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 учебной 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

Учебная практика является частью программы подготовки профессионального 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 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

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;

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. Установка, настройка и эксплуатация сетевых операционных систем.	1.1. Установка программного обеспечения в соответствии с технической документацией	12
	1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.	6
	1.3. Настройка компонентов подсистем защиты информации операционных систем.	6
	1.4. Управление учетными записями пользователей	6
	1.5. Работа в операционных системах с соблюдением действующих требований по защите информации	6
	1.6. Установка обновления программного обеспечения	6
	1.7. Контроль целостность подсистем защиты информации операционных систем.	6
	1.8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных	6
	1.9. Использование программных средств для архивирования информации	6
Раздел 2. Проведение аудита защищенности автоматизированной системы.	2.1. Проведение аудита защищенности автоматизированной системы	6

	2.2. Установка, настройка и эксплуатация сетевых операционных систем	6
	2.3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.	6
	2.4. Организация работ с удаленными хранилищами данных и базами данных.	6
	2.5. Организация защищенной передачи данных в компьютерных сетях.	6
	2.6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.	6
	2.7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.	6
	2.8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	6
Всего:		108

3. Условия реализации программы практики

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).

3. 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).

2. Дополнительная литература

1. Сидорова, Н. П. Базы данных / Н. П. Сидорова. – Москва, Берлин : Директ-Медиа, 2020. – 93 с. – ISBN 9785449907998. – URL: http://biblioclub.ru/index.php?page=book_red&id=575080 (дата обращения: 26.09.2023). – Текст : электронный.

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 учебной практике по профессиональному модулю "Эксплуатация автоматизированных (информационных"

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	**Знать:** теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; **Уметь:** организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять	Проверка отчёта по разделам практики.

		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	**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;	Проверка отчёта по разделам практики.
	ПК 1.4	**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	Проверка отчёта по разделам практики.

		работоспособности автоматизированных (информационных) систем в защищенном исполнении;	

4.2. Типовые контрольные задания или иные материалы

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

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

4.2.1. Оценочные средства при текущем контроле

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

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

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

Критерии оценивания:

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

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

Примеры типовых заданий на практику:

1.1. Установка программного обеспечения в соответствии с технической документацией

Задание 1. Изучите техническую документацию устанавливаемого ПО; порядок установки модулей ПО; структуру будущих каталогов; аппаратные требования к компьютеру, на котором планируется развернуть ПО.

Задание 2. Выполните первичную установку ПО на заданный компьютер, удовлетворяющий аппаратным требованиям.

Задание 3. Выполните тонкую настройку ПО в соответствии с документацией

Задание 4. Создайте (если нужно) тестовую учетную запись условного пользователя и проверьте доступ к основному функционалу ПО

1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.

Задание 1. Выполните тонкую настройку ПО / СУБД, включая вопросы информационной безопасности, сетевое взаимодействие (если нужно)

Задание 2. Выполните подключение требуемой БД к настроенной ранее СУБД

Задание 3. Проверьте от имени рядового пользователя и администратора функции СУБД по управлению БД.

Задание 4. Проверьте возможность экспорта (выгрузки) и импорта (загрузки) данных в/из БД с помощью СУБД

Задание 5. Проверьте с помощью инструментов SQL возможность доступа к БД.

1.3. Настройка компонентов подсистем защиты информации операционных систем.

Задание 1. Настроить штатную (защитник Windows) или внешнюю антивирусную программу на автоматическое сканирование исполняемых файлов и регулярное автоматическое обновление антивирусных баз. При необходимости добавить надежные специфичные программы в категорию «Доверенные» или «Исключения»
Задание 2. Настроить межсетевой экран для домашних, корпоративных, общественных сетей на блокировку внешнего трафика в данный компьютер. При необходимости для доверенных источников настроить исключения.

1.4. Управление учетными записями пользователей

Задание 1. Создать нужное количество учетных записей, присвоить им соответствующие полномочия и задать пароли для локального компьютера.
Задание 2. Ввести компьютер в домен, а затем ввести учетную запись пользователя в соответствующую доменную группу.
Задание 3. Настроить для пользователя перемещаемый профиль в пределах домена.

1.5. Работа в операционных системах с соблюдением действующих требований по защите информации

Задание 1. Подключить к компьютеру и настроить средство аппаратной аутентификации пользователя.
Задание 2. Настроить групповую политику безопасности так, чтобы требовалась длина пароля не менее 8 символов, с учетом сложности пароля и смены его 1 раз в месяц.
Задание 3. Для наиболее важных папок установить режим шифрования в свойствах
Задание 4. Настроить синхронизацию требуемой папки с облачным диском.

1.6. Установка обновления программного обеспечения

Задание 1. Получить информацию о текущей версии ПО и проверить наличие обновлений.
Задание 2. Выяснить способы установки обновлений
Задание 3. Прочитать перечень исправлений в данном обновлении и возможные проблемы.
Задание 4. Принять решение о необходимости установки обновлений и если положительное, то установить его.
Задание 5. Проверить работу ПО после установки обновления.

1.7. Контроль целостность подсистем защиты информации операционных систем.

Задание 1. Ознакомиться с настройками групповых и локальных политик безопасности на компьютере, если он не в домене. Если в составе домена, то изучить групповую принадлежность пользователя и его полномочия.
Задание 2. Ознакомиться с перечнем установленных обновлений, касаемо информационной безопасности ОС, и если имеются не установленные обновления, то установить их.
Задание 3. При помощи специальных утилит выполнить проверку целостности подсистем защиты информации в данной ОС, получить отчет и сделать вывод

1.8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных

Задание 1. Настроить автоматическую архивацию данных с заданной периодичностью.
Задание 2. Включить и настроить возможность автоматического создания точек восстановления системы
Задание 3. Создание диска аварийного восстановления системы и проверка его работоспособности.
Задание 4. Настроить и проверить работу автоматической регулярной архивации БД на заданный диск

1.9. Использование программных средств для архивирования информации

Задание 1. Сравнить степень сжатия наиболее полярных архиваторов: WinRAR, 7-Zip, WinZip, используя один и тот же тестовый файл.
Задание 2. Изучите функционал, удобство использования и возможность интеграции архивирующего ПО в состав ОС (контекстное меню)
Задание 3. Установите и настройте вами выбранный архиватор, проверьте его работу.

2.1. Проведение аудита защищенности автоматизированной системы

Задание 1. Ознакомиться с перечнем критериев защищенности АИС в таблице, если его нет, то составить.
Задание 2. Заполнить таблицу ответами на вопросы по каждому критерию.
Задание 3. При наличии специализированного ПО выполнить тесты для анализа уязвимости и получить отчет.

2.2. Установка, настройка и эксплуатация сетевых операционных систем

Задание 1. Выполнить первичную установку ОС Windows Server 2012 (2016) на сервер либо его эмуляцию в среде виртуальных машин
Задание 2. Настроить сервер в качестве домен-контроллера локальной сети, а также службы DHCP и DNS. Проверить их работу.
Задание 3. В соответствии с разработанной политикой безопасности (если не разработана, то сделать это) выполнить настройку безопасности, а также политику локальных, глобальных и универсальных групп пользователей.

2.3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.

Задание 1. Изучить системные журналы ОС, относящиеся к подсистеме безопасности. При наличии проблем выписать их.
Задание 2. С помощью системных мониторов ресурсов оценить степень загрузки и производительности данного компьютера.
Задание 3. С помощью специализированного ПО, типа Traffic Inspector (или аналогичного) изучить эффективность работы сети и степень загрузки сетевого канала, проходящего через данный компьютер.

2.4. Организация работ с удаленными хранилищами данных и базами данных.

Задание 1. Настроить пользовательский компьютер для работы с удаленным хранилищем данных. Разрешение на удаление и изменение файлов – в соответствии с политикой безопасности. Как вариант – в качестве удаленного хранилища могут использоваться облачные диски. Синхронизация должна выполняться автоматически.
Задание 2. Настроить клиентскую СУБД для работы с удаленной БД в соответствии с политикой безопасности.
Задание 3. От имени администратора получить информацию о количестве и источнике запросов на примере одного пользователя.

2.5. Организация защищенной передачи данных в компьютерных сетях.

Задание 1. Выбрать наиболее подходящие защищенные протоколы передачи данных для соответствующего уровня модели OSI.
Задание 2. Выбрать наиболее подходящие ПО для шифрования файлов и генерации ключей.
Задание 3. Выполнить настройку выбранных протоколов и ПО шифрования и генерации ключей на клиентского компьютера. Настроить защищенный канал на основе соединения проводной локальной сети.

2.6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.

Задание 1. Выполнить монтаж фрагмента (или полностью) локальной сети Ethernet в соответствии со схемой с размещения в кабель-каналах и установкой настенных информационных розеток.
Задание 2. Установить (по возможности) в геометрическом центре локальной сети коммутатор и подключить к нему сегменты сети по топологии «Звезда».
Задание 3. Проверить на узлах сети наличие сетевых драйверов и при необходимости установить их.
Задание 4. При отсутствии DHCP – сервера настроить ручную IP-адресацию согласно протоколу TCP/IP на каждом сетевом узле.
Задание 5. Если требуется выход из локальной сети в сеть Интернет, то выполнить настройку межсетевого экрана на каждом сетевом узле.

2.7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.

Задание 1. С помощью специального инструмента (оборудования) определите место обрыва кабеля «витая пара».

Задание 2. С помощью сетевого сканера определите наиболее и наименее загруженные направления передачи пакетов. Попытайтесь найти закономерность появления пиковых значений.

Задание 3. На одном из компьютеров в локальной сети сетевая карта имеет «флуд», что дестабилизирует работу сети. Необходимо обнаружить проблемную сетевую карту.

Задание 4. С помощью ПО профессионального файерволла, установленного на компьютере проанализируйте попытки тестовых атак.

Задание 5. Проанализируйте системные журналы безопасности и сформируйте список проблем и возможных решений.

2.8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.

Задание 1. Составьте таблицу в Excel или Word, в столбцах которой будет следующая информация:

- дата обращения клиента
- дата устранения проблемы
- описание проблемы со слов клиента
- описание проблемы специалистом после ее анализа
- замеченные сопутствующие проблемы в сети и рекомендации по устранению
- работы по устранению проблемы специалистом с указанием типа работ – плановые / аварийные
- подпись специалиста

Задание 2. Внесите информацию о недавно проведенных работах и представьте для проверки преподавателю.

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 к защите отчетов:

Раздел 1. Установка, настройка и эксплуатация сетевых операционных систем.

1.1. Установка программного обеспечения в соответствии с технической документацией.

1. На что нужно обратить внимание при выборе аппаратного и системного обеспечения для развертывания специального ПО или АИС?
2. Что делать, если пароль учетной записи с административными правами утерян, но нужно установить ПО?
3. Что включает в себя первичная установка ПО? Опишите кратко её алгоритм.
4. Что включает в себя тонкая настройка ПО после первичной установки?
5. Что делать, если установка или настройка ПО не идет по заданному алгоритму и выдает ошибку?

1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.

1. Какие параметры относятся к информационной безопасности при настройке ПО / СУБД?
2. Какие действия выполняются при подключении требуемой БД к имеющейся СУБД?
3. Какие действия при работе с БД часто запрещены некоторым пользователям?
4. В каких форматах могут быть импортированы / экспортированы данные по запросу из / в БД?
5. Какие команды SQL чаще всего используют администраторы БД для доступа и проверки БД?

1.3. Настройка компонентов подсистем защиты информации операционных систем.

1. Какие компоненты входят в состав подсистемы защиты информации операционных систем?
2. В каких консолях / апплетах находятся инструменты для настройки компонентов подсистем защиты информации операционных систем на примере ОС Windows.
3. Каким угрозам может противостоять подсистема защиты информации операционных систем?
4. Каким образом выполняется настройка безопасности локального компьютера?
5. Каким образом выполняется настройка безопасности компьютера, включенного в состав домена?

1.4. Управление учетными записями пользователей

1. Какие действия выполняются при настройке учетных записей на локальном компьютере?
2. Как и кто может внести существующего пользователя домена в группу с более высокими полномочиями?
3. Опишите кратко алгоритм создания перемещаемого профиля пользователя
4. Как выполняется ввод / вывод пользовательского компьютера в / из домена?
5. Является ли встроенная системная учетная запись Администратор аналогом созданной учетной записи с правами администратора?

1.5. Работа в операционных системах с соблюдением действующих требований по защите информации

1. Каким минимальным требованиям должен удовлетворять пароль, чтобы данный компьютер считался защищенным и безопасным?
2. Какими должны быть настройки спящего режима и заставки, чтобы данный компьютер считался защищенным и безопасным?
3. Как можно сформулировать одним предложением более жесткую политику информационной безопасности, применяемой на компьютере и при работе в сети?
4. Что дает включение параметра «шифрование» в свойствах файла?
5. Какие параметры политик безопасности локального компьютера больше всего влияют на защиту информации?

1.6. Установка обновления программного обеспечения

1. Каким образом на примере ОС Windows можно узнать какие обновления установлены?
2. Какие способы установки обновлений ПО существуют?
3. Как выполняется обновление прошивки (firmware) для различных устройств?
4. Всегда ли нужно сразу устанавливать обновление ПО?
5. Можно ли удалить установленное обновление ПО?

1.7. Контроль целостность подсистем защиты информации операционных систем.

1. Какие факторы влияют на целостность подсистем защиты информации операционных систем?
2. Какими внешними средствами можно усилить целостность подсистем защиты информации операционных систем?
3. Какими программными средствами можно оценить целостность и надежность подсистем защиты информации операционных систем?
4. Возможно ли эксплуатировать компьютер, на котором обнаружена брешь в подсистеме защиты информации операционной системы?
5. Если на компьютере в составе офисной локальной сети обнаружена уязвимость в целостности подсистемы защиты информации, то что нужно сделать в первую очередь?

1.8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных

1. Как настроить автоматическую архивацию данных на примере ОС Windows? Опишите кратко алгоритм.
2. Для чего нужны точки восстановления системы, какие проблемы можно решить с помощью их?
3. На какие носители рекомендуется делать резервное копирование данных?
4. С какой периодичностью рекомендуется выполнять резервное копирование данных?
5. Какими программными средствами можно создать образ операционной системы?

1.9. Использование программных средств для архивирования информации

1. В чем отличие встроенных в ОС средств архивации данных и архиваторов?
2. Какой архиватор поддерживает большее количество форматов архивов?
3. Какие параметры архивирования можно настраивать в архиваторах?
4. Можно ли использовать архиватор в режиме командной строки?
5. Какими дополнительными функциями кроме архивации / деархивации обладает архиватор WinRAR ?

Раздел 2. Проведение аудита защищенности автоматизированной системы.

2.1. Проведение аудита защищенности автоматизированной системы

1. Какие критерии используются для анализа защищенности АИС?
2. Кто уполномочен проводить аудит защищенности автоматизированной системы?
3. Кто должен устранять выявленные в ходе аудита несоответствия?
4. Какие части АИС подлежат проверке в ходе аудита защищенности автоматизированной системы?
5. Какое специальное ПО / тесты используются для проведения аудита защищенности автоматизированной системы?

2.2. Установка, настройка и эксплуатация сетевых операционных систем

1. Какие основные сетевые настройки необходимо сделать в установленной сетевой ОС?
2. Какие сетевые модули и компоненты есть в ОС Windows Server Standard 2012 (2016) ?
3. К чему сводится настройка службы DHCP на сервере и клиенте?
4. К чему сводится настройка службы DNS на сервере и клиенте?
5. Какие компоненты сетевого подключения как минимум должны быть активны и настроены для взаимодействия компьютеров в локальной сети?

2.3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.

1. Где в ОС Windows находятся системные журналы ОС, относящиеся к подсистеме безопасности?
2. Поясните кратко где находится и как пользоваться системными мониторами ресурсов?
3. Кратко опишите основные возможности ПО типа Traffic Inspector (или аналогичного)
4. Какими программными и аппаратными средствами можно диагностировать состояния подсистем безопасности сетевой ОС?
5. Возможно ли как-то активно управлять нагрузкой сетевой операционной системы?

2.4. Организация работ с удаленными хранилищами данных и базами данных.

1. Опишите кратко алгоритм работы с удаленным хранилищем данных или БД
2. Опишите основные действия по настройке клиентскую СУБД для работы с удаленной БД в соответствии с политикой безопасности.
3. Как организовать сетевой канал для работы с жестким диском, расположенным на компьютере, находящемся в другом городе?
4. Что такое репликация БД и для чего она нужна?
5. Какие сетевые протоколы используются для работы с удаленными хранилищами данных или БД?

2.5. Организация защищенной передачи данных в компьютерных сетях.

1. Приведите примеры защищенных сетевых протоколов
2. Как обеспечить защиту проводной компьютерной сети от распространения ею ПЭМИН, а также защиту самой сети от внешних ПЭМИН?
3. Какие каналы передачи данных являются более защищенными – выделенные или коммутируемые?
4. В каких случаях оправдано использование протокола https ?
5. Какой физический канал передачи данных обеспечивает наибольшую защищенность данных?

2.6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.

1. Перечислите основные правила монтажа кабеля витая пара для сети 1 Gb / s.
2. Какие существуют варианты размещения сетевых коммутаторов?
3. Какие основные настройки требуется выполнить на сетевых адаптерах компьютера и в каких случаях?
4. В каких случаях используется сетевой протокол TCP/IP версии 6 ?
5. Как настроить вход из сети Интернет на конкретный компьютер локальной сети?

2.7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.

1. Чем отличается сетевой сканер от сетевого тестера?
2. Какими средствами можно определить трафик сети, ошибки, коллизии?
3. К каким негативным явлениям приводит наличие сетевых петель и всегда ли они вредны?
4. Какие существуют виды межсетевых экранов?
5. Существует ли в ОС Windows системный журнал, отражающий нарушения в работе сети ? Если да, то где именно?

2.8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.

1. Кто и для чего должен заполнять отчетную документацию по техническому обслуживанию и ремонту компьютерных сетей?
2. В каком виде и формате может вестись отчетная документация по техническому обслуживанию и ремонту компьютерных сетей?
3. Ведется ли отчетная документация для сети Wi-Fi, имеющейся в организации?
4. Где должна храниться отчетная документация по техническому обслуживанию и ремонту компьютерных сетей?
5. Является ли отчетная документация по техническому обслуживанию и ремонту компьютерных сетей документом повышенной секретности?

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.