МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт профессионального образования

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: институт профессионального образования
Должность: директор института
Дата: 19.06.2024 11:58:00

Сьянова Татьяна Юрьевна

Программа учебной практики

по профессиональному модулю
«Защита информации техническими средствами»

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Присваиваемая квалификация
"Техник по защите информации "

Формы обучения
очная

Кемерово 2024 г.

1712023495

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 25.03.2024 16:32:52

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 3 от 25.03.2024

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 25.03.2024 16:34:06

Прокопенко Евгения Викторовна

Согласовано цикловой-методической комиссией по направлению подготовки (специальности) 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Протокол № от 19.06.2024

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 25.03.2024 16:34:30

Прокопенко Евгения Викторовна

Согласовано заместителем директора по УР ИПО

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: Заместитель директора по учебной работе
Дата: 25.03.2024 16:34:30

Полуэктова Наталья Сергеевна

Согласовано заместителем директора по МР ИПО

1. Общая характеристика рабочей программы практики

Учебная практика является частью программы подготовки профессинального модуля «Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин» основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Прохождение практики направлено на формирование компетенций:

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
Знать: порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
Иметь практический опыт: установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации;

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
Знать: физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
Уметь: применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
Иметь практический опыт: применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
Знать: номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации;
Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
Иметь практический опыт: проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
Знать: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
Иметь практический опыт: проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации;

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.
Знать: основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации;
Уметь: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации;
Иметь практический опыт: установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты;

2. Структура и содержание рабочей программы практики

2.1 Объем практики и виды работы

Вид учебной работы	Объем часов
Обязательная нагрузка (всего)	**72 часа**
Промежуточная аттестация в форме .	

2.2 Тематический план и содержание практики

Наименование тем практики	Виды работ	Объем часов
Вид профессиональной деятельности: Защита информации техническими средствами		
Техническая защита информации	Измерение параметров физических полей	4
	Определение каналов утечки ПЭМИН.	4
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	4
	Установка и настройка технических средств защиты информации.	4
	Проведение измерений параметров побочных электромагнитных излучений и наводок.	4
	Проведение аттестации объектов информатизации.	4

Наименование тем практики	Виды работ	Объем часов
Вид профессиональной деятельности: Защита информации техническими средствами		
Инженерно-технические средства физической защиты объектов информатизации	Монтаж различных типов датчиков.	4
	Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	4
	Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.	4
	Рассмотрение системы контроля и управления доступом.	4
	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.	4
	Рассмотрение датчиков периметра, их принципов работы.	4
	Выполнение звукоизоляции помещений системы зашумления.	4
	Реализация защиты от утечки по цепям электропитания и заземления.	6
	Разработка организационных и технических мероприятий по заданию преподавателя.	6
	Разработка основной документации по инженерно-технической защите информации.	8
Всего:		72

3. Условия реализации программы практики

3.1 Требования к минимальному материально-техническому обеспечению

Оборудование рабочих мест:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональный компьютер.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

2. Специальное помещение № 1435 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3. Специальное помещение № 1251 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

4. Специальное помещение № 1139 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

5. Специальное помещение № 1147 представляет собой помещение для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь

Помещение для самостоятельной работы обучающихся:

6. Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,

Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

Помещение для самостоятельной работы обучающихся:

7. Специальное помещение № 1211 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:

проектор, экран настенный моторизованный.

Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

Специальное помещение №1134 представляет собой компьютерный класс оснащенный современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах:

Перечень основного оборудования:

Специализированная мебель (столы и стулья), лабораторное оборудование, персональные компьютеры

Перечень программного обеспечения: СПРУТ, Autodesk AutoCAD 2017, Autodesk

Inventor, СПРУТ-ТП, SprutCAD, Autodesk AutoCAD 2018, КОМПАС-3D, Microsoft Windows, SprutCAM,

СПРУТ-ОКП.

8. Специальное помещение № 1149 представляет собой лабораторию технических средств защиты информации, оснащенную аппаратными средствами аутентификации пользователя; средствами защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок; средствами измерения параметров физических полей (в том

числе электромагнитных излучений и наводок, акустических (виброакустических) колебаний); стендами физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов виртуализации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Сетевое оборудование, технические, программные и программно-аппаратные средства защиты информации и средства контроля защищенности информации.

Моноблок (Intel Core i5-10400 / 8 Gb RAM); горизонт кабельный организатор (25B-1U-02BL); коммутац панель кат.5 (27B-U5-24BL 24 ports); коммутац панель кат.6 (27B-U6-24BL 24 ports); шкаф коммутац Eurolan (S3000-22U 600x600 мм, перед - стекло, зад - металл, 60F-22-66-31BL); коммутатор управляемый (D-Link DGS-3130-54TS 48 ports); программно-аппаратный комплекс (Infotecs IDS-1000); модуль доверенной загрузки ("Соболь-4"); средство активной защиты информации от утечки за счет наводок информ сигнала на цепи заземления и электропитания ("Соната-PC3"); точка доступа Wi-fi двухдиапазонная (D-Link DWL-8620AP); патч-корды кат 5 (Eurolan); патч-корды кат 6 (Eurolan);

кабельный тестер (CableMaster-800); коммутатор управляемый (D-Link DES-1210-28 28 ports); коммутатор неуправляемый (D-Link DSS-100E-9P 8+1 ports); маршрутизатор проводной (D-Link DSR-150 8 ports); Wi-Fi маршрутизатор двухдиапазонный (D-Link DWR-980 4 Lan-ports).

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3.2 Информационное обеспечение реализации программы

3.2.1 Основная литература

1. Батаев, А. В. Операционные системы и среды : учебник для образовательных учреждений среднего профессионального образования по укрупненной группе специальностей "Информатика и вычислительная техника" / А. В. Батаев, Н. Ю. Налютин, С. В. Синицын ; А. В. Батаев, Н. Ю. Налютин, С. В. Синицын. – 5-е издание переработанное – Москва : Академия, 2021. – 285 с. с. – (Профессиональное образование : Информатика и вычислительная техника). – URL: https://academia-moscow.ru/reader/?id=539321 (дата обращения: 05.02.2024). – Текст : электронный.

3.2.2 Дополнительная литература

1. Никулин, В. В. Безопасность и защита информации. Лабораторный практикум : учебно-методическое пособие / В. В. Никулин. — Брянск : Брянский ГАУ, 2021. — 128 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/304352 (дата обращения: 05.02.2024). — Режим доступа: для авториз. пользователей.

2. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703 (дата обращения: 05.02.2024). — Режим доступа: для авториз. пользователей.

3. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491 (дата обращения: 05.02.2024). — Режим доступа: для авториз. пользователей.

4. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / Внуков А. А.. – 2-е изд., испр. и доп. – Москва : Юрайт, 2022. – 246 с. – ISBN 978-5-534-01679-6. – URL: https://urait.ru/book/zaschita-informacii-v-bankovskih-sistemah-490278 (дата обращения: 05.02.2024). – Текст : электронный.

5. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / Внуков А. А.. – 2-е изд., испр. и доп. – Москва : Юрайт, 2023. – 246 с. – ISBN 978-5-534-01679-6. – URL: https://urait.ru/book/zaschita-informacii-v-bankovskih-sistemah-512269 (дата обращения: 05.02.2024). – Текст : электронный.

6. Сычев, Ю. Н. Защита информации и информационная безопасность : Учебное пособие / Ю. Н. Сычев. – Москва : НИЦ ИНФРА-М, 2023. – 201 с. – ISBN 978-5-16-016583-7. – URL: https://znanium.com/catalog/document?id=416550 (дата обращения: 05.02.2024). – Текст : электронный.

7. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/293009 (дата обращения: 05.02.2024). — Режим доступа: для авториз. пользователей.

8. Внуков, А. А. Защита информации: учебное пособие для вузов / Внуков А. А.. – 3-е изд., пер. и доп. – Москва : Юрайт, 2023. – 161 с. – ISBN 978-5-534-07248-8. – URL: https://urait.ru/book/zaschita-informacii-512268 (дата обращения: 05.02.2024). – Текст : электронный.

9. Щеглов, А. Ю. Защита информации: основы теории.: учебник для вузов / Щеглов А. Ю., Щеглов К. А.. – Москва : Юрайт, 2023. – 309 с. – ISBN 978-5-534-04732-5. – URL: https://urait.ru/book/zaschita-informacii-osnovy-teorii-511998 (дата обращения: 05.02.2024). – Текст : электронный.

10. Зенков, А. В. Информационная безопасность и защита информации.: учебное пособие для вузов / Зенков А. В.. – Москва : Юрайт, 2023. – 104 с. – ISBN 978-5-534-14590-8. – URL: https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-520063 (дата обращения: 05.02.2024). – Текст : электронный.

3.2.3 Методическая литература

1. Профессиональный цикл : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 290 с. – URL: http://library.kuzstu.ru/meto.php?n=9964 (дата обращения: 05.02.2024). – Текст : электронный.

2. Методические указания по оформлению отчетов по практике, курсовых работ (проектов) и выпускных квалификационных работ : для всех специальностей СПО / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информатики и информационных систем, составители: Н. С. Полуэктова, Т. С. Семенова. – Кемерово : КузГТУ, 2022. – 1 файл (762 Кб). – URL: http://library.kuzstu.ru/meto.php?n=10478 (дата обращения: 05.02.2024). – Текст : электронный.

3.2.4 Ресурсы информационно-телекоммуникационной сети «Интернет»

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.

3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.

4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.

5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.

6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.

7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.

9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.

10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.

11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. Фонд оценочных средств

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по учебной практике по профессиональному модулю "Защита информации техническими средствами"

4.1. Паспорт фонда оценочных средств

Планируемые результаты обучения по практике.

Практика направлена на формирование следующих компетенций выпускника:

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
Защита информации техническими средствами	ПК 3.1	**Знания:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации;	Проверка отчёта по разделам практики.
	ПК 3.2	**Знания:** физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; **Практический опыт:** применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;	Проверка отчёта по разделам практики.
	ПК 3.3	**Знания:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	Проверка отчёта по разделам практики.
	ПК 3.4	**Знания:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации;	Проверка отчёта по разделам практики.
	ПК 3.5	**Знания:** основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации; **Умения:** применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации; **Практический опыт:** установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты;	Проверка отчёта по разделам практики.

4.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.**4.2.1. Оценочные средства при текущем контроле**

Текущий контродь по учебной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

90-100 баллов – при раскрытии всех разделов в полном объеме;
80-89 баллов – при раскрытии всех разделов с недочетами;
60-79 баллов – при раскрытии не всех разделов в полном объеме;
0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Измерение параметров физических полей

Задание 1. С помощью электронного вольтметра и рамочной антенны с известными характеристиками выполнить измерение напряженности методом эталонной антенны. Для расчета напряженности поля использовать формулу $E = e / h_д$, где e – значение ЭДС, измеренное вольтметром, а $h_д$ – действующая высота эталонной антенны.

Задание 2. С помощью электронного вольтметра и рамочной антенны с подключенным к ней переменным конденсатором, выполните измерение напряженности электрического поля методом сравнения. Для этого: сначала медленно вращайте антенну в разных плоскостях и как только значения вольтметра будут максимальные, изменяйте емкость переменного конденсатора до получения максимального значения, запишите полученное значение. Далее включите внутренний генератор эталонного электрического поля и запишите текущее значение вольтметра. Для расчета напряженности поля использовать формулу $E = 3 * 10^8 * U_c * R_p * C_0 / SN$, где U_c – напряжение на конденсаторе; R_p– активное сопротивление антенны на рабочей частоте; C_0 – емкость конденсатора в момент резонанса; S – площадь рамки; N – число витков рамки.

Задание 3. С помощью цифрового измерителя магнитного поля измерить величину поля, создаваемого динамиком на расстоянии 100 мм от датчика прибора. Постепенно удаляя динамик от датчика, найдите расстояние, на котором величина магнитного поля не превышает фоновых значений. Как вариант вместо цифрового измерителя можно использовать и компас, однако в этом случае точность измерений будет существенно ниже.

Задание 4. На катушку соленоида подайте напряжение (сердечника внутри катушки быть не должно). С торца катушки на расстоянии 100 мм от нее поднесите датчик измерителя электромагнитного поля. проведите измерения в нескольких положения датчика – от непосредственного внесения его внутрь соленоида по центру до расстояния 1м. Найдите границы чувствительности прибора и запишите измеренные значения напряженности поля. Измените напряжение в большую и меньшую сторону и для каждого изменения повторите серию замеров, как это было сделано в первом варианте.

Задание 5. Внутри стеклянного лабораторного контейнера, защищающего установку от колебаний воздуха на поперечной штанге подвесьте вертикально карболитовый стержень известного размера, зарядите его от подобного стержня, натертого мехом. Рядом на расстоянии около 100 мм подвесьте вертикально полоску бумаги известного размера и измеренной величиной электрического заряда. С помощью червячного механизма медленно перемещайте полоску бумаги к карболитовому стержню, и как только нижний край полоски начнет отклоняться измерьте это расстояние. Продолжайте приближать полоску до начала притягивания ее к стержню. С помощью закона Кулона определите силу притяжения двух тел в воздушной среде на двух расстояниях – начало отклонения полоски бумаги и начало притяжения полоски к стержню. Проверьте применимость формулы напряженности поля точечного заряда в воздушной среде: $E = (k * q_0) / (e * r^2)$

Тема 1.2. Определение каналов утечки ПЭМИН.

Задание 1. Ознакомьтесь с имеющимся оборудованием для измерения ПЭМИН по проводному каналу, радиоканалу, визуальному каналу.

Задание 2. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от проходящего кабеля UTP (неэкранированная витая пара), а затем повторите процедуру возле офисной телефонной линии.

Задание 3. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от обычного проводного телефонного аппарата, а затем проведите измерения возле специальным образом защищенного телефонного аппарата. Сравните результаты.

Задание 4. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от питающего кабеля 220 В, выходящего из рабочего кабинета.

Задание 5. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от LCD монитора с задней стороны (под крышкой стола).

Тема 1.3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

Задание 1. Ознакомьтесь с оборудованием для измерения параметров физических полей, создаваемых техническими средствами защиты информации.

Задание 2. Определите уровень фонового шума и параметры физического поля в непосредственной близости от генератора пространственного шума для защиты радиоканала. Повторите измерения на расстояниях 10, 25, 50, 100 м от генератора.

Задание 3. Определите уровень фонового шума и параметры физического поля в непосредственной близости от генератора линейного шума для защиты проводного слаботочного канала (например, локальной компьютерной сети или офисной телефонной сети).

Задание 4. Определите уровень фонового шума и параметры физического поля в непосредственной близости от генератора линейного шума для защиты силовой питающей сети

Задание 5. Определите уровень фонового шума и параметры физического поля в непосредственной близости от активного блокировщика телефонной линии при ее прослушивании.

Задание 6. Определите уровень фонового шума и параметры физического поля в непосредственной близости от устройства импульсной защиты телефонной линии методом «выжигания» подслушивающей аппаратуры, подключенной к линии.

Тема 1.4. Установка и настройка технических средств защиты информации.

Задание 1. Ознакомиться с характеристиками и инструкцией по установке и настройке имеющихся технических средств защиты информации.

Задание 2. Установить линейный генератор зашумления для локальной сети (телефонной линии) учреждения по инструкции разработчика. Проверить его работу и физические параметры.

Задание 3. Установить пространственный генератор шума для защиты от утечек по радиоканалу. Проверить его работу и физические параметры.

Задание 4. Подключить к ПК, входящему в состав информационной системы устройство аппаратного доступа (биометрический сканер / считыватель смарт-карт/ считыватель чипов и т.п.) через USB-порт, настроить его и проверить работу.

Задание 5. Подключить к офисной телефонной линии активный блокировщик, защищающий линию от прослушивания. Проверить его работу, например, путем временного подключения параллельного телефонного аппарата, имитирующего прослушивание линии.

Задание 6. На входе учреждения Интернет-канала перед серверами установить аппаратный межсетевой экран, настроить его и проверить работу путем попытки из внешней сети Интернет подключиться к серверу от имени клиентской учетной записи. В то же время от имени учетной записи системного администратора такая возможность должна быть обеспечена, если иного не оговорено информационной политикой предприятия.

Тема 1.5. Проведение измерений параметров побочных электромагнитных излучений и наводок.

Задание 1. Выполните измерение уровня ПЭМИН в середине рабочего кабинета, в котором расположен 1 ПК.

Задание 2. Повторите измерение электромагнитного поля в непосредственной близости от системного блока.

Задание 3. Выполните измерение уровня ПЭМИН в непосредственной близости от проходящего кабеля UTP (неэкранированная витая пара), а затем повторите процедуру возле офисной телефонной линии.

Задание 4. Выполните измерение уровня ПЭМИН в непосредственной близости от LCD-

монитора.

Задание 5. Выполните измерение уровня ПЭМИН в непосредственной близости от мобильного телефона в режиме ожидания, а затем в режиме разговора.

Тема 1.6. Проведение аттестации объектов информатизации.

Задание 1. Подготовить аттестационные листы и листы замечаний для каждого объекта информатизации – компьютерное рабочее место (АРМ), хранилище документации, архивы, любые другие отделы предприятия, в которых есть ИС и планируется ее внедрение.

Задание 2. Составить схему маршрута обхода проверок по принципу «от низшей иерархии объектов информатизации к высшей».

Задание 3. Провести проверку каждого объекта информатизации по всем необходимым критериям: защита помещений от перехвата информации через строительные элементы и окна; защита помещения от физического проникновения посторонних лиц; оснащение помещения средствами пожарной, охранной защитой и средствами видеонаблюдения; защита сети электропитания; защита информационной сети; защита компьютерного рабочего места и ограничение доступа к нему; если в помещении расположены дополнительные коммутирующие устройства, то они также должны быть защищены от доступа посторонних лиц; правила и места хранения сменных носителей информации, а также устройств аппаратной защиты ПК и носителей с электронной цифровой подписью (ЭЦП).

Задание 4. По окончании проверки сформировать и распечатать листы замечаний для устранения замеченных нарушений. Сформировать сводный общий протокол проведения аттестации.

Тема 2.1. Монтаж различных типов датчиков.

Задание 1. Используя инструкцию и необходимые инструменты, установить нужное количество охранных датчиков (объемных или движения) под потолком в охраняемом помещении. Кабельные линии от них расположить в кабель-каналах, либо под подвесным потолком, связав попутные линии капроновыми стяжками. Выполнить ориентацию датчиков за счет угла поворота и наклона в режиме тестирования.

Задание 2. Используя инструкцию и необходимые инструменты, установить нужное количество пожарных (температуры или дымовых) датчиков на потолке в охраняемом помещении с учетом его площади. Кабельные линии от них расположить в кабель-каналах, либо под подвесным потолком, связав попутные линии капроновыми стяжками.

Задание 3. Используя инструкцию и необходимые инструменты, установить на периметральное металлическое ограждение нужное количество тензометрических датчиков. Кабельные линии от них расположить в гофро-рукавах и прикрепить к ограждению капроновыми стяжками либо металлическими скобами. Перед установкой датчиков необходимо проверить жесткость конструкции, а при необходимости усилить ее, в противном случае будут наблюдаться ложные срабатывания от ветра.

Задание 4. Используя инструкцию и необходимые инструменты подготовить поверхность уличного грунта для установки сейсмологических датчиков. Для этого нужно выкопать небольшие траншеи заданной глубины и ширины. По определенной сетке с заданным шагом разместить на нужной глубине датчики и подвести к каждому из них кабель заключенный в гофро-рукав или трубу (ПВХ или металлическую). Засыпать траншею и разровнять грунт.

Задание 5. Установка радиоволновых периметральных датчиков (излучателей) возможно на местности с достаточно ровным рельефом, отсутствием кустарников, деревьев и травы выше 30 см. В случае несоответствия этих требований необходимо предварительно подготовить местность (как минимум – скосить высокую траву). Используя инструкцию и необходимые инструменты, установить необходимое количество датчиков на заданной высоте от поверхности грунта, направив их попарно навстречу друг другу. Для размещения датчиков можно использовать жестко закрепленное ограждение, столбики ограды, мачты освещения, стены здания. Кабель закрепить в зависимости от несущей поверхности, т.е. скобами или капроновыми стяжками, но в любом случае он должен быть защищен гофро-рукавом, трубой или кабель-каналом.

Задание 6. Уличные датчики освещенности обычно крепят на стене здания с теневой стороны. Провода необходимо защитить гофро-рукавом, трубой или кабель-каналом. После установки и подключения необходимо отрегулировать порог срабатывания в зависимости от освещенности.

Тема 2.2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.

Задание 1. Ознакомьтесь с техническим заданием заказчика системы пожарно-охранной сигнализации. Выберите наилучшим образом подходящее оборудование, исходя из условий будущей эксплуатации и выполните его закупку.

Задание 2. Используя в качестве основы техническое задание и поэтажный план здания, разместить на нем в требуемых помещениях датчики пожарно-охранной сигнализации, исходя из

необходимого количества и площади помещения, приняв во внимание рекомендации их изготовителя.

Задание 3. Используя поэтажный план здания, рассчитать трассу прокладки кабелей и их расход до места установки пультов управления.

Задание 4. На посту круглосуточной охраны (чаще всего – рабочее место вахтера) установить пульты управления сигнализацией, а также источник бесперебойного питания (ИБП)

Задание 5. Используя схему размещения датчиков, созданную на основе поэтажного плана здания, а также кабель-каналы или гофро-рукава, подготовить кабельную трассу. При необходимости используйте существующие слаботочные трассы, штроба. Возможно потребуется сверление отверстий в стенах с помощью перфоратора.

Задание 6. В соответствии со схемой и инструкциями изготовителя установите совмещенные или раздельные пожарно-охранные датчики во всех помещениях, а затем подведите к ним проводные шлейфы, вторые концы которых будут подключены к пульту управления.

Задание 7. Если оговорено техническим заданием, то к пульту подключите проводные шлейфы исполнительных устройств, например, система автоматического пожаротушения, электромагнитные замки, включение световой тревожной сигнализации и т.п. При отсутствии данных требований этот пункт пропустить.

Задание 8. Выполнить настройку системы с помощью пульта управления, и если необходимо, то подключив к нему компьютер в соответствии с инструкцией. Возможно потребуется отрегулировать пороги срабатывания датчиков или сопротивление линейных проводных шлейфов.

Задание 9. При успешном тестировании представить готовую систему заказчику и при отсутствии замечаний с его стороны подписать акт сдачи-приемки (акт выполненных работ).

Тема 2.3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации

Задание 1. Ознакомиться с оборудованием, использующимся для ремонтных и пуско-наладочных работ со средствами защиты информации – осциллографов, частотомеров, анализаторов спектра, генераторов частоты для проводных линий, генераторов радиочастоты, панорамных приемников.

Задание 2. Подключите универсальный генератор импульсов в защищаемую линию, а на выход линии осциллограф и проверьте форму сигнала в линии. Измерения провести при включенном и выключенном генераторе, а также при отсутствии и наличии устройств несанкционированного съема информации, либо его имитации. Рекомендуется периодически проводить такую проверку для ранней диагностики неисправностей, связанных, например, со старением радиоэлементов или изменением их характеристик.

Задание 3. Подключите частотомер параллельно к исследуемой линии питания и измерьте частоту переменного тока. Определите процент отклонения частоты и возможность использовать данное питание для работы устройств защиты информации без дополнительной фильтрации.

Задание 4. Настройте радиочастоту генератора пространственного зашумления на доминирующую радиочастоту спектра, присутствующего в данном помещении или другом объекте защиты. Для контроля настройки использовать панорамный радиоприемник.

Задание 5. Оцените эффективность устройства фильтрации питания. Сначала подключите осциллограф напрямую к питающей линии и изучите форму импульса. Затем подключите осциллограф к линии через фильтрующее устройство и снова изучите форму импульса. Сделайте вывод об эффективности фильтрующего устройства с нагрузкой и без нее.

Тема 2.4. Рассмотрение системы контроля и управления доступом.

Задание 1. Изучить общую схему системы контроля и управления доступом. Ознакомиться с назначением каждого элемента системы.

Задание 2. Изучить требования к установке, эксплуатации, обслуживанию системы в целом и каждого элемента.

Задание 3. Изучить варианты подключения к СКУД исполнительных устройств.

Задания 4. Изучить варианты хранения информации в системе, форматы выходной информации, формируемой СКУД, а также способы ее обработки и передачи.

Тема 2.5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.

Задание 1. Изучить принцип работы системы видеонаблюдения и возможные варианты ее реализации.

Задание 2. Изучить принцип работы и назначение каждого элемента системы, а также его типовые характеристики.

Задание 3. На основе технического задания, представленного заказчиком, выбрать наиболее подходящее оборудование и выполнить его закупку.

Задание 4. На карту-план объекта нанести и расположить элементы системы видеонаблюдения, уделяя особое внимание размещению видеокамер с учетом высоты, угла обзора, освещения внешними источниками света и т.п…

Задание 5. Рассчитать длину кабеля (если камеры не беспроводные) и количество расходных материалов с запасом 5-10%

Задание 6. При отсутствии разногласии с заказчиком по техническому заданию подписать его со своей стороны, как исполнителя, приложить перечень (спецификацию) оборудования также подписанную двумя сторонами и можно приступать к монтажу системы.

Тема 2.6. Рассмотрение датчиков периметра, их принципов работы

Задание 1. Изучить ассортимент выпускаемых российскими и зарубежными производителями датчиков охраны периметра.

Задание 2. Изучить принципы действия каждого типа датчиков периметра (радиоволновые, ИК, лазерные, сейсмические, геофонные, тензометрические, емкостные, индуктивные, сопротивления) и провести их классификацию по характеристикам, оценить их преимущества и недостатки.

Задание 3. Изучить характеристики пультов управления (контроллеров) для нескольких комплектов различных датчиков, принципы регулировки системы, возможность и необходимость сопряжения с компьютером, например, для сохранения и дальнейшей передачи информации для анализа охраняемого объекта.

Тема 2.7. Выполнение звукоизоляции помещений системы зашумления

Задание 1. Ознакомиться с основными принципами активной и пассивной защиты помещений от прослушивания. Ознакомиться с техническим заданием. Провести классификацию средств и методов защиты.

Задание 2. С помощью строительной документации и/или личным осмотром провести оценку модернизируемого помещения на предмет звуковых утечек. Оценке подлежат все строительные элементы помещения – пол, потолок, стены, окна, дверные проемы, а также металлические конструкции, проходящие через помещение. Результаты оценки свести в специальный журнал или бланк. В качестве измерительных приборов использовать генератор тестового шума, установленный в помещении, а также шумомер, установленный за пределами помещения.

Задание 3. Проанализировать результаты проведенной оценки и предложить для каждого строительного элемента, неудовлетворяющего условиям звукоизоляции, варианты улучшения звукоизолирующих и звукопоглощающих характеристик за счет применения звукопоглощающих и звукоотражающих материалов, создания тамбура двери, замена или уплотнение дверей, при необходимости – замена окон.

Задание 4. Сформировать перечень необходимых работ и материалов, выполнить калькуляцию затрат и закупку материалов.

Задание 5. Выполнить работы по модернизации помещения с точки зрения звукоизоляции, а затем с помощью генератора тестового шума, установленного в помещении, а также шумомера, установленного за пределами помещения, измерить уровень шума. Зафиксировать полученные показатели после модернизации помещения.

Задание 6. Если оговорено в техническом задании, то на окна установить генераторы виброаккустического шума в качестве системы активной защиты от прослушивания извне.

Задание 7. При отсутствии разногласии с заказчиком подписать двумя сторонами акт сдачи-приемки (акт выполненных работ).

Тема 2.8. Реализация защиты от утечки по цепям электропитания и заземления

Задание 1. Изучить приборы для определения уровня утечек информации по цепям электропитания и заземления.

Задание 2. Ознакомиться с методами устранения утечек информации через цепи электропитания и выбрать наиболее подходящий для данных условий – развязывающий трансформатор или генератор линейного зашумления.

Задание 3. Измерить уровень утечек по сети электропитания при работе на компьютере, подключенном к ЛВС; при разговоре по проводному офисному телефону; при обычном разговоре. Записать полученные измерения.

Задание 4. Для случая если бы выбран развязывающий трансформатор, то выбрать из выпускаемого ассортимента подходящий по мощности, исполнению и установить его в цепь питания кабинета, отдела, этажа или здания (потребуется помощь электрика).

Задание 5. Для случая если был выбран генератор линейного зашумления, то подключить его к электрощитку кабинета, этажа или здания, а затем провести измерения по аналогии с заданием 3.

Задние 6. При наличии возможности – сравнить эффективность защиты от утечек, устраняемых

двумя методами (задание 4 и 5) и выбрать более эффективный. Для повышения эффективности каждое рабочее место должно быть запитано через качественный сетевой фильтр или через источник бесперебойного питания (ИБП).

Задание 7. При наличии утечки по каналам заземления необходимо провести анализ качества существующего контура заземления и при необходимости провести его реконструкцию. Если контур выполнен по всем правилам, то попытайтесь подключить к нему генератор линейного шума и замерить уровень утечек. В совокупности использование высокоэффективных сетевых фильтров, качественного заземления, развязывающего трансформатора и генератора линейного шума обычно дает максимальный эффект защиты от утечек.

Тема 2.9. Разработка организационных и технических мероприятий по заданию преподавателя.

Задание 1. Выберите произвольное учреждение федерального уровня, имеющее филиал в данном городе, например:

- налоговая инспекция
- пенсионный фонд
- казначейство
- таможенная служба
- центр занятости населения
- филиал Центробанка

и определите для каждого из них класс (уровень) необходимой защиты. В качестве облегченного варианта можно рассмотреть не все учреждение, а только 1 из его отделов.

Задание 2. Сформируйте на ваш взгляд возможный перечень угроз, которым может подвергаться учреждение, а также каналы угроз.

Задание 3. Разработайте перечень административно-организационных мероприятий по защите от угроз для выбранного учреждения и сведите их в таблицу.

Задание 4. Разработайте перечень технических мероприятий по защите от угроз для выбранного учреждения (порядок их выполнения пока не имеет значения) и сведите их в таблицу.

Задание 5. Сформируйте сводную таблицу, в которой в столбцах будет следующая информация: Тип угрозы / Объект угрозы / Канал распространения угрозы / Вероятность совершения угрозы / Предполагаемый метод нейтрализации угрозы.

Тема 2.10. Разработка основной документации по инженерно-технической защите информации

Задание 1. В виде таблицы или списка сформировать перечень объектов защиты с помощью инженерно-технических средств.

Задание 2. Для каждого объекта в таблице сопоставить соответствующее средство инженерно-технической защиты.

Задание 3. Собрать сводную информацию с основными характеристиками и кратким описанием по каждому средству защиты в таблицу.

Задание 4. Начертить схему расположения средств инженерно-технической защиты, а также схему всех коммуникаций к ним (питающая сеть, информационная сеть). Каждый отдельный комплекс (система средств) защиты должен быть связан на схеме линиями определенного цвета. При большом количестве средств и комплексов защиты во избежание загромождения схемы рекомендуется каждый комплекс (систему) изобразить на отдельном листе.

Задание 5. Собрать воедино информацию об обслуживающих организациях комплексов защиты, их контактные данные, реквизиты.

Задание 6. Привести к единому стилю документации журнал обслуживания оборудования, в котором должно быть указано: выполненные работы (в т.ч. и профилактические), выявленные поломки или замечания, дата обслуживания, ФИО обслуживающего персонала, дата очередной проверки оборудования. Всю информацию можно создавать и хранить в бумажном и/или электронном виде.

4.2.2. Оценочные средства при промежуточном контроле (зачет, диффиринцированный зачет)

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Измерение параметров физических полей.

1. Приведите примеры физических полей

2. Какие методы измерения напряженности электрического поля используют на практике?

3. На каком максимальном расстоянии можно уловить магнитное поле звукового динамика?

4. От каких параметров зависит сила электромагнитного поля, создаваемого внутри катушки соленоида?

5. Возможно ли применить формулу напряженности поля точечного заряда в воздушной среде: $E = (k * q_0) / (e * r^2)$ к заряженной поверхности (стержню) ?

Тема 1.2. Определение каналов утечки ПЭМИН.

1. Приведите пример оборудования для измерения ПЭМИН по проводному каналу, радиоканалу, визуальному каналу.

2. На каком расстоянии от кабельной линии локальной сети или телефонной сети с помощью приборов можно обнаружить ПЭМИН, достаточные для нелегального прослушивания и съема информации?

3. На сколько единиц уровень ПЭМИН у защищенного проводного телефонного аппарата меньше, чем у обычного?

4. На каком расстоянии от силовой кабельной линии электропитания с помощью приборов можно обнаружить ПЭМИН, достаточные для нелегального прослушивания и съема информации?

5. С какой стороны монитора LCD уровень ПЭМИН максимальный и на каком расстояние они обнаруживаются приборами?

Тема 1.3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

1. Приведите пример оборудования для измерения параметров физических полей, создаваемых техническими средствами защиты информации

2. На каком максимальном расстоянии от генератора пространственного зашумления можно достичь эффективной защиты радиоканала, т.е. отсутствие возможности подслушивания и перехвата информации?

3. Зависит ли длина защищаемой слаботочной проводной линии от мощности генератора линейного шума?

4. Различаются ли генераторы линейного зашумления для слаботочных и силовых питающих линий?

5. Какие технические средства защиты информации создают максимальные фоновые шумы и физические поля, а какие минимальные?

Тема 1.4. Установка и настройка технических средств защиты информации

1. Какие характеристики наиболее важны для линейного генератора зашумления?

2. Какие характеристики наиболее важны для пространственного генератора зашумления?

3. В чем заключается настройка устройств аппаратного доступа (биометрический сканер / считыватель смарт-карт / считыватель чипов и т.п.)?

4. Какие характеристики наиболее важны для активного блокировщика телефонной линии от прослушивания?

5. Какими параметрами характеризуется аппаратный межсетевой экран и в чем его преимущество перед программным?

Тема 1.5. Проведение измерений параметров побочных электромагнитных излучений и наводок

1. Каков примерный радиус распространения ПЭМИН от типового стационарного ПК, обнаруживаемый приборами?

2. Какие приборы используются для измерения ПЭМИН в офисных помещениях? Приведите примеры.

3. Какой примерно уровень ПЭМИН исходит от неэкранированной (UTP), экранированной (STP,

FTP) витой пары, а также от офисной телефонной линии?.

4. Каков типовой уровень ПЭМИН исходит в непосредственной близости от LCD-монитора?

5. Каков радиус распространения ПЭМИН в непосредственной близости от мобильного телефона в режиме ожидания и в режиме разговора?

Тема 1.6. Проведение аттестации объектов информатизации.

1. Что указывается как минимум в листах аттестации и замечаний, используемых для проведения аттестации объектов информатизации? Существуют ли какие-либо федеральные стандарты на эти документы?

2. Каким принципом нужно руководствоваться при составлении схемы маршрута обхода проверок?

3. Какие критерии защиты учитываются при проведении аттестации объектов информатизации?

4. Чем заканчивается процедура аттестации объектов информатизации? Какие формируются документы?

5. Кто имеет право проводить аттестацию объектов информатизации?

Тема 2.1. Монтаж различных типов датчиков.

1. Перечислите основные требования к установке охранных и пожарных датчиков внутри помещений.

2. Какие инструменты используются при монтаже различных датчиков?

3. Перечислите основные требования к установке периметральных радиоволновых датчиков (излучателей).

4. Перечислите основные требования к установке датчиков освещенности на улице.

5. Перечислите основные требования к установке тензометрических и вибрационных датчиков.

Тема 2.2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация

1. Какие основные моменты должны быть указаны в техническом задании на проектирование установки системы пожарно-охранной сигнализации?

2. Какие существуют требования к прокладки кабелей для пожарно-охранных сигнализаций?

3. Какие типы кабелей используются в качестве шлейфов для датчиков пожарно-охранных сигнализаций?

4. Какие типы кабелей используются для подключения исполнительных устройств пожарно-охранных сигнализаций? Отчего зависит их выбор?

5. Какие работы могут потребоваться после окончания монтажа охранных комплексов перед вводом в эксплуатацию?

Тема 2.3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.

1. Каковы основные принципы измерения физических величин с помощью осциллографа? Какие параметры наиболее важны для осциллографа?

2. Каковы основные принципы измерения с помощью частотомера? Какие параметры наиболее важны для частотомера?

3. Какие существуют виды генераторов, применяемых для лабораторных экспериментов в электронике, электротехнике, радиосвязи?

4. Существует ли отличие генератора импульсов от генератора частоты? Если да, то в чем?

5. Приведите примеры практического применения частотомера и генератора частоты / импульсов.

Тема 2.4. Рассмотрение системы контроля и управления доступом.

1. Что входит в состав системы контроля и управления доступом (СКУД)?

2. Что является центральным узлом, управляющим всей СКУД?

3. Как может быть организовано хранение информации, формируемой СКУД?

4. Каким образом к СКУД подключаются исполнительные устройства, учитывая то, что они могут потреблять гораздо больший ток, чем центральный узел?

5. Какие меры принимаются в СКУД на случай аварийного отключения электроэнергии?

Тема 2.5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.

1. Какие компоненты входят в систему видеонаблюдения?

2. Какие характеристики наиболее важны для видеокамер?

3. Какие виды кабеля чаще всего используются для подключения видеокамер?

4. Что может являться хранилищем информации для системы видеонаблюдения?

5. Что представляет собой пульт управления системы видеонаблюдения? Какой функционал

могут иметь пульты управления системой видеонаблюдения?

Тема 2.6. Рассмотрение датчиков периметра, их принципов работы

1. Какие существуют по типу и принципу действия датчики охраны периметра?

2. Какие периметральные датчики наиболее эффективны и надежны?

3. Какие бывают типы пультов и контроллеров управления периметральными датчиками?

4. В каком виде хранится и как может передаваться информация с контроллера управления периметральными датчиками для анализа и мониторинга во внешнюю среду?

5. Какие типы неисправностей могут быть у различных типов периметральных датчиков?

Тема 2.7. Выполнение звукоизоляции помещений системы зашумления

1. Какие существуют методы для уменьшения / устранения возможности аккустического прослушивания?

2. Приведите пример пассивных методов уменьшения / устранения возможности аккустического прослушивания.

3. Приведите пример активных методов уменьшения / устранения возможности аккустического прослушивания.

4. Какими приборами измеряется уровень утечки / уровень защиты от аккустического прослушивания?

5. Какие существуют две категории материалов для уменьшения / устранения возможности аккустического прослушивания?

Тема 2.8. Реализация защиты от утечки по цепям электропитания и заземления

1. Какие приборы используются для определения уровня утечек информации по цепям электропитания и заземления?

2. Какие существуют методы для определения уровня утечек информации по цепям электропитания и заземления?

3. Через какие устройства возникают утечки информации по цепям электропитания и заземления?

4. В какой участок электроцепи должен подключаться генератор линейного зашумления?

5. Насколько эффективен сетевой фильтр для устранения утечек информации по цепям электропитания и заземления?

Тема 2.9. Разработка организационных и технических мероприятий по заданию преподавателя.

1. Сколько существует классов информационной защиты для предприятий и учреждений?

2. Приведите пример угроз и каналов их осуществления для любого федерального учреждения.

3. Приведите примеры административно-организационных мероприятий по защите от угроз для выбранного учреждения.

4. Приведите примеры технических мероприятий по защите от угроз для выбранного учреждения.

5. Как оценивается эффективность выбранных или реализованных мероприятий?

Тема 2.10. Разработка основной документации по инженерно-технической защите информации

1. Какие виды документов входят в комплект основной документации по инженерно-технической защите информации?

2. Какими средствами можно создать схему расположения средств инженерно-технической защиты, а также схему всех коммуникаций к ним (питающая сеть, информационная сеть)?

3. В каком формате можно создать и хранить основную документацию по инженерно-технической защите информации?

4. Кто отвечает за создание и актуализацию основной документации по инженерно-технической защите информации?

5. Существует ли какое-либо специальное программное средство для автоматизации процесса разработки основной документации по инженерно-технической защите информации? Если да, то приведите пример.

4.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта, необходимых для формирования соответствующих компетенций

По итогам практики аттестуются обучающиеся, выполнившие программу практики и представившие индивидуальные отчеты по практике.

Формой итогового контроля прохождения практики является зачет с оценкой.

Зачет проводится с учетом защиты отчетов, составленных в соответствии с требованиями

программы практики, на основании утвержденного задания на практику.

Защита отчета проводится руководителем практики от кафедры.

При проведении текущего контроля обучающийся представляет выполненные элементы (разделы) отчета по практике.

Преподаватель анализирует их содержание на соответствие, после чего оценивает достигнутый результат.

При проведении промежуточной аттестации обучающийся представляет отчет по практике.

Преподаватель анализирует содержание отчета, затем путем беседы с обучающимся выявляет его способность обосновывать принятые решения.

5. Иные сведения и (или) материалы

Отчет по практике является основным документом, характеризующим работу обучающегося во время практики. Отчет составляется в соответствии с программой практики и содержит следующие разделы:

1. Титульный лист.
2. Рабочий график (план) практики, утвержденный заведующим кафедрой и согласованный с руководителем практики от КузГТУ и (или) предприятия.
3. Введение.
4. Выполнение индивидуального задания.
5. Выводы.
6. Список использованных источников и литературы.

Требования к оформлению отчета

Результаты практики должны быть оформлены в форме отчета, в соответствии с требованиями:

Страницы не обводятся в рамках, поля не отделяюся чертой. Размеры полей не менее: левого - 30 мм, правого - 10 мм, верхнего - 20 мм и нижнего - 20 мм. Нумерация страниц отчета - сквозная: от титульного листа до последнего листа приложений.

Номер страницы на титульном листе не проставляют.

Номер страницы ставят в центре нижней части листа, точка после номера страницы не ставится.

Страницы, занятые таблицами и иллюстрациями, включают в сквозную нумерацию.

Объем отчета по практике должен быть не менее 16 страниц (без учета приложений) машинописного текста (шрифт 14пт, Times New Roman, через 1 интервал). Отчет должен быть отпечатан на формате А4 и подшит. Описания должны быть сжатыми. Объем приложений не регламентируется, а их содержание определяется обучающимся самостоятельно.

Оформление формул

Формулы должны быть оформлены в редакторе формул. В формулах в качестве символов следует применять обозначения, установленные соответствующими государственными стандартами. Расчет по формулам ведется в основных единицах измерения, формулы записываются следующим образом: сначала записывается формула в буквенном обозначении, после знака равенства вместо каждой буквы подставляется ее численное значение в основной системе единиц измерения; затем ставится знак равенства и записывается конечный результат с единицей измерения. Пояснения символов и числовых коэффициентов, входящих в формулу, если они не пояснены ранее в тексте, должны быть приведены непосредственно под формулой. Пояснения каждого символа следует давать с новой строки в той последовательности, в которой символы приведены в формуле. Первая строка пояснения должна начинаться со слова «где» без двоеточия после него.

Переносить формулы на следующую строку допускается только на знаках выполняемых операций, причем знак в начале следующей строки повторяют. При переносе формулы на знаке умножения применяют знак «×».

Формула нумеруется, если далее по тексту она будет востребована. Формулы, за исключением формул, помещаемых в приложении, должны нумероваться сквозной нумерацией арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Допускается нумерация в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой.

Ссылки в тексте на порядковые номера формул дают в круглых скобках, например, в формуле (9.1).

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией, арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения

приложения. Например, формула (А.1).

Оформление иллюстраций

Иллюстрационный материал может быть представлен в виде схем, графиков и т.п. Иллюстрации, помещенные в тексте и приложениях отчета, именуются рисунками.

Иллюстрации выполняются в графических редакторах и располагаются после первой ссылки на них и как можно ближе к ссылке на них в тексте.

Иллюстрации, за исключением иллюстраций приложений, следует нумеровать арабскими цифрами в пределах раздела, либо сквозной нумерацией. Например, «Рисунок 1», «Рисунок 1.1», «Рисунок 2.1».

Ссылку на иллюстрацию дают в следующем виде: «в соответствии с рисунком 1».

Иллюстрация при необходимости может иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок" и наименование помещают после пояснительного текста без точки в конце.

Все рисунки формата большего, чем А4, выносятся в приложения.

Построение таблиц

Слово «Таблица», ее номер и название помещают слева над таблицей. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Название таблицы записывают через тире после слова «Таблица» с прописной буквы без точки в конце. Например: «Таблица 2.1 – Технические данные».

Заголовки граф и строк таблицы пишутся с прописной буквы, а подзаголовки граф- со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц точки не ставят. Заголовки и подзаголовки граф указывают в единственном числе.

Заголовки граф записывают параллельно строкам таблицы. При необходимости допускается перпендикулярное расположение заголовков граф.

Таблицу в зависимости от ее размера помещают под текстом, в котором впервые дана ссылка на нее, или на следующей странице, а при необходимости, в приложении к документу. Допускается помещать таблицу вдоль длинной стороны листа документа.

Если в конце страницы таблица прерывается, ее продолжение помещают на следующей странице. При переносе таблицы на другую страницу название помещают только над первой частью таблицы. Слово «Таблица» указывают только один раз слева над первой частью таблицы а, над другими частями пишут слова «Продолжение таблицы» с указанием номера таблицы.

Все таблицы, за исключением таблиц приложений, нумеруются арабскими цифрами сквозной нумерацией. Допускается нумеровать таблицы в пределах раздела. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенного точкой.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавления перед цифрой обозначения приложения, например, «Таблица А.1», если она приведена в приложении А.

На все таблицы документа должны быть приведены ссылки в тексте, при ссылке слово «таблица» пишется полностью с указанием ее номера.

Оформление списка литературы

Список литературы является обязательным (ненумерованным) разделом отчета, оформляется в соответствии с ГОСТ 7.1-2003 "Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления", включается в содержание отчета.

Список должен содержать сведения обо всех источниках, использованных при составлении отчета. Располагать источники в списке рекомендуется в порядке появления ссылок в тексте. Возможно и другое разрешенное нормативными документами расположение источников в списке.

Оформление приложений

Приложения оформляют как продолжение отчета и помещают в конце отчета в порядке ссылок на них в тексте. В тексте отчета на все приложения должны быть даны ссылки. Каждое приложение следует начинать с нового листа с указанием на верху посредине страницы слова «ПРИЛОЖЕНИЕ» и его обозначения, например, «ПРИЛОЖЕНИЕ А». Приложение должно иметь заголовок, который записывается симметрично относительно текста с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами алфавита, начиная с А, кроме букв Е, З, Й, О, Ч, Ь, Ы, Ъ. Допускается обозначение приложения буквами латинского алфавита, за исключением букв I и O. Приложения выполняют на листах формата А4, А3, А4Х3,А4х4, А2, А1 по ГОСТ 2.301.

Приложения должны иметь общую с остальной частью документа сквозную нумерацию страниц.

Все приложения должны быть перечислены в содержании отчета и с указанием их номеров и заголовков.

Документ подписан электронной подписью
Яковлев Алексей Николаевич
Ректор
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф. ГОРБАЧЕВА"

00E16CF19AEF1B29DB06BEB121D580D3D8
Срок действия с 19.03.2024 до 12.06.2025
УЦ: Казначейство России

Подписано: 30.09.2024 11:21 (UTC+7)

1712023495