Структура информационных ресурсов и администрирование в компьютерных системах
Цель занятия**:** Определение конфигурации информационных ресурсов компьютерных систем. Администрирование в компьютерных системах.
Продолжительность практического занятия-4 часа
Задание.

ЗАДАНИЕ № 1

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

Цель работы.

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

Продолжительность занятия: полтора учебных часа.

Задания.

4. Изучить теоретическую часть Задания №1.
5. Выполнить практическую часть Задания №1:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

6. 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.

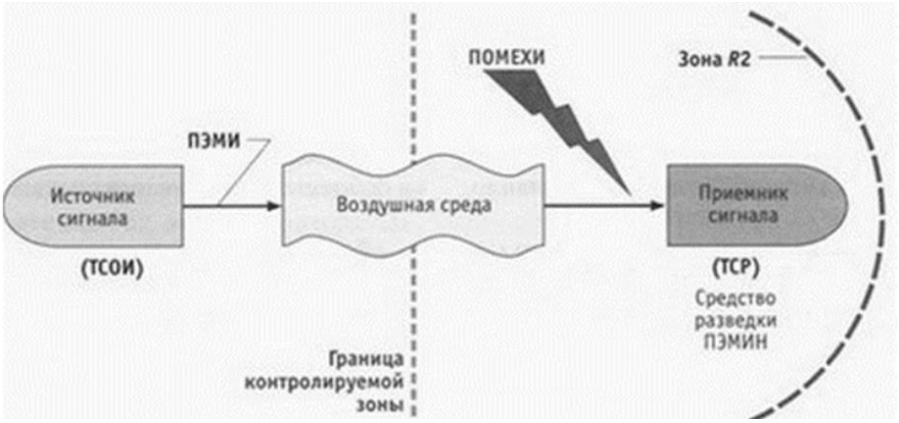

Рисунок 1. Схема ТКУИ за счет ПЭМИ

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

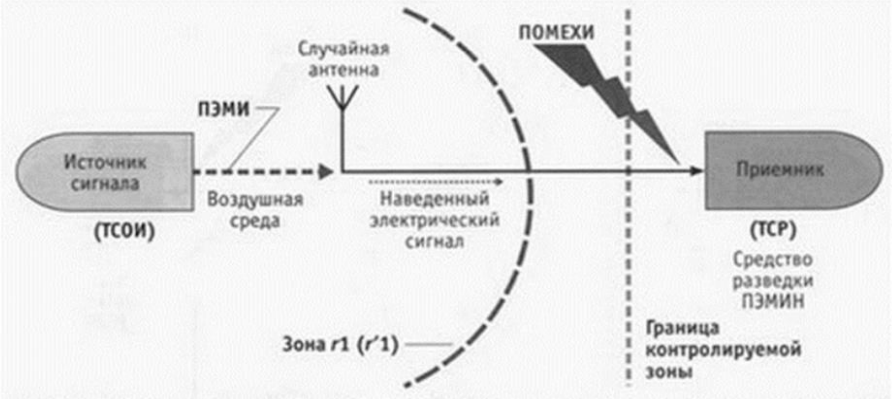

Рисунок 2. Схема ТКУИ за счет ПЭМИН

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:

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

Практические задания:

3) Опишите собственными словами следующие определения. ОТСС; ВТСС; ТКУИ.

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

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

Лабораторная работа № 2. Анализ угроз информационной безопасности

Цель работы: Изучить и научиться выполнять анализ условий и факторов воздействующих на защищаемую информацию. Классификация угроз. Естественные и искусственные угрозы. Основные направления и методы реализации угроз.

Основные виды атак на КС, их классификация. Проблемы обеспечения информационной безопасности в проводных КС.

Беспроводной доступ к локальным сетям. Угрозы и уязвимости в беспроводных компьютерных системах.

Задание.

ЗАДАНИЕ № 2

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

Цель работы.

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

Продолжительность занятия: полтора учебных часа.

Задания.

7. Изучить теоретическую часть Задания №2.

8. Выполнить практическую часть Задания №2:

а) ответить на вопросы для самопроверки;

б) выполнить практические задания.

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

Теоретическая часть.

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

Рисунок 1. ПАК «Сигурд М18»

Требования к антеннам.

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

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

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

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

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

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

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

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

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

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

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

Требования к анализатору.

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

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

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

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

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

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

Иметь полосы пропускания в диапазоне 1 кГц...3 МГц. Погрешность, вносимая собственными шумами, должна быть не более 1 дБ. Анализатор спектра должен обеспечивать звуковой контроль ПЭМИ,

имеющих амплитудную и частотную (на частотах свыше 30 МГц) модуляцию, с помощью встроенных или подключаемых приборов или устройств.

Примерный перечень оборудования приведен в (табл. 1).

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

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

Альтернативная измерительная площадка.

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

Однако, шумовая обстановка на объекте информатизации весьма нестабильна. Помимо нестабильности она абсолютно неисследованная.

Оператор при проведении измерений может столкнуться с таким явлением как «стоячая волна».

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

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

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

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

Практическая часть.

Вопросы для самопроверки:

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

Практические задания:

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

Продолжительность практического занятия-4 часа

3. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1	**Введение**	1. Определение понятия “Интеллектуальная система”. 2. Обеспечение работы ИИС 3. Виды интеллектуальных систем. 4. Отличия ИИС и экспертных систем (ЭС) от других программных средств. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
2	**Классификация ИИС по решаемым задачам, по типу ЭВМ по степени интеграции с другими программами**	1. Классификация задач, решаемых ИИС. 2. Экспертные системы (собственно экспертные системы (ЭС), интерактивные баннеры (web + ЭС)). 3. Вопросно-ответные системы (в некоторых источниках «системы общения»). 4. Интеллектуальные поисковики (например, система Старт). 5. Виртуальные собеседники. 6. Виртуальные цифровые помощники. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
3	**Экспертные системы. Архитектура и составные части экспертных систем комплексной оценки безопасности автоматизированных телекоммуникационных систем**	1. Состав и структура ЭС 2. Назначение базы знаний (ядра ЭСКОБ) 3. Механизм вывода. 4. Вывод на знаниях. 5. Машина вывода. 6. Механизмы приобретения и объяснения знаний. 7. Принцип работы интеллектуального интерфейса. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
4	**Организация базы знаний ЭСОБ. Формы представления**	1. Составные части базы знаний ***2.*** Языки представления знаний. 3. Предметное и проблемное представление знаний.

	знаний	4. Декларативная и процедурная форма представления знаний. 5. Семантические сети 6. Фреймы 7. Продукционная *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
5	**Методы представления знаний. Методы рассуждения в ИИС. Нечеткий вывод знаний.**	1. Методы представления знаний. 2. Методы рассуждения в ИИС. 3. Нечеткий вывод знаний 4. Раздел математики “Нечёткая логика”, его использование в ЭСОБ. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

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, необходимой для освоения дисциплины

Основная литература:

1.Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара : ПГУТИ, 2020. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255575 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103203 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110328 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 374 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11381 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

5.Экспертные системы САПР: учебное пособие / А.Л. Ездаков. - М.: ИД ФОРУМ, 2012. - 160 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0398-8

6.Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7

7.Информационные технологии и системы: Учебное пособие / Е.Л. Федотова. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 352 с.: ил.; 60x90 1/16. ISBN 978-5-8199-0376-6

Дополнительная литература

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., и др..Технические средства и методы защиты информации. Учебное пособие Под ред. А.П.Зайцева и А.А.Шелупанова. 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012.- 616с..

2. Основы теории передачи информации: Учебное пособие - М.:, Литвинская О.С. , КНОРУС, 2010. ISBN 978-5-406-00049-6

3. Торокин А.А. Инженерно-техническая защиты информации: Учебное пособие. М.: Гелиос АРВ, 2008.

4. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации: Учебное пособие. М.: «Академия», 200

5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Учебное пособие. –М.: Горячая линия – Телеком, 2005.
6. ГОСТ 12.1.050-86 «Методы измерения шума на рабочих местах».
7. ГОСТ 29216-91 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний.»
8. ГОСТ 22505-83 «Радиопомехи индустриальные от приемников телевизионных и приемников радиовещательных частотно-модулированных сигналов в диапазоне УКВ. Нормы и методы измерений.»
9. Инструкция по эксплуатации измерителя шума и вибрации ВШВ-003-М3.
6. Инструкция по эксплуатации скоростного поискового приемника радиосигналов «Скорпион», БНТИ-ТСС, Москва, 2006.
10. Руководство пользователя комплекса «Омега», ОАО НОВО, Москва, 2005.
11.Малышева Е.Н. Экспертные системы/Издательство**:** КемГУКИ (Кемеровский государственный университет культуры и искусств), 2010.
12.Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2004.
13.Квашнина Г. А. Донозологический мониторинг комплексной оценки управления адаптивного состояния субъекта в условиях экстремальной ситуации: монография / Г. А. Квашнина, Я. О. Мун. Воронеж: ВГТУ, 2008. 150 с.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

15. **http://eup.ru/catalog/all-all.asp – научно-образовательный портал.**
16. **http://informika.ru/ – образовательный портал.**
17. **www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.**
18. www.biblioclub.ru - Универсальная библиотека онлайн.
19. www.rucont.ru - ЭБС «Руконт».
20. **http://www.academy.it.ru/ – академия АЙТИ.**
21. **http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации**
22. **http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.**
23. **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 дисцмплине

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

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