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.

Рабочая программа производственной практики по профессиональному модулю «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении»

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Форма обучения
очная

Год набора 2023

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

Новокузнецк 2024 г.

РАБОЧУ ПРОГРАММУ ПРАКТИКИ СОСТАВИЛ

Преподаватель первой категории _____ С.А. Строкин

(подпись)

СОГЛАСОВАНО

Заведующий отделением СПО _____ Т.В. Гуменникова

(подпись)

СОГЛАСОВАНО

Заместитель директора по УР _____ Т.А. Евсина

(подпись)

Рабочая программа обсуждена на заседании

учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол №9 от 27.06.2024г.

1. Общая характеристика рабочей программы практики

Производственная практика является частью программы подготовки профессинального модуля «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении» основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Прохождение практики направлено на формирование компетенций:

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
Знать: теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;
Уметь: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;
Иметь практический опыт: администрирование автоматизированных систем в защищенном исполнении;

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
Знать: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;
Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;
Иметь практический опыт: эксплуатация компонентов систем защиты информации автоматизированных систем;

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
Знать: принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;
Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности;
Иметь практический опыт: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении;

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 .	

2.2 Тематический план и содержание практики

Наименование тем практики	Виды работ	Объем часов
Вид профессиональной деятельности: Эксплуатация автоматизированных (информационных) систем в защищённом исполнении		

Раздел 1. Операционные системы и базы данных	Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	6
	Обслуживание средств защиты информации прикладного и системного программного обеспечения	6
	Настройка программного обеспечения с соблюдением требований по защите информации	6
	Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	6
	Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением	6
	Настройка встроенных средств защиты информации программного обеспечения	6
	Проверка функционирования встроенных средств защиты информации программного обеспечения	6
	Своевременное обнаружение признаков наличия вредоносного программного обеспечения	6
Раздел 2. Сети и системы передачи информации, эксплуатация компьютерных сетей, автоматизированных (информационных) систем в защищенном исполнении	Обслуживание средств защиты информации в компьютерных системах и сетях	6
	Обслуживание систем защиты информации в автоматизированных системах	6
	Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем	6
	Проверка работоспособности системы защиты информации автоматизированной системы	6
	Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	6

	Контроль стабильности характеристик системы защиты информации автоматизированной системы	8
	Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	10
	Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	2
Всего:		108

3. Условия реализации программы практики

3.1 Требования к минимальному материально-техническому обеспечению

3.1 Требования к минимальному материально-техническому обеспечению

Наличия учебного кабинета «информационной безопасности, лаборатории информационных технологий».

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий «Информационная безопасность»;
- электронное учебное пособие.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением, мультимедийный диапроектор, интерактивная доска.

3.2 Информационное обеспечение реализации программы

1. Основная литература

1.Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/472333 (дата обращения: 11.11.2023).

2.Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2021. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475896 (дата обращения: 11.11.2023).

2. Дополнительная литература

1.Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/474839 (дата обращения: 11.11.2023).

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: 26.09.2023). – 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: 26.09.2023). – Текст : электронный.

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 "Эксплуатация автоматизированных (информационных) систем в защищённом исполнениии"

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**
Эксплуатация автоматизированных (информационных) систем в защищённом исполнении)	ПК 1.1	**Знать:** состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств; **Уметь:** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; **Иметь практический опыт:** установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем;	Проверка отчёта по разделам практики.
	ПК 1.2	**Знания:** теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; **Умения:** организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации	Проверка отчёта по разделам практики.

		автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; **Практический опыт:** администрирование автоматизированных систем в защищенном исполнении;	
	ПК 1.3	**Знания:** порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; **Умения:** настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; **Практический опыт:** эксплуатация компонентов систем защиты информации автоматизированных систем;	Проверка отчёта по разделам практики.
	ПК 1.4	**Знания:** принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; **Умения:** обеспечивать работоспособность, обнаруживать и устранять неисправности; **Практический опыт:** диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении;	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 установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

Задание 1. Изучите эксплуатационную документацию к АИС. Выясните порядок установки ее компонентов, описание средств информационной защиты, требования к аппаратному обеспечению, на которое планируется установить АИС.

Задание 2. По заданию наставника выполните первичную установку указанных компонентов АИС на заданный компьютер, удовлетворяющий аппаратным требованиям.

Задание 3. Пронаблюдайте и законспектируйте действия наставника по настройке системы информационной защиты АИС.

Задание 4. По заданию наставника выполните тесты для проверки функционирования АИС и ее системы защиты. Законспектируйте полученные навыки.

Тема 1.2. Обслуживание средств защиты информации прикладного и системного программного обеспечения.

Задание 1. Ознакомьтесь с вариантами средств защиты информации прикладного и системного программного обеспечения. Проанализируйте каждое из средств.

Задание 2. Сделайте выбор средства защиты информации и выполните его установку и настройку.

Задание 3. Выполните полную настройку установленного средства защиты информации.

Задание 4. Проверьте отсутствие конфликтов с основным защищаемым прикладным и системным ПО, а также степень загрузки аппаратной системы (память, жёсткий диск, процессор, сеть). При чрезмерной загрузке удалите данное средство защиты и установите другое, повторив п. 2 – 4.

Тема 1.3. Настройка программного обеспечения с соблюдением требований по защите информации.

Задание 1. Изучите требования по защите информации для заданного ПО.

Задание 2. Оцените возможность удовлетворения требований по защите информации в данных конкретных условиях.

Задание 3. Если вышеуказанные требования применимы, то выполнить настройку внутренних средств защиты информации, а при необходимости в соответствии с п.1 применить внешние средства защиты информации.

Тема 1.4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам

Задание 1. Выполнить первичную установку антивирусного ПО, настроить обновление антивирусных баз.

Задание 2. Изучить возможные варианты настроек для автоматизации поиска и устранения вирусных угроз.

Задание 3. Настроить работу антивирусного ПО в соответствии с заданными шаблонами (какие объекты проверять автоматически при запуске, что делать с зараженными объектами, уровень безопасности, исключения и т.п.).

Тема 1.5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением

Задание 1. Объяснить пользователям опасность и серьезность возможных информационных угроз при работе с программным обеспечением.

Задание 2. Привести типовые примеры реализации информационных угроз.

Задание 3. Объяснить пользователям основные моменты политики информационной безопасности в данном учреждении, их ответственность за соблюдение и как правильно соблюдать правила этой политики. Потребовать росписи всех пользователей в специальном журнале по окончании инструктажа.

Задание 4. Выслать по корпоративной почте всем пользователям краткую памятку по соблюдению информационной безопасности.

Тема 1.6. Настройка встроенных средств защиты информации программного обеспечения

Задание 1. Изучить встроенные средства защиты информации в составе ПО.

Задание 2. Выполнить настройку встроенных средств защиты информации.

Тема 1.7. Проверка функционирования встроенных средств защиты информации программного обеспечения.

Задание 1. Разработать тесты, имитирующие угрозы или некорректные действия пользователя в различных аспектах

Задание 2. Выполнить разработанные тесты, имитирующие угрозы или некорректные действия пользователя в различных аспектах. Зафиксировать успешность или неуспешность прохождения тестов.

Задание 3. При наличии неуспешных тестов проанализировать имеющиеся проблемы информационной защиты и предложить возможное решение.

Тема 1.8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения

Задание 1. Изучить имеющие настройки ПО, осуществляющего защиту от вредоносного кода.

Задание 2. Написать или найти в сети Интернет тестовые вредоносные коды и изучить реакцию защищающего ПО на эти коды.

Задание 3. При неверной реакции или ее отсутствии на вредоносный код выполнить перенастройку системы защиты. Проверить повторно реакцию защиты на вредоносные коды, которые ранее не были обработаны или замечены.

Задание 4. При повторном отсутствии или неверной реакции на вредоносный код предложить альтернативное или дополнительное решение для повышения эффективности системы защиты.

Тема 2.1. Обслуживание средств защиты информации в компьютерных системах и сетях

Задание 1. Ознакомиться с настройками встроенного в ОС клиентского компьютера и шлюза межсетевых экранов, при необходимости откорректировать их.

Задание 2. На серверах и шлюзе проверить настройки внешнего программного или программно-аппаратного межсетевого экрана.

Задание 3. Изучить документацию к системе защиты от ПЭМИН в локальной сети / раздел «обслуживание» и при необходимости выполнить требуемые рекомендации по обслуживанию.

Задание 4. На клиентских компьютерах, использующих дополнительные средства аппаратной аутентификации изучить содержимое системных журналов на предмет возможных ошибок в работе этих средств. Если имеются многочисленные жалобы на работу этих устройств и профилактические меры (например, протирка лазерного или ИК – датчика) не дают эффекта, то принять решение о замене этого устройства.
Задание 5. В сетях, использующих генераторы электромагнитного шума, проверить работу последних в соответствии с инструкцией. При неудовлетворительной их работе выполнить регулировку или замену.

Тема 2.2. Обслуживание систем защиты информации в автоматизированных системах.

Задание 1. Проанализировать системные отчеты АИС на предмет выявленных ошибок.
Задание 2. Разработать план устранения этих ошибок (если они были обнаружены). Разделить мероприятия по устранению ошибок на программные и аппаратные.
Задание 3. Приступить к устранению ошибок на основе разработанного плана.
Задание 4. Проверить работу подсистемы архивации данных, а также состояние дисковых накопителей архивации. При необходимости заменить их.
Задание 5. С помощью рекомендованных тестов выполнить комплексную проверку АИС. Все результаты зафиксировать в журнале.

Тема 2.3. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем.

Задание 1. Изучить инструкции по проведению регламентных работ по эксплуатации систем защиты информации автоматизированных систем. При необходимости законспектировать наиболее важные моменты.
Задание 2. По заданию наставника выполнить определенные процедуры, при необходимости задать вопросы наставнику.
Задание 3. Пронаблюдать выполнение финальных процедур в регламентных работах, выполняемых наставником. При необходимости задать вопросы и законспектировать.
Задание 4. По заданию и / или наблюдением наставника выполнить тестирование системы защиты информации АИС после выполнения регламентных работ и доложить о результатах теста наставнику.

Тема 2.4. Проверка работоспособности системы защиты информации автоматизированной системы.

Задание 1. Изучить инструкцию и ознакомиться с компонентами системы защиты информации автоматизированной системы.
Задание 2. Выполнить аппаратную проверку, при необходимости – и электрические измерения, используя осциллограф и мультиметр.
Задание 3. Выполнить тесты, рекомендованные разработчиком системы на предмет надежности системы защиты информации. При обнаружении проблем в тестах выписать их, проанализировать и разработать план мероприятий по устранению проблем.

Тема 2.5. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации.

Задание 1. Изучить документацию к системе защиты информации автоматизированной системы.
Задание 2. Изучить реальные условия, в которых работает АИС и система ее защиты.
Задание 3. Сравнить параметры паспортные и реальные, выписать несоответствия конфигурации в системе защиты информации АИС. Сделать записи в журнал и принять решении об устранении несоответствий.

Тема 2.6. Контроль стабильности характеристик системы защиты информации автоматизированной системы.

Задание 1. С помощью инструкции к системе защиты информации АИС выполнить измерение характеристик системы защиты в нескольких различных режимах.
Задание 2. Проанализировать стабильность измеренных характеристик и величину их отклонения от паспортных. Результаты зафиксировать.

Задание 3. Предложить варианты приведения характеристик, имеющих значительные отклонения к норме.
Задание 4. После устранения отклонений провести повторные измерения требуемых характеристик в соответствии с инструкцией.

Тема 2.7. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем.

Задание 1. Составьте в Excel таблицу со следующими столбцами:

- наименование и модель модуля защиты.
- место установки и работы модуля защиты
- дата предыдущего обслуживания (плановая или аварийная)
- дата текущего обслуживания
- дата рекомендуемого очередного обслуживания
- выполненные работы и замененные компоненты (при необходимости)
- Роспись исполнителя
- Примечания и рекомендации

Задание 2. Для облегчения заполнения таблицы вставьте элемент «Раскрывающий список», который позволит быстро выбирать наиболее часто используемые типовые параметры. Проверьте работу вставленных элементов автоматизации.
Задание 3. Проверьте возможность печати фрагмента таблицы с размещением ее на одну страницу по ширине, при необходимости произведите коррекцию полей, колонтитулов, ширины столбцов, высоты строк, шрифта и т.п….

Тема 2.8. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.

Задание 1. Изучить инструкцию по выводу из эксплуатации АИС
Задание 2. По заданию наставника произвести демонтаж всех носителей информации и сдать их наставнику. Уделить особое внимание безопасному надежному хранению (утилизации) дисковых накопителей информации. При хранении (утилизации) все носители, имеющие отношение к выводимой АИС должны быть сданы по роспись ответственному лицу с соответствующей записью в журнале.
Задание 3. Пронаблюдать процедуру сдачи на хранение или утилизацию ответственному лицу и заполнение журнала.
Задание 4. Выполнить физическое и / или программное отключение линии локальной сети, к которой была подключена выведенная из эксплуатации АИС.

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. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

1. На какие типы делятся системы защиты АИС?
2. Какие параметры операционных систем являются критичными при установке на компьютер (или подключение его к) АИС?
3. Какие параметры аппаратного обеспечения являются критичными при установке на компьютер (или подключение его к) АИС?.
4. В чем заключается настройка системы информационной защиты АИС?
5. Какие типы тестов используются для проверки функционирования АИС и ее системы защиты?

Тема 1.2. Обслуживание средств защиты информации прикладного и системного программного обеспечения.

1. Какие существуют виды средств защиты информации прикладного и системного программного обеспечения?
2. В чем заключается процедура обслуживания средств защиты информации прикладного ПО?
3. В чем заключается процедура обслуживания средств защиты информации системного ПО?
4. Какие вспомогательные инструменты и средства используются в процессе обслуживания средств защиты информации прикладного и системного ПО?
5. Что является критерием исправности средств защиты информации прикладного и системного ПО?

Тема 1.3. Настройка программного обеспечения с соблюдением требований по защите информации.

1. Какие требования по защите информации предъявляются чаще всего к настройке программного обеспечения?
2. Оказывает ли какое-либо негативное влияние система защиты информации на работу ПО с точки зрения надежности и скорости работы?
3. Каким образом выполняется проверка корректности настроек ПО с учетом требований по защите информации?
4. Какие дополнительные знания и умения нужны сотруднику, использующему ПО в условиях защищенности информации?
5. Чем опасна неверная настройка или неисправность системы защиты информации при работе ПО?

Тема 1.4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам

1. Что такое шаблоны настроек и для чего они нужны?
2. Какие рутинные действия в антивирусной программе можно автоматизировать?
3. Какие уровни реакции (политики) существуют в антивирусной программе на примере одного из продукта: Kaspersky Antivirus, Eset NOD32, Dr WEB?
4. Чем следует руководствоваться при составлении шаблона настроек?
5. Можно ли сохранить фал конфигурации (шаблонов) на случай переустановки антивирусного ПО?

Тема 1.5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением.

1. Какие аргументы серьезности проблемы информационной безопасности нужно использовать для сотрудников, являющихся непрофессионалами в области ИТ?
2. Какие типовые примеры реализации информационных угроз рекомендуется использовать для сотрудников, являющихся непрофессионалами в области ИТ?
3. Что относится к основным моментам политики информационной безопасности в данном учреждении?
4. Какова допустимая длительность озвучивания инструктажа для наилучшего усвоения?
5. Какие моменты инструктажа лучше всего изложить и донести до пользователей в текстовом виде?

Тема 1.6. Настройка встроенных средств защиты информации программного обеспечения

1. Каким образом могут быть реализованы встроенных средств защиты информации программного обеспечения?
2. В чем заключается настройка встроенных средств защиты информации программного обеспечения?
3. Что является критерием правильности настроек встроенных средств защиты информации программного обеспечения?
4. Всегда и любое ли ПО имеет встроенные средства защиты информации программного обеспечения?
5. Всегда ли достаточно встроенных средств защиты информации программного обеспечения?

Тема 1.7. Проверка функционирования встроенных средств защиты информации программного обеспечения.

1. Какие существуют методы проверки функционирования встроенных средств защиты информации программного обеспечения?
2. Какие существуют инструменты проверки функционирования встроенных средств защиты информации программного обеспечения?
3. Что является критерием качества функционирования встроенных средств защиты информации программного обеспечения?
4. В каких случаях требуется проверка функционирования встроенных средств защиты информации программного обеспечения?
5. Как фиксируется факт проведения проверки функционирования встроенных средств защиты информации программного обеспечения?

Тема 1.8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения

1. Какими средствами осуществляется своевременное обнаружение признаков вредоносного кода?
2. Каковы критерии своевременности обнаружения признаков вредоносного кода?
3. Что является признаками вредоносного кода?
4. Каким действиям со стороны системы защиты должен подвергаться вредоносный код в ПО?
5. Какие действия должны периодически выполняться ИТ- специалистом, чтобы обнаружение признаков наличия вредоносного программного обеспечения было всегда своевременным?

Тема 2.1. Обслуживание средств защиты информации в компьютерных системах и сетях

1. Какие средства входят в состав систем защиты информации в компьютерных системах и сетях?
2. Какие типовые шаблоны настроек межсетевых экранов используются в большинстве случаев на клиентских ПК, серверах, а также на специально выделенных программных или программно-аппаратных межсетевых экранах?
3. Что включает в себя процедура настройки межсетевого экрана?
4. В чем заключается обслуживание средств защиты информации в компьютерных системах и сетях?
5. Как производится проверка средств защиты информации в компьютерных системах и сетях перед или после обслуживания?

Тема 2.2. Обслуживание систем защиты информации в автоматизированных системах

1. В каком виде могут быть представлены системные отчеты АИС на предмет выявленных ошибок в работе систем защиты информации?
2. Назовите основные принципы и правила разработки плана устранения ошибок в работе системы защиты информации в АИС?
3. Какие ошибки в работе системы защиты информации АИС устраняются в первую очередь?
4. Как выполняется проверка накопителей информации и подсистемы архивации данных?
5. Какие тесты, например, могут использоваться для комплексной проверки работы АИС и системы защиты информации в них?

Тема 2.3. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем.

1. Что включают в себя регламентные работы по эксплуатации систем защиты информации АИС?

2. Какие программные и аппаратные средства используются при регламентных работах по эксплуатации систем защиты информации АИС?
3. Какие проблемы могут быть обнаружены чаще всего при регламентных работах по эксплуатации систем защиты информации АИС?
4. Какова периодичность проведения регламентных работ по эксплуатации систем защиты информации АИС?
5. Кто проводит и кто принимает выполнение регламентных работ по эксплуатации систем защиты информации АИС?

Тема 2.4. Проверка работоспособности системы защиты информации автоматизированной системы.

1. В чем заключается проверка работоспособности системы защиты информации АИС?
2. Требуются ли измерения каких-либо физических величин при проверке работоспособности системы защиты информации АИС?
3. Какими программными и /или аппаратными средствами проводится проверка работоспособности системы защиты информации АИС?
4. Допускается ли отклонение каких-либо параметров в работе системы защиты информации АИС, и если да, то каких и насколько?
5. Является ли проверка работоспособности системы защиты информации АИС гарантом того, что в течение определенного времени вероятность сбоя системы будет равна нулю?

Тема 2.5. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации.

1. Какие параметры конфигурации систем защиты информации АИС подлежат контролю на соответствие эксплуатационной документации? Приведите примеры.
2. Как осуществляется контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации?
3. Допустимо ли некоторое отклонение от соответствия конфигурации системы защиты информации АИС ее эксплуатационной документации?
4. Как документируется процесс контроля соответствия конфигурации системы защиты информации АИС ее эксплуатационной документации?
5. Что делать в том случае, если обнаружены существенные несоответствия конфигурации системы защиты информации АИС ее эксплуатационной документации, а привести их в соответствие оперативно невозможно?

Тема 2.6. Контроль стабильности характеристик системы защиты информации автоматизированной системы.

1. Перечислите возможные воздействия, способные оказать негативное влияние на стабильность характеристик системы защиты информации автоматизированной системы.
2. Как осуществляется контроль стабильности характеристик системы защиты информации автоматизированной системы?
3. Чем опасны нестабильные характеристики системы защиты информации автоматизированной системы?
4. Какие из характеристик систем защиты информации АИС нуждаются в особом контроле на предмет стабильности?
5. Какие существуют средства для повышения стабильности характеристик системы защиты информации автоматизированной системы?

Тема 2.7. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем.

1. Какие сведения необходимо отражать в рабочем журнале по обслуживанию систем защиты информации автоматизированных систем?
2. Какими программными средствами удобнее всего формировать и вести рабочий журнал по обслуживанию систем защиты информации автоматизированных систем?
3. Где и как должен храниться рабочий журнал по обслуживанию систем защиты информации автоматизированных систем?

4. Где и как должна храниться инструкция разработчика системы защиты информации автоматизированных систем?
5. Кто имеет право ознакомиться с информацией в рабочем журнале по обслуживанию систем защиты информации автоматизированных систем?

Тема 2.8. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.

1. В чем заключаются основные принципы вывода эксплуатации АИС с точки зрения защиты информации?
2. Что представляет собой наибольшую «стратегическую» ценность в любой АИС, в т.ч. и выводимой из эксплуатации?
3. Как обеспечить невозможность дальнейшей нелегальной эксплуатации, выводимой из работы АИС?
4. Какие части инфраструктуры, выводимой из работы АИС должны быть защищены от нелегального использования для обеспечения защиты информации?
5. Опишите кратко процесс документирования при выводе АИС из эксплуатации?

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.