МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
КОЛЛЕДЖ ДГУ

ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	*10.02.05 Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовке*
Уровень образования, на базе которого осваивается ППССЗ:	*Основное общее образование*
Квалификация:	*Техник по защите информации*
Форма обучения:	*Очная*

Махачкала, 2020

Программа учебной практики разработана на основе требований Федерального государственного образовательного стандарта (далее – ФГОС) СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования

Организация-разработчик: Колледж федерального государственного бюджетного образовательного учреждения высшего образования «Дагестанский государственный университет»

Разработчики:

Пирбудагова Д.Ш. - к.ю.н., доцент кафедры конституционного и международного права

Магдилова Л.В. - к.э.н., доцент кафедры информационного права и информатики

Рецензент:

Камилов М.-К. Б, к.э.н., доцент, зав. кафедрой прикладной информатики ДГУ

Программа учебной практики рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин Колледжа ДГУ

Протокол № 7 от «29» февраля 2020 г.

Зав. кафедрой _____ / Магдилова Л.В.

Программа учебной практики согласована с учебно-методическим управлением

«26» 03 2020 г. _____
(подпись)

Программа учебной практики согласована с представителем работодателя

Зам. министра Минцифры _____ Магомедов Б.А.

СОДЕРЖАНИЕ

1. Паспорт программы учебной практики

1.1. Область применения программы учебной практики

Учебная практика является частью ОПОП ПССЗ по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» в части освоения основного вида профессиональной деятельности: эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

Практика направлена на формирование у студента общих и профессиональных компетенций, получение практического опыта по каждому из видов профессиональной деятельности, подготовку к осознанному и углубленному изучению отдельных специальных дисциплин.

1.2. Цели и задачи учебной практики, требования к результатам

1.2.1. Цели практики:

- улучшение качества профессиональной подготовки студентов;
- закрепление и систематизация полученных знаний в сфере профессиональной деятельности;
- овладение профессиональными умениями и навыками в сфере профессиональной деятельности;
- закрепление и углубление теоретических знаний, полученных в процессе обучения;
- формирование у обучающихся нравственных качеств личности;
- повышение мотивации к профессиональному самосовершенствованию, расширение профессионального кругозора;
- приобретение опыта работы в коллективах при решении ситуационных социально-правовых задач: изучение принципов разработки модулей программного обеспечения для компьютерных систем, применяемых на практике, а также приобретение практического опыта их разработки, изучение дополнительного материала, публикуемого в периодической печати, с целью актуализации знаний, полученных в процессе обучения.

1.2.2. Задачи практики:

- развитие профессионального мышления;
- приобретение практических умений по определению характеристик средств защиты,
- использование основных методик процессов обеспечения информационной безопасности,
- оптимизация эксплуатации автоматизированных информационных систем и компьютерных сетей в защищенном исполнении,
- сбор материалов, необходимых для составления отчета о прохождении практики в соответствии с дневником практики.

1.3 Место учебной практики в структуре ОПОП ПССЗ

Учебная практика согласно ОПОП ПССЗ проводится после прохождения основных междисциплинарных курсов (МДК) в рамках профессионального модуля «Эксплуатация автоматизированных систем в защищенном исполнении».

1.4 Трудоемкость и сроки проведения практики

Трудоемкость учебной практики в рамках освоения профессионального модуля «Эксплуатация автоматизированных систем в защищенном исполнении» составляет 144 часа (четыре недели).

Сроки проведения практики определяются рабочим учебным планом по специальности СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и графиком учебного процесса. Практика проводится концентрировано на 3 курсе, в пятом семестре.

1.5 Место прохождения учебной практики

Практика проводится в учебно-методических кабинетах колледжа ДГУ, факультета информатики и информационных технологий ДГУ. Учебная практика проводится в форме различных тренингов, встреч с практикующими работниками в осваиваемой профессии, а также различных форм самостоятельной работы по получению первичных профессиональных умений и навыков.

2. Перечень планируемых результатов освоения программы учебной практики

Результатом прохождения учебной практики в рамках освоения профессионального модуля «Разработка модулей программного обеспечения для компьютерных систем» является овладение обучающимися соответствующими видами профессиональной деятельности по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», в том числе профессиональными компетенциями (ПК).

Компетенции	Формулировка компетенции из ФГОС	Планируемые результаты обучения (показатели достижения заданного уровня освоения 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. Владеть: навыками установки и настройки 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, 6 конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты

		информации автоматизированной системы. Владеть: навыками конфигурирования, настройки компонентов систем защиты информации автоматизированных систем;
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. Владеть: навыками эксплуатации 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. Владеть: навыками диагностики компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

3. Структура и содержание учебной практики

№ п/п	Разделы (этапы) практики	Форма контроля (Компетенции)			Форма контроля (Компетенции)
		Всего	аудиторн		
			практ	консульт	
1	Организационные вопросы оформления, установочная лекция, инструктаж по технике безопасности, распределение по рабочим местам	20	18	2	Отчет, дневник практики (ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4)
2	Получение обучающимися информации о будущей профессиональной деятельности, связанной с обеспечением	20	18	2	Отчет, дневник практики (ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4)

	информационной безопасности, ознакомление с правилами организации работы техника по защите информации в организации, должностные обязанности техника по защите информации.				
3	Обслуживание средств защиты информации прикладного и системного программного обеспечения. Настройка программного обеспечения с соблюдением требований по защите информации. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением.	20	18	2	Обобщение собранного материала в отдельном разделе отчета (ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4)
4	Настройка встроенных средств защиты информации программного обеспечения. Проверка функционирования встроенных средств защиты информации программного обеспечения.	24	22	2	Перечень используемых систем программирования (ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4)
5	Обслуживание средств защиты информации в компьютерных системах и сетях. Обслуживание систем защиты информации в автоматизированных системах. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем. Проверка работоспособности системы защиты информации автоматизированной системы. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации.	24	20	4	Отчет, дневник практики ((ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4)

	Контроль стабильности характеристик системы защиты информации автоматизированной системы. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.				
6.	Подготовка отчета. Систематизация и анализ выполненных заданий, оформление отчетной документации.	36	30	6	Отчет, дневник практики (ПК-1.1, ПК-1.2, ПК-1.3, ПК-1.4)
7.	Защита отчета				Отчет
	Итого:	144			

4. Условия реализации программы учебной практики

4.1. Требования к проведению учебной практики

Продолжительность рабочей недели обучающихся при прохождении практики составляет не более 36 часов в неделю.

С момента зачисления обучающихся в период практики в качестве практикантов на рабочие места на них распространяются правила охраны труда и правила внутреннего распорядка, действующие в организации.

Обязанности обучающегося-практиканта:

- до начала практики обучающийся должен ознакомиться с Правилами внутреннего трудового распорядка организации, техники безопасности и охраны труда.
- подчиняться требованиями трудовой и производственной дисциплины, установленной в организации, являющейся базой практики;
- подготовить отчет об учебной практике и защитить его в установленные сроки.

Руководство практикой обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю или наличие высшего профессионального образования и дополнительного профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем». Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за руководство производственной практикой. Руководитель практики определяется университетом в начале учебного года. Руководитель по практике консультирует обучающихся по всем вопросам данной программы практики, осуществляет прием отчетов и проводит аттестацию по результатам практики.

Контроль за работой обучающихся осуществляют руководитель практики.

Аттестация по итогам практики проводится на основании оформленного в соответствии с установленными требованиями письменного отчета и отзыва преподавателя - руководителя практики. По итогам практики выставляется оценка «зачтено» или «не зачтено».

4.2. Требования к минимальному материально-техническому обеспечению

Реализация программы учебной практики требует наличия: учебного кабинета.

Оборудование рабочих мест проведения учебной практики:
- ПК с доступом к сети Интернет
- калькуляторы
- принтер
- сканер
- программное обеспечение общего и профессионального назначения
- комплекс учебно-методической документации.

4.3. Учебно-методическое и информационное обеспечение практики.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Конституция Российской Федерации: принята всенар. голосованием 12.12.1993 г. // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.
2. Гражданский кодекс РФ (часть 4): Федеральный закон от 18.12.2006 N 230-ФЗ //СЗ РФ. – 2006. - №52. – Ст. 5496.
3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149 – ФЗ // СЗ РФ. – 2006. - №31 (1ч.). – Ст. 3448.
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638
19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008
20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2 Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3 Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4 Выбор защитных мер
26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5 Руководство по менеджменту безопасности сети
27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2 Функциональные требования безопасности
30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3 Требования доверия к безопасности
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013

35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014
36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000
37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006
38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005
39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993
40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014
41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных электромагнитных воздействий. Общие требования. Росстандарт, 2014
42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель. Росстандарт, 2012
43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2 Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013
44. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002
46. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006
47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006
48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002
49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17
50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
51. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Дополнительные источники:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва

: Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933
3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792
4. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356
5. Стружкин, Н. П. Базы данных: проектирование. Практикум : учебное пособие для среднего профессионального образования / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2020. — 291 с. — (Профессиональное образование). — ISBN 978-5-534-08140-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455865
6. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456638
7. 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, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455863

Интернет-ресурсы

1. Электронно-библиотечная система издательства ЮРАЙТ - URL: www.: biblio-online.ru
2. Электронно-библиотечная система «Университетская библиотека онлайн» www.biblioclub.ru
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. URL: http://elibrary.ru
4. Национальная электронная библиотека [Электронный ресурс]. URL: http://нэб.рф/.
5. Справочно-правовая система «КонсультантПлюс». URL: http://www.consultant.ru
6. Справочно-правовая система «Гарант». URL: http://www.garant.ru.

5. Контроль и оценка результатов учебной практики

5.1. Формы отчетности по практике

К защите по итогам практики студенты должны представить следующую документацию:

- характеристику студента с места прохождения практики;
- дневник;
- отчет по практике.

В характеристике фиксируется степень подготовленности студента для работы по данной специальности, уровень теоретических знаний, умение организовать свой рабочий день и другие качества, проявленные студентом в период практики, замечания и пожелания студенту, а также общий вывод руководителя практики о выполнении студентом программы практики.

По окончании практики, каждый студент составляет в письменном виде отчет о прохождении практики (далее – отчет):

- отчет утверждается практическим работником, осуществлявшим непосредственное руководство практикой студента.
- отчет выполняется в машинописной форме на листе формата А4, шрифт TimesNewRoman, размер 14, интервал полуторный, левое поле 3 см, правое поле 1 см, верхнее и нижнее поля 2-2,5 см. Объем отчета должен составлять 1-5 страниц.

Содержание отчета должно включать в себя:

- место и время прохождения практики;
- информацию об организации, отделе, структуре организации, анализ ее деятельности;

- краткое описание работы по отдельным разделам программы практики;
- определение проблем, возникших в процессе практики и предложения по их устранению;
- выводы по итогам практики о приобретенных навыках и практическом опыте.

- отчет должен отражать выполнение индивидуального задания программы практики, заданий и поручений, полученных от руководителя практики от организации.

В период прохождения практики студентом ведется дневник практики. В дневнике практики записываются краткие сведения о проделанной работе в течение дня в соответствии с планом работы. В качестве приложения к дневнику практики обучающийся оформляет графические, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

Контроль и оценка результатов прохождения учебной практики осуществляется руководителями практики от образовательного учреждения и организации в процессе выполнения обучающимися заданий, проектов, выполнения практических проверочных работ.

5.2. Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только форсированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты обучения (освоенные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Общие компетенции		
ПК.1.1 Формировать алгоритмы разработки программных модулей в соответствии с техническим заданием	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Наблюдение за процессом выполнения учебно-производственных работ: -составление алгоритма; Оценка в ходе защиты учебно-производственных работ.
ПК.1.2 Разрабатывать программные модули в соответствии с техническим заданием	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении.	Наблюдение за процессом выполнения учебно-производственных работ: -разработка кода программы; Оценка в ходе защиты учебно-производственных работ.
ПК.1.3 Выполнять отладку программных модулей с использованием специализированных программных средств	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Наблюдение за процессом выполнения учебно-производственных работ: -выполнение отладки; Оценка в ходе защиты учебно-производственных работ.
ПК.1.4 Выполнять тестирование программных модулей	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности	Наблюдение за процессом выполнения учебно-производственных работ: -выполнение тестирования программы;

	автоматизированных (информационных) систем в защищенном исполнении.	Оценка в ходе защиты учебно-производственных работ.

5.3. Типовые индивидуальные (контрольные) задания

Индивидуальные задания

1. Основы теории операционных систем. Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.
2. Машинно-зависимые и машинно-независимые свойства операционных систем. Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода. Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам. Модульная структура операционных систем, пространство пользователя. Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.
3. Управление памятью. Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти.
4. Управление процессами, многопроцессорные системы. Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок.
5. Виртуализация и облачные технологии. Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования. Облачные технологии. Исследования в области виртуализации и облаков.
6. Принципы построения защиты информации в операционных системах. Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.
7. Операционные системы UNIX, Linux, MacOS и Android. Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX. Операционные системы семейства Mac OS: особенности, преимущества и недостатки. 13 Архитектура Android. Приложения Android.
8. Операционная система Windows. Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.
9. Основные понятия теории баз данных. Модели данных. Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных. Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.
10. Основы реляционной алгебры. Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.

11. Базовые понятия и классификация систем управления базами данных. Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору).
12. Целостность данных как ключевое понятие баз данных. Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.
13. Информационные модели реляционных баз данных. Типы информационных моделей. Логические модели данных. Физические модели данных.
14. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами. Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.
15. Средства автоматизации проектирования. CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.
16. Создание базы данных. Манипулирование данными. Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.
17. Индексы. Связи между таблицами. Объединение таблиц. Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.
18. Структурированный язык запросов SQL. Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.
19. Операторы и функции языка SQL. Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.
20. Архитектуры распределенных баз данных. Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных. Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.
21. Серверная часть распределенной базы данных. Планирование и развёртывание СУБД для работы с клиентскими приложениями.
22. Клиентская часть распределенной базы данных. Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация. Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа. Оптимизация производительности работы СУБД.
23. Обеспечение целостности, достоверности и непротиворечивости данных. Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.
24. Перехват исключительных ситуаций и обработка ошибок. Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.

25. Механизмы защиты информации в системах управления базами данных. Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Средства защиты информации в базах данных.
26. Копирование и перенос данных. Восстановление данных. Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных.

Варианты контрольных работ

Вариант 1
1. Виртуальные машины. Создание, модификация, работа
2. Проектирование структуры базы данных

Вариант 2
1. Установка ОС
2. Проектирование базы данных с использованием CASE-средств

Вариант 3
1. Создание и изучение структуры разделов жесткого диска
2. Создание взаимосвязей

Вариант 4
1. Операции с файлами.
2. Сортировка, поиск и фильтрация данных

Вариант 5
1. Работа в консольном и графическом режимах
2. Способы объединения таблиц

Вариант 6
1. Мониторинг за использованием памяти
2. Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL

Вариант 7
1. Управление процессами
2. Создание и использование запросов. Группировка и агрегирование данных

Вариант 8
1. Наблюдение за использованием ресурсов системы
2. Коррелированные вложенные запросы

Вариант 9
1. Управление учетными записями пользователей и доступом к ресурсам
2. Создание в запросах вычисляемых полей. Использование условий

Вариант 10
1. Аудит событий системы
2. Управление доступом к объектам базы данных

Вариант 11
1. Изучение штатных средств защиты информации в операционных системах
2. Установка СУБД. Настройка компонентов СУБД.

Вариант 12
1. Создание дистрибъютиваLinux. Установка.
2. Создание форм и отчетов

Вариант 13

1. Работа в ОС Linux.
2. Создание меню. Генерация, запуск.

Вариант 14

1. Установка и первичная настройка Windows.
2. Профилирование запросов клиентских приложений.

Вариант 15

1. Работа с сетевой файловой системой.
2. Разработка хранимых процедур и триггеров

Вариант 16

1. Работа с серверной ОС, например, AltLinux.
2. Управление правами доступа к базам данных

Вариант 17

1. Операции над отношениями БД
2. Аудит данных с помощью средств СУБД и триггеров

Вариант 18

1. Проектирование инфологической модели данных
2. Резервное копирование и восстановление баз данных

Перечень тем презентаций

1. Создание виртуальной машины.
2. Установка операционной системы.
3. Анализ журнала аудита ОС на рабочем месте.
4. Изучение аналитических обзоров в области построения систем безопасности операционных систем.
5. Проектирование инфологической модели базы данных.
6. Нормализация отношений.
7. Развитие СУБД.
8. Создание базы данных. Создание таблиц. Организация межтабличных связей.
9. Организация запросов.
10. Создание пользовательского приложения средствами СУБД.
11. Разбор синтаксиса хранимых процедур и триггеров.
12. Организация и использование механизмов защиты базы данных.
13. Установка программного обеспечения в соответствии с технической документацией.
14. Настройка параметров работы программного обеспечения, включая системы управления базами данных.
15. Настройка компонентов подсистем защиты информации операционных систем.
16. Управление учетными записями пользователей.
17. Работа в операционных системах с соблюдением действующих требований по защите информации.
18. Установка обновления программного обеспечения.
19. Контроль целостность подсистем защиты информации операционных систем.
20. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных
21. Использование программных средств для архивирования информации.

Требования к презентации:

Презентация должна содержать не более 15 слайдов. В оформлении презентаций выделяют два блока: оформление слайдов и представление информации на них. Для создания качественной презентации необходимо соблюдать ряд требований, предъявляемых к оформлению данных блоков.

Оформление слайдов:

	Требования	Примечания
Основные слайды презентации	1. Титульный лист. 2. Желательно слайд с фотографией автора и контактной информацией (почта, телефон). 3. Содержание с кнопками навигации. 4. Основные пункты презентации. 5. Список источников 6. Завершающий слайд. Обычно копия слайда №2 с контактной информацией об авторе. Можно объединить слайд №1 и слайд №2.	· Кнопки навигации нужны для быстроты перемещения внутри презентации. К любому слайду можно добраться в 2 щелчка. · Желательно указать исходные материалы (откуда взяли иллюстрации, звуки, тексты, ссылки).
Размещение изображений (фотографий), их оптимизация	В презентации размещать только оптимизированные (например уменьшенные с помощью Microsoft Office Picture Manag er) изображения. В результате фото «весом» в 2 Мб превращается в 50 – 200 Кб Материалы располагаются на слайдах так, чтобы слева, справа, сверху, снизу от края слайда оставалось свободные поля.	Плохой считается презентация, которая долго загружается из-за изображений имеющих большой размер.
Сохранение презентаций	Сохранять презентацию лучше как «Демонстрация PowerPoint». С расширением **.pps**	Тогда в одном файле окажутся все приложения (музыка, ссылки и.т.д.)
Воздействие цвета	На одном слайде рекомендуется использовать не более трех цветов: один для фона, один для заголовков, один для текста. Для фона и текста используйте контрастные цвета. **Обратите особое внимание на цвет гиперссылок (до и после использования).**	Помните – презентация нужна для демонстрации, для дополнения вашего выступления (а не дублирования его)
Цвет фона Единство стиля	Для фона выбирайте более холодные тона (синий или зеленый). **Пёстрый фон не применять.** Для лучшего восприятия старайтесь придерживаться единого формата слайдов (одинаковый тип шрифта, сходная цветовая гамма).	Текст должен быть хорошо виден.
Анимационные эффекты	**Анимация не должна быть навязчивой.** Желательно не использовать побуквенную или аналогичную анимацию текста, а также сопровождение появления текста звуковыми эффектами (из стандартного набора звуков PowerPoint) **Не рекомендуется** применять эффекты анимации к заголовкам,	Исключения составляют динамические презентации.

	особенно такие, как «Вращение», «Спираль» и т.п. В информационных слайдах анимация объектов допускается только в случае, если это необходимо для отражения изменений и если очередность появления анимированных объектов соответствует структуре урока.	
Использование списков	Списки использовать только там где они нужны. Возможно, использовать 3 – 5 пунктов. Большие списки и таблицы разбивать на 2 слайда. Чем проще, тем лучше.	Каждый пункт лаконичен - в одно предложение.
Содержание информации	При подготовке слайдов в обязательном порядке должны соблюдаться принятые правила орфографии, пунктуации, сокращений и правила оформления текста (отсутствие точки в заголовках и т.д.)	**В презентациях для начальной школы точка в заголовках ставится.**
Расположение информации на странице	Проще считывать информацию расположенную горизонтально, а не вертикально. Наиболее важная информация должна располагаться в центре экрана. Желательно форматировать текст по ширине. Не допускать «рваных» краёв текста. Уровень запоминания информации зависит от её расположения на экране. **33%** 28% 16% 23%	**В левом верхнем углу слайда располагается самая важная информация.**
Шрифт	**Текст должен быть хорошо виден.** Размер шрифта не должен быть мелким. Самый «мелкий» для презентации - шрифт 22 пт. **Отказаться от курсива.** Больше «воздуха» между строк (межстрочный интервал полуторный).	Использовать шрифты без засечек (их легче читать**): Arial, Verdana.** Желательно устанавливать единый стиль шрифта для всей презентации.
Способы выделения информации	Следует использовать: рамки, границы, заливку, разные цвета шрифтов, штриховку, стрелки. Если хотите привлечь внимание к информации, используйте: рисунки, диаграммы, схемы.	Это достигается использованием разных видов слайдов
Объем информации	**Не стоит заполнять один слайд слишком большим объемом информации**: люди могут	Размещать много мелкого текста на слайде недопустимо.

	единовременно запомнить не более трех фактов, выводов, определений. Наибольшая эффективность достигается тогда, когда ключевые пункты отображаются по одному на каждом отдельном слайде.	
Разветвлённая навигация	Используйте навигацию для обеспечения интерактивности и нелинейной структуры презентации. Это расширит ее область применения. (Навигация это - переход на нужный раздел из оглавления).	Навигация по презентации должна осуществляться за 3 щелчка.
Звук	Музыка должна быть ненавязчивая. И её выбор оправдан.	Не использовать стандартные для Power Point звуки.
Требования к завершающим слайдам презентации	Последний слайд копирует первый.	

При создании презентации, можно использовать рекомендуемую литературу, так и ресурсы Интернет.