Автономная некоммерческая профессиональная
образовательная организация
«Тамбовский колледж бизнес-технологий»

Рабочая программа
учебной практики

для специальности среднего профессионального образования

10.02.05. Обеспечение информационной безопасности автоматизированных систем

на базе основного и среднего общего образования

Тамбов
2022

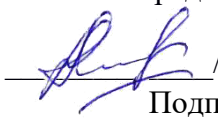
Разработана на основе:

- Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного Минобрнауки России от 9 декабря 2016 года № 1553 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г. № 44938, в редакции Приказа Минпросвещения России от 17.12.2020 № 747)

Одобрена

ПЦК информационных и математических дисциплин

Председатель ПЦК


/ Д.Ю. Самсонов к.э.н.

Подпись ФИО

Составитель (автор): Попова Т.Н., к.т.н

ФИО, ученая степень

Лист согласования
учебной практики
программы подготовки специалистов среднего звена

по специальности **10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Составитель (автор-разработчик):
Попова Т.Н., к.т.н., преподаватель АНПОО «Тамбовский колледж бизнес-технологий»
ФИО, ученая степень, звание, должность, наименование ОУ

Предприятие (организация) работодателя:

- ✓ ООО «ТИГРИС»

Заключение

Представленная для согласования рабочая программа учебной практики программы подготовки специалистов среднего звена по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

СООТВЕТСТВУЕТ:
-требованиям ФГОС СПО, утвержденным приказом Минобрнауки России от 9 декабря 2016 года № 1553 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г. № 44938, в редакции Приказа Минпросвещения России от 17.12.2020 № 747)
-запросам работодателей.
-контрольно-измерительные материалы актуальны, обоснованы, соответствуют базовому уровню среднего профессионального образования.

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Нормативные документы и область применения программы учебной практики

Программы практик сформированы в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденным приказом Минобрнауки России от 9 декабря 2016 года № 1553 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г. № 44938, в редакции Приказа Минпросвещения России от 17.12.2020 № 747)а также Приказом Минобрнауки РФ N 885, Минпросвещения РФ N 390 от 05.08.2020 «О практической подготовке обучающихся» (в ред. Приказа Минобрнауки РФ N 1430, Минпросвещения РФ N 652 от 18.11.2020). Согласно Приказу Министерства просвещения Российской Федерации от 17.12.2020 N 747 и изменениям, внесенным в ФГОС СПО, пункт 1.8 дополнен словами - Образовательная деятельность при освоении образовательных программ или отдельных ее компонентов организуется в форме практической подготовки.

Рабочая программа учебной практики является частью программы подготовки специалистов среднего звена (далее ППССЗ) по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основных видов профессиональной деятельности:

- обработка отраслевой информации;
- разработка, внедрение и адаптация программного обеспечения отраслевой направленности;
- сопровождение и продвижение программного обеспечения отраслевой направленности;
- обеспечение проектной деятельности;

и предназначена для реализации основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Выполнение программы учебной практики обучающимися с ограниченными возможностями здоровья осуществляется в соответствии с Приказом Министерства образования и науки РФ от 9 ноября 2015 г. № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», Положением о порядке обучения обучающихся – инвалидов и лиц с ограниченными возможностями здоровья, утвержденным приказом директора от 12.07.2017 г.. Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится преподавателями с учетом индивидуальных психофизиологических особенностей обучающихся и специфики приема-передачи учебной информации. С обучающимися по индивидуальному плану и индивидуальному графику проводятся индивидуальные занятия и консультации.

1.2. Вид, способы, форма проведения и аттестация итогов учебной практики требования к руководителям практик

Вид практики: учебная.

Способы проведения учебной практики): стационарная.

Стационарная учебная практика проводится образовательным учреждением при освоении студентами профессиональных компетенций в рамках профессиональных модулей.

Форма проведения учебной практики – самостоятельное выполнение обучающимися заданий и практических проверочных работ под руководством

руководителя практики от АНПОО «Тамбовский колледж бизнес-технологий» (стационарная практика), а также самостоятельная работа студентов.

Аттестация по итогам учебной практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ в форме *дифференцированного зачет*а.

Все руководители учебной практики назначаются соответствующими приказами организации.

Требования к руководителям практики от образовательного учреждения

Реализация программы учебной практики от образовательного учреждения обеспечивается педагогическими кадрами АНПОО «Тамбовский колледж бизнес-технологий», имеющими высшее образование, соответствующее профилю подготовки. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального учебного цикла. Преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

1.3. Указание места программы учебной практики в структуре основной профессиональной образовательной программы

Практика является обязательным разделом ОП. Она представляет собой вид учебных занятий, обеспечивающих практико-ориентированную подготовку обучающихся. При реализации образовательной программы специалистов среднего профессионального образования предусматривается два вида практики: учебная и производственная.

Учебная практика проводится при освоении обучающимися профессиональных компетенций в рамках профессиональных модулей и реализуются концентрированно.

Учебная практика в объеме 13 недель (468 часов) реализуется по каждому из видов профессиональной деятельности, предусмотренных ФГОС СПО:

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении (108 часов);

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами (108 часов);

ПМ.03 Защита информации техническими средствами (108 часов);

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (144 часов)

2. ЦЕЛЬ И ЗАДАЧИ УЧЕБНОЙ ПРАКТИКИ ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ

2.1. Цели учебной практики

Рабочая программа учебной практики разработана в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273 - ФЗ «Об образовании в Российской Федерации», Приказом Министерства образования и науки Российской Федерации от 14 июня 2013 г. № 464 «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования» с изменениями и дополнениями, Приказом Министерства науки и высшего образования Российской Федерации и Приказом Министерства просвещения Российской Федерации № 885/390 от 05.08.2020 г. «О

практической подготовке обучающихся», Федеральными государственными образовательными стандартами среднего профессионального образования (далее – ФГОС СПО), Уставом АНО ВО «Российский новый университет», Положением о практической подготовке обучающихся по образовательным программам высшего и среднего профессионального образования в АНО ВО «Российский новый университет», 2020 года и предназначена для реализации основной образовательной программы по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Учебная практика направлена на обобщение и систематизацию знаний и навыков работы по дисциплинам учебных циклов, а также профессиональных модулей.

Учебная практика предусмотрена графиком учебного процесса в течение одиннадцати недель в рамках профессиональных модулей специальности. Целями учебной практики являются:

- углубление и закрепление теоретических знаний, полученных при изучении учебных циклов и профессиональных модулей;
- комплексное освоение всех видов профессиональной деятельности;
- приобретение первоначальных практических навыков и профессиональных умений по избранной специальности;
- формирование общих и профессиональных компетенций;
- приобретение практических навыков в будущей профессиональной деятельности или в отдельных ее разделах.

Задачи учебной практики:

- подготовка специалистов к осознанному и углубленному изучению дисциплин учебных циклов и профессиональных модулей, привитие им первичных умений и навыков по избранной специальности;
- овладение профессиональной деятельностью по специальности, развитие профессионального мышления;
- закрепление, расширение, углубление и систематизация знаний, полученных при изучении дисциплин, определяющих профиль специальности;
- формирование представлений о культуре труда, культуре и этике межличностных отношений, потребности бережного отношения к рабочему времени, качественного выполнения заданий, соблюдению правил и норм охраны труда, технике безопасности и противопожарной защите.

В ходе учебной практики обучающийся должен овладеть следующими видами деятельности:

1. **Вид профессиональной деятельности**: Эксплуатация автоматизированных (информационных) систем в защищённом исполнении.

приобрести умения:

иметь практический опыт:

- эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности, контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации;
- администрирования автоматизированных систем в защищенном исполнении, контроля стабильности характеристик системы защиты информации;
- установке компонентов систем защиты информации автоматизированных информационных систем.

уметь:

- обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку

автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;

- обеспечивать проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения;
- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;
- организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;
- устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами;
- настраивать и устранять неисправности программно-аппаратных средств
- защиты информации в компьютерных сетях по заданным правилам

2. **Вид профессиональной деятельности:** Защита информации в автоматизированных системах программными и программно-аппаратными средствами

приобрести умения:

иметь практический опыт:

- защиты информации типовых конфигураций программно-аппаратных средств
- в обеспечении разграничения доступа; правил безопасного хранения эталонной копии аутентификационной информации;
- безопасной передачи по каналам связи аутентификационной информации;
- в аутентификации с использованием паролей, внешних носителей информации, биометрической аутентификации;
- основных требований к политике аудита;
- основных методах защиты программ и данных от несанкционированного копирования;
- основных методах взлома систем защиты программ и данных от несанкционированного копирования;
- методах противодействия компьютерным вирусам и программным закладкам;

уметь:

- применять типовые программно-аппаратные средства защиты информации; - проводить типовые операции настройки политики безопасности UNIX и Windows;
- обнаруживать и обезвреживать компьютерные вирусы и программные закладки с использованием типовых антивирусных средств.

3. Вид профессиональной деятельности: Защита информации техническими средствами.

получить практический опыт:

иметь практический опыт:

- правила безопасной передачи по каналам связи аутентификационной информации;
- основные методы защиты программ и данных от несанкционированного копирования;
- работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами;

- основные подходы к обеспечению разграничения доступа; правила безопасного хранения эталонной копии аутентификационной информации;

уметь:

- планировать и реализовывать собственное профессиональное и личностное развитие.
- осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации
- осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
- организовывать отдельные работы по физической защите объектов информатизации. **4. Вид профессиональной деятельности:** Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

получить практический опыт:

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 компьютерной системе.

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**.**

2.2. Планируемые результаты учебной практики

Результатом учебной практики является **освоение общих (ОК) компетенций**:

Код	**Наименование результатов практики**
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
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. (компетенция введена приказом Минпросвещения России от 17.12.2020 № 747)

Освоение профессиональных (ПК) компетенций:

Вид профессиональной деятельности	**Код**	**Наименование результатов практики**
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	ПК 1.1 – 1.4	• Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

		• Администрировать программные и программноаппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении • Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации • Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК 2.1 – ПК.2.6.	• Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации • Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. • Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации • Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПМ.03 Защита информации техническими средствами	ПК 3.1 – ПК 3.5	• Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации • Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации • Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа • Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации • Организовывать отдельные работы по физической защите объектов информатизации
ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	ПК 4.1. – ПК 4.4.	• Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения • Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах • Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета • Обеспечивать применение средств защиты информации в компьютерной системе

3 ОБЪЕМ И ВРЕМЯ УЧЕБНОЙ ПРАКТИКИ

В соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем в учебном плане по направлению подготовки по данной специальности в соответствии с основными видами деятельности для проведения учебной практики определено 13 недель.

Время проведения: после окончания теоретического обучения в рамках освоения профессиональных модулей.

4 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Коды формируемых компетенций	**Наименование профессионального модуля**	**Объем времени, отводимый на практику (часов, недель)**	**Сроки проведения**
ОК 1-11, ПК 1.1 - ПК 1.4	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	108 часов, 3 недели	3 курс, 6 сем.
ОК 1-11, ПК 2.1 - ПК.2.6	ПМ.02 Защита информации в автоматизированных системах программными и программноаппаратными средствами	108 часов, 3 недели	4 курс, 7 сем
ОК 1-11, ПК 3.1 – ПК 3.5	ПМ.03 Защита информации техническими средствами	108 часа, 3 недели	4 курс, 7 сем
ОК 1-11, ПК 4.1 – ПК 4.4	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	144 часов, 4 недели	2 курс, 4 сем
	Всего	468 часов, 13 недель	

3.2. Содержание учебной практики

Виды деятельности	Виды работ	Содержание освоенного учебного материала, необходимого для выполнения видов работ	Наименование учебных дисциплин, междисциплинарных курсов с указанием конкретных разделов (тем), обеспечивающих выполнение видов работ	Количество часов (недель)
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	1. Проведение аудита защищенности автоматизированной системы. 2. Установка, настройка и эксплуатация сетевых операционных систем. 3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 4. Организация работ с удаленными хранилищами данных и базами данных. 5. Организация защищенной передачи данных в компьютерных сетях. 6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Аутентификация, авторизация, аудит. Управление учетными записями пользователей и доступом к ресурсам. Аудит событий системы. Изучение штатных средств защиты информации в операционных системах. Угрозы целостности СУБД. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию. Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность,	**МДК.01.01 Операционные системы** Раздел 2. Безопасность операционных систем **МДК.01.02 Базы данных** Раздел 9. Администрирование и безопасность **МДК.01.03 Сети и системы передачи информации** Раздел 3. Разработка защищенных автоматизированных (информационных) систем **МДК.01.05. Эксплуатация компьютерных сетей** Раздел 6. Технологии коммутации и маршрутизации современных сетей	108 часов (3 недели)

	неисправностей. 8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	безопасность. Основные особенности современных проектов АИС. Электронный документооборот. Организационные, правовые, программно-аппаратныеОрганизационные, правовые, программноаппаратные, криптографические, технические меры защиты информации в автоматизированных системах. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним. Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем. автоматизированных системах. Нормативноправовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним. Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании) Разработка технического задания на проектирование автоматизированной системы Категорирование информационных ресурсов. Создание сетевого кабеля на основе неэкранированной витой пары (UTP) Сварка оптического волокна Разработка топологи сети небольшого предприятия Построение одноранговой сети Изучение адресации канального уровня. MAC-адреса.	Ethernet	

		Создание коммутируемой сети. Настройка беспроводного сетевого оборудования. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов. Команды управления таблицами коммутации MAC- и IP- адресов, ARP-таблицы Настройка VLAN на основе стандарта IEEE 802.1Q Настройка протокола GVRP. Настройка сегментации трафика без использования VLAN Настройка функции Q-inQ (Double VLAN). Настройка протоколов связующего дерева STP, RSTP, MSTP. Настройка функции защиты от образования петель LoopBackDetection Агрегирование каналов. Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP. Работа с протоколом RIP. Работа с протоколом OSPF.		
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах. 2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности. 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности. 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации. 5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной	Установка операционной системы Windows XP на виртуальной машине. Использование редактора реестра. Управление дисками из командной строки Обеспечение безопасности папок и документов Реализация подсистем аутентификации в распространенных операционных системах. Аудит в Windows. Просмотр и работа с журналом аудита Противодействие взлому. Работа со зловредными программами. Архитектуры информационных сетей. Структурные элементы сети ЭВМ. Эффективность обработки данных в вычислительной сети. Параметры информационной сети: топология, операционные возможности сети, производительность сети, время доставки сообщений, цена обработки данных. Кабельная система информационной сети: витая пара, коаксиальные кабели, оптоволоконные линии. Управление процессом доступа к передающей среде: методы селективного и	**МДК.02.01. Программные и программно-аппаратные средства защиты информации** Раздел 1. Основные принципы программной и программно-аппаратной защиты информации Раздел 2. Защита автономных автоматизированных систем Раздел 3. Защита информации в локальных сетях Раздел 4. Защита информации в сетях	108 часов (3 недели)

	информации. 6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 7. Устранение замечаний по результатам проверки. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. 8. Применение математических методов для оценки качества и выбора наилучшего программного средства. 9. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.	случайного доступа, маркерные методы. Internet Назначение и функции сети. Состав протоколов. Аппаратные средства. Адресация и маршрутизация. Информационный и вычислительный сервис сети. Структура и функции локальных вычислительных сетей. Системы связи. Функционирование ЛВС. Компоненты ЛВС. Типы топологии вычислительных сетей. Методы доступа в ЛВС. Реализация ЛВС. Перспективы развития ЭВМ и ТВС.	общего доступа Раздел 5. Мониторинг систем защиты **МДК.02.02. Криптографические средства защиты информации** Раздел 3. Современная криптография.	
ПМ.03 Защита информации техническими средствами	Измерение параметров физических полей. 2.Определение каналов утечки ПЭМИН. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. 4.Установка и настройка технических средств защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров электромагнитных излучений и	Сертификация средств защиты информатизации; лицензирование; основные НМД по защите информации; типовая схема утечки информации за пределы. способы обнаружения скрытых видеокамер: обнаружение видеокамер с помощью НЛ; обнаружение беспроводных видеокамер с помощью средств радиомониторинга; обнаружение видеокамер за счет анализа ПЭМИ; Средства: индикаторы поля, устройства, работающих по оптическому принципу Классификация акустических каналов утечки информации: воздушные, вибрационные, электроакустические, оптико-электронный, параметрические классификация акустоэлектрических преобразователей по физическим процессам, создающим опасные сигналы.	**МДК.03.01 Техническая защита информации** Раздел 2. Теоретические основы инженерно-технической защиты информации Раздел 3. Физические основы технической защиты информации Раздел 4. Системы защиты от утечки информации Раздел 5. Применение и эксплуатация	108 часов (3 недели)

	наводок. Проведение аттестации объектов информатизации. Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной электромагнитных излучений и наводок. 6.Проведение аттестации объектов информатизации. 7.Монтаж различных типов датчиков. 8.Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. .Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; 9.Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 10.Рассмотрение системы контроля и управления доступом. 11.Рассмотрение принципов работы системы видеонаблюдения и ее	по способам формирования электрического сигнала активные акустоэлектрические преобразователи могут быть: • электродинамическими, • электромагнитными.электромагнитными. Классификация закладочных устройств: - по каналу передачи информации; - по способу восприятия информации; - по наличию устройства управления; - по внешнему виду; - по используемому источнику питания. Процедура спецобследования по этапам: - подготовительный этап: - инструментальный контроль: - анализ выявленных демаскирующих признаков; - подготовка отчетной документации. Рассмотрение инженерных конструкций, применяемых для предотвращения проникновения злоумышленника к источникам информации. Монтаж датчиков пожарной и охранной сигнализации Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя Рассмотрение принципов устройства, работы и применения средств контроля доступа Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	технических средств защиты информации **МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации** Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты Раздел 3. Применение и эксплуатация инженерно-техническх средств физической защиты	

	проектирование. 12.Рассмотрение датчиков периметра, их принципов работы. 13.Выполнение звукоизоляции помещений системы зашумления. 14.Реализация защиты от утечки по цепям электропитания и заземления. 15.Разработка организационных и технических мероприятий по заданию преподавателя; 16.Разработка основной документации по инженерно-технической защите информации			
ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	1. Создание и обмен письмами электронной почты. Навигация по Вебресурсам Интернета с помощью программы Веб-браузера. 2. Поиск, сортировка и анализ информации с помощью поисковых интернетсайтов. Пересылка и публикация файлов данных в Интернете. 3. Разработка и утверждение плана технического задания на создание или модификацию ИС в защищенном исполнении. 4. Детализация разделов плана технического задания на создание или модификацию ИС в защищенном исполнении. Утверждение технического задания на создание ИС в защищенном исполнении 5. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.	Работа с устройствами компьютерной системы. Работа с программным обеспечением компьютерной системы. Диагностика неисправностей системы, ведение документации. Работа в текстовом процессоре. Работа в редакторе электронных таблиц. Работа в программе подготовки и просмотра презентаций. Работа в системе управления базами данных Работа в графических редакторах. Работа с ресурсами Интернета. Защита информации при работе с офисными приложениями.	**МДК.04.01 Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»** Раздел 3. Использование ресурсов технологий и сервисов Интернета	144 часа (4 недели)

5. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

5.1. Требования к документации, необходимой для проведения практики

Для проведения учебной практики в образовательной организации предусматривается следующая документация:

- годовой план проведения учебной практики;
- график учебной практики;
- рабочие программы учебной практики;

5.2. Требования к минимальному материально-техническому обеспечению, необходимому для проведения учебной практики

Для проведения учебной практики разработаны и имеются в наличии учебно-методические комплексы по всем профессиональным модулям и дисциплинам.

5.2.1. Перечень кабинетов, лабораторий и других помещений

Реализация программы учебной практики требует наличия учебных кабинетов для самостоятельной работы учащихся.

Кабинеты:

– архитектуры электронно-вычислительных машин и вычислительных систем;

– безопасности жизнедеятельности и охраны труда;

– документационного обеспечения управления;

– иностранного языка;

– математики;

– операционных систем и сред;

– социально-экономических дисциплин;

– теории информации.

Лаборатории:

– обработки информации отраслевой направленности;

– разработки, внедрения и адаптации программного обеспечения отраслевой направленности.

Залы:

– актовый зал;

– библиотека, читальный зал с выходом в сеть Интернет.

5.2.2. Методическое и техническое оборудования учебных кабинетов и лабораторий

Методическое оборудование учебных кабинетов и лабораторий:

– рабочее место преподавателя;

– посадочные места обучающихся (по количеству обучающихся);

– раздаточный материал (тесты) из ФОС по дисциплинам;

– специализированная мебель, включая классную доску.

Технические средства обучения лабораторий:

Оборудование лабораторий (аудитория 203):

- автоматизированное рабочее место преподавателя с одним ПК;

- 18 посадочных мест обучающихся, оборудованных ПК с операционной системой Windows XP\7\10;

- переносной мультимедийный проектор Epson;

- переносной экран на штативе classic solution;

- локальная сеть с выходом в Интернет;
- кондиционер помещения.

Основной перечень компьютерных программ и сред, автоматизированных систем (АИС), справочных правовых систем (СПС)

Тип программы	ПО
Программное обеспечение сетевого оборудования	• Эмулятор GNS3 • Eve-NG
ПО межсетевого экранирования и мониторинга технического состояния активного сетевого оборудования	• Межсетевой экран SecretNet Studio • Система мониторинга Cacti®
Антивирусные комплексы	• Dr.Web Desktop Security Suite
Программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности	• Межсетевой экран SecretNet Studio
Программные средства обнаружения вторжений	• Secret Net Studio
Средства уничтожения остаточной информации в запоминающих устройствах	• KillDisk
Программные средства выявления уязвимостей в автоматизированных системах и средствах вычислительной техники	• Kali Linux
Программные средства криптографической защиты информации	• VipNet • Crypto Pro
Программные средства защиты среды виртуализации	• VMware • vGate
Дополнительные	
Базы данных	• MySQL • PostgreSQL • SoQoL • Redis • MongoDB
Системы программирования	• Visual Studio Code • NetBeans • Eclipse • Lazarus • Python • C#
3d моделирование	• Blender • FreeCAD • Autodesk 3Ds Max
Обработка текста, процессор таблиц, создание презентаций	• MS Word, • MS Excel, • MS Power Point, • LibreOffice Writer, • LibreOffice Calc, • LibreOffice Impress
СПС	• "Консультант Плюс"
Вспомогательное ПО	• Microsoft Windows XP, 7, 8, 8.1, 10; • Ubuntu Mint; AntiX

	• веб-браузер (Google Chrome, Mozilla Firefox, Internet Explorer др.); • цифровой образовательный ресурс IPRSmart; • образовательную платформу ЮРАЙТ; • Adobe Reader, 7z920; • 1С: Предприятие 8.3

5.3. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, интернет-ресурсов, дополнительной литературы

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, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467356

2. Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453469

3. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2020. — 159 с. — (Профессиональное образование). — ISBN 978-5-534-10682-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456799

Дополнительная литература:

4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548

6. Стружкин, Н. П. Базы данных: проектирование. Практикум : учебное пособие для среднего профессионального образования / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2020. — 291 с. — (Профессиональное образование). — ISBN 978-5-534-08140-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/455865

в) стандарты

1. ГОСТ 34.603-92. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Виды испытаний автоматизированных систем
2. ГОСТ 6.01.1-87. Единая система классификации и кодирования технико-экономической информации
3. Стандарт ISO/IEC 12207:1995 «Information Technology — Software Life Cycle Processes» (информационные технологии – жизненный цикл программного обеспечения), ГОСТ Р ИСО/МЭК 12207-99.
4. ГОСТ Р ИСО/МЭК 15288-2005. Системная инженерия. Процессы жизненного цикла систем
5. ГОСТ Р ИСО/МЭК ТО 16326-2002. Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом
6. ISO 10014. Управление качеством — Указания по получению финансовых и экономических выгод.

г) Интернет-ресурсы:

1. Автоматизированные системы и технологии онлайн [Электронный ресурс]: офиц. сайт. – Электрон. дан. – Режим доступа: http://lessons.study.ru
2. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс]: офиц. сайт. – Электрон. дан. – Режим доступа: http://school-collection.edu.ru
3. Единое окно доступа к образовательным ресурсам Российской Федерации [Электронный ресурс]: офиц. сайт. – Электрон. дан. – Режим доступа: http:// www.window.edu.ru.
4. Мегаэнциклопедия Кирилла и Мефодия, разделы «Наука / Математика. Кибернетика» и «Техника / Компьютеры и Интернет» [Электронный ресурс]: офиц. сайт. – Электрон. дан. – Режим доступа: http://www.megabook.ru.
5. Научная электронная библиотека eLIBRARY.ru [Электронный ресурс]: раздел Информатика. — Электрон. дан. — Режим доступа: http://www.elibrary.ru/defaultx.asp
6. Научная электронная онлайн-библиотека Порталус [Электронный ресурс]: раздел Информатика. — Электрон. дан. — Режим доступа:http://www.portalus.ru
7. Открытые интернет-курсы «Интуит» по курсу «Автоматизированные системы и технологии» [Электронный ресурс]: офиц. сайт. – Электрон. дан. – Режим доступа: http://www.intuit.ru/studies/courses.
8. Открытая электронная библиотека «ИИТО ЮНЕСКО» по ИКТ в образовании [Электронный ресурс]: офиц. сайт. – Электрон. дан. – Режим доступа: http://http://ru.iite.unesco.org/publications.
9. Портал «Информационно-коммуникационные технологии в образовании» [Электронный ресурс]: офиц. сайт. – Электрон. дан. – Режим доступа: http://www.ict.edu.ru.
10. Электронная библиотека книг [Электронный ресурс]: раздел Информатика. — Электрон. дан. — Режим доступа: http://www.kodges.ru
11. Электронный информационный ресурс для преподавателей компании КонсультантПлюс [Электронный ресурс]: раздел Информатика. — Электрон. дан. — Режим доступа: http://www.edu.consultant.ru
12. Электронные учебники издательства "Юрайт" [Электронный ресурс]: офиц.сайт — Электрон. версия печ. публикации. — Режим доступа: http://www.my-shop.ru

5.4. Требования к соблюдению техники безопасности и пожарной безопасности

В образовательном учреждении имеется инструкция по технике безопасности и охране труда для обучающихся, проходящих учебную практику (приложение 1).

Обучающиеся, вышедшие на практику допускаются к выполнению работы только при наличии установленного набора документов (договор, дневник, индивидуальное

задание и т. п.), после прохождения вводного инструктажа по охране труда, инструктажа по охране труда на рабочем месте, а также повторения приемов оказания первой доврачебной помощи пострадавшим от несчастных случаев (при получения травмы в период практики).

Каждый инструктаж обучающихся, выходящих на производственную практику (преддипломную), заканчивается обязательной проверкой его усвоения. Первичный инструктаж проводится руководителями практики от организации, последующие — руководителями практики по месту ее прохождения.

Проведение всех видов инструктажей регистрируется в журналах регистрации инструктажей с обязательными подписями получившего и проводившего инструктаж. Каждому обучающемуся, выходящему на учебную практику, необходимо:

– знать место хранения медицинской аптечки;

– уметь оказать первую помощь при производственных травмах;

– уметь правильно действовать при возникновении пожара и в других экстремальных и других чрезвычайных ситуациях;

– изучить планы эвакуации и расположение эвакуационных выходов.

Всем обучающимся, проходящим производственную практику (преддипломную), следует:

– знать и соблюдать правила личной гигиены;

– оставлять верхнюю одежду, обувь, головной убор в гардеробной или иных местах, предназначенных для хранения верхней одежды;

– иметь опрятный вид в соответствии с требованиями делового этикета;

– не принимать пищу на рабочем месте.

Учитывая разъездной характер работы, сотрудники должны приходить на работу в удобной обуви и одежде, соответствующей сезону.

6 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ

По итогам учебной практики проводится защита в форме *дифференцированного зачета* на основе отчета о прохождении данной практики

При определении окончательной оценки по учебной практике учитываются:

– доклад обучающегося, культура речи, логика мышления и ясность изложения;

– умение слушать вопросы экзаменатора и отвечать на них;

– умение грамотно обосновывать свою точку зрения, использовать ссылки на научно-техническую литературу;

– оценка в характеристике, поставленная руководителем практики от предприятия;

Результаты обучения по итогам практики представлены в нижеследующей таблице.

Результаты обучения (приобретенный практический опыт, освоенные умения, усвоенные знания) по видам профессиональной деятельности	**Коды формируемых компетенций**	**Формы и методы контроля и оценки результатов обучения**
1	2	3
1.Вид профессиональной деятельности: *Эксплуатация автоматизированных (информационных) систем в защищенном исполнении*		
Иметь практический опыт:	ПК1.1-	Дифференци

– 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	ПК1.5	рованный зачет по практике
Уметь: – Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении	ПК1.1-ПК1.5	
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.	ОК1 – ОК11; ПК1.1-ПК1.5	
2.Вид профессиональной деятельности: *Защита информации в автоматизированных системах программными и программно-аппаратными средствами*		
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.	ПК2.1-ПК2.6	Дифференцированный зачет по практике
Уметь:	ПК2.1-	

– 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	ПК2.6	
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.	ОК1 – ОК11; ПК2.1-ПК2.6	
3.Вид профессиональной деятельности: *Защита информации техническими средствами*		
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,	ПК3.1-ПК3.4	Дифференцированный зачет по практике

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..		
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	ПК3.1-ПК3.4	
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;	ОК1 – ОК11 ПК3.1-ПК3.4	

– номенклатуру применяемых средств физической защиты объектов информатизации..		
4. Вид профессиональной деятельности: *Выполнять работы по профессии «Оператор электронно-вычислительных и вычислительных машин*»		
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..	ПК4.1-ПК4.5	Дифференцированный зачет по практике
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	ПК4.1-ПК4.5	

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		
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.	ОК1 - ОК11; ПК4.1-ПК4.5	

ПРИЛОЖЕНИЕ 1

Инструкция по охране труда и технике безопасности для пользователей персональных электронно-вычислительных машин (ПЭВМ)

Введение

Настоящая инструкция предназначена для предотвращения неблагоприятного воздействия на человека вредных факторов, сопровождающих работы со средствами вычислительной техники и периферийным оборудованием.

Настоящая инструкция подлежит обязательному и безусловному выполнению. За нарушение инструкции виновные несут ответственность в административном и судебном порядке в зависимости от характера последствий нарушения.

Соблюдение правил безопасной работы является необходимым условием предупреждения производственного травматизма.

Общие положения

Область распространения и порядок применения инструкции:

Настоящая инструкция распространяется на персонал, эксплуатирующий средства вычислительной техники и периферийное оборудование. Инструкция содержит общие указания по безопасному применению электрооборудования в учреждении. Требования настоящей инструкции являются обязательными, отступления от нее не допускаются.

Требования к персоналу, эксплуатирующему средства вычислительной техники и периферийное оборудование:

К самостоятельной эксплуатации электроаппаратуры допускается только специально обученный персонал не моложе 18 лет, пригодный по состоянию здоровья и квалификации к выполнению указанных работ.

Перед допуском к работе персонал должен пройти вводный и первичный инструктаж по технике безопасности с показом безопасных и рациональных приемов работы. Затем не реже одного раза в 6 месяцев проводится повторный инструктаж, возможно, с группой сотрудников одинаковой профессии в составе не более 20 человек. Внеплановый инструктаж проводится при изменении правил по охране труда, при обнаружении нарушений персоналом инструкции по технике безопасности, изменении характера работы персонала.

В помещениях, в которых постоянно эксплуатируется электрооборудование должны быть вывешены в доступном для персонала месте Инструкции по технике безопасности, в которых также должны быть определены действия персонала в случае возникновения аварий, пожаров, электротравм.

Руководители структурных подразделений несут ответственность за организацию правильной и безопасной эксплуатации средств вычислительной техники и периферийного оборудования, эффективность их использования; осуществляют контроль за выполнением персоналом требований настоящей инструкции по технике безопасности.

Виды опасных и вредных факторов

Эксплуатирующий средства вычислительной техники и периферийное оборудование персонал может подвергаться опасным и вредным воздействия, которые по природе действия подразделяются на следующие группы:

- поражение электрическим током,
- механические повреждения,

- электромагнитное излучение,
- инфракрасное излучение,
- опасность пожара,
- повышенный уровень шума и вибрации.

Для снижения или предотвращения влияния опасных и вредных факторов необходимо соблюдать Санитарные правила и нормы, гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы (Утверждено Постановлением Госкомсанэпиднадзора России от 14 июля 1996 г. N 14 СанПиН 2.2.2.542-96), и Приложение 1,2)

Требования электробезопасности

При пользовании средствами вычислительной техники и периферийным оборудованием каждый работник должен внимательно и осторожно обращаться с электропроводкой, приборами и аппаратами и всегда помнить, что пренебрежение правилами безопасности угрожает и здоровью, и жизни человека

Во избежание поражения электрическим током необходимо твердо знать и выполнять следующие правила безопасного пользования электроэнергией:

1. Необходимо постоянно следить на своем рабочем месте за исправным состоянием электропроводки, выключателей, штепсельных розеток, при помощи которых оборудование включается в сеть, и заземления. При обнаружении неисправности немедленно обесточить электрооборудование, оповестить администрацию. Продолжение работы возможно только после устранения неисправности.
2. Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается:

а) вешать что-либо на провода;

б) закрашивать и белить шнуры и провода;

в) закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы;

г) выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.

3. Для исключения поражения электрическим током запрещается:

а) часто включать и выключать компьютер без необходимости;

б) прикасаться к экрану и к тыльной стороне блоков компьютера;

в) работать на средствах вычислительной техники и периферийном оборудовании мокрыми руками;

г) работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками электрического напряжения на корпусе

д) класть на средства вычислительной техники и периферийном оборудовании посторонние предметы.

3. Запрещается под напряжением очищать от пыли и загрязнения электрооборудование.
4. Запрещается проверять работоспособность электрооборудования в неприспособленных для эксплуатации помещениях с токопроводящими полами, сырых, не позволяющих заземлить доступные металлические части.
5. Ремонт электроаппаратуры производится только специалистами-техниками с соблюдением необходимых технических требований.
6. Недопустимо под напряжением проводить ремонт средств вычислительной техники и периферийного оборудования.

7. Во избежание поражения электрическим током, при пользовании электроприборами нельзя касаться одновременно каких-либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей.

8. При пользовании электроэнергией в сырых помещениях соблюдать особую осторожность.

9. При обнаружении оборвавшегося провода необходимо немедленно сообщить об этом администрации, принять меры по исключению контакта с ним людей. Прикосновение к проводу опасно для жизни.

10. Спасение пострадавшего при поражении электрическим током главным образом зависит от быстроты освобождения его от действия током.

Во всех случаях поражения человека электрическим током немедленно вызывают врача. До прибытия врача нужно, не теряя времени, приступить к оказанию первой помощи пострадавшему.

Необходимо немедленно начать производить искусственное дыхание, наиболее эффективным из которых является метод «рот в рот» или «рот в нос», а также наружный массаж сердца.

Искусственное дыхание пораженному электрическим током производится вплоть до прибытия врача.

Требования по обеспечению пожарной безопасности

На рабочем месте запрещается иметь огнеопасные вещества.

В помещениях запрещается:

а) зажигать огонь;

б) включать электрооборудование, если в помещении пахнет газом;

в) курить;

г) сушить что-либо на отопительных приборах;

д) закрывать вентиляционные отверстия в электроаппаратуре.

Источниками воспламенения являются:

а) искра при разряде статического электричества;

б) искры от электрооборудования;

в) искры от удара и трения;

г) открытое пламя.

При возникновении пожароопасной ситуации или пожара персонал должен немедленно принять необходимые меры для его ликвидации, одновременно оповестить о пожаре администрацию.

Помещения с электрооборудованием должны быть оснащены огнетушителями типа ОУ-2 или ОУБ-3.

Время регламентированных перерывов в зависимости от продолжительности рабочей смены, вида и категории трудовой деятельности с ПЭВМ

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работ с ПЭВМ			Суммарное время регламентированных перерывов, мин.	
	Группа А, количество знаков	Группа Б, количество знаков	Группа В, час.	при 8-ми часовой смене	при 12-ти часовой смене
I	до 20 000	до 15 000	до 2,0	30	70
II	до 40 000	до 30 000	до 4,0	50	90
III	до 60 000	до 40 000	до 6,0	70	120

Примечание: время перерывов дано при условии соблюдения требований СанПиН 2.2.272.4.1340-03. При несоответствии фактических условий труда требованиям СанПиН 2.2.272.4.1340-03, время регламентированных перерывов следует увеличить на 30%.

Согласно требованиям к организации режима работы с ВДТ и ПЭВМ студентов высших учебных заведений (см. 9.2. СанПин 2.2.2.542-96) регламентируются нормы времени работы за ПК: после каждого академического часа занятий с ВДТ или ПЭВМ следует устраивать перемены длительностью 15 - 20 минут с обязательным выходом учащихся из класса (кабинета) и организацией сквозного проветривания (п. 9.3.2. СанПин 2.2.2.542-96).

Ниже представлены некоторые выдержки из СанПин 2.2.2.542-96, имеющие непосредственное отношение к обеспечению безопасности пользования ПК для студентов высших учебных заведений.

Для студентов первого курса оптимальное время учебных занятий при работе с ВДТ или ПЭВМ составляет 1 час, для студентов старших курсов - 2 часа, с обязательным соблюдением между двумя академическими часами занятий перерыва длительностью 15-20 минут. Допускается время учебных занятий с ВДТ и ПЭВМ увеличивать для студентов первого курса до 2 часов, а для студентов старших курсов до 3 академических часов, при условии что длительность учебных занятий в дисплейном классе (аудитории) не превышает 50% времени непосредственной работы на ВДТ или ПЭВМ и при соблюдении профилактических мероприятий: упражнения для глаз, физкультминутка и физкультпауза.