МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол №*3*	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

ПП.01.01 Производственная практика (Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель	_____	Г.Ю. Белова
должность	подпись	инициалы, фамилия

Директор Технического колледжа

_____	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
ПК 1.1	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.2	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
ПК 1.3	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.4	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении

1.2. В результате прохождения практики обучающийся должен:

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;
– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;
– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;

принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

уметь:
– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;
– 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
– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;

обеспечивать работоспособность, обнаруживать и устранять неисправности

иметь практический опыт:
– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем;
– администрирования автоматизированных систем в защищенном исполнении;
– эксплуатации компонентов систем защиты информации автоматизированных систем;

диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении.

– выявления событий и инцидентов безопасности в автоматизированной системе.

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Способ проведения практики: концентрированная.

Объем практики составляет 144 часа.

3. СОДЕРЖАНИЕ ПРАКТИКИ

3 курс

Темы практики и виды работ			Количество часов
6 семестр			**144**
Тема 1.	**Организация (предприятие) – база прохождения практики**		**20**
	Виды работ:		
	1.	**Проведение вводного инструктажа по правилам внутреннего трудового распорядка предприятия**	1
	2.	**Общие сведения об организации (предприятии)** Знакомство с предприятием, режимом его работы. Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации). Знакомство с историей предприятия (организации).	3
	3.	**Организационная структура организации (предприятия)**	4
	4.	**Виды деятельности организации (предприятия)** Изучение видов деятельности предприятия (организации), выпускаемой продукции, партнеров.	4
	5.	**Структурные подразделения, в которых проходила практика, их функции, задачи** Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика	4
	6.	**Сбор информации о видах обеспечения автоматизированных систем предприятия (организации)** Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для выполнения заданий на время прохождения производственной практики.	4
Тема 2.	**Выполнение заданий согласно программе практики**		**122**
	Виды работ:		
	1.	Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	12
	2.	Обслуживание средств защиты информации прикладного и системного программного обеспечения	6
	3.	Настройка программного обеспечения с соблюдением требований по защите информации	6
	4.	Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	6
	5.	Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением	2
	6.	Настройка встроенных средств защиты информации программного обеспечения	12
	7.	Проверка функционирования встроенных средств защиты информации программного обеспечения	12
	8.	Своевременное обнаружение признаков наличия вредоносного программного обеспечения	6
	9.	Обслуживание средств защиты информации в компьютерных системах и сетях	6
	10.	Обслуживание систем защиты информации в автоматизированных системах	6
	11.	Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем	6

	12.	Проверка работоспособности системы защиты информации автоматизированной системы	6
	13.	Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	6
	14.	Контроль стабильности характеристик системы защиты информации автоматизированной системы	6
	15.	Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем	12
	16.	Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	12
	Дифференцированный зачет		**2**
	Итого:		**144 часа**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования [Электронный ресурс] / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — Режим доступа: https://www.biblio-online.ru/bcode/431332
2. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования [Электронный ресурс] / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/442312.
3. Мэйволд Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 571 c. — 5-9570-0046-9. — Режим доступа: http://www.iprbookshop.ru/73727.html
4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 c. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/63800.html
5. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс] : учебное пособие / БехроузА. Фороузан. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 782 c. — 978-5-4487-0143-6. — Режим доступа: http://www.iprbookshop.ru/72337.html

4.2. Дополнительная литература

1. Информационный мир XXI века. Криптография – основа информационной безопасности [Электронный ресурс] / Б. П. Елисеев, Э. А. Болелов, О. Д. Гаранина [и др.] ; под ред. Э. А. Болелова. — 3-е изд. — Электрон. текстовые данные. — М. : Дашков и К, Московский государственный технический университет гражданской авиации, 2019. — 126 c. — Режим доступа: http://www.iprbookshop.ru/85368.html
2. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования [Электронный ресурс]/ К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2019. — 363 с. — Режим доступа: https://www.biblio-online.ru/bcode/430406.
3. Горев А.И. Обработка и защита информации в компьютерных системах [Электронный ресурс] : учебно-практическое пособие / А.И. Горев, А.А. Симаков. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2016. — 88 c. — Режим доступа: http://www.iprbookshop.ru/72856.html
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования [Электронный ресурс]/ Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2019. — 325 с. — Режим доступа: https://www.biblio-online.ru/bcode/434576.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;
- приложения.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Лаборатория «Программных и программно – аппаратных средств защиты информации» (ауд. 105 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности: ПАК Аккорд-NT, № 52202314; ПАК «Соболь» 3.0, № 7CJJC4GW; «Dallas Lock 8.0-C», № 29093-4159-1156. Программные и программно-аппаратные средства обнаружения вторжений: система обнаружения и предотвращения вторжений Dallas Lock, № 29093-4159-1156	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 CodeGear RAD Studio 2007 Professional Лицензия №32954 Бессрочная Гос. Контракт №35-03/161 от 19.08.2008г

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1	2	3
1.	Центр по проблемам информационной безопасности ТГТУ	г.Тамбов, ул.Советская, д.106
2.	Тамбовский филиал ПАО «Ростелеком»	г. Тамбов, ул. Астраханская, д.2в
3.	ООО «Объединенные системы связи»	г. Тамбов, бул. Строителей, 6А
4.	ООО ”Тамбовский редуктор	г. Тамбов, ул. Заводская, д.4, пом. 16
5.	Территориальный орган Федеральной службы государственной статистики по Тамбовской области (Тамбовстат)	г. Тамбов, Интернациональный проезд,14
6.	Магазин “ABS Центр”	г.Тамбов, ул. Им.Вадима Подбельского д78
7.	АО Банк «ТКПБ»	г. Тамбов, Советская 118

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	6

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать состав и принципы работы автоматизированных систем, операционных систем и сред	Зач01
Знать принципы разработки алгоритмов программ, основных приемов программирования	Зач01
Знать модели баз данных	Зач01
Знать принципы построения, физические основы работы периферийных устройств	Зач01
Знать теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации	Зач01
Знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях	Зач01
Знать принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	Зач01
Уметь осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем	Зач01
Уметь организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней	Зач01
Уметь осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем	Зач01
Уметь производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	Зач01
Уметь настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	Зач01
Уметь обеспечивать работоспособность, обнаруживать и устранять неисправности	Зач01
Иметь практический опыт установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем	Зач01
Иметь практический опыт администрирования автоматизированных систем в защищенном исполнении	Зач01
Иметь практический опыт эксплуатации компонентов систем защиты информации автоматизированных систем	Зач01
Иметь практический опыт диагностики компонентов систем защиты информации автоматизированных систем,	Зач01

Результаты обучения	Контрольные мероприятия
Иметь практический опыт устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении	Зач01

Вопросы к защите отчета по практике Зач01

1. В какой организации (предприятии) проходила практика?
2. Какую деятельность осуществляет организация (предприятие)?
3. Расскажите об организационной структуре организации (предприятии)?
4. Каковы виды деятельности организации (предприятия)**?**
5. В каком структурном подразделении проходила практика?
6. Какие технические характеристики имелись на компьютере, за которым осуществлялась работа?
7. Расскажите о программном обеспечении, установленном на этом компьютере.
8. Состав, структура и функции технического обеспечения в автоматизированных информационных системах.
9. Состав и структура комплекса технических средств.
10. Требования к техническим средствам.
11. Порядок описания комплекса технических средств.
12. Функция автоматизированной системы.
13. Подсистемы АИС.
14. Задачи автоматизированных систем.
15. Подсистема сбора информации.
16. Классификация компьютерных сетей по признакам функциональности, целевого назначения и области применения.
17. Подсистема представления и обработки информации.
18. Подсистема выдачи информации.
19. Классификация компьютерных сетей.
20. Сетевое оборудование и программное обеспечение
21. Какие физические компоненты сетей присутствуют в организации?
22. Назовите соединительные устройства локальной сети организации.

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол №*3*	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

УП.01.01 Учебная практика (Эксплуатация
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)
автоматизированных (информационных) систем
в защищенном исполнении

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель	_____	Г.Ю. Белова
должность	подпись	инициалы, фамилия

Директор Технического колледжа

_____	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
ПК 1.1	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.2	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
ПК 1.3	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.4	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении

1.2. В результате прохождения практики обучающийся должен:

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;
– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;
– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;

принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

уметь:

– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;
– 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
– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;

обеспечивать работоспособность, обнаруживать и устранять неисправности

иметь практический опыт:

– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем;
– администрирования автоматизированных систем в защищенном исполнении;
– эксплуатации компонентов систем защиты информации автоматизированных систем;

диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении.

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: учебная.
Способ проведения практики: рассредоточенная.

Объем практики составляет 144 часа.

3. СОДЕРЖАНИЕ ПРАКТИКИ

Темы практики и виды работ			Количество часов
5 семестр			**72**
Тема 1	**Установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем**		**48**
	Виды работ:		
	1.	Инструктаж по технике безопасности при работе за ПК. Установка программного обеспечения в соответствии с технической документацией.	4
	2.	Настройка параметров работы программного обеспечения, включая системы управления базами данных	8
	3.	Настройка компонентов подсистем защиты информации операционных систем.	8
	4.	Установка обновления программного обеспечения.	4
	5.	Установка, настройка и эксплуатация сетевых операционных систем	12
	6.	Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.	12
Тема 2	**Администрирование автоматизированных ситсем в защищенном исполнении**		**24**
	Виды работ:		
	1.	Инструктаж по технике безопасности при работе за ПК. Управление учетными записями пользователей.	8
	2.	Организация работ с удаленными хранилищами данных и базами данных.	8
	3.	Организация защищенной передачи данных в компьютерных сетях.	8

Темы практики и виды работ			Количество часов
6 семестр			**72**
Тема 3.	**Эксплуатация компонентов систем защиты информации автоматизированных систем**		**44**
	Виды работ:		
	1.	Инструктаж по технике безопасности при работе за ПК. Работа в операционных системах с соблюдением действующих требований по защите информации.	12
	2.	Контроль целостности подсистем защиты информации операционных систем.	8
	3.	Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных	8
	4.	Использование программных средств для архивирова-	4

		ния информации.	
	5.	Проведении аудита защищенности автоматизированной системы	12
Тема 4.	**Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении**		**26**
	Виды работ:		
	1.	Инструктаж по технике безопасности при работе за ПК. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.	6
	2.	Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.	12
	3.	Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	8
	Дифференцированный зачет		**2**
	Итого		**72 часа**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1. Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования [Электронный ресурс] / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — Режим доступа: https://www.biblio-online.ru/bcode/431332
2. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования [Электронный ресурс] / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/442312.
3. Мэйволд Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 571 c. — 5-9570-0046-9. — Режим доступа: http://www.iprbookshop.ru/73727.html
4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 c. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/63800.html
5. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс] : учебное пособие / БехроузА. Фороузан. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 782 c. — 978-5-4487-0143-6. — Режим доступа: http://www.iprbookshop.ru/72337.html

4.2. Дополнительная литература

1. Информационный мир XXI века. Криптография – основа информационной безопасности [Электронный ресурс] / Б. П. Елисеев, Э. А. Болелов, О. Д. Гаранина [и др.] ; под ред. Э. А. Болелова. — 3-е изд. — Электрон. текстовые данные. — М. : Дашков и К, Московский государственный технический университет гражданской авиации, 2019. — 126 c. — Режим доступа: http://www.iprbookshop.ru/85368.html
2. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования [Электронный ресурс]/ К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2019. — 363 с. — Режим доступа: https://www.biblio-online.ru/bcode/430406.
3. Горев А.И. Обработка и защита информации в компьютерных системах [Электронный ресурс] : учебно-практическое пособие / А.И. Горев, А.А. Симаков. — Электрон. текстовые данные. — Омск: Омская академия МВД России, 2016. — 88 c. — Режим доступа: http://www.iprbookshop.ru/72856.html
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования [Электронный ресурс]/ Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2019. — 325 с. — Режим доступа: https://www.biblio-online.ru/bcode/434576.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;
- приложения.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Лаборатория «Информационных технологий, сетей и систем передачи информации, программирования и баз данных» (ауд. 111 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Стенды: Телекоммуникационные линии связи Сетевая безопасность Корпоративные компьютерные сети	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition №1688-181008-182042-963-980 Право на использование ПО с 09.10.2018 до 24.10.2020
Лаборатория «Программных и программно – аппаратных средств защиты информации» (ауд. 105 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности: ПАК Аккорд-NT, № 52202314; ПАК «Соболь» 3.0, № 7CJJC4GW; «Dallas Lock 8.0-C», № 29093-4159-1156. Программные и программно-аппаратные средства обнаружения вторжений: система обнаружения и предотвращения вторжений Dallas Lock, № 29093-4159-1156	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 CodeGear RAD Studio 2007 Professional Лицензия №32954 Бессрочная Гос. Контракт №35-03/161 от 19.08.2008г

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	6

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать состав и принципы работы автоматизированных систем, операционных систем и сред	Зач01
Знать принципы разработки алгоритмов программ, основных приемов программирования	Зач01
Знать модели баз данных	Зач01
Знать принципы построения, физические основы работы периферийных устройств	Зач01
Знать теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации	Зач01
Знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях	Зач01
Знать принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	Зач01
Уметь осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем	Зач01
Уметь организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней	Зач01
Уметь осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем	Зач01
Уметь производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	Зач01
Уметь настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	Зач01
Уметь обеспечивать работоспособность, обнаруживать и устранять неисправности	Зач01
Иметь практический опыт установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем	Зач01
Иметь практический опыт администрирования автоматизированных систем в защищенном исполнении	Зач01
Иметь практический опыт эксплуатации компонентов систем защиты информации автоматизированных систем	Зач01
Иметь практический опыт диагностики компонентов систем защиты информации автоматизированных систем,	Зач01

Результаты обучения	Контрольные мероприятия
Иметь практический опыт устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении	Зач01

Вопросы к защите отчета по практике Зач01

1. Понятие операционной системы.
2. Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.
3. Основные виды ресурсов. Многозадачность.
4. Понятия «файл», «файловая система» и «система управления файлами».
5. Модульная структура операционных систем, пространство пользователя
6. Управление памятью
7. Понятие безопасности ОС. Классификация угроз ОС.
8. Порядок обеспечения безопасности информации при эксплуатации операционных систем.
9. Штатные средства ОС для защиты информации
10. Задачи интерфейсов операционных систем.
11. Обзор системы Linux
12 .Серверные ОС
13. Принцип совместимости. Общая характеристика операционных систем UNIX, особенности архитектуры семейства ОС UNIX.
14. Основные понятия и определения теории баз данных.
15. Типы полей данных. Свойства полей
16. Основные объекты баз данных: таблицы, запросы, формы, отчеты, макросы, модули.
17. Основные этапы проектирования баз данных.
18. Классификация, назначение, базовые понятия СУБД
19. Современные СУБД – характеристика и особенности наиболее распространенных СУБД.
20. Понятие запроса. Запросы на изменение. Запросы на выборку. Групповые запросы. Перекрестные запросы.
21. Макросы в MS Access, создание макросов.
22. Возможности языка SQL
23. Задачи администрирования БД. Привилегия, доступ.
24. Виды пользователей и группы привилегий, соответствующие виду пользователя.
25. Возможности SQL для администрирования
26. Защита базы данных. Понятие информационной безопасности
27. Методы и средства защиты базы данных.
28. Контроль доступа к данным. Управление привилегиями пользователей базы данных
29. Основные понятия компьютерных сетей. Типы сетевых архитектур. Типы серверов. Отличия сетевых топологий.
30. Требования, предъявляемые к современным вычислительным сетям
31. Методы цифрового кодирования. Способы модуляции
32. Принципы передачи информации по сети.
33. Назначение и типы информационных пакетов, структура пакетов.
34. Методы управления обменом в сетях с разной топологией.
35. Способы разделения канала по частоте и времени
36. Стандартная модель взаимодействия открытых систем OSI, уровни функций, выполняемых при взаимодействии по сети.
37. Принципы работы протоколов разных уровней
38. Принципы адресации в IP – сетях.
39. Пространство доменных имен, принципы их распределения и распознавания. Организация доменов и доменных имен.

40. Принципы маршрутизации. Маршрутизаторы. Маршрут передачи пакетов. Принципы маршрутизации с использованием масок
41. Защита информации в сетях
42. Автоматизированные информационные системы: основные понятия и определения.
43. Принципы создания, реализация информационного обеспечения.
44. Назначение, состав и структура математического обеспечения АС. Уровни математического обеспечения.
45. Назначение модели. Математическое моделирование
46. Состав и структура комплекса технических средств. Требования к техническим средствам. Порядок описания комплекса технических средств.
47. Понятие жизненного цикла АИС.
48. Процессы жизненного цикла АИС: основные, вспомогательные, организационные.
49. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение.
50. Модели жизненного цикла АИС.
51. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования.
52. Требования к автоматизированной системе в защищенном исполнении.
53. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении.
54. Требования по защите сведений о создаваемой автоматизированной системе.
55. Угрозы безопасности информации в автоматизированных системах
56. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.
57. Механизмы и методы защиты информации в распределенных автоматизированных системах.
58. Архитектура механизмов защиты распределенных автоматизированных систем
59. Классификация компьютерных сетей.
60. Сетевое оборудование в топологии.
61. Обзор сетевых топологий. Методы совместного использования среды передачи канала связи.
62. Оптоволоконные линии связи . Стандарты кабелей. Электрическая проводка. Беспроводная среда передачи.
63. Локальные сети Ethernet. Локальные сети Token Ring. Локальные сети FDDI. Локальные сети AppleTalk.Локальные сети ARCnet.
64. Глобальные сети, обзор глобальных сетей (Wide Area Network - WAN).
65. Сетевое оборудование и программное обеспечение
66. Физические компоненты сетей: коаксиальные кабели, витые пары, волоконно-оптические кабели, беспроводные технологии.
67. Модели сетевого взаимодействия
68. Соединительные устройства: повторители, концентраторы, маршрутизаторы и коммутаторы
69. Физические компоненты сетей: коаксиальные кабели, витые пары, волоконно-оптические кабели, беспроводные технологии.
70. Соединительные устройства: повторители, концентраторы, маршрутизаторы и коммутаторы
71. Защита информационных систем от несанкционированного доступа
72. Утечка информации и ее особенности.
73. Подходы к оценке уровня угрозы.
74. Факторы, влияющие на возможность реализации угроз информационной безопасности

Практические задания к защите отчета по практике Зач01

Задание 1

Дана схема автоматизированной системы в защищенном исполнении. Описать технические и организационные средства и проведенные строительно-монтажные работы, примененные для защиты автоматизированной системы:

Задание 2

Ниже приведены примеры использования зарезервированных имен, расшифровать их:

- copy myfile.txt prn – _____
- copy con a.txt - _____
- copy a.txt con – _____
- copy a.txt a: > nul - _____
- copy a:*.* nul - _____

Задание 3

Выполнить задание, используя команды MS DOS.

- Создать каталог с именем TEST. Перейти в данный каталог. В каталоге TEST создать еще два подкаталога. Один из них удалить, другой переименовать, затем перейти в него.
- Создать текстовый файл, записать туда несколько строк. Создать копию данного файла (в текущем каталоге). Скопировать файл в каталог верхнего уровня (в корневой каталог). Переименовать файл. Удалить.
- Создать текстовый файл A.TXT, содержащий несколько фамилий (не упорядоченных по алфавиту). Упорядочить данный файл с выводом результатов на экран. Упорядочить данный файл с выводом результатов в файл B.TXT.
- С помощью команды TYPE проверить, есть ли в файлах A.TXT и B.TXT фамилия “Сидоров”.
-Привести другие примеры работы с командой DIR. В чем состоит недостаток данной команды?

Задание 4

Заполнить таблицу.

Метод запуска Проводника	**Используемый элемент управления**	**Папка открытия**
1) Через контекстное меню кнопки Пуск	*Кнопка Пуск*	*Главное меню*
2)…	*…*	*…*
3)…	*…*	*…*
4)		
5)		

Задание 5

1. Создание концептуальной, логической и физической модели данных

Разработать концептуальную и логическую модель данных для заданной предметной области, создать таблицы и установить связи между таблицами

Ответ на задание 1 должен содержать:

Словесное описание предметной области, например

Компания, занимается оптовой продажей различных товаров. Задачей является отслеживание финансовой стороны ее работы.

Деятельность компании организована следующим образом: компания торгует товарами из определенного спектра. Каждый из этих товаров характеризуется ценой, справочной информацией и признаком наличия или отсутствия доставки. В вашу компанию обращаются заказчики. Для каждого из них вы запоминаете в базе данных стандартные данные (наименование, адрес, телефон, контактное лицо) и составляете по каждой сделке документ, запоминая наряду с заказчиком количество купленного им товара и дату покупки.

Возможный набор сущностей

Товары (Код товара, Цена, Доставка, Описание).

Заказчики (Код заказчика, Наименование, Адрес, Телефон, Контактное лицо).

Заказы (Код заказа, Код заказчика, Код товара, Количество, Дата).

Доставка разных товаров может производиться способами, различными по цене и скорости. Нужно хранить информацию о том, какими способами может осуществляться доставка каждого товара, и о том, какой вид доставки (а соответственно, и какую стоимость доставки) выбрал клиент при заключении сделки.

Рисунок 1 – Пример концептуальной модели предметной области «Продажи товаров»

Рисунок 2 – Структура логической модели БД «Сотрудники»

2. Разработка серверной части базы данных в инструментальной оболочке

1. На основе разработанной логической модели БД, разработать схему базы данных
2. Произвести проектирование таблиц на языке SQL

Ответ на задание 2 должен содержать:

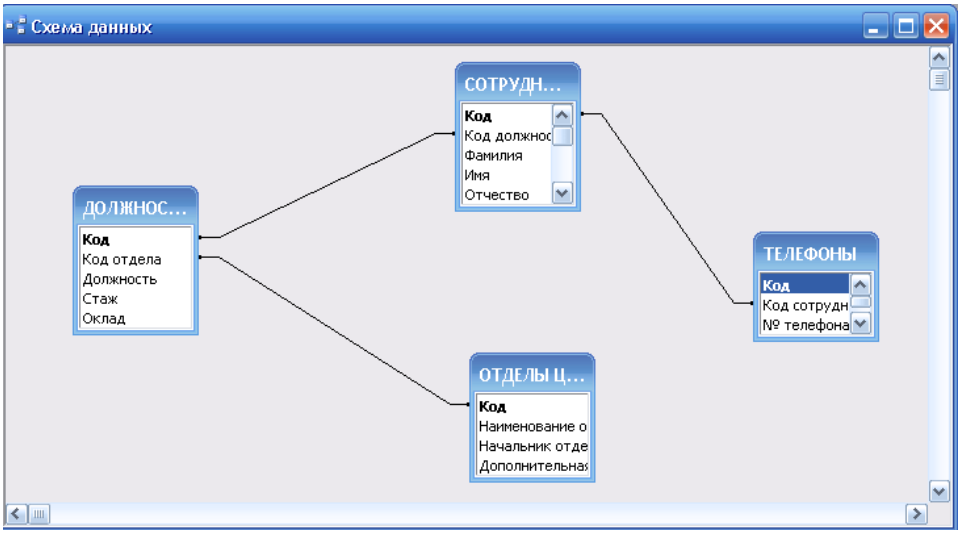


Рисунок 3 – Схема данных

Сотрудники
Код сотрудника- счетчик, Код должности - целый, Код населенного пункта- целый, Фамилия- текстовый, Имя – текстовый , Отчество, Улица, Дом, Квартира, Серия паспорта, Номер паспорта, Кем выдан, Дата выдачи, Стаж
Должности
Код должности, Код отдела, Наименование должности, Оклад
Телефон
Код телефона, Код сотрудника, № телефона сотовый, № телефона домашний
Отделы ЦНТИ
Код отдела, Наименование отдела, Начальник отдела, Дополнительная информация

Запрос на создание таблицы Товары
CREATE TABLE Товары([№] integer,
[Вид_товара] text,
[Тип_товара] text,

[Наименование] text ,
[Стоимость] int,
CONSTRAINT [Индекс1] PRIMARY KEY ([№]));

3. Разработка клиентской части базы данных в инструментальной оболочке

1. Описать задачи клиентской части базы данных
2. Привести их программную реализацию на языке SQL

Ответ на задание 3 должен содержать:

1.1 Показать время обработки запроса
1.2 Показать заявку с максимальной ценой
1.3 Показать количество каждого прихода материала
1.4 Показать максимальную выручку с заявки
1.5 Показать сколько работник получит зарплату
1.6 Показать информацию о работнике по введенному номеру
1.7 Показать номера работников 10,15,20
1.8 Показать информацию о работнике по введенному номеру с начального до конечного
1.9 Показать информацию о нужном материале
1.10 Показать остаток материалов

2.1 SELECT дата_получения, дата_сдачи, дата_сдачи-дата_получения AS Время_работы
FROM работа;
2.2 SELECT заявка
FROM работа
WHERE выручка=(select max(выручка)from работа);
2.3 SELECT приход, count(приход) AS Количество
FROM материалы
GROUP BY приход;
2.4 SELECT max(Выручка) AS Максимальная_выручка
FROM Работа;
2.5 SELECT фамилия, имя, отчество, оклад, премия, ([оклад]+[премия])/100*13 AS [Подоходный налог], [оклад]+[премия]-[Подоходный налог] AS [На выдачу]
FROM Оплата, Должностя, работники
WHERE работники.№=[Должностя].код_должности And [Должностя].код_должности=оплата.№_сотрудника;
2.6 SELECT Работники.№, Работники.Фамилия, Работники.Имя, Работники.Отчество, Работники.Телефон
FROM Работники
WHERE № Like [Введите номер работника];
2.7 SELECT Работники.№, Работники.Фамилия, Работники.Имя, Работники.Отчество, Работники.Телефон
FROM Работники
WHERE № In (10,15,20);
2.8 SELECT Работники.№, Работники.Фамилия, Работники.Имя, Работники.Отчество, Работники.Телефон
FROM Работники
WHERE №>=[Введите начальный номер] And №<=[Введите конечный номер];
2.9 SELECT наименование, приход, расход
FROM материалы
WHERE наименование like [Введите нужный материал];
2.10 SELECT Наименование, Материалы.Приход, Материалы.Расход, [приход]-[расход] AS

Остаток
FROM Материалы;

4. Построение запросов различных типов к базе данных на языке SQL

1. Создать запросы на добавление данных
2. Создать запросы на удаление данных
3. Создать запросы на обновление данных
4. Создать запросы на создание таблиц

5. Команды манипулирования данными

1. Создать различные запросы на выборку, используя возможности языка SQL для манипулирования данными

Ответ на задание 5 должен содержать:

1. 1Вывести все данные из таблиц товары и покупатели
SELECT Товары.*, Покупатели.*
FROM Товары, Покупатели, Товары_покупатели
WHERE Товары.Код_товара=Товары_покупатели.Код_товара And Покупатели.Код_покупателя=Товары_покупатели.Код_покупателя;

1.2. Вывести информацию о товаре с определенным названием:
SELECT *
FROM Товары
WHERE Наименование Like [Введите Наименование];

6. Разработка пользовательского интерфейса

1. Разработать пользовательский интерфейс приложения, учитывая особенности предметной области и потребности пользователей базы данных

Ответ на задание 6 должен содержать:

Словесное описание назначения всех элементов формы

Задание 6

По заданным IP-адресу сети и маске определите адрес сети:
IP-адрес: 145.92.137.88
Маска: 255.255.240.0
14. По заданным IP-адресу узла сети и маске определите адрес сети:
IP-адрес: 10.8.248.131
Маска: 255.255.224.0

Задание 7

Заполнить таблицу.

Класс адреса	Маска сети по умолч.	Количество хостов (используемых адресов) в сети
D		
C		

Задание 8

С помощью программы MS Windows "Сведения о системе" и соответствующих команд соберите информацию о системе и заполните таблицу:

Имя узла	Название ОС	Версия ОС	Изготовитель ОС	Параметры ОС

Задание 9

1. Построить модель угроз автоматизированной системы учета клиентов фирмы
2. Разработать функциональную подсистему ввода-вывода информации автоматизированной информационной системы «Ремонт бытовой техники» на основе СУБД
3. Разработать функциональную подсистему манипулирования автоматизированной информационной системы «Компьютерные комплектующие» на основе СУБД
4. Разработать структуру автоматизированной информационной системы «Ремонт бытовой техники»
5. Разработать интерфейс автоматизированной информационной системы «Компьютерные комплектующие» на основе СУБД
6. Разработать техническое задание на проектирование автоматизированной системы «Кадры»
7. Разработать техническое задание на проектирование автоматизированной системы «Товарный склад»
8. Осуществить разграничение доступа к устройствам с помощью Secret Net 4.0
9. Осуществить настройку Secret Net 4.0
10. Построить модель угроз АС учета результатов обучения студентов

Задание 10

1. Произвести анализ сетевого трафика
2. Произвести анализ основных направлений затрат проектирования локальной сети офиса (в сети 3 ПК)
3. Определить характеристики используемого программного обеспечения проектирования локальной сети офиса (в сети 3 ПК)
4. С помощью программы MS Windows "Сведения о системе" и systeminfo собрать информацию о системе
5. Определить состав и основные характеристики оборудования и системного программного обеспечения, установленного на компьютере.
6. Определить сетевое имя компьютера и рабочую группу, в которую он входит.
7. Определить состав установленных в компьютере сетевых адаптеров
8. Определить текущее состояние сетевых подключений Вашего компьютера
9. Осуществить отслеживание трафика многоадресной рассылки
10. Осуществить настройку межсетевого экрана

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характери-

стику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол №*3*	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

ПП.02.01 Производственная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами)
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель	_____	Н.Г. Мосягина
должность	подпись	инициалы, фамилия

Директор Технического колледжа

_____	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

1.2. В результате прохождения практики обучающийся должен:

знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации;

– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа

уметь:

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– применять программные и программно-аппаратные средства для защиты информации в базах данных;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– применять математический аппарат для выполнения криптографических преобразований;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– применять средства гарантированного уничтожения информации;

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

иметь практический опыт:

– установки, настройки программных средств защиты информации в автоматизированной системе;

– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

– тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;

– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

– работы с подсистемами регистрации событий;

– выявления событий и инцидентов безопасности в автоматизированной системе.

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Способ проведения практики: концентрированная.

Объем практики составляет 108 часов.

3. СОДЕРЖАНИЕ ПРАКТИКИ

4 курс

Темы практики и виды работ			Количество часов
7 семестр			**108**
Тема 1	**Организация (предприятие) – база прохождения практики**		**20**
	Виды работ:		
	1.	**Проведение вводного инструктажа по правилам внутреннего трудового распорядка предприятия**	1
	2.	**Общие сведения об организации (предприятии)** Знакомство с предприятием, режимом его работы. Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации). Знакомство с историей предприятия (организации).	3
	3.	**Организационная структура организации (предприятия)**	4
	4.	**Виды деятельности организации (предприятия)** Изучение видов деятельности предприятия (организации), выпускаемой продукции, партнеров.	4
	5.	**Структурные подразделения, в которых проходила практика, их функции, задачи** Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика	4
	6.	**Сбор информации о видах обеспечения автоматизированных систем предприятия (организации)** Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для выполнения заданий на время прохождения производственной практики.	4
Тема 2	**Выполнение заданий согласно программе практики**		**86**
	Виды работ:		
	1.	Анализ принципов построения систем информационной защиты производственных подразделений.	16
	2.	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы	12
	3.	Участие в диагностировании программно-аппаратных средств обеспечения информационной безопасности	8
	4.	Участие в устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности	8
	5.	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	16
	6.	Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.	8
	7.	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	18
	Дифференцированный зачет		**2**
	Итого:		**108 часов**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1. Основная литература

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, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433

2. 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, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525

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, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524

4. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89455.html

4.2. Дополнительная литература

5. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования [Электронный ресурс] / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/442312.

6. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html

7. Информационный мир XXI века. Криптография – основа информационной безопасности [Электронный ресурс] / Б. П. Елисеев, Э. А. Болелов, О. Д. Гаранина [и др.] ; под ред. Э. А. Болелова. — 3-е изд. — Электрон. текстовые данные. — М. : Дашков и К, Московский государственный технический университет гражданской авиации, 2019. — 126 с. — Режим доступа: http://www.iprbookshop.ru/85368.html

8. 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 ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;
- приложения.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Лаборатория «Программных и программно – аппаратных средств защиты информации» (ауд. 105 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности: ПАК Аккорд-NT, № 52202314; ПАК «Соболь» 3.0, № 7CJJC4GW; «Dallas Lock 8.0-C», № 29093-4159-1156. Программные и программно-аппаратные средства обнаружения вторжений: система обнаружения и предотвращения вторжений Dallas Lock, № 29093-4159-1156	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 CodeGear RAD Studio 2007 Professional Лицензия №32954 Бессрочная Гос. Контракт №35-03/161 от 19.08.2008г

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1	2	3
1.	Центр по проблемам информационной безопасности ТГТУ	г.Тамбов, ул.Советская, д.106
2.	Тамбовский филиал ПАО «Ростелеком»	г. Тамбов, ул. Астраханская, д.2в
3.	ООО «Объединенные системы связи»	г. Тамбов, бул. Строителей, 6А
4.	ООО ”Тамбовский редуктор	г. Тамбов, ул. Заводская, д.4, пом. 16
5.	Территориальный орган Федеральной службы государственной статистики по Тамбовской области (Тамбовстат)	г. Тамбов, Интернациональный проезд,14
6.	Магазин “ABS Центр”	г.Тамбов, ул. Им.Вадима Подбельского д78
7.	АО Банк «ТКПБ»	г. Тамбов, Советская 118

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	7

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Зач01
Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Зач01
Знать типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации	Зач01
Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации	Зач01
Знать особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	Зач01
Знать типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Зач01
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями	Зач01
Уметь диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	Зач01
Уметь применять программные и программно-аппаратные средства для защиты информации в базах данных	Зач01
Уметь проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	Зач01
Уметь применять математический аппарат для выполнения криптографических преобразований	Зач01
Уметь использовать типовые программные криптографические средства, в том числе электронную подпись	Зач01
Уметь применять средства гарантированного уничтожения информации	Зач01
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Зач01

Результаты обучения	Контрольные мероприятия
Иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе	Зач01
Иметь практический опыт обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами	Зач01
Иметь практический опыт тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации	Зач01
Иметь практический опыт решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации	Зач01
Иметь практический опыт применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	Зач01
Иметь практический опыт учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности	Зач01
Иметь практический работы с подсистемами регистрации событий	Зач01
Иметь практический опыт выявления событий и инцидентов безопасности в автоматизированной системе	Зач01

Вопросы к защите отчета по практике Зач01

1. . В какой организации (предприятии) проходила практика?
2. Какую деятельность осуществляет организация (предприятие)?
3. Расскажите об организационной структуре организации (предприятии)?
4. Каковы виды деятельности организации (предприятия)?
5. В каком структурном подразделении проходила практика?
6. Какие технические характеристики имелись на компьютере, за которым осуществлялась работа?
7. Расскажите о программном обеспечении, установленном на этом компьютере.
8. Методы создания безопасных систем обработки информации
9. Стандарты информационной безопасности и их роль
10. Угрозы безопасности компьютерных систем
11. Методы взлома компьютерных систем
12. Защита компьютерной системы от взлома
13. Защита компьютерной системы от программных закладок
14. Защита от компьютерных вирусов
15. Что такое монитор безопасности?
16. Формирование и поддержка изолированной программной среды
17. Процедура идентификации и аутентификации

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положитель-

ную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол №*3*	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

УП.02.01 Учебная практика (Защита информации в автоматизированных системах программными и программно-аппаратными средствами)

(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель		Н.Г. Мосягина
должность	подпись	инициалы, фамилия

Директор Технического колледжа

	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компью-

Код компетенции	Формулировка компетенции
	терных атак

1.2. В результате прохождения практики обучающийся должен:

знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации;

– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа

уметь:

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– применять программные и программно-аппаратные средства для защиты информации в базах данных;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– применять математический аппарат для выполнения криптографических преобразований;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– применять средства гарантированного уничтожения информации;

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

иметь практический опыт:

– установки, настройки программных средств защиты информации в автоматизированной системе;

– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

– тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;

– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

– работы с подсистемами регистрации событий;

– выявления событий и инцидентов безопасности в автоматизированной системе.

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: учебная.
Способ проведения практики: рассредоточенная.

Объем практики составляет 144 часа.

3. СОДЕРЖАНИЕ ПРАКТИКИ

Темы практики и виды работ			Количество часов
6 семестр			**72**
Тема 1	**Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах**		**38**
	Виды работ:		
	1.	Проведение инструктажа по технике безопасности при работе на ЭВМ. Проведение диагностики и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	4
	2.	Выявление и устранение отказов программно-аппаратных средств обеспечения информационной безопасности	4
	3.	Тестирование функций программно-аппаратных средств обеспечения информационной безопасности	4
	4.	Проведение оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	4
	5.	Применение математических методов для оценки качества и выбора наилучшего программного средства	8
	6.	Обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами	6
	7.	Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов	8
Тема 2	**Участие в обеспечении учета, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности**		**32**
	Виды работ:		
	1.	Проведение инструктажа по технике безопасности при работе на ЭВМ Осуществление установки и настройки типовых программных средств защиты информации	4
	2.	Осуществление установки и настройки средств антивирусной защиты в соответствии с предъявляемыми требованиями	2
	3.	Применение программных и программно-аппаратных средств для защиты информации в базах данных;	6
	4.	Решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации	6
	5.	Проверка выполнения требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	4
	6.	Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	6
	7.	Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации	4
	Дифференцированный зачет		**2**

	Итого	**72 часа**

Темы практики и виды работ			Количество часов
7 семестр			**72**
Тема 3	**Мониторинг систем защиты**		**22**
	Виды работ:		
	1.	Проведение инструктажа по технике безопасности при работе на ЭВМ Выявление событий и инцидентов безопасности в автоматизированной системе	4
	2.	Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов	8
	3.	Осуществление мониторинга и регистрации сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	6
	4.	Устранение замечаний по результатам проверки	4
Тема 4	**Использование криптографических методов защиты информации**		**48**
	Виды работ:		
		Проведение инструктажа по технике безопасности при работе на ЭВМ Применение математического аппарата для выполнения криптографических преобразований	6
		Применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	6
		Выполнение учебно-тренировочных операций по монтажу криптографических электронных схем и блоков	12
		Моделирование стандартных цифровых подписей и хэш-функций, создание собственных вариантов простейших цифровых подписей с применением ПК	12
		Составление криптографических моделей сообщений	8
		Применение средств гарантированного уничтожения информации	4
	Дифференцированный зачет		**2**
	Итого		**72 часа**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1. Основная литература

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, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433 (дата обращения: 21.02.2022).

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, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525

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, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524
4. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89455.html

4.2 Дополнительная литература

5. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования [Электронный ресурс] / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/442312.
6. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html
7. Информационный мир XXI века. Криптография – основа информационной безопасности [Электронный ресурс] / Б. П. Елисеев, Э. А. Болелов, О. Д. Гаранина [и др.] ; под ред. Э. А. Болелова. — 3-е изд. — Электрон. текстовые данные. — М. : Дашков и К, Московский государственный технический университет гражданской авиации, 2019. — 126 с. — Режим доступа: http://www.iprbookshop.ru/85368.html
8. 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 ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889 (дата обращения: 21.02.2022).

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;
- приложения.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Лаборатория «Программных и программно – аппаратных средств защиты информации» (ауд. 105 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности: ПАК Аккорд-NT, № 52202314; ПАК «Соболь» 3.0, № 7CJJC4GW; «Dallas Lock 8.0-C», № 29093-4159-1156. Программные и программно-аппаратные средства обнаружения вторжений: система обнаружения и предотвращения вторжений Dallas Lock, № 29093-4159-1156	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 CodeGear RAD Studio 2007 Professional Лицензия №32954 Бессрочная Гос. Контракт №35-03/161 от 19.08.2008г

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	6
Зач02	Дифференцированный зачет	7

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Зач01
Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Зач01
Знать типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации	Зач01
Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации	Зач02
Знать особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	Зач01
Знать типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Зач02
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями	Зач01
Уметь диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	Зач01
Уметь применять программные и программно-аппаратные средства для защиты информации в базах данных	Зач01
Уметь проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	Зач02
Уметь применять математический аппарат для выполнения криптографических преобразований	Зач02
Уметь использовать типовые программные криптографические средства, в том числе электронную подпись	Зач02
Уметь применять средства гарантированного уничтожения информации)	Зач01
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь осуществлять мониторинг и регистрацию сведений, необходимых для	Зач02

Результаты обучения	Контрольные мероприятия
защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	
Иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе	Зач01
Иметь практический опыт обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами	Зач01
Иметь практический опыт тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации	Зач01
Иметь практический опыт решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации	Зач01
Иметь практический опыт применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	Зач02
Иметь практический опыт учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности	Зач01
Иметь практический работы с подсистемами регистрации событий	Зач02
Иметь практический опыт выявления событий и инцидентов безопасности в автоматизированной системе	Зач02

Вопросы к защите отчета по практике Зач01

1. Классификация методов и средств программно-аппаратной защиты информации
2. Автоматизация процесса обработки конфиденциальной информации
3. Стандарты информационной безопасности и их роль
4. Угрозы безопасности компьютерных систем
5. Методы взлома компьютерных систем
6. Защита компьютерной системы от взлома
7. Защита компьютерной системы от программных закладок. Защита от компьютерных вирусов
8. Реализация механизмов безопасности на аппаратном уровне
9. Контроль и управление доступом
10. Управление рисками
11. Аудит информационной безопасности
12. Механизмы и службы защиты
13. Сетевые атаки
14. Обобщенный сценарий атаки
15. Параметры атаки
16. Классификация удаленных атак
17. Оценивание степени серьезности атак
18. Основы построения защищенных сетей
19. Сети, работающие по технологии коммутации пакетов
20. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

Практические задания к защите отчета по практике Зач01

1. Дано: описание алгоритма хэширования паролей в базах данных аутентификации Windows NT/2000 (Lan manager):

Для формирования хэша пароля все буквенные символы исходной строки пользовательского пароля приводятся к верхнему регистру, и если пароль содержит меньше 14 символов, то он дополняется нулями. Из каждой 7-байтовой половины преобразованного таким

образом пароля пользователя (длина пароля в Windows NT/2000/XP ограничена 14 символами), отдельно формируется ключ для шифрования некоторой фиксированной 8-байтовой последовательности по DES-алгоритму с ключом 64(56)бит. При этом в качестве ключа используется PID (персональный идентификатор) пользователя). Полученные в результате две 8-байтовые половины хешированного пароля Lan Manager еще раз шифруются по DES-алгоритму и помещаются в базу данных SAM.

Проанализируйте уровень защищенности баз данных аутентификации операционных систем, связанную с описанным алгоритмом.

2. Дано: имеется сервер, работающий под управлением ОС Windows Server 2003. На сервере запущена СУБД Oracle 9i. С помощью каких программных средств можно составить список возможных уязвимостей и определить уровень угроз?
   Опишите известные Вам виды уязвимостей, присущие предложенной конфигурации сервера и способы защиты от них.

3. Имеется процедура добавления (регистрации) нового покупателя на PL/SQL следующего содержания:

```
Create procedure NewCustomer(CName
varchar2,CPassword
varchar2,CInfo varchar2) as
Begin
Insert into CustomersTable (Name,Password,Info) values('||CName||'
,*||CPassword||'
,'||CInfo||');
End;
```

Какой способ SQL Injection необходимо применить, чтобы в поле CInfo занести пароль пользователя «Иванов» из этой же таблицы. Как обнаружить и предотвратить попытку SQL Injection

4.Дано: имеется функция проверки аутентификации покупателя по имени пользователя и паролю на PL/SQL следующего содержания:

```
Create function GetCustomerInfo(CName
varchar2,CPassword
varchar2) return varchar2 as CInfo
varchar2(200);
Begin
Select Info into CInfo from CustomersTable
where
Name='||CName||'
and Password='||CPassword||';
Return
CInfo;
End;
```

Какой способ SQL Injection необходимо применить, чтобы злоумышленник зарегистрировался под пользователем «Иванов» из этой же таблицы без знания пароля. Как обнаружить и предотвратить попытку SQL Injection

Вопросы к защите отчета по практике Зач02

1. Основные определения криптографии
2. Шифры замены и их свойства.
3. Шифрование методом перестановки. Шифрование методом гаммирования
4. Криптографические параметры узлов и блоков шифраторов
5. Криптографическая стойкость шифров.

6. Российский стандарт шифрования ГОСТ 28147-89
7. Стандарт шифрования США AES
8. Принципы построение и свойства хэш-функций.
9. Российский стандарт хэширования ГОСТ Р 34.11-2012
10. Стандарт хэширования США. Хэш-функция Keccak
11. «Слепая» цифровая подпись
12. Методы получения случайных и псевдослучайных последовательностей.
13. Генератор псевдослучайных чисел «Fortuna»
14. Арифметика по модулю простого числа. Китайская теорема об остатках.
15. Алгоритм Диффи – Хеллмана. Базовый алгоритм.
16. Атака посредника. Надежные простые числа. Практические правила
17. Построение алгоритма RSA. Генерация ключей с помощью алгоритма RSA. Шифрование с помощью алгоритма RSA
18. Создание цифровой подписи с помощью алгоритма RSA.
19. Введение в криптографические протоколы. Роли. Доверие. Риск. Стимул.
20. Классификация атак направленных на криптографические протоколы
21. Безопасный канал общения
22. Криптографические протоколы Интернета (SSL, PPTP, SET).

Практические задания к защите отчета по практике Зач02

1 Вы едете в поезде, чтобы не скучать, она зашифровываете названия разных городов, заменяя буквы их порядковыми номерами в алфавите. Когда вы зашифровала пункты прибытия и отправления поезда, то обнаружили, что они записываются с помощью всего лишь двух цифр: 21221 - 211221.
Откуда и куда шел поезд?

Русский алфавит:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ъ	Ю	Я
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

2. Дана криптограмма

ФН * Ы = ФАФ
\+ * -
ЕЕ + Е = НЗ
= = =
ИША + МП = ИМН

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст.

3. Ключом шифра, называемого «поворотная» решетка, является трафарет, изготовленный из квадратного листа клетчатой бумаги размера $n * n$. Некоторые из клеток вырезаются. Одна из сторон трафарета помечена.

При наложении этого трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, причем каждая клетка оказывается под вырезом ровно один раз. Буквы сообщения, имеющего длину n^2, последовательно вписываются в вырезы трафарета, сначала наложенного на чистый лист бумаги помеченной стороной вверх. После заполнения всех вырезов трафарета буквами сообщения трафарет располагается в следующем положении и т.д. После снятия трафарета на листе оказывается зашифрованное сообщение.

Найдите число различных ключей для произвольного четного числа n.

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол №*3*.	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

ПП.03.01 Производственная практика (Защита информации техническими средствами)

(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель	_____	М.В. Самородова
должность	подпись	инициалы, фамилия

Директор Технического колледжа

_____	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
ПК 3.1	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.2	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.3	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.4	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации

1.2. В результате прохождения практики обучающийся должен:

знать:

– порядок технического обслуживания технических средств защиты информации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– основные принципы действия и характеристики технических средств физической защиты;

– основные способы физической защиты объектов информатизации;

– номенклатуру применяемых средств физической защиты объектов информатизации.

уметь:

– применять технические средства для криптографической защиты информации конфиденциального характера;

– применять технические средства для уничтожения информации и носителей информации;

– применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

– применять инженерно-технические средства физической защиты объектов информатизации.

иметь практический опыт:

– установки, монтажа и настройки технических средств защиты информации;

– технического обслуживания технических средств защиты информации;

– применения основных типов технических средств защиты информации;

– выявления технических каналов утечки информации;

– участия в мониторинге эффективности технических средств защиты информации;

– диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

– проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

– проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.03 «Защита информации техническими средствами».

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная
Способ проведения практики: концентрированная.

Объем практики составляет 108 часа(ов).

3. СОДЕРЖАНИЕ ПРАКТИКИ

Темы практики и виды работ			Количество часов
8 семестр			**108**
Тема 1	**Организация (предприятие) – база прохождения практики**		**20**
	Виды работ:		
	1.	Проведение вводного инструктажа по правилам внутреннего трудового распорядка предприятия Инструктаж по технике безопасности	1
	2.	Общие сведения об организации (предприятии) Знакомство с предприятием, режимом его работы. Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации). Знакомство с историей предприятия (организации).	3
	3.	Организационная структура организации (предприятия)	4
	4.	Виды деятельности организации (предприятия) Изучение видов деятельности предприятия (организации), выпускаемой продукции, партнеров.	4
	5.	Структурные подразделения, в которых проходила практика, их функции, задачи Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика	4
	6.	Сбор информации о видах обеспечения автоматизированных систем предприятия (организации) Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для выполнения заданий на время прохождения производственной практики.	4
Тема 2	**Выполнение заданий согласно программе практики**		**86**
	Виды работ:		
	1.	Инструктаж по технике безопасности	
	2.	Участие в монтаже, установке, и настройке технических средств защиты информации	12
	3.	Участие в обслуживании и эксплуатации технических средств защиты информации	12
	4.	Участие в мониторинге эффективности технических средств защиты информации	8
	5.	Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности	12
	6.	Участие в монтаже, обслуживании и эксплуатации средств инженерной защиты и технической охраны объектов	12
	7.	Участие в монтаже, обслуживании и эксплуатации систем видеонаблюдения	12
	8.	Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
	9.	Участие в обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим ка-	6

		налам;	
	10	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	6
Дифференцированный зачет			**2**
Итого			**108**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1. Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования [Электронный ресурс] / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — Режим доступа: https://www.biblio-online.ru/bcode/431332

2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 c. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/63800.html

3. Полякова, Т.А., Стрельцов, А.А., Чубукова, С.Г., Ниесов, В.А.; Отв. ред. Полякова Т.А., Стрельцов А.А. Организационно и правовое обеспечение информационной безопасности. Учебник и практикум для СПО.- Научная школа: Всероссийский государственный университет юстиции (РПА Минюста России) (г. Москва), 2019/Гриф УМО СПО.-326 с.- Режим доступа: https://www.biblio-online.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-434576#page/5

4.2. Дополнительная литература

1. Нестеров, С.А. Информационная безопасность. Учебник и практикум для СПО.- Научная школа: Санкт-Петербургский политехнический университет Петра Великого (г. Санкт-Петербург), 2019/Гриф УМО СПО.- 322 с.- Режим доступа: https://www.biblio-online.ru/viewer/informacionnaya-bezopasnost-442312#page/6

2. Казарин, О.В., Шубинский И.Б. Основы информационной безопасности: надежность и безопасность программного обеспечения. Учебное пособие для СПО.-Научнавя школа: Российский государственный гумсанитарный университет (г. Москва). Московский государственный университет имени М.В. Ломоносовак (г. Москва), 2019/Гриф УМО СПО .- 343 с.- Режим доступа: https://www.biblio-online.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-431080#page/9

3. Петренко, В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html

4. Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 242 c. — 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся направление на практику, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

По результатам производственной практики руководителями практики от предприятия и колледжа формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций, а также характеристика на обучающегося по освоению им общих компетенций в период прохождения производственной практики.

Аттестация по итогам производственной практики проводится с учетом (или на основании) результатов ее прохождения, подтверждаемых документами соответствующих организаций.

Практика является завершающим этапом освоения профессионального модуля по виду профессиональной деятельности.

Производственная практика завершается зачетом при условии положительного аттестационного листа об уровне освоения профессиональных компетенций, наличия положительной характеристики от организации на обучающегося по освоению общих компетенций в период прохождения практики, полноты ведения дневника практики и своевременности предоставления отчета по итогам практики.

Обучающиеся, не выполнившие программы практики по уважительной причине, направляются на практику вторично, в свободное от учебы время.

Обучающиеся, не выполнившие программы практики без уважительной причины или получившие отрицательную оценку, не допускаются к прохождению государственной итоговой аттестации и могут быть отчислены из состава обучающихся, как имеющие академическую задолженность в связи с невыполнением учебного плана по специальности.

В период прохождения производственной практики обучающимся ведется дневник практики. В качестве приложения к дневнику практики обучающийся оформляет графические, аудио-, фото-, видеоматериалы, наглядные образцы изделий, подтверждающие практический опыт, полученный на практике.

По результатам производственной практики обучающимся составляется отчет, который утверждается организацией. В отчете в систематизированном виде должны быть освещены основные вопросы, предусмотренные программой практики, а также сформулированы выводы, к которым пришел практикант, и предложения. В качестве приложения к отчету могут прилагаться таблицы, схемы, графики, В качестве приложения к отчету могут прилагаться таблицы, схемы, графики, наглядные образцы изделий и другие материалы, подтверждающие практический опыт, полученный на практике.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Лаборатория «Технических средств защиты информации» (ауд. 105 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Аппаратные средства аутентификации пользователя: ПАК Аккорд-NT, № 52202314; ПАК «Соболь» 3.0, № 7CJJC4GW; «Dallas Lock 8.0-C», № 29093-4159-1156. Средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок: Учебный стенд «Полнофункциональный автоматизированный комплекс защиты информации от утечки по техническим каналам»; генератор шума «Гром – ЗИ - 4»; синтезатор помехового сигнала «Мозаика - М», № 057777; Средства измерения параметров физических полей (в том числе электромагнитных излучений и наводок, акустических (виброакустических) колебаний): селективный микровольтметр SMV-11, № 08332; селективный микровольтметр SMV-8,5, № 08199; селективный нановольтметр Unipan 233, № 55563; анализатор спектра «СК4-Белан 22», № 150; токосъемник измерительный ТИ2-3, № 0191; токосъёмник измерительный ТИ2-1, № 0371; антенна измерительная АИ5-0, № 287; антенна измерительная АИ4-1, № 01270; точный импульсный шумомер, № 01279; система измерительная автомати-	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 CodeGear RAD Studio 2007 Professional Лицензия №32954 Бессрочная Гос. Контракт №35-03/161 от 19.08.2008г

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
	зированная К6-6 (Трап), № 64; многофункциональный прибор ST 031P «Пиранья», № 1156. Стенд физической защиты объектов информатизации, оснащенный средствами контроля доступа, системами видеонаблюдения и охраны объектов	

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1.	ПАО «Тамбовский завод «Электроприбор»	392000,г. Тамбов, ул. Моршанское шоссе, 36 8 (4752) 57-73-03
2.	ОАО «Объединенные системы связи»	392000, г. Тамбов, бульвар Строителей, 6А 8 4752 63-33-13, 8 4752 63-33-07
3.	ООО «Инженерные системы»	г. Тамбов, ул. Ипподромная, 6 8 (4752) 49-23-29
4.	Тамбовский ЦНТИ-филиал ФГБУ «РЭА» Минэнерго России	г. Тамбов, ул. Советская, 182 8 (4752) 53-24-87; 8 (4752) 53-63-03
5.	ТОГОАУ ДПО «Институт повышения квалификации работников образования»	г. Тамбов, ул. Советская, 108 8 (4752) 63-05-10
6.	ООО «Дэмис Групп»	г. Тамбов, ул. Интернациональная, д.16 А +7(4752) 55-94-04
7.	ТОГКУ «Центр экспертизы образовательной деятельности»	г. Тамбов, ул. Лаврова, 9 8 (4752) 72-47-71
8.	ООО «Гибрид»	г. Тамбов, ул. Чичканова, 57 «А» 8 (4997) 03-14-32
9.	ООО «Химтехстрой».	г.Тамбов, улица Монтажников, дом 1 8 (4752) 53-31-01
10.	ООО ПК «Модуль»	г. Тамбов, Моршанское шоссе, д. 36 8 (4752) 57-73-20

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	8

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать порядок технического обслуживания технических средств защиты информации	Зач01
Знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;	Зач01
Знать физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;	Зач01
Знать порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;	Зач01
Знать методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;	Зач01
Знать номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;	Зач01
Знать основные принципы действия и характеристики технических средств физической защиты;	Зач01
Знать основные способы физической защиты объектов информатизации;	Зач01
Знать номенклатуру применяемых средств физической защиты объектов информатизации.	Зач01
Уметь применять технические средства для криптографической защиты информации конфиденциального характера;	Зач01
Уметь применять технические средства для уничтожения информации и носителей информации;	Зач01
Уметь применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;	Зач01
Уметь применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;	Зач01

Результаты обучения	Контрольные мероприятия
Уметь применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	Зач01
Уметь применять инженерно-технические средства физической защиты объектов информатизации.	Зач01
Иметь практический опыт установки, монтажа и настройки технических средств защиты информации;	Зач01
Иметь практический опыт технического обслуживания технических средств защиты информации;	Зач01
Иметь практический опыт применения основных типов технических средств защиты информации;	Зач01
Иметь практический опыт выявления технических каналов утечки информации;	Зач01
Иметь практический опыт участия в мониторинге эффективности технических средств защиты информации;	Зач01
Иметь практический опыт диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;	Зач01
Иметь практический опыт проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	Зач01
Иметь практический опыт проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;	Зач01
Иметь практический опыт установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.	Зач01

Вопросы к защите отчета по практике Зач01

1. В какой организации (предприятии) проходила практика?
2. Какую деятельность осуществляет организация (предприятие)?
3. Расскажите об организационной структуре организации (предприятии)?
4. Каковы виды деятельности организации (предприятия)?
5. В каком структурном подразделении проходила практика?
6. Какие технические характеристики имелись на компьютере, за которым осуществлялась работа?
7. Расскажите о программном обеспечении, установленном на этом компьютере.
8. Виды телевизионных камер и систем обработки видеосигналов.
9. Оборудование ограниченного доступа в помещение.
10. Основные задачи технической диагностики ТСЗИ.
11. Стандарты и виды диагностических моделей эксплуатируемых ТСЗИ.
12. Эксплуатация видеокамер систем видеонаблюдения.
13. Эксплуатация противопожарных датчиков.
14. Эксплуатация приборов контроля движения и звука.
15. Охранное видеонаблюдение в системе защиты информации, общие понятия.
16. Выбор конкретных точек установки телекамер в зависимости от их параметров.
17. Оперативные элементы охранного телевидения.
18. Цифровые системы видеонаблюдения.
19. Особенности охраны объектов ограниченного доступа. Общие положения
20. Назначение и виды эксплуатационных документов.

21.Рекомендации по ведению эксплуатационной документации.
22. Метрологическое обеспечение эксплуатации ТСЗИ.
23. Организация проведения и обработки результатов измерений.
24. Планово предупредительные работы при эксплуатации ТСЗИ

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол №*3*.	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

УП.03.01 Учебная практика (Защита информации техническими средствами)
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель		М.В. Самородова
должность	подпись	инициалы, фамилия

Директор Технического колледжа

	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
ПК 3.1	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.2	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.3	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.4	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации

1.2. В результате прохождения практики обучающийся должен:

знать:

– порядок технического обслуживания технических средств защиты информации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– основные принципы действия и характеристики технических средств физической защиты;

– основные способы физической защиты объектов информатизации;

– номенклатуру применяемых средств физической защиты объектов информатизации.

уметь:

– применять технические средства для криптографической защиты информации конфиденциального характера;

– применять технические средства для уничтожения информации и носителей информации;

– применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

– применять инженерно-технические средства физической защиты объектов информатизации.

иметь практический опыт:

– установки, монтажа и настройки технических средств защиты информации;

– технического обслуживания технических средств защиты информации;

– применения основных типов технических средств защиты информации;

– выявления технических каналов утечки информации;

– участия в мониторинге эффективности технических средств защиты информации;

– диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

– проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

– проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.03 «Защита информации техническими средствами».

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: учебная
Способ проведения практики: концентрированная.

Объем практики составляет 72 часа(ов).

3. СОДЕРЖАНИЕ ПРАКТИКИ

Темы практики и виды работ			Количество часов
8 семестр			**72**
Тема 1	**Техническая защита информации**		**24**
	Виды работ:		
	1	Соблюдение техники безопасности при работе за ПК Установка и настройка технических средств защиты информации.	4
	2	Определение каналов утечки ПЭМИН	4
	3	Измерение параметров физических полей	4
	4	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации	4
	5	Проведение измерений параметров побочных электромагнитных излучений и наводок	4
	6	Проведение аттестации объектов информатизации	4
Тема 2	**Инженерно-технические средства физической защиты объектов информатизации**		**46**
	Виды работ:		
	1	Соблюдение техники безопасности при работе за ПК Монтаж различных типов датчиков.	4
	2	Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация	4
	3	Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации	4
	4	Рассмотрение системы контроля и управления доступом	4
	5	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование	4
	6	Рассмотрение датчиков периметра, их принципов работы.	4
	7	Выполнение звукоизоляции помещений системы зашумления	4
	8	Реализация защиты от утечки по цепям электропитания и заземления	4
	90	Разработка организационных и технических мероприятий по заданию преподавателя	8
	10	Разработка основной документации по инженерно-технической защите информации	6
Дифференцированный зачет			**2**
Итого			**72**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1. Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования [Электронный ресурс] / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — Режим доступа: https://www.biblio-online.ru/bcode/431332

2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 c. — 978-5-4488-0091-7. — Режим доступа: http://www.iprbookshop.ru/63800.html

3. Полякова, Т.А., Стрельцов, А.А., Чубукова, С.Г., Ниесов, В.А.; Отв. ред. Полякова Т.А., Стрельцов А.А. Организационно и правовое обеспечение информационной безопасности. Учебник и практикум для СПО.- Научная школа: Всероссийский государственный университет юстиции (РПА Минюста России) (г. Москва), 2019/Гриф УМО СПО.-326 с.- Режим доступа: https://www.biblio-online.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-434576#page/5

4.2. Дополнительная литература

1. Нестеров, С.А. Информационная безопасность. Учебник и практикум для СПО.- Научная школа: Санкт-Петербургский политехнический университет Петра Великого (г. Санкт-Петербург), 2019/Гриф УМО СПО.- 322 с.- Режим доступа: https://www.biblio-online.ru/viewer/informacionnaya-bezopasnost-442312#page/6

2. Казарин, О.В., Шубинский И.Б. Основы информационной безопасности: надежность и безопасность программного обеспечения. Учебное пособие для СПО.-Научнавя школа: Российский государственный гумсанитарный университет (г. Москва). Московский государственный университет имени М.В. Ломоносовак (г. Москва), 2019/Гриф УМО СПО .- 343 с.- Режим доступа: https://www.biblio-online.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-431080#page/9

3. Петренко, В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html

4. Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 242 c. — 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

Для успешного приобретения студентами необходимых умений и навыков, формирования профессиональных компетенций необходимо выполнение ряда условий и методических рекомендаций.

Практика имеет целью комплексное освоение обучающимися всех видов профессиональной деятельности по специальности среднего профессионального образования, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и опыта практической работы по специальности

Учебная практика проводится, как правило, в мастерских, лабораториях, на учебных полигонах, в учебных хозяйствах и других подразделениях Технического колледжа. Учебная практика проводится мастерами производственного обучения и/или преподавателями профессионального цикла.

Учебная практика осуществляется как непрерывно, так и путем чередования с теоретическими занятиями по дням (неделям) при условии обеспечения связи между содержанием практики и результатами обучения в рамках модулей по осваиваемой профессии.

Задачей учебной практики является формирование у обучающихся практических профессиональных умений в рамках модулей ОПОП СПО по основным видам профессиональной деятельности для освоения рабочей профессии, обучение трудовым приемам, операциям и способам выполнения трудовых процессов, характерных для соответствующей профессии и необходимых для последующего освоения ими общих и профессиональных компетенций по избранной профессии;

Результатом каждого этапа учебной практики является оценка, которая выставляется в приложение к диплому о среднем профессиональном образовании. Студенты, не выполнившие без уважительной причины требований программы практики или получившие отрицательную оценку, отчисляются из учебного заведения как имеющие академическую задолженность. В случае уважительной причины студенты направляются на практику вторично, в свободное от учебы время.

Итоговая оценка по учебной практике ставится на основании текущих оценок, аттестационного листа, характеристики, отчета и дневника.

Работа, оцененная неудовлетворительно, выполняется повторно во внеурочное время.

В процессе прохождения учебной практики необходимо обращать внимание в первую очередь на те методы, при которых слушатели идентифицируют себя с учебным материалом, включаются в изучаемую ситуацию, побуждаются к активным действиям, переживают состояние успеха и соответственно мотивируют свое поведение. Весь учебный процесс должен быть ориентирован на достижение задач выраженных в форме компетенций, освоение, которых является результатом обучения.

По окончании практики студент сдает зачет.

Основанием для допуска студента к зачету по практике является полностью оформленный отчет по учебной практике в соответствии с программой производственной практики.

При оценке учитываются содержание и правильность оформления студентом дневника его полнота и своевременность предоставления, отчет по практике в соответствии с заданием на практику; отзывы руководителей практики.

Студент, не выполнивший программу практики без уважительной причины или получивший отрицательный отзыв о работе, может быть отчислен из колледжа за академическую задолженность.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Лаборатория «Технических средств защиты информации» (ауд. 105 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Аппаратные средства аутентификации пользователя: ПАК Аккорд-NT, № 52202314; ПАК «Соболь» 3.0, № 7CJJC4GW; «Dallas Lock 8.0-C», № 29093-4159-1156. Средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок: Учебный стенд «Полнофункциональный автоматизированный комплекс защиты информации от утечки по техническим каналам»; генератор шума «Гром – ЗИ - 4»; синтезатор помехового сигнала «Мозаика - М», № 057777; Средства измерения параметров физических полей (в том числе электромагнитных излучений и наводок, акустических (виброакустических) колебаний): селективный микровольтметр SMV-11, № 08332; селективный микровольтметр SMV-8,5, № 08199; селективный нановольтметр Unipan 233, № 55563; анализатор спектра «СК4-Белан 22», № 150; токосъемник измерительный ТИ2-3, № 0191; токосъёмник измерительный ТИ2-1, № 0371; антенна измерительная АИ5-0, № 287; антенна измерительная АИ4-1, № 01270; точный импульсный шумомер, № 01279; система измерительная автомати-	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 CodeGear RAD Studio 2007 Professional Лицензия №32954 Бессрочная Гос. Контракт №35-03/161 от 19.08.2008г

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
	зированная К6-6 (Трап), № 64; многофункциональный прибор ST 031P «Пиранья», № 1156. Стенд физической защиты объектов информатизации, оснащенный средствами контроля доступа, системами видеонаблюдения и охраны объектов	

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	8

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать порядок технического обслуживания технических средств защиты информации	Зач01
Знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;	Зач01
Знать физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;	Зач01
Знать порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;	Зач01
Знать методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;	Зач01
Знать номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;	Зач01
Знать основные принципы действия и характеристики технических средств физической защиты;	Зач01
Знать основные способы физической защиты объектов информатизации;	Зач01
Знать номенклатуру применяемых средств физической защиты объектов информатизации.	Зач01
Уметь применять технические средства для криптографической защиты информации конфиденциального характера;	Зач01
Уметь применять технические средства для уничтожения информации и носителей информации;	Зач01
Уметь применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;	Зач01
Уметь применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;	Зач01

Результаты обучения	Контрольные мероприятия
Уметь применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	Зач01
Уметь применять инженерно-технические средства физической защиты объектов информатизации.	Зач01
Иметь практический опыт установки, монтажа и настройки технических средств защиты информации;	Зач01
Иметь практический опыт технического обслуживания технических средств защиты информации;	Зач01
Иметь практический опыт применения основных типов технических средств защиты информации;	Зач01
Иметь практический опыт выявления технических каналов утечки информации;	Зач01
Иметь практический опыт участия в мониторинге эффективности технических средств защиты информации;	Зач01
Иметь практический опыт диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;	Зач01
Иметь практический опыт проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	Зач01
Иметь практический опыт проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;	Зач01
Иметь практический опыт установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.	Зач01

Вопросы к защите отчета по практике Зач01

1. Обслуживание систем видеонаблюдения. Параметры, подлежащие проверке при ППР.
2. Виды телевизионных камер и систем обработки видеосигналов. Организация проведения и обработки результатов измерений.
3. Обслуживание охранной сигнализации периметров. Планово предупредительные работы при эксплуатации ТСЗИ.
4. Система охраны периметра как обеспечение раннего определения вторжения объекта.
5. Обслуживание пожарной сигнализации. Метрологическое обеспечение эксплуатации ТСЗИ.
6. Оборудование ограниченного доступа в помещение. Назначение, виды состав и содержание ремонтных документов.
7. Система управления ограниченного доступа в помещение. Рекомендации по ведению эксплуатационной документации.
8. Нелинейные локаторы. Физические принципы, используемые в нелинейной локации.
9. Виды нелинейных локаторов, оборудование для нелинейной локации.
10. Основные задачи технической диагностики ТСЗИ.
11. Алгоритмы технического диагностирования эксплуатируемых ТСЗИ.
12. Стандарты и виды диагностических моделей эксплуатируемых ТСЗИ.
13. Вероятность возникновения отказа, приводящего к ложному срабатыванию.
14. Положения для разработки технических требований на диагностику эксплуатируемых ТСЗИ.

15. Обеспечения устойчивости программных средств ТСЗИ к НСД. Общие положения Назначение и виды эксплуатационных документов.
16. Автоматизация технического диагностирования эксплуатируемых ТСЗИ.
17. Требования к устойчивости режимов работы при сбоях автоматики эксплуатационно-техническое диагностирование эксплуатируемых ТСЗИ.
18. Эксплуатация видеокамер систем видеонаблюдения.
19. Эксплуатация и программирование устройств регистрации и обработки Видеоинформации.
20. Параметры устройств регистрации и обработки видеоинформации систем видеонаблюдения. Заградительные устройства.
21. Эксплуатация противопожарных датчиков. Цифровые системы видеонаблюдения.
22. Условия расположения противопожарных датчиков на объекте.
23. Эксплуатация приборов контроля движения и звука.
24. Эксплуатация и программирование оконечных проборов и пультов ОПС.
25. Работы по программированию и эксплуатации пультами аналоговых, координатных и сетевых проборов контроля. Особенности охраны объектов ограниченного доступа. Общие положения.
26. Эксплуатация нелинейных локаторов и анализаторов спектра.
27. Охранное видеонаблюдение в системе защиты информации, общие понятия.
28. Выбор конкретных точек установки телекамер в зависимости от их параметров.
29. Оперативные элементы охранного телевидения.
30. Организация интегрированной системы охранного телевидения.

Практические задания к защите отчета по практике Зач01

Задание 1

1. Запустить антивирусную программу.
2. Открыть справочную систему антивирусной программы.
3. Ознакомиться с интерфейсом приложения (зарисовать и записать основные компоненты с помощью справочной системы).
4. Ознакомиться с помощью справочной системы, как можно проверить на вирусы файлы, каталоги и диски.
5. Отчеты.
6. Осуществить проверку на наличие вирусов папки «Мои документы».
7. Осуществить проверку на наличие вирусов группы файлов.
8. Вывести отчет и сохранить его в текстовом файле на рабочем столе.

Заполнить таблицу.

Тип антивирусной программы Недостатки Достоинства

Задание 2

Реализация атаки

Для реализации атаки "Троянский конь" создаются два каталога, соответствующих различным уровням секретности (например, SECRET и NONSEC). Регистрируются два пользователя, имеющих такие права доступа к этим каталогам:

- Пользователь А имеет права на чтение и запись в каталог SECRET, а также права на запись в каталог NONSEC.
- Пользователь В имеет права на чтение и запись в каталог NONSEC.
- Пользователь А имеет право запускать программы из каталога NONSEC.

Пользователь В в такой ситуации может реализовать атаку типа "Троянский конь" для раскрытия секретной информации пользователя А. Пусть пользователь А создал файл Secret.txt в каталоге SECRET. Тогда в соответствии с правами пользователь В не имеет возможности читать этот файл. Раскрытие его содержимого и есть задача нарушителя. Он создает троянскую программу с безобидным названием, например, Tetris.exe, помещает ее в каталог NONSEC и ждет, пока пользователь А запустит ее. Программа в фоновом режиме копирует файл Secret.txt из каталога SECRET в каталог NONSEC, причем копия может быть зашифрована по какому-либо алгоритму. Это копирование возможно, так как оно не противоречит маске прав пользователя А. Таким образом, содержимое секретного файла Secret.txt становится известным пользователю, не имеющему прав на доступ к ней. Атака завершена и останется незамеченной, если действия троянца будут замаскированы.
Троянская программа должна без потерь копировать файлы произвольной длины.

Задание 3

Преобразователь интерфейсов С2000-ПИ, ПИ-ГР

Порядок выполнения работы

Собрать схемы, представленные в методических указаниях, на стенде без включения питания.

Включение питания осуществляется после проверки собранных схем преподавателем.

Монтаж, установку и техническое обслуживание производить только после отключения основных и резервных источников электропитания прибора!

Задание 4

Видеокамеры

Порядок выполнения работы

Собрать схемы, представленные в методических указаниях, на стенде без включения питания.

Включение питания осуществляется после проверки собранных схем преподавателем.

Монтаж, установку и техническое обслуживание производить только после отключения основных и резервных источников электропитания прибора!

Задание 5

По рисунку описать выполнение конфиденциальности информации, передаваемой по каналам связи.

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол № *3*	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

УП.04.01 Учебная практика (Выполнение работ по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин)

(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель		С.В. Колмыкова
должность	подпись	инициалы, фамилия

Директор Технического колледжа

	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
ПК 4.1	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4	Обеспечивать применение средств защиты информации в компьютерной системе

1.2. В результате прохождения практики обучающийся должен:
знать:

- требования техники безопасности при работе с вычислительной техникой;

−основные принципы устройства и работы компьютерных систем и периферийных устройств;

−классификацию и назначение компьютерных сетей;

−виды носителей информации;

−программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета;

−основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

уметь:

− - выполнять требования техники безопасности при работе с вычислительной техникой;

− производить подключение блоков персонального компьютера и периферийных устройств;

− производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники;

− диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники;

− выполнять инсталляцию системного и прикладного программного обеспечения;

− создавать и управлять содержимым документов с помощью текстовых процессоров;

− создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц;

− создавать и управлять содержимым презентаций с помощью редакторов презентаций;

− использовать мультимедиа проектор для демонстрации презентаций;

− вводить, редактировать и удалять записи в базе данных;

− эффективно пользоваться запросами базы данных;

– создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;

− производить сканирование документов и их распознавание;

− производить распечатку, копирование и тиражирование документов на принтере и других устройствах;

− управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;

− осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера;

− осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;

− осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;

осуществлять резервное копирование и восстановление данных.

иметь практический опыт:

- выполнения требований техники безопасности при работе с вычислительной техникой;

−организации рабочего места оператора электронно-вычислительных и вычислительных машин;

−подготовки оборудования компьютерной системы к работе;

−инсталяции, настройки и обслуживания программного обеспечения компьютерной системы;

−управления файлами;

−применения офисного программного обеспечения в соответствии с прикладной задачей;

−использования ресурсов локальной вычислительной сети;

−использования ресурсов, технологий и сервисов Интернет;

−применения средств защиты информации в компьютерной системе.

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: учебная
Способ проведения практики: концентрированная

Объем практики составляет 144 часа

3. СОДЕРЖАНИЕ ПРАКТИКИ

Темы практики и виды работ			Количество часов
4 семестр			**144(4 недели)**
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения			**18**
Тема 1.1	**Работа с устройствами компьютерной системы**		**8**
	Виды работ:		
	1	Соблюдение техники безопасности при работе на ЭВМ. Инструктаж по технике безопасности	2
	2	Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ	2
	3	Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка	2
	4	Установка и замена расходных материалов для принтеров, ксерокса, плоттера.	2
Тема 1.2	**Работа с программным обеспечением компьютерной системы**		**6**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК. Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети).	2
	2.	Установка прикладных программ	2
	3.	Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете	2
Тема 1.3	**Диагностика неисправностей системы, ведение документации**		**4**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники	2
	2.	Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ	2
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах			**104**
Тема 2.1	**Работа в текстовом процессоре**		**40**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК Сканирование текстовых документов и их распознавание	2
	2.	Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации,	4

		сохранение документов	
	3.	Форматирование и редактирование документов в текстовом процессоре.	12
	4.	Работа с таблицами в текстовом процессоре	8
	5.	Работа с диаграммами в текстовом процессоре	4
	6.	Работа с графическими объектами в текстовом процессоре.	8
	7.	Печать документов в текстовом процессоре.	2
Тема 2.2	**Работа в редакторе электронных таблицах**		**32**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК Создание и форматирование таблицы в редакторе электронных таблиц	4
	2.	Вычисление с помощью формул в электронной таблице	4
	3.	Работа со встроенными функциями в электронной таблице	12
	4.	Работа со списками в электронной таблице	2
	5.	Создание форм для ввода данных в таблицы	2
	6.	Создание и работа с диаграммами и графиками	6
	7.	Обмен данными между текстовым процессором и электронной таблицей	2
Тема 2.3	**Работа в программе подготовки и просмотра презентаций**		**8**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК Построение презентации различными способами	2
	2.	Обработка объектов слайдов презентации	2
	3.	Настройка анимации объектов	2
	4.	Настройка показа и демонстрация результатов работы средствами мультимедиа	2
Тема 2.4	**Работа в системе управления базами данных**		**10**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК. Ввод данных в таблицы базы данных	4
	2.	Создание простых запросов без параметров и с параметрами. Создание отчетов.	6
Тема 2.5	**Работа в графических редакторах**		**16**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК Рисование объектов средствами графического редактора.	2
	2.	Работа с заливками и контурами в программе векторной графики.	2
	3.	Работа с текстом в программе векторной графики.	2
	4.	Работа с эффектами в программе векторной графики.	2
	5.	Вставка и редактирование готового изображения с использо-	2

		ванием программ растровой графики.	
	6.	Работа с цветом с использованием программ растрой графики.	2
	7.	Работа со слоями с использованием программ растрой графики.	2
	8.	Работа со спецэффектами с использованием программ растровой графики.	2
Раздел 3. Использование ресурсов технологий и сервисов Интернета			**8**
Тема 3.1	**Работа с ресурсами Интернета**		**8**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК Создание и обмен письмами электронной почты.	2
	2.	Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера.	2
	3.	Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов.	2
	4.	Пересылка и публикация файлов данных в Интернете.	2
Раздел 4. Обеспечение защиты информации в компьютерной системе			**8**
Тема 4.1	**Защита информации при работе с офисными приложениями**		**8**
	Виды работ:		
	1.	Соблюдение техники безопасности при работе за ПК Использование штатных средств защиты операционной системы и прикладных программ.	2
	2.	Применение парольной защиты.	2
	3.	Установка антивирусных программ, их настройка. Обновление базы.	2
	4.	Выполнение архивирования данных. Выполнение резервного копирования и восстановления данных	2
Дифференцированный зачет			**4**
Итого			**144 часа 4 недели**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1 Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования [Электронный ресурс] / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — Режим доступа: https://www.biblio-online.ru/bcode/431332
2. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования [Электронный ресурс] / О. М. Замятина. — Москва : Издательство Юрайт, 2019. — 159 с. — Режим доступа: https://www.biblio-online.ru/bcode/431174
3. Гаврилов, М. В. Информатика и информационные технологии: учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 383 с. — Режим доступа: https://www.biblio-online.ru/bcode/433276
4. Стружкин, Н. П. Базы данных: проектирование: учебник для среднего профессионального образования [Электронный ресурс] / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2019. — 477 с. — Режим доступа: https://www.biblio-online.ru/bcode/445776

…

4.2. Дополнительная литература

1. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — М. : Ай Пи Ар Медиа, 2020. — 236 с. — Режим доступа: https://www.iprbookshop.ru/95150.html
2. Новожилов, О. П. Информатика: учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 620 с. — Режим доступа: https://www.biblio-online.ru/bcode/427004
3. Разработка баз данных [Электронный ресурс] : учебное пособие / А.С. Дорофеев [и др.]. — Электрон. текстовые данные. — Саратов: Ай Пи Эр Медиа, 2018. — 241 с. — 978-5-4486-0114-9. — Режим доступа: http://www.iprbookshop.ru/70276.html
4. Власов, Ю.В. Администрирование сетей на платформе MS Windows Server [Электронный ресурс] / Ю.В. Власов, Т.И. Рицкова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2018. — 622 с. — 978-5-94774-858-1. — Режим доступа: http://www.iprbookshop.ru/52219.html.— ЭБС «IPRbooks»
5. Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2018. — 242 с. — 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html
6. Горбенко, А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс] : учебное пособие / А.О. Горбенко. — Электрон. текстовые данные. — СПб. : Интермедия, 2019. — 335 с. — 978-5-4383-0136-3. — Режим доступа: http://www.iprbookshop.ru/66797.html
7. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования [Электронный ресурс]/ Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2019. — 325 с. — Режим доступа: https://www.biblio-online.ru/bcode/434576

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;
- приложения.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

Обязательные приложения к отчету:

- образец выполнения работ по теме№4
- образец выполнения работ по теме№5
- образец выполнения работ по теме№8

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Кабинет «Информатики» (ауд. 203 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition №1688-181008-182042-963-980 Право на использование ПО с 09.10.2018 до 24.10.2020

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	4

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать требования техники безопасности при работе с вычислительной техникой	Зач01
Знать основные принципы устройства и работы компьютерных систем и периферийных устройств	Зач01
Знать классификацию и назначение компьютерных сетей;	Зач01
Знать виды носителей информации	Зач01
Знать программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета	Зач01
Знать основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.)	Зач01
Уметь выполнять требования техники безопасности при работе с вычислительной техникой	Зач01
Уметь производить подключение блоков персонального компьютера и периферийных устройств	Зач01
Уметь производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники	Зач01
Уметь диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники	Зач01
Уметь выполнять инсталляцию системного и прикладного программного обеспечения	Зач01
Уметь создавать и управлять содержимым документов с помощью текстовых процессоров	Зач01
Уметь создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц	Зач01
Уметь создавать и управлять содержимым презентаций с помощью редакторов презентаций	Зач01
Уметь использовать мультимедиа проектор для демонстрации презентаций	Зач01
Уметь вводить, редактировать и удалять записи в базе данных	Зач01
Уметь эффективно пользоваться запросами базы данных	Зач01
Уметь создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики	Зач01

Результаты обучения	Контрольные мероприятия
Уметь производить сканирование документов и их распознавание	Зач01
Уметь производить распечатку, копирование и тиражирование документов на принтере и других устройствах	Зач01
Уметь управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете	Зач01
Уметь осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера	Зач01
Уметь осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов	Зач01
Уметь осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ	Зач01
Уметь осуществлять резервное копирование и восстановление данных	Зач01
Иметь практический опыт выполнения требований техники безопасности при работе с вычислительной техникой	Зач01
Иметь практический опыт организации рабочего места оператора электронно-вычислительных и вычислительных машин	Зач01
Иметь практический опыт подготовки оборудования компьютерной системы к работе	Зач01
Иметь практический опыт инсталляции, настройки и обслуживания программного обеспечения компьютерной системы	Зач01
Иметь практический опыт инсталляции, настройки и обслуживания программного обеспечения компьютерной системы	Зач01
Иметь практический опыт управления файлами	Зач01
Иметь практический опыт применения офисного программного обеспечения в соответствии с прикладной задачей	Зач01
Иметь практический опыт использования ресурсов локальной вычислительной сети	Зач01
Иметь практический опыт использования ресурсов, технологий и сервисов Интернет	Зач01
Иметь практический опыт применения средств защиты информации в компьютерной системе	Зач01

Вопросы к защите отчета по практике Зач01

1. Соблюдение техники безопасности при работе на ЭВМ

2. Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ

3. Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка

4. Установка и замена расходных материалов для принтеров, ксерокса, плоттера.

5. Установка операционной среды, настройка интерфейса ОС (рабочий стол, безопасность системы, подключение к сети).

6. Установка прикладных программ.

7. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете

8Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники

9. Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ

10. Сканирование текстовых документов и их распознавание

11. Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов

12. Форматирование и редактирование документов в текстовом процессоре.

13. Работа с таблицами в текстовом процессоре.

14. Работа с диаграммами в текстовом процессоре

15. Создание и форматирование таблицы в редакторе электронных таблиц

16. Вычисление с помощью формул в электронной таблице
17. Работа со встроенными функциями в электронной таблице
18. Работа со списками в электронной таблице
19. Создание форм для ввода данных в таблицы
20. Создание и работа с диаграммами и графиками
21. Обмен данными между текстовым процессором и электронной таблицей
22. Построение презентации различными способами
23. Обработка объектов слайдов презентации
24. Настройка анимации объектов
25. Ввод данных в таблицы базы данных
26. Создание простых запросов без параметров и с параметрами. Создание отчетов
27. Рисование объектов средствами графического редактора.
28. Работа с заливками и контурами в программе векторной графики.
29. Работа с текстом в программе векторной графики.
30. Работа с эффектами программе векторной графики.
31. Вставка и редактирование готового изображения с использованием программ растровой графики.
32. Работа с цветом с использованием программ растрой графики.
33. Работа со слоями с использованием программ растрой графики.
34. Работа со спецэффектами с использованием программ растровой графики
35. Создание и обмен письмами электронной почты.
36. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера.
37. Поиск, сортировка и анализ информации с помощью поисковых интернет сайтов.
38. Пересылка и публикация файлов данных в Интернете.
39. Использование штатных средств защиты операционной системы и прикладных программ.
40. Применение парольной защиты.
41. Установка антивирусных программ, их настройка. Обновление базы.
42. Выполнение архивирования данных.
43. Выполнение резервного копирования и восстановления данных

Практические задания к защите отчета по практике Зач01

Практическое задание № 1

Создать документ по образцу в текстовом редакторе, установив следующие параметры: поля – левое и правое – 2 см, верхнее и нижнее – 1,5 см; отступ первой строки – 1,25 см, размер шрифта – 11.

Вставка разрыва и номера страниц, колонтитулов, символов, буквицы.

Разрыв страницы, номер страницы и символ можно найти в п.м. Вставка.

Для вставки номера страницы *– Вставка, Номера страниц, в ДО можно выбрать* ***положение номера*** *– внизу страницы или вверху,* ***выравнивание номера –*** *слева, от центра, справа, внутри или снаружи. Если убрать флажок в поле* ***Номер на первой странице,*** *то нумерация начнется со второй страницы.*

Для получения дополнительных эффектов необходимо воспользоваться кнопкой Формат в нижнем левом углу окна. ***Здесь можно выбрать формат номера, включить главу, начать или продолжить нумерацию.***

Для удаления нумерации – двойной щелчок по номеру на любой странице, затем выделить номер, кнопка Delete.

Для вставки разрыва *–* ***Вставка, Разрыв, в окне выбрать Начать новую страницу, колонку или строку. Также можно начать новый раздел со следующей, текущей, четной или нечетной страницы.***

Для вставки символа – *Вставка, Символ, в окне есть две вкладки (Символ и Специальные знаки). При вставке символа важно выбрать шрифт, для каждого шрифта свои символы. Выбрать нужный и нажать кнопку Вставить, закрыть окно. Там, где в документе стоял курсор, вставится символ.*

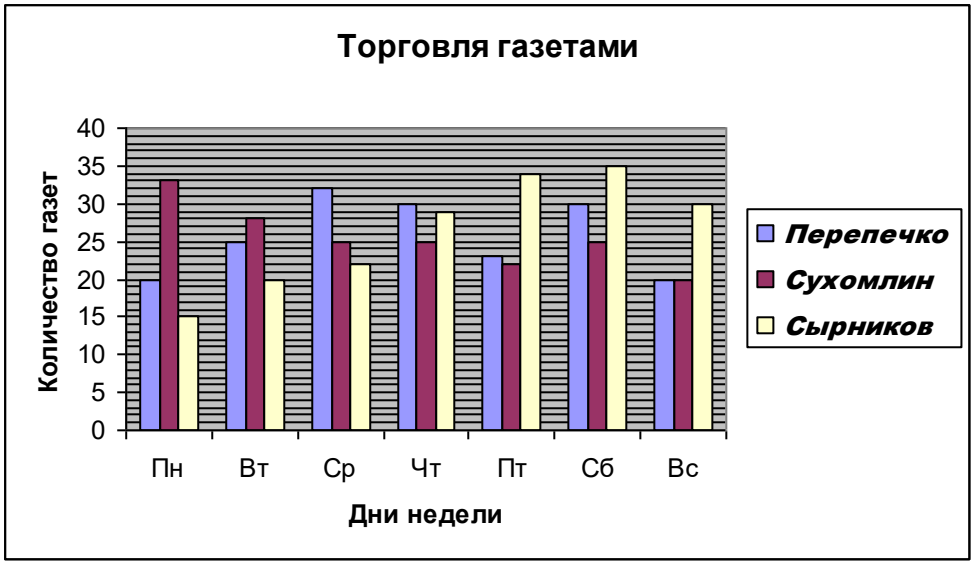
Практическое задание № 2
Задание:

1. Создать электронную таблицу по образцу.
2. Посчитать стоимость
3. Посчитать общую сумму, используя функцию

Грузоотправитель и адрес					
Грузоотправитель и адрес					
К Реестру №		Дата получения "_____" _____ 20____ г			
СЧЕТ №123 от 15.07.2010					
Поставщик Торговый Дом Пресненский					
Адрес123456, Москва, Родчельская ул., 4					
Р/счет №456789 в АВС-банке, МФО 987654					
Дополнения					
№ п/п	**Наименование**	**Ед. измерения**	**Кол-во**	**Цена**	**Сумма**
1	Пиломатериалы	м³	50	30	"
2	Евровагонка	погонный метр	100	200	"
3	Рейки	погонный метр	35	15	"
4	Наличники	погонный метр	45	25	"
ИТОГО					
Руководитель предприятия				Чижов Е.Ю.	
Главный бухгалтер				Стасова А.И.	

Практическое задание № 3
Задание:
Создать диаграмму по образцу с помощью электронных таблиц по готовой таблице.

	Пн	Вт	Ср	Чт	Пт	Сб	Вс
Перепечко	20	25	32	30	23	30	20
Сухомлин	33	28	25	25	22	25	20
Сырников	15	20	22	29	34	35	30



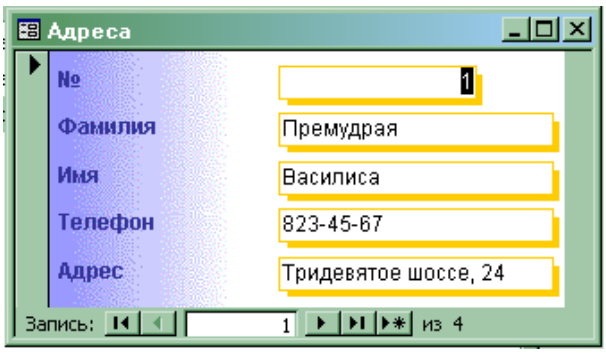
Практическое задание № 4

Создать таблицу по образцу в БД MS Access. Сохранить базу данных в своем профиле с именем Адреса.mdb.

2. Определите типы полей. Для поля Телефон – задать маску ввода.

3. Создать форму для таблицы Адреса по образцу.

Адреса				
№	Фамилия	Имя	Телефон	Адрес
1	Премудрая	Василиса	823-45-67	Тридевятое шоссе, 24
2	Никитич	Добрыня	823-87-45	Рязанская ул., 333
3	Муромец	Илья	856-87-23	Муромский пер., 100
4	Бессмертный	Кощей	823-54-88	Тридесятый проспект, 999



Практическое задание № 5

Создать таблицы БД MS Access. Сохранить базу данных в своем профиле с именем Сессия.mdb.

Создать связь между таблицами.

Таблица-анкета.	Таблица-ведомость.
Создайте таблицу, содержащую следующие поля (в скобках указан тип данных). • ФИО (текстовый)	Создайте таблицу, содержащую следующие поля (в скобках указан тип данных). • ФИО (текстовый)

• Номер группы (числовой) • Год рождения (числовой) • Адрес (текстовый) • Телефон (текстовый, создайте маску ввода). Заполните таблицу (не менее пяти записей) Сохраните таблицу под названием Анкета. Определите ключевым поле ФИО.	• Зачет № 1 (числовой) • Зачет № 2 (числовой) • Зачет № 3 (числовой) Заполните таблицу (оценку за зачеты проставить по пятибалльной системе) Сохраните таблицу под названием Ведомость. Определите ключевым поле ФИО.

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол № *3*	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

ПП.04.01 Производственная практика (Выполнение работ
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)
по профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель		С.В. Колмыкова
должность	подпись	инициалы, фамилия

Директор Технического колледжа

	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
ПК 4.1	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4	Обеспечивать применение средств защиты информации в компьютерной системе

1.2. В результате прохождения практики обучающийся должен:

– требования техники безопасности при работе с вычислительной техникой;

– основные принципы устройства и работы компьютерных систем и периферийных устройств;

– классификацию и назначение компьютерных сетей;

– виды носителей информации;

– программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета;

– основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

уметь:

– выполнять требования техники безопасности при работе с вычислительной техникой;

– производить подключение блоков персонального компьютера и периферийных устройств;

– производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники;

– диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники;

– выполнять инсталляцию системного и прикладного программного обеспечения;

– создавать и управлять содержимым документов с помощью текстовых процессоров;

– создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц;

– создавать и управлять содержимым презентаций с помощью редакторов презентаций;

– использовать мультимедиа проектор для демонстрации презентаций;

– вводить, редактировать и удалять записи в базе данных;

– эффективно пользоваться запросами базы данных;

– создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;

– производить сканирование документов и их распознавание;

– производить распечатку, копирование и тиражирование документов на принтере и других устройствах;

– управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;

– осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера;

– осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;

– осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;

– осуществлять резервное копирование и восстановление данных.

иметь практический опыт:

– выполнения требований техники безопасности при работе с вычислительной техникой;

– организации рабочего места оператора электронно-вычислительных и вычислительных машин;

– подготовки оборудования компьютерной системы к работе;

– инсталляции, настройки и обслуживания программного обеспечения компьютерной системы;

– управления файлами;

– применения офисного программного обеспечения в соответствии с прикладной задачей;

– использования ресурсов локальной вычислительной сети;

– использования ресурсов, технологий и сервисов Интернет;

применения средств защиты информации в компьютерной системе;

1.3. Практика входит в состав профессионального цикла образовательной программы и является частью профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Способ проведения практики: концентрированная.

Объем практики составляет 144 часов.

3. СОДЕРЖАНИЕ ПРАКТИКИ

2 курс

Темы практики и виды работ			Количество часов (недель)
4 семестр			**144 (4 нед.)**
Тема 1	**Организация (предприятие) – база прохождения практики**		**20**
	Виды работ:		
	1.	Вводный инструктаж по правилам внутреннего трудового распорядка предприятия	1
	2.	Общие сведения об организации (предприятии)	3
	3.	Организационная структура организации (предприятия)	4
	4.	Виды деятельности организации (предприятия)	4
	5.	Структурные подразделения, в которых проходила практика, их функции, задачи	4
	6.	Сбор информации о видах обеспечения автоматизированных систем предприятия (организации)	4
Тема 2	**Выполнение заданий согласно программе практики**		**122**
	Виды работ:		
	1.	Подготовка периферийных устройств, компьютерной оргтехники и персонального компьютера к работе	8
	2.	Работа в операционных системах	16
	3.	Распечатка, копирование и тиражирование документов на принтер и другие периферийные устройства вывода. Сканирование оригиналов	16
	4.	Создание и управление содержимым документов в офисных пакетах прикладных программ	42
	5.	Создание и редактирование графических объектов с помощью программ для обработки растровой и векторной графики	16
	6.	Осуществление навигации по Веб-ресурсам Интернета, поиска, сортировки и анализа информации с помощью поисковых интернет-сайтов	16
	7.	Осуществление антивирусной защиты персонального компьютера и мероприятий по защите персональных данных	8
	Дифференцированный зачет		**2**
	Итого:		**144 часа 4 недели**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1 Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования [Электронный ресурс] / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — Режим доступа: https://www.biblio-online.ru/bcode/431332
2. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования [Электронный ресурс] / О. М. Замятина. — Москва : Издательство Юрайт, 2019. — 159 с. — Режим доступа: https://www.biblio-online.ru/bcode/431174
3. Гаврилов, М. В. Информатика и информационные технологии: учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 383 с. — Режим доступа: https://www.biblio-online.ru/bcode/433276
4. Стружкин, Н. П. Базы данных: проектирование: учебник для среднего профессионального образования [Электронный ресурс] / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2019. — 477 с. — Режим доступа: https://www.biblio-online.ru/bcode/445776

…

4.2. Дополнительная литература

1. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — М. : Ай Пи Ар Медиа, 2020. — 236 с. — Режим доступа: https://www.iprbookshop.ru/95150.html
2. Новожилов, О. П. Информатика: учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 620 с. — Режим доступа: https://www.biblio-online.ru/bcode/427004
3. Разработка баз данных [Электронный ресурс] : учебное пособие / А.С. Дорофеев [и др.]. — Электрон. текстовые данные. — Саратов: Ай Пи Эр Медиа, 2018. — 241 с. — 978-5-4486-0114-9. — Режим доступа: http://www.iprbookshop.ru/70276.html
4. Власов, Ю.В. Администрирование сетей на платформе MS Windows Server [Электронный ресурс] / Ю.В. Власов, Т.И. Рицкова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2018. — 622 с. — 978-5-94774-858-1. — Режим доступа: http://www.iprbookshop.ru/52219.html.— ЭБС «IPRbooks»
5. Лапонина, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2018. — 242 с. — 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html
6. Горбенко, А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс] : учебное пособие / А.О. Горбенко. — Электрон. текстовые данные. — СПб. : Интермедия, 2019. — 335 с. — 978-5-4383-0136-3. — Режим доступа: http://www.iprbookshop.ru/66797.html
7. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования [Электронный ресурс]/ Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2019. — 325 с. — Режим доступа: https://www.biblio-online.ru/bcode/434576

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся, утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет.
- приложения.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Кабинет «Информатики» (ауд. 203 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition №1688-181008-182042-963-980 Право на использование ПО с 09.10.2018 до 24.10.2020

Профильные организации

№ п/п	Наименование организации	Юридический адрес организации
1	2	3
1.	ПАО «Тамбовский завод «Электроприбор»	392000,г. Тамбов, ул. Моршанское шоссе, 36 8 (4752) 57-73-03
2.	ОАО «Объединенные системы связи»	392000, г. Тамбов, бульвар Строителей, 6А 8 4752 63-33-13, 8 4752 63-33-07
3.	ООО «Инженерные системы»	г. Тамбов, ул. Ипподромная, 6 8 (4752) 49-23-29
4.	Тамбовский ЦНТИ-филиал ФГБУ «РЭА» Минэнерго России	г. Тамбов, ул. Советская, 182 8 (4752) 53-24-87; 8 (4752) 53-63-03
5.	Филиал ФГУП «Охрана» Росгвардия – Управление ведомственной охраны по Тамбовской области	г. Тамбов, Комсомольская площадь, д. 3, офис 113 8 (4752) 45-14-17
6.	ТОГОАУ ДПО «Институт повышения квалификации работников образования»	г. Тамбов, ул. Советская, 108 8 (4752) 63-05-10
7.	ООО «Дэмис Групп»	г. Тамбов, ул. Интернациональная, д.16 А +7(4752) 55-94-04
8.	ТОГКУ «Центр экспертизы образовательной деятельности»	г. Тамбов, ул. Лаврова, 9 8 (4752) 72-47-71
9.	ООО «Гибрид»	г. Тамбов, ул. Чичканова, 57 «А» 8 (4997) 03-14-32
10.	ООО «Химтехстрой».	г.Тамбов, улица Монтажников, дом 1 8 (4752) 53-31-01
11.	ООО ПК «Модуль»	г. Тамбов, Моршанское шоссе, д. 36 8 (4752) 57-73-20

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	4

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Зач01
Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Зач01
Знать типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации	Зач01
Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации	Зач01
Знать особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	Зач01
Знать типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Зач01
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями	Зач01
Уметь диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	Зач01
Уметь применять программные и программно-аппаратные средства для защиты информации в базах данных	Зач01
Уметь проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	Зач01
Уметь применять математический аппарат для выполнения криптографических преобразований	Зач01
Уметь использовать типовые программные криптографические	Зач01

Результаты обучения	Контрольные мероприятия
средства, в том числе электронную подпись	
Уметь применять средства гарантированного уничтожения информации	Зач01
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Зач01
Иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе	Зач01
Иметь практический опыт обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами	Зач01
Иметь практический опыт тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации	Зач01
Иметь практический опыт решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации	Зач01
Иметь практический опыт применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	Зач01
Иметь практический опыт учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности	Зач01
Иметь практический работы с подсистемами регистрации событий	Зач01
Иметь практический опыт выявления событий и инцидентов безопасности в автоматизированной системе	Зач01

Вопросы к защите отчета по практике Зач01

1. В какой организации (предприятии) проходила практика?
2. Какую деятельность осуществляет организация (предприятие)?
3. Расскажите об организационной структуре организации (предприятии)?
4. Каковы виды деятельности организации (предприятия)**?**
5. В каком структурном подразделении проходила практика?
6. Какие технические характеристики имелись на компьютере, за которым осуществлялась работа?
7. Расскажите о программном обеспечении, установленном на этом компьютере.
8. С каким программным обеспечением работали во время практики?
9. Какие работы производили на компьютере во время практики

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Тамбовский государственный технический университет»
(ФГБОУ ВО «ТГТУ»)

РАССМОТРЕНО И ПРИНЯТО	СОГЛАСОВАНО	СОГЛАСОВАНО
на заседании Совета Технического колледжа	Президент компании ОАО «Объединенные системы связи»	И.о. директора ТОГБУ «Региональный информационно-технический центр»
«*24*» *марта* 20*22* г.	_____С.И. Королев	_____ В.В. Сергеев
протокол №*3*	«*21*» *марта* 20*22* г.	«*21*» *марта* 20*22* г.

ПРОГРАММА ПРАКТИКИ

ПДП Производственная практика (Преддипломная)
(шифр и наименование практики в соответствии с утвержденным учебным планом подготовки)

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Квалификация: *техник по защите информации*

Составитель:

преподаватель		С.В. Колмыкова
должность	подпись	инициалы, фамилия

Директор Технического колледжа

	А.П. Денисов
подпись	инициалы, фамилия

Тамбов 2022

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ И ЕЕ МЕСТО В СТРУКТУРЕ ОПОП

1.1. Прохождение практики направлено на формирование у обучающихся следующих компетенций (Таблица 1.1).

Таблица 1.1 – Формируемые компетенции

Код компетенции	Формулировка компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
ПК 1.1	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2	Осуществлять защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного

Код компетенции	Формулировка компетенции
	доступа.
ПК 2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ПК 3.1	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации.
ПК 4.1	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения.
ПК 4.2	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах.
ПК 4.3	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета.
ПК 4.4	Обеспечивать применение средств защиты информации в компьютерной системе.

1.2. В результате прохождения практики обучающийся должен:

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;

−теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;

−порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;

−принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

−особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

−методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

−типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

−основные понятия криптографии и типовых криптографических методов и средств защиты информации;

−особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

−типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

−порядок технического обслуживания технических средств защиты информации;

−номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

−физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

−порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

−методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

−номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

−основные принципы действия и характеристики технических средств физической защиты;

−основные способы физической защиты объектов информатизации;

−номенклатуру применяемых средств физической защиты объектов информатизации.

уметь:

−осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;

−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;

−настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;

−обеспечивать работоспособность, обнаруживать и устранять неисправности;

−устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

− устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

−диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

− применять программные и программно-аппаратные средства для защиты информации в базах данных;

−проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

−применять математический аппарат для выполнения криптографических преобразований;

−использовать типовые программные криптографические средства, в том числе электронную подпись;

−применять средства гарантированного уничтожения информации;

−устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

−осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

−применять технические средства для криптографической защиты информации конфиденциального характера;

−применять технические средства для уничтожения информации и носителей информации;

−применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

−применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

−применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

−применять инженерно-технические средства физической защиты объектов информатизации.

иметь практический опыт:

−установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем;

−администрирования автоматизированных систем в защищенном исполнении;

−эксплуатации компонентов систем защиты информации автоматизированных систем;

−диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении;

−установки, настройки программных средств защиты информации в автоматизированной системе;

−обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

−тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;

−решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

−применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;

−учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

–работы с подсистемами регистрации событий;

–выявления событий и инцидентов безопасности в автоматизированной системе;

–установки, монтажа и настройки технических средств защиты информации;

–технического обслуживания технических средств защиты информации;

–применения основных типов технических средств защиты информации;

–выявления технических каналов утечки информации;

–участия в мониторинге эффективности технических средств защиты информации;

–диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

–проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

–проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

–установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

1.3. Практика входит в состав профессионального цикла образовательной программы.

2. ВИД, ОБЪЁМ ПРАКТИКИ И СПОСОБ ЕЁ ПРОВЕДЕНИЯ

Вид практики: производственная.
Способ проведения практики: концентрированная.
Объем практики составляет 144 часа.

3. СОДЕРЖАНИЕ ПРАКТИКИ

Темы практики и виды работ			Количество часов
8 семестр			**144**
Тема 1.	**Организация (предприятие) – база прохождения практики**		**20**
	Виды работ:		
	1.	**Инструктаж по технике безопасности по правилам внутреннего трудового распорядка предприятия.** Соблюдение техники безопасности при работе за ПК	1
	2.	**Общие сведения об организации (предприятии)** Знакомство с предприятием, режимом его работы. Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации). Знакомство с историей предприятия (организации).	3
	3.	**Организационная структура организации (предприятия)**	4
	4.	**Виды деятельности организации (предприятия)** Изучение видов деятельности предприятия (организации), выпускаемой продукции, партнеров.	4
	5.	**Структурные подразделения, в которых проходила практика, их функции, задачи** Изучение деятельности структурного подразделения, функций, задач, структуры, в котором проходит практика	4
	6.	**Сбор информации о видах обеспечения автоматизированных систем предприятия (организации)** Изучение технической документации ПЭВМ и периферийных устройств, имеющихся на данном предприятии. Технические характеристики ПК, предоставленного обучающемуся для выполнения заданий на время прохождения производственной практики.	4
Тема 2.	**Сбор материалов для дипломного проектирования.** Соблюдение техники безопасности при работе за ПК		**12**
Тема 3.	**Выполнение заданий согласно программе практики**		**110**
	Виды работ:		
	1.	Анализ информационной архитектуры системы. Соблюдение техники безопасности при работе за ПК	8
	2.	Определение класса защищённости автоматизированной системы	8
	3.	Разработка модели угроз	12
	4.	Модель нарушителя	12
	5.	Выбор механизмов и средств защиты информации от НСД	16
	6.	Разработка подсистемы контроля и управления доступом	16

	7.	Система противодействия утечке информации по техническим каналам	16
	8.	Защита персональных данных	4
	9.	Инструкция пользователя по соблюдению режима информационной безопасности	4
	10.	Инструкция пользователя по работе в автоматизированной информационной системе	4
	11.	Инструкция по безопасному уничтожению информации и оборудования	4
	12.	Правила осуществления удаленного и локального доступа	6
	Дифференцированный зачет		**2**
	Итого:		**144 часа**

4. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

4.1. Основная литература

1. 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, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525

2. 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, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433

3. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования [Электронный ресурс] / О. М. Замятина. — Москва : Издательство Юрайт, 2019. — 159 с. — Режим доступа: https://www.biblio-online.ru/bcode/431174

4. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89455.html

4.2. Дополнительная литература

5. Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования [Электронный ресурс] / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/442312.

6. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html

7. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. - Режим доступа: http://www.iprbookshop.ru/97571.html

8. 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 ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРАКТИКИ

Руководитель от образовательной организации проводит собрание, на котором выдает каждому обучающемуся утвержденное задание на практику, дает необходимые разъяснения по организации и проведению практики, оформлению и защите отчета.

Обучающимся необходимо ознакомиться с настоящей программой практики, шаблонами отчета по практике, дневника практики, аттестационного листа, характеристики, принять задание на практику к исполнению.

Обучающийся обязан своевременно прибыть на место прохождения практики, имея при себе направление на практику, задание на практику, шаблон дневника практики, иные документы, предусмотренные правилами внутреннего распорядка профильной организации.

Обучающийся при прохождении практики обязан:

- пройти необходимые инструктажи (в первый день практики);
- соблюдать правила внутреннего трудового распорядка;
- соблюдать требования охраны труда и пожарной безопасности;
- участвовать в деятельности организации, выполняя все виды работ, предусмотренные программой практики и заданием на практику;
- регулярно вести дневник практики;
- оформить и в установленные сроки представить руководителю практики от образовательной организации отчет по практике установленной формы;
- защитить отчет по практике.

Защита отчета по практике обычно проводится в последний день практики.

Отчет по практике, формируемый обучающимся по итогам прохождения практики, содержит:

- титульный лист;
- задание на практику;
- дневник практики;
- аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций;
- характеристику на обучающегося по освоению общих и профессиональных компетенций в период прохождения практики;
- аннотированный отчет;
- приложения.

Аннотированный отчет о прохождении практики должен включать краткое описание проделанной работы (1-2 страницы).

Обязательные приложения к отчету:

- текстовые, графические, фотоматериалы, подтверждающие практический опыт, полученный на практике.

Колледж заключает договоры на производственную практику студентов с предприятиями и организациями.

Студенты направляются на производственную практику приказом директора колледжа, в котором указывается конкретное место практики каждого обучающегося.

Студентам и их родителям предоставляется право самостоятельного подбора организации - базы практики по месту жительства, с целью трудоустройства. Заявление студента и заявка организации предоставляются на имя директора колледжа не позднее, чем за 1 месяц до начала практики.

Руководитель практики от колледжа выдает на руки каждому студенту задание на практику, а также проводит целевой инструктаж по охране труда с регистрацией в журнале инструктажа на рабочем месте.

Руководитель практики от колледжа осуществляет контроль за прохождением производственной практики студентами, сотрудничает с работодателями (руководителями практики от предприятия) и родителями. При необходимости ставит в известность администрацию колледжа о нарушениях дисциплины, графика практики и т.п.

Студенты в период прохождения производственной практики обязаны:

-выполнять задания, предусмотренные программой практики и выданные руководителем.

- соблюдать требования Устава университета, правила внутреннего трудового распорядка предприятия – базы практики, трудовую дисциплину.

- соблюдать требования охраны труда и пожарной безопасности.

По результатам производственной практики руководителями практики от предприятия и от колледжа формируется аттестационный лист, содержащий сведения об уровне освоения обучающимся профессиональных компетенций и характеристику на обучающегося по освоению им общих компетенций.

В период прохождения практики обучающимися ведется дневник практики, в котором фиксируется задание и оценка, полученная студентом по итогам выполнения задания.

По результатам практики обучающимся составляется отчет, который утверждается предприятием – базой практики.

В качестве приложения к дневнику практики обучающийся оформляет графические, аудио-, фото-, видео-, материалы, наглядные образцы изделий, подтверждающие практический опыт, полученный на практике.

Аттестация по итогам производственной практики проводится с учетом результатов ее прохождения, подтверждаемых документами предприятий – баз практики.

Производственная практика завершается дифференцированным зачетом при условии положительного аттестационного листа об уровне освоения профессиональных компетенций, наличия положительной характеристики по освоению общих компетенций, полноты и своевременности предоставления отчета по практике в соответствии с заданием и программой учебной практики.

Результаты производственной практики учитываются при прохождении государственной итоговой аттестации.

Студенты, не прошедшие производственную практику без уважительной причины, отчисляются из колледжа как имеющие академическую задолженность.

Оформление результатов производственной практики

Требования к ведению Дневника по производственной практике:

• Дневник является документом, подтверждающим выполнение заданий, предусмотренных программой практики;

• Записи в дневнике должны содержать сведения о всех рабочих днях, а так же выполненных работах.

• Дневник ежедневно проверяет руководитель практики от предприятия и выставляет оценку;

• По окончании практики дневник заверяется печатью организации – базы практики. Дневник и отчет по практике сдается для проверки руководителю практики от колледжа.

Отчет о практике должен включать текстовый, графический и другой материал.

При подготовке дневника и отчёта изученный материал должен быть изложен без дословного заимствования из учебников и других литературных источников. Особое внимание необходимо обратить на грамотность изложения. Нормативно-справочные документы предприятия, должны соответствовать году прохождения практики.

Объём отчёта по производственной практике по профилю специальности – от 10 до 15 листов, по преддипломной практике 15-20 листов формата А4 (без учёта приложений).

По окончании практики руководитель практики от организации составляет на студента характеристику. В характеристике указывается фамилия, имя, отчество студента,

место прохождения практики, дата начала и окончания прохождения практики. Также в характеристике отражается:

- полнота и качество выполнения программы практики, отношение студента к выполнению заданий, полученных в период практики, оценка результатов практики студента;

- проявленные студентом профессиональные и личные качества;

- выводы о профессиональной пригодности студента.

Характеристика с места прохождения практики подписывается руководителем практики от организации (учреждения) и заверяется печатью.

Подведение итогов практики

По окончании практики студент сдает зачет.

Основанием для допуска студента к зачету по практике является полностью оформленный отчет по производственной практике в соответствии с программой производственной практики.

К отчёту по производственной практике прилагаются:

• Дневник по производственной практике оформленный в соответствии с установленными требованиями, заверенный печатью организации - базы практики и подписью руководителя практики от предприятия.

• Аттестационный лист с указанием видов и качества выполненных работ в период производственной практики, уровня освоения профессиональных компетенций.

• Характеристика по освоению студентом общих компетенций в период прохождения практики, заверенная подписью руководителя и печатью организации;

При оценке учитываются содержание и правильность оформления студентом дневника его полнота и своевременность предоставления, отчет по практике в соответствии с заданием на практику; отзывы руководителей практики от организации и колледжа.

Студент, не выполнивший программу практики без уважительной причины или получивший отрицательный отзыв о работе, может быть отчислен из колледжа за академическую задолженность.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения практики используется материально-техническая база в следующем составе.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения / Реквизиты подтверждающего документа
Лаборатория «Информационных технологий, сетей и систем передачи информации, программирования и баз данных» (ауд. 111 /Щ)	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: компьютерная техника с подключением к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации. Стенды: Телекоммуникационные линии связи Сетевая безопасность Корпоративные компьютерные сети	Windows, MS Office /Корпоративные академические лицензии бессрочные Microsoft Open License №47425744, 48248803, 41251589, 46314939, 44964701, 43925361, 45936776, 47425744, 41875901, 41318363, 60102643 Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition №1688-181008-182042-963-980 Право на использование ПО с 09.10.2018 до 24.10.2020

Профильные организации.

№ п/п	Наименование организации	Юридический адрес организации
1	2	3
1.	ПАО «Тамбовский завод «Электроприбор»	392000,г. Тамбов, ул. Моршанское шоссе, 36 8 (4752) 57-73-03
2.	ОАО «Объединенные системы связи»	392000, г. Тамбов, бульвар Строителей, 6А 8 4752 63-33-13, 8 4752 63-33-07
3.	ООО «Инженерные системы»	г. Тамбов, ул. Ипподромная, 6 8 (4752) 49-23-29
4.	Тамбовский ЦНТИ-филиал ФГБУ «РЭА» Минэнерго России	г. Тамбов, ул. Советская, 182 8 (4752) 53-24-87; 8 (4752) 53-63-03
5.	Филиал ФГУП «Охрана» Росгвардия – Управление ведомственной охраны по Тамбовской области	г. Тамбов, Комсомольская площадь, д. 3, офис 113 8 (4752) 45-14-17
6.	ТОГОАУ ДПО «Институт повышения квалификации работников образования»	г. Тамбов, ул. Советская, 108 8 (4752) 63-05-10
7.	ООО «Дэмис Групп»	г. Тамбов, ул. Интернациональная, д.16 А +7(4752) 55-94-04

№ п/п	Наименование организации	Юридический адрес организации
1	2	3
8.	ТОГКУ «Центр экспертизы образовательной деятельности»	г. Тамбов, ул. Лаврова, 9 8 (4752) 72-47-71
9.	ООО «Гибрид»	г. Тамбов, ул. Чичканова, 57 «А» 8 (4997) 03-14-32
10.	ООО "Стройсервистамбов"	г. Тамбов, ул. Ипподромная,д7
11.	ООО "СОНАТАСТРОЙ"	Г. Тамбов, Ипподромная улица, дом 14 «И»
12.	ООО "Гром Картридж"	г. Тамбов, ул. Монтажников, д1
13.	ООО "Андора"	г. Тамбов, улица Московская, 1А

7. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОХОЖДЕНИЯ ПРАКТИКИ

Проверка достижения результатов обучения по практике осуществляется в рамках промежуточной аттестации, которая проводится в виде защиты отчета по практике.

7.1. Промежуточная аттестация

Формы промежуточной аттестации по практике приведены в таблице 7.1.

Таблица 7.1 – Формы промежуточной аттестации

Обозначение	Форма отчетности	Семестр
Зач01	Дифференцированный зачет	8

7.2. Оценочные средства

Оценочные средства соотнесены с результатами обучения по дисциплине.

Таблица 7.2 – Результаты обучения и контрольные мероприятия

Результаты обучения	Контрольные мероприятия
Знать состав и принципы работы автоматизированных систем, операционных систем и сред	Зач01
Знать принципы разработки алгоритмов программ, основных приемов программирования	Зач01
Знать модели баз данных	Зач01
Знать принципы построения, физические основы работы периферийных устройств	Зач01
Знать теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации	Зач01
Знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях	Зач01
Знать принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	Зач01
Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Зач01
Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Зач01
Знать типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации	Зач01
Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации	Зач01
Знать особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	Зач01
Знать типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Зач01
Знать порядок технического обслуживания технических средств	Зач01

Результаты обучения	Контрольные мероприятия
защиты информации	
Знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам	Зач01
Знать физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации	Зач01
Знать порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации	Зач01
Знать методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации	Зач01
Знать номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации	Зач01
Знать основные принципы действия и характеристики технических средств физической защиты	Зач01
Знать основные способы физической защиты объектов информатизации	Зач01
Знать номенклатуру применяемых средств физической защиты объектов информатизации	Зач01
Уметь осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем	Зач01
Уметь организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней	Зач01
Уметь осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем	Зач01
Уметь производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	Зач01
Уметь настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	Зач01
Уметь обеспечивать работоспособность, обнаруживать и устранять неисправности	Зач01
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями	Зач01
Уметь диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	Зач01
Уметь применять программные и программно-аппаратные	Зач01

Результаты обучения	Контрольные мероприятия
средства для защиты информации в базах данных	
Уметь проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	Зач01
Уметь применять математический аппарат для выполнения криптографических преобразований	Зач01
Уметь использовать типовые программные криптографические средства, в том числе электронную подпись	Зач01
Уметь применять средства гарантированного уничтожения информации	Зач01
Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Зач01
Уметь осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Зач01
Уметь применять технические средства для криптографической защиты информации конфиденциального характера	Зач01
Уметь применять технические средства для уничтожения информации и носителей информации	Зач01
Уметь применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами	Зач01
Уметь применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных	Зач01
Уметь применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом	Зач01
Уметь применять инженерно-технические средства физической защиты объектов информатизации	Зач01
Иметь практический опыт установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем	Зач01
Иметь практический опыт администрирования автоматизированных систем в защищенном исполнении	Зач01
Иметь практический опыт эксплуатации компонентов систем защиты информации автоматизированных систем	Зач01
Иметь практический опыт диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении	Зач01
Иметь практический опыт установки, настройки программных средств защиты информации в автоматизированной системе	Зач01
Иметь практический опыт обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами	Зач01
Иметь практический опыт тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информа-	Зач01

Результаты обучения	Контрольные мероприятия
ции	
Иметь практический опыт решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации	Зач01
Иметь практический опыт применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	Зач01
Иметь практический опыт учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности	Зач01
Иметь практический опыт работы с подсистемами регистрации событий	Зач01
Иметь практический опыт выявления событий и инцидентов безопасности в автоматизированной системе	Зач01
Иметь практический опыт установки, монтажа и настройки технических средств защиты информации	Зач01
Иметь практический опыт технического обслуживания технических средств защиты информации	Зач01
Иметь практический опыт применения основных типов технических средств защиты информации	Зач01
Иметь практический опыт выявления технических каналов утечки информации	Зач01
Иметь практический опыт участия в мониторинге эффективности технических средств защиты информации	Зач01
Иметь практический опыт диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации	Зач01
Иметь практический опыт проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации	Зач01
Иметь практический опыт проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Зач01
Иметь практический опыт установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты	Зач01

Вопросы к защите отчета по практике Зач01

1. В какой организации (предприятии) проходила практика?
2. Какую деятельность осуществляет организация (предприятие)?
3. Расскажите об организационной структуре организации (предприятии)?
4. Каковы виды деятельности организации (предприятия)**?**
5. В каком структурном подразделении проходила практика?
6. Какие технические характеристики имелись на компьютере, за которым осуществлялась работа?

7. Расскажите о программном обеспечении, установленном на этом компьютере.
8. Состав, структура и функции технического обеспечения в автоматизированных информационных системах.
9. Состав и структура комплекса технических средств.
10. Требования к техническим средствам.
11. Порядок описания комплекса технических средств.
12. Функция автоматизированной системы.
13. Подсистемы АИС.
14. Задачи автоматизированных систем.
15. Подсистема сбора информации.
16. Классификация компьютерных сетей.
17. Сетевое оборудование и программное обеспечение
18. Какие физические компоненты сетей присутствуют в организации?
19. Назовите соединительные устройства локальной сети организации.
20. Методы создания безопасных систем обработки информации
21. Стандарты информационной безопасности и их роль
22. Угрозы безопасности компьютерных систем
23. Методы взлома компьютерных систем
24. Защита компьютерной системы от взлома
25. Защита компьютерной системы от программных закладок
26. Защита от компьютерных вирусов
27. Что такое монитор безопасности?
28. Формирование и поддержка изолированной программной среды
29. Процедура идентификации и аутентификации
30. Эксплуатация видеокамер систем видеонаблюдения.
31. Эксплуатация противопожарных датчиков.
32. Эксплуатация приборов контроля движения и звука.
33. Охранное видеонаблюдение в системе защиты информации, общие понятия.
34. Оперативные элементы охранного телевидения.
35. Цифровые системы видеонаблюдения.
36. Особенности охраны объектов ограниченного доступа. Общие положения
37. .Назначение и виды эксплуатационных документов.
38. Рекомендации по ведению эксплуатационной документации.

7.3. Критерии и шкалы оценивания

При оценивании результатов обучения по практике в ходе промежуточной аттестации в форме дифференцированного зачета используются следующие критерии и шкалы.

Оценка «отлично» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и дал исчерпывающие ответы на заданные вопросы.

Оценка «хорошо» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), полностью соответствующий установленным требованиям, и уверенно отвечал на заданные вопросы, допуская несущественные ошибки.

Оценка «удовлетворительно» выставляется обучающемуся, если он представил на защиту отчет по практике (включая положительный аттестационный лист и положительную характеристику), в целом соответствующий установленным требованиям, при ответах на некоторые вопросы допускал существенные ошибки.

Во всех остальных случаях обучающемуся выставляется оценка «неудовлетворительно».