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: 21.04.2026 14:04:02

Сьянова Татьяна Юрьевна

Программа производственной 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 2026 г.


1770004964

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационной безопасности
Должность: заведующий кафедрой (к.н.,спд)
Дата: 02.02.2026 12:37:14

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 8 от 16.04.2026

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационной безопасности
Должность: заведующий кафедрой (к.н.,спд)
Дата: 21.04.2026 11:19:52

Прокопенко Евгения Викторовна

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

Протокол № 8 от 16.04.2026

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационной безопасности
Должность: заведующий кафедрой (к.н.,спд)
Дата: 21.04.2026 11:20:17

Прокопенко Евгения Викторовна

Согласовано заместителем директора по УР ИПО

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационной безопасности
Должность: Заместитель директора по учебной работе
Дата: 21.04.2026 11:20:17

Полуэктова Наталья Сергеевна

Согласовано заместителем директора по МР ИПО


1770004964

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: кафедра информационной безопасности
Должность: Заместитель директора по методической работе
Дата: 21.04.2026 11:20:17

Бекшенева Ксения Игоревна


1770004964

1. Общая характеристика рабочей программы практики

Производственная 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)	**108 часов**
Промежуточная аттестация в форме зачета .	

2.2 Тематический план и содержание практики

Наименование тем практики	**Виды работ**	**Объем часов**
Вид профессиональной деятельности: Защита информации техническими средствами		
	Консультация	2
Техническая защита информации и инженерно-технические средства физической защиты объектов информатизации	Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;	24
	Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	24
	Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	34
	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	24
Всего:		108

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. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1191479 (дата обращения: 27.03.2026)

2. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для СПО / Внуков А. А.. – 3-е изд., пер. и доп. – Москва : Юрайт, 2024. – 161 с. – ISBN 978-5-534-13948-8. – URL: https://urait.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-542340 (дата обращения: 02.02.2026). – Текст : электронный.

3.2.2 Дополнительная литература

1. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1189341 (дата обращения: 27.03.2026)

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: 02.02.2026). – Текст :

электронный.

2. Методические указания по оформлению отчетов по практике, курсовых работ (проектов) и дипломных проектов (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: 02.02.2026). – 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 производственной 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 производственной 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. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации

Задание 1. Ознакомьтесь с перечнем технических средств, с которыми предстоит работать.

Задание 2. По заданию наставника выполните физическую установку технических средств защиты информации, а также соединение кабелей. До проверки наставником не подавать питающее напряжение.

Задание 3. Пронаблюдайте за действиями наставника и законспектируйте наиболее важные моменты по настройке и регулировке технических средств защиты информации.

Задание 4. Пронаблюдайте за действиями наставника и законспектируйте наиболее важные моменты по программной настройке технических средств защиты информации.

Задание 5. Под наблюдением наставника выполните программную проверку установленных и настроенных технических средств защиты информации.

Тема 1.2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

Задание 1. Ознакомьтесь с перечнем оборудования, с которыми предстоит работать.

Задание 2. По заданию наставника выполните физическую установку заданного оборудования, а также монтаж и подключение кабелей, при необходимости оконцовку кабелей разъемами. До проверки наставником не подавать питающее напряжение.

Задание 3. Пронаблюдайте процесс установки наиболее сложных устройств и оборудования, выполняемый наставником или внешними специалистами. Законспектируйте наиболее важные моменты

Задание 4. Пронаблюдайте за процессом настройки оборудования, выполняемым наставником или внешними специалистами.

Задание 5. Пронаблюдайте за процессом проверки оборудования, выполняемым наставником или внешними специалистами. Законспектируйте наиболее важные моменты.

Тема 1.3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам.

Задание 1. Ознакомьтесь с перечнем средств защиты информации от несанкционированного съёма и утечки по техническим каналам, с которыми предстоит работать.

Задание 2. По заданию наставника выполните физическую установку заданных средств, а также монтаж и подключение кабелей. До проверки наставником не подавать питающее напряжение.

Задание 3. Пронаблюдайте процесс установки наиболее сложных средств защиты, выполняемый наставником или внешними специалистами. Законспектируйте наиболее важные моменты

Задание 4. Пронаблюдайте за процессом настройки средств защиты, выполняемым наставником или внешними специалистами.

Задание 5. Пронаблюдайте за процессом проверки средств защиты, выполняемым наставником или внешними специалистами. Законспектируйте наиболее важные моменты.

Тема 1.4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.

Задание 1. Найти в сети Интернет, а также с помощью справочно-правовых систем «Консультант+» и «Гарант» нормативно правовые акты. относящиеся к обеспечению защиты информации техническими средствами и ознакомиться с ними.

Задание 2. При наличии приложенной к комплексу технических средств нормативных методических документов по обеспечению защиты информации техническими средствами, а при их отсутствии найти в Интернете эти документы и ознакомиться с ними.

Задание 3. На основании анализа полученной информации в нормативно правовых актах, нормативных методических документах по обеспечению защиты информации техническими средствами сделать вывод о том, как в данной организации соблюдаются все пункты этих документов.

Задание 4. Выписать те пункты, которые не соблюдаются и предложить варианты по их соблюдению.

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. Анализ принципов построения систем информационной защиты производственных подразделений.

1. Перечислите наиболее распространенные типы технических средств защиты информации
2. Какие требования предъявляются к монтажу технических средств защиты информации с точки зрения скрытности и в то же время возможности проверки и обслуживания?
3. Какие приборы и инструменты используются при настройке технических средств защиты информации?
4. Какие параметры технических средств защиты информации настраиваются программным путем?
5. Как и с помощью чего выполняется программная проверка установленных и настроенных технических средств защиты информации?

Тема 1.2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

1. Приведите примеры средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.
2. Перечислите некоторые наиболее распространенные требования по установке оборудования и систем охраны, обеспечения безопасности и инженерной защиты.
3. Кто уполномочен выполнять установку, настройку, обслуживание оборудования и систем охраны, обеспечения безопасности и инженерной защиты?
4. В чем заключается настройка каждого типа оборудования и систем охраны, обеспечения безопасности и инженерной защиты (кратко)?
5. Как, кем и с помощью чего выполняется проверка оборудования и систем охраны, обеспечения безопасности и инженерной защиты?

Тема 1.3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам.

1. Приведите примеры наиболее распространенных средств защиты информации от несанкционированного съёма и утечки по техническим каналам.

2. Перечислите наиболее важные требования к эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам?

3. На чем основано действие наиболее распространенных средств защиты информации от несанкционированного съёма и утечки по техническим каналам?

4. В чем заключается настройка средств защиты информации от несанкционированного съёма и утечки по техническим каналам?

5. Что включает в себя процедура обслуживания средств защиты информации от несанкционированного съёма и утечки по техническим каналам?

Тема 1.4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.

1. В чьей юрисдикции находится разработка нормативно правовых актов по обеспечению защиты информации техническими средствами?

2. В чьей юрисдикции находится разработка нормативных методических документов по обеспечению защиты информации техническими средствами?

3. Могут ли внешние нормативные и методические документы дополняться внутренними документами и правилами предприятия?

4. Кто имеет право проверять соблюдение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами?

5. Кто отвечает за соблюдение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами на предприятии?

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 отделяются 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.