МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Димитровградский инженерно-технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(ДИТИ НИЯУ МИФИ)

СОГЛАСОВАНО
От работодателя:
Зам. директора ООО "АИС Город"
должность, название предприятия
_____ Я.Н. Насальник
«15» апреля 2022 г.
М.П.

УТВЕРЖДАЮ
Руководитель ДИТИ НИЯУ МИФИ
должность и название образовательного учреждения
_____ И.И. Бегинина
«12» мая 2022 г.
М.П.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
(по профилю специальности)

Раздел ПП.03.01 Производственная практика

ПМ.03ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМ СРЕДСТВАМИ

Специальность	10.02.05 Обеспечение информационной безопасности автоматизированных систем
Квалификация выпускника	техник по защите информации
Форма обучения	очная

Разработчикрабочей программы:Т.И. Катина, преподаватель техникума ДИТИ НИЯУ МИФИ

Димитровград

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) ПП.03.01 ПРОИЗВОДСТВЕННАЯ ПРАКТИКА ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Область применения программы:

Программа производственной практики (по профилю специальности) ПП.03.01 Производственная практика – является элементом профессионального модуля ПМ.03Защита информации техническими средствами и частью программы подготовки специалистов среднего звена (ППССЗ) в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Цели и задачи производственной практики (по профилю специальности)

Производственная практика (по профилю специальности) направлена на формированиеу студента общих и профессиональных компетенций, совершенствование практического опыта и реализуется в рамках модуля ПМ.03 Защита информации техническими средствами ППССЗ специальности10.02.05 Обеспечение информационной безопасности автоматизированных системпо каждому из видов профессиональной деятельности, предусмотренных ФГОС СПО по специальности

С целью овладения видом профессиональной деятельности, определяемым профессиональным модулем по специальности в ходе освоения программы производственной практики (по профилю специальности)по основному виду деятельности Защита информации техническими средствамистудент должен:

освоить следующие общие и профессиональные 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 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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 (ПЭМИН), 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.

овладеть следующими воспитательными компетенциями:

В17 - формирование чувства личной ответственности за научно-технологическое развитие России, за результаты исследований и их последствия

В18 - формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения

В19 - формирование научного мировоззрения, культуры поиска нестандартных научно-технических решений, критического отношения к исследованиям лженаучного толка

В20 - формирование навыков коммуникации, командной работы и лидерства

В21 - формирование способности и стремления следовать в профессии нормам поведения, обеспечивающим нравственный характер трудовой деятельности и неслужебного поведения

В25 - формирование творческого инженерного мышления, навыков организации коллективной проектной деятельности

В26 - формирование культуры информационной безопасности

В29 - формирование профессионально значимых установок в области защиты информации

приобрести 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.

приобрести умения:

– 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

приобрести знания:

– порядка технического обслуживания технических средств защиты информации;

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

– физических основ, структуры и условий формирования технических каналов утечки информации, способов их выявления и методов оценки опасности, классификации существующих физических полей и технических каналов утечки информации;

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

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

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

– основных принципов действия и характеристик технических средств физической защиты;

– основных способов физической защиты объектов информатизации;

– номенклатуры применяемых средств физической защиты объектов информатизации.

Практика по профилю специальности предусматривает выполнение студентами производительного труда на производственных объектах предприятия, с которым заключен договор. Предприятие может представить студентам-практикантам рабочие места, соответствующие рабочей профессии.

Практика по профилю специальности проводится, в организациях на основе договоров, заключаемых между образовательным учреждением и этими организациями, направление деятельности которых соответствует профилю подготовки обучающихся.

Практика по профилю специальности организуется на предприятиях соответствующих профилю специальности, а также в подразделениях учебного заведения, оснащенных компьютерной техникой, которые отвечает требованиям программы практики.

Итогом практики является оценка, которая выставляется руководителем практики от учебного заведения на основании собеседования со студентом в ходе дифференцированного зачета, выполнения им индивидуального задания, составленного в соответствии с программой практики, полноты и глубины содержания дневника практики и отчета по практике, а также характеристики, составленной руководителем практики от предприятия.

Студенты, не выполнившие требования программы практики или получившие отрицательную характеристику, отчисляются из учебного заведения и им, выдается справка установленного образца.

При наличии уважительной причины невыполнение требований программы практики студент оставляется на повторное обучение на данном курсе без права получения стипендии на период повторного обучения.

2. ОРГАНИЗАЦИЯ И РУКОВОДСТВО ПРОИЗВОДСТВЕННОЙ ПРАКТИКОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Обучающиеся направляются для прохождения практики на основании приказа руководителя ДИТИ НИЯУ МИФИ с указанием закрепления каждого обучающегося за организацией, а также вида и сроков прохождения практики.

Обучающиеся, совмещающие обучение в ДИТИ НИЯУ МИФИ с трудовой деятельностью, вправе проходить учебную и производственную практику в организации по месту работы, в случаях, если осуществляемая ими профессиональная деятельность соответствует целям практики.

По решению руководителя ДИТИ НИЯУ МИФИ обучающимся по индивидуальному плану, разрешается прохождение практики в индивидуальном порядке. Основанием для такого решения является поступившее в ДИТИ НИЯУ МИФИ письмо от сторонней организации о готовности принять обучающихся на практику. Между ДИТИ НИЯУ МИФИ и сторонней организацией заключается договор о проведении практики в установленном порядке. Тематика индивидуального задания разрабатывается сторонней организацией и ДИТИ НИЯУ МИФИ совместно с обязательным выполнением программы практики и предоставляется руководителю практики от техникума для утверждения.

Базами производственной практики выпускников специальности 10.02.05 Обеспечение информационной безопасности автоматизированных системявляются:

– предприятия и организации всех форм собственности;
– образовательные учреждения любого уровня;
– учреждения дошкольного образования;
– предприятия среднего и малого бизнеса;
– консультационные центры по обслуживанию и установке программного обеспечения;
– органы власти муниципального и регионального уровня;
– учреждения банковской сферы;
– органы социального обеспечения;
– предприятия розничной и оптовой торговли;
– территориальные органы Федеральной налоговой службы;
– территориальные органы внутренних дел и др.;
– вычислительные центры и отделы автоматизации АО ГНЦ РФ «НИИАР», ООО «НИИАР-ГЕНЕРАЦИЯ» и др.

В качестве базы для прохождения практики по профилю специальности студент вправе самостоятельно выбирать предприятие (организацию, учреждение) соответствующее профилю преддипломной практики.

Целесообразна практика по профилю специальности по месту предстоящей работы выпускника.

Во время практики студенты выполняют обязанности техников по защите информации в соответствии с требованиями ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, а при

наличии вакантных мест они могут зачисляться на штатные должности, если работа на них соответствует требованиям программы.

Во время прохождения практики студент должен соблюдать все требования правил внутреннего распорядка и охраны труда на предприятии.

Работа в период практики осуществляется бесплатно или за оплату (по усмотрению руководства предприятия). Рабочее время практики определяется в соответствии с внутренним распорядком предприятия.

Организационное и учебно-методическое руководство практикой студентов осуществляется руководителями практики от образовательного учреждения и от организации.

В качества руководителя практики по профилю специальности практики от техникума назначаются преподаватели общепрофессиональных, профессиональных дисциплин или профессиональных модулей. После окончательного распределения студентов по местам практики в техникуме ДИТИ РИЯУ МИФИ оформляется приказ о закреплении студентов за конкретной организацией с указанием фамилии, имени, отчества руководителя практики от техникума.

Непосредственное руководство практикой по профилю специальности практикой возлагается на одного из квалифицированных специалистов предприятия – базы практики.

Обязанности руководителей практики.

Руководитель практики от техникума обязан:

– проверить наличие и организовать обеспечение студентов направлениями на практику, графиками ее выполнения, утверждёнными заведующей отделением, формами дневника по производственной практике (по профилю специальности);

– выдать каждому студенту индивидуальное задание, содержание которого должно способствовать выполнению программы производственной практики (по профилю специальности) соответствующего профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении, самостоятельной творческой работы, использованию современных методов анализа и планирования эксперимента с элементами научного исследования, разработке практических вопросов в области определяемого направления деятельности;

– составить график прохождения практики;

– провести обязательный инструктаж со студентами о порядке прохождения практики, охране труда и безопасности жизнедеятельности;

– направить студентов на практику по профилю специальности в соответствии с приказом;

– проводить регулярные консультации для студентов-практикантов по теоретическим и практическим вопросам практики;

– осуществлять постоянный контроль за прохождением практики студентами и выполнением ими индивидуальных заданий и календарных графиков;

– контролировать ведение студентами-практикантами дневников, подготовку и составление отчётов;

– совместно с руководителем практики от организации, участвующей в

организации и проведении практики, организовать процедуру оценки выполнения программы практики и качества составления отчета, принять защиту отчёта в виде собеседования со студентом и сделать соответствующую запись в экзаменационной ведомости и зачётной книжке студента.

Руководитель практики оторганизации-базы практики обязан:

– согласовывать программу практики, планируемые результаты практики, индивидуальное задание на практику;

– создать условия для обеспечения выполнения программы практики по профилю специальности и сбора материалов для ВКР;

– участвовать в организации и оценке результатов прохождения практики;

– составить мотивированное заключение на результаты выполнения программы практики студентом;

– обеспечить безопасные условия прохождения практики студентами, отвечающие санитарным правилам и требованиям охраны труда;

– организовать проведение инструктажа студентов по ознакомлению с требованиями охраны труда и техники безопасности в организации.

Обязанности студентов-практикантов.

Студент обязан:

– перед началом прохождения практики получить у руководителя индивидуальное задание, развёрнутый план и календарный график работы на весь период с указанием сроков выполнения отдельных этапов, утвержденное заведующей отделением;

– своевременно и полностью выполнять задания, предусмотренные дневником, индивидуальным заданием и календарным графиком;

– соблюдать действующие в организациях правила внутреннего трудового распорядка; строго соблюдать требования охраны труда и пожарной безопасности;

– сохранять в тайне коммерческую информацию о деятельности предприятия;

– своевременно оформлять результаты проведенных исследований;

– регулярно заполнять дневник прохождения практики, занося в него краткие сведения о проделанной работе;

– составить отчёт по практике в соответствии с установленными требованиями;

– получить у руководителя практики от организации заключение о результатах прохождения практики;

– своевременно сдать руководителю практики на проверку правильно оформленные дневник и отчёт о практике;

– защитить отчёт у руководителя практики в виде собеседования.

При наличии нескольких практикантов на одной базе практики не допускается дублирование записей в отчетах и выполнение комплексного отчета**.**

2.1. Рекомендуемое количество часов на освоение производственной практики:

всего – 75 часов, из них:

ПП.03.01 – 72 часа (2 недели)

Консультации – 3 часа.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙПРАКТИКИ

Наименование профессионального модуля	Виды выполняемых работ	Объём часов
1	**2**	**3**
ПМ.03 Защита информации техническими средствами ПП.03.01	1. Знакомство с задачами, поставленными в подразделении, где проходит практика. 2. Анализ и описание принципов построения систем информационной защиты производственных подразделений. 3. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 4. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 5. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 6. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами	72

4. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Учебно-методическая документация:

1. Программа производственной практики (по профилю специальности) ПП.03.01;
2. Дневник по практике по профилю специальности;
3. Методические указания по оформлению дневника и отчета практики.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники

1. Бубнов, А.А. Основы информационной безопасности: учебник / А.А. Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. – 3-е изд., стер. - М.: Академия, 2017. – 256 с.

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. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491

4. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/206279

5. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 96 с. — ISBN 978-5-8114-9562-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/200480

6. Петренко, Ю. В. Теоретические основы электротехники: от теории к практике : учебно-методическое пособие / Ю. В. Петренко. — Новосибирск : НГТУ, 2021. — 87 с. — ISBN 978-5-7782-4424-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216191

7. Сычев Ю.Н. Защита информации и информационная безопасность / Ю.Н. Сычев. - Москва : Инфра-М, 2021. - 201 с. - ISBN 978-5-16-016583-7. - URL: https://ibooks.ru/bookshelf/378002/reading

8. Раков, А.С. Техническая защита информации : учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара : ПГУТИ, 2020. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/255575

Дополнительные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10.Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11.Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12.Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13.Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14.Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15.Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16.Требования о защите информации, не составляющей государственную тайну, 115 содержащейся в государственных информационных системах.

Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17.Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18.Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21.Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

22.ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

23.ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24.ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25.ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26.ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27.ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

28.ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29.ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30.ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31.ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32.ГОСТ Р 50922-2006 Защита информации. Основные термины и

определения. 116 Ростехрегулирование, 2006.

33.ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34.ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35.ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36.ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37.ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38.ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

39.ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40.ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41.ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43.Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44.Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45.ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46.ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47.Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48.Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. 117

49.Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50.Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

9. Сайт Научной электронной библиотеки www.elibrary.ru

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ КОМПЕТЕНЦИЙ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

5.1 Формы и методы контроля

Контроль за ходом практики со стороны техникума осуществляется в форме периодических посещений мест практики руководителем и беседой со студентами, их консультацией по программе практики.

При обнаружении нарушений со стороны студентов в дневник заносится замечание с указанием сроков исправления допущенных промахов.

Для окончательного оформления отчёта студенту отводится 2–3 дня в конце практики. Отчёт и дневник представляются для проверки руководителю в 5-дневный срок по окончании срока практики.

Оценка результатов освоения производственной практики (по профилю специальности) соответствует оценке результатов соответствующего профессионального модуля.

Студент, не выполнивший программу практики и получивший отрицательный отзыв о работе или неудовлетворительную оценку при защите отчета, направляется на практику повторно или отчисляется из техникума.

Контроль и оценка результатов производственной практики (по профилю специальности) осуществляется совместно представителями предприятий – баз практики и отражается в аттестационных листах по каждому направлению деятельности (по каждому профессиональному модулю) и дневниках практики с учетом основных показателей оценки сформированности профессиональных и общих компетенций и руководителями практики от техникума ДИТИ НИЯУ МИФИ на основе представленных документов по окончанию практики (дневника, отчета, аттестационного листа и производственной характеристики). Если хотя бы одна из компетенций не освоена, то практика в целом считается не выполненной.

При оценки уровня профессиональной подготовки установлено следующее соответствие:

- уровень освоения высокий – оценка «отлично»;
- уровень освоения средний – оценка «хорошо»;
- уровень освоения удовлетворительный – оценка «удовлетворительно»;
- уровень освоения низкий - оценка «неудовлетворительно».

5.2. Контроль и оценка результатов производственной практики (по профилю специальности) профессионального модуля

ПМ.03Защита информации техническими средствами

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
1	**2**	**3**
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрация умения и практических навыков в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	– составления отчета по практике – решение ситуационных задач; – оценки выполнения индивидуального задания по практике – оценка результатов выполнения видов работ на практике Итоговый контроль в форме дифференцированного зачета
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявление умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проведение работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проведение самостоятельных измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявление знаний в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	

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

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
1	**2**	**3**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- выбор метода и способа решения профессиональных задач с соблюдением техники безопасности и согласно заданной ситуации; - оценка эффективности и качества выполнения согласно заданной ситуации	Оценка процесса и результатов выполнения видов работ на практике
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- эффективный поиск необходимой информации; - информация, подобранная из разных источников в соответствии с заданной ситуацией	Оценка процесса и результатов выполнения видов работ на практике
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- демонстрация собственной деятельности в условиях коллективной и командной работы в соответствии с заданной ситуацией; - демонстрация собственной деятельности в роли руководителя команды в соответствии с заданными условиями.	Оценка процесса и результатов выполнения видов работ на практике
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективное использование информационнокоммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Оценка процесса и результатов выполнения видов работ на практике