

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 ПП.03.01 Производственной практике
по профессиональному модулю
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 текущего контроля, промежуточной аттестации обучающихся производственной практики по профессиональному модулю ПМ.03 «Защита информации техническими средствами»

1. Фонд оценочных средств

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

1.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по практике.

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; 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 защиты информации; методики инструментального контроля эффективности защиты</p>	Проверка отчёта по разделам практики.

		<p>информации, обрабатываемой средствами вычислительной техники на объектах</p>	
		<p>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;</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 условия формирования технических каналов утечки информации;</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 ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по</p>	Проверка отчёта по разделам практики.

		требованиям безопасности информации;	
	ПК 3.4	<p>Знания: номенклатуру действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; 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 средств физической защиты объектов информатизации;</p> <p>Умения: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации;</p> <p>Практический опыт: установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты;</p>	Проверка отчёта по разделам практики.

1.3. Оценочные средства при текущем контроле

Текущий контроль 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

1.4. 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 производственной практики по ПМ.03 «Защита информации техническими средствами»

Код компетенции	Типы заданий и диагностические задания	Эталонные ответы
ПК 3.1.	<i>Прочитайте текст и дайте ответ на вопрос</i> Кто уполномочен выполнять установку, настройку, обслуживание оборудования и систем охраны, обеспечения безопасности и инженерной защиты?	Техник по защите информации
	<i>Прочитайте текст и дополните ответ</i> Если граждане и должностные лица работают с закрытыми сведениями то на них распространяется федеральный закон «_____»	О государственной тайне
	<i>Прочитайте текст и дополните ответ</i> Перехват, который осуществляется путем использования оптической техники называется _____	Видеоперехват
	<i>Прочитайте текст и дополните ответ</i> Пошаговая инструкция по выполнению задач называется _____	Процедура
	<i>Прочитайте текст и ответьте на вопрос</i> Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?	Поддержка руководства
	ПК 3.2	<i>Прочитайте текст и дайте ответ на вопрос</i> Что включает в себя процедура обслуживания средств _____

	защиты информации от несанкционированного съёма и утечки по техническим каналам?	
	<i>Прочитайте текст и дополните ответ</i> Непосредственная причина возникновения угрозы называется:	Источник угрозы
	<i>Прочитайте текст и дополните ответ</i> Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей	Фишинг
	<i>Прочитайте текст и дополните ответ</i> Основными рисками информационной безопасности являются потеря, искажение и информации.	Утечка
	<i>Прочитайте текст и дополните ответ</i> Основными субъектами информационной безопасности являются государство и _____.	Бизнес
ПК.3.3	<i>Прочитайте текст и дайте ответ на вопрос</i> Кто отвечает за соблюдение нормативно-правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами на предприятии?	Администрация
	<i>Прочитайте текст и дополните ответ</i> Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это _____	Пароль пользователя
	<i>Прочитайте текст и дополните ответ</i> Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это _____	Защита информации
	<i>Прочитайте текст и дополните ответ</i> Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных называется _____ безопасность.	Компьютерная
	<i>Прочитайте текст и дополните ответ</i> Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это _____ оружие.	Информационное
ПК.3.4	<i>Прочитайте текст и дайте ответ на вопрос</i> С помощью чего выполняется программная проверка установленных и настроенных технических средств защиты информации?	Антивирусная защита
	<i>Прочитайте текст и дополните ответ</i>	Коммерческая тайна

	Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынках товаров, работ или услуг это	
	<i>Прочитайте текст и дополните ответ</i> Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется	Сканер
	<i>Прочитайте текст и дополните ответ</i> Исследование возможности расшифрования информации без знания ключей	Криптоанализ
	<i>Прочитайте текст и дополните ответ</i> Вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач называется	Информационные ресурсы
ПК.3.5	<i>Прочитайте текст и дайте ответ на вопрос</i> Какие параметры технических средств защиты информации настраиваются программным путем?	Контроль работоспособности
	<i>Прочитайте текст и дополните ответ</i> Для реализации технологии RAID создается	Псевдодрайвер
	<i>Прочитайте текст и дополните ответ</i> Едиственный ключ используется в криптосистемах называется	Симметричный
	<i>Прочитайте текст и дополните ответ</i> Запись определенных событий в журнал безопасности сервера называется	Аудитом
	<i>Прочитайте текст и дополните ответ</i> Главным параметром криптосистемы является показатель	Криптостойкости

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.