

МИНОБРНАУКИ РОССИИ

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

Филиал КузГТУ в г. Новокузнецке

УТВЕРЖДАЮ

Заместитель директора по УР,
совмещающая обязанности по должности
директора филиала КузГТУ в г. Новокузнецке

_____ Т.А. Евсина

«27» июня 2024 г.

**Фонд оценочных средств
по УП.03.01 Учебной практике
по ПМ 03 «Защита информации техническими средствами»**

Специальность

«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обучения
очная

Год набора 2022

Срок обучения на базе
среднего общего образования – 2 года 10 месяцев

Новокузнецк 2024 г.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по учебной практике по ПМ 03 «Защита информации техническими средствами»

1. Фонд оценочных средств

1.1 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	<p>Знания: порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;</p> <p>Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;</p> <p>Практический опыт: установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации;</p>	Проверка отчёта по разделам практики.
	ПК 3.2	<p>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</p>	Проверка отчёта по разделам практики.

		<p>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;</p> <p>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;</p> <p>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;</p>	
	ПК 3.3	<p>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</p>	Проверка отчёта по разделам практики.

		<p>утечки информации; Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;</p> <p>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;</p>	
	ПК 3.4	<p>Знания: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;</p> <p>Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;</p> <p>Практический опыт: проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации;</p>	Проверка отчёта по разделам практики.
	ПК 3.5	<p>Знания: основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации;</p> <p>Умения: применять средства охранной сигнализации, охранного телевидения и систем</p>	Проверка отчёта по разделам практики.

		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;	
--	--	---	--

1.2 Оценочные средства при текущем контроле

Текущий контроль 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

1.3. Оценочные средства при промежуточном контроле (зачет, дифференцированный 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 промежуточной 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

2. Примеры заданий по учебной практике по ПМ.03 «Защита информации техническими средствами»

Код компетенции	Типы заданий и диагностические задания	Эталонные ответы
ПК 3.1	<i>Прочитайте текст и ответьте на вопрос</i> На каком расстоянии от силовой кабельной линии электропитания с помощью приборов можно обнаружить ПЭМИН, достаточные для нелегального прослушивания и съема информации?	300 метров
	<i>Прочитайте текст и ответьте на вопрос</i> Какие периметральные датчики наиболее эффективны и надежны?	Радиолучевые, инфракрасные
	<i>Прочитайте текст и ответьте на вопрос</i> Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?	Руководство
	<i>Прочитайте текст и ответьте на вопрос</i> Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?	Препятствие
	<i>Прочитайте текст и ответьте на вопрос</i> Как называется попытка реализации угрозы?	Атака
ПК 3.2	<i>Прочитайте текст и ответьте на вопрос</i> На каком максимальном расстоянии от генератора пространственного зашумления можно достичь эффективной защиты радиоканала, т.е. отсутствие возможности подслушивания и перехвата информации?	100 метров
	<i>Прочитайте текст и ответьте на вопрос</i> Какой из приборов используется для определения уровня утечек информации по цепям электропитания и заземления?	Генератор зашумления
	<i>Прочитайте текст и дополните ответ</i> К основным типам средств воздействия на компьютерную сеть относится	Логические закладки
	<i>Прочитайте текст и ответьте на вопрос</i> Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?	Физические
ПК 3.3	<i>Прочитайте текст и ответьте на вопрос</i> Какая характеристика наиболее важна для активного блокировщика телефонной линии от прослушивания?	Помехи
	<i>Прочитайте текст и ответьте на вопрос</i> Сколько существует классов информационной защиты для предприятий и учреждений?	4
	<i>Прочитайте текст и дополните ответ</i> Угроза информационной системе (компьютерной сети) – это _____ событие.	Вероятное
	<i>Прочитайте текст и ответьте на вопрос</i>	Доступность

	Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?	
ПК 3.4	<i>Прочитайте текст и ответьте на вопрос</i> Каков радиус распространения ПЭМИН в непосредственной близости от мобильного телефона в режиме ожидания и в режиме разговора?	30 см от антенны
	<i>Прочитайте текст и ответьте на вопрос</i> В каком формате можно создать и хранить основную документацию по инженерно-технической защите информации?	Бумажном и электронном
	<i>Прочитайте текст и дополните ответ</i> Окончательно, ответственность за защищенность данных в компьютерной сети несет	Владелец сети
	<i>Прочитайте текст и дополните ответ</i> Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это	Информационная война
	<i>Прочитайте текст и дополните ответ</i> Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано называется	Надежность
ПК 3.5	<i>Прочитайте текст и ответьте на вопрос</i> Какие существуют методы для уменьшения / устранения возможности акустического прослушивания?	Звукоизоляция, шумление
	<i>Прочитайте текст и дополните ответ</i> Недостатком дискретных моделей политики безопасности является _____	Статичность
	<i>Прочитайте текст и дополните ответ</i> Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется _____	Профилем защиты
	<i>Прочитайте текст и дополните ответ</i> Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет _____	Криптоанализ
	<i>Прочитайте текст и ответьте на вопрос</i> Какое количество уровней адекватности, которое определяют «Европейские критерии»?	7

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.