

РАБОЧАЯ ПРОГРАММА

| | |
|---------------------------|--|
| Производственная практика | ПП.02.01 Производственная практика |
| Профессиональный модуль | ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| Код, специальность: | 10.02.05 Обеспечение информационной безопасности автоматизированных систем |
| Квалификация: | Техник по защите информации |

СОГЛАСОВАНА:
Цикловой методической
комиссией
«10.02.05 Профессиональных
модулей»

Протокол № 6-21/22 ЗК
от «15» января 2022 года

Разработана на основе Федерального государственного
образовательного стандарта по специальности среднего
профессионального образования
специальность: 10.02.05 Обеспечение
информационной безопасности автоматизированных
систем
квалификация: техник по защите информации

Председатель цикловой
методической комиссии


Подпись
М.А. Молотков
Инициалы Фамилия

Заместитель директора по учебной работе


Подпись
Д.А. Клопов
Инициалы Фамилия

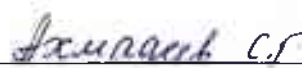
УТВЕРЖДЕНА:
Директор техникума


Подпись
А.В. Чурилов
Инициалы Фамилия

Составители (авторы):

Прищеп Михаил Сергеевич, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова
Молотков Максим Алексеевич, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова

Кузнецов Павел Олегович, преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова

СОГЛАСОВАНО: 
представитель работодателя

Рецензент: _____

Ф.И.О., ученая степень, звание, должность, наименование

СОДЕРЖАНИЕ

| | Стр. |
|---|------|
| 1. Паспорт программы практики..... | 4 |
| 2. Результаты практики | 9 |
| 3. Структура и содержание практики..... | 10 |
| 4. Условия реализации программы практики | 14 |
| 5. Контроль и оценка результатов освоения практики..... | 17 |

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ ПП.02.01 ПРОИЗВОДСТВЕННАЯ ПРАКТИКА

1.1. Область применения программы практики

Программа производственной практики является частью программы подготовки специалистов среднего звена, обеспечивающей реализацию ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Практика является частью учебного процесса и направлена на формирование у студентов практических профессиональных умений, приобретение первоначального практического опыта по основным видам профессиональной деятельности для последующего освоения ими профессиональных компетенций по избранной специальности:

ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3 Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5 Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6 Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2. Цели и задачи практики – требования к результатам освоения практики, формы отчетности

В ходе освоения программы практики студент должен:

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.

Уметь:

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

- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- применять программные и программно-аппаратные средства для защиты информации в базах данных;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- применять математический аппарат для выполнения криптографических преобразований;
- использовать типовые программные криптографические средства, в том числе электронную подпись;
- применять средства гарантированного уничтожения информации;
- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

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.

По окончании практики студент сдаёт отчет в соответствии с содержанием тематического плана практики и по форме, установленной в МПТ ФГБОУ ВО «РЭУ им. Г.В. Плеханова».

Итоговая аттестация проводится в форме - **дифференцированного зачёта**.

1.3. Количество часов на освоение программы практики

Рабочая программа практики рассчитана на прохождение студентами практики в объеме **108** часов.

2. РЕЗУЛЬТАТЫ ПРАКТИКИ

| Код | Наименование результата обучения |
|---------|--|
| ПК 2.1. | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. |
| ПК 2.2. | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. |
| ПК 2.3. | Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. |
| ПК 2.4. | Осуществлять обработку, хранение и передачу информации ограниченного доступа. |
| ПК 2.5. | Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. |
| ПК 2.6. | Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. |

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

3.1 Тематический план практики

| Наименование профессионального модуля | Коды формируемых компетенций | Объем времени, отводимый на практику | Сроки проведения практики |
|--|------------------------------|--------------------------------------|---------------------------|
| 1 | 2 | 3 | 4 |
| ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами | ПК 2.1. | <i>3 недели – 108 часа</i> | <i>8 семестр</i> |
| | ПК 2.2. | | |
| | ПК 2.3. | | |
| | ПК 2.4. | | |
| | ПК 2.5. | | |
| | ПК 2.6. | | |

3.2. Содержание практики

| Наименование разделов и тем | Содержание освоенной учебной информации, виды работ, выносимые на практику в соответствии с рабочими программам профессиональных модулей | Объем часов | Коды профессиональных компетенций |
|---|--|-------------|-----------------------------------|
| 1 | 2 | 3 | 5 |
| Раздел 1. Организационно-подготовительный этап прохождения практики на предприятии | | 4 | |
| Тема 1.1. Инструктаж по прохождению производственной практики и правилам безопасности работы на предприятии. | <p style="text-align: center;"><i>Содержание выполняемых работ</i></p> <p>Знакомство с общими функциональными обязанностями, правилами техники безопасности на предприятии, на конкретном рабочем месте, при работе с электрическими приборами (устройствами)</p> | 4 | |
| Раздел 2. Ознакомление со структурой и характером деятельности подразделения | | 8 | |
| Тема 2.1. Ознакомление с организацией работы на предприятии или в структурном подразделении | <p style="text-align: center;"><i>Содержание выполняемых работ</i></p> <p>Знакомство с режимом работы, формой организации труда и правилами внутреннего распорядка, структурными подразделениями предприятия, штатным расписанием; с принципами управления, руководства и осуществления должностных обязанностей</p> | 4 | ПК 2.1-2.6 |
| Тема 2.2. Ознакомление с должностными и функциональными обязанностями | <p style="text-align: center;"><i>Содержание выполняемых работ</i></p> <p>Изучение прав и обязанностей сотрудника, должностной инструкции, регламентирующей его деятельность; знакомство с правами и обязанностями других сотрудников и руководителей; согласование с руководителем практики задание, постановку целей и задач практики</p> | 4 | ПК 2.1-2.6 |
| Раздел 3. Работа на рабочих местах или в подразделениях предприятия | | | |
| Тема 3.1. Ознакомление: с организацией информационного | <p style="text-align: center;"><i>Содержание выполняемых работ</i></p> <p>Ознакомление с производственными характеристиками и показателями</p> | 36 | |
| | | 2 | ПК 2.1-2.6 |

| | | | |
|---|---|-----------|-------------------|
| <p>обеспечения подразделения; с процессом защиты на уровне проектирования и эксплуатации информационных средств; с методами планирования и проведения мероприятий по созданию (разработке) проекта (подсистемы) информационной среды предприятия для решения конкретной задачи.</p> | <p>деятельности предприятия. Изучение новых технологических средств в современных информационных системах, применяемых на предприятии. Изучение основных проектных решений по информационным системам на предприятии (в организации). Ознакомление с методологией проектирования, внедрения и эксплуатации актуальных информационных систем. Изучение технологии сбора, регистрации и обработки информации на данном предприятии. Проектирование подсистем защиты. Обеспечения защиты информации от несанкционированного доступа</p> | | |
| <p>Тема 3.2. Изучение структурных и функциональных схем предприятия, организации деятельности подразделения; порядка и методов ведения делопроизводства; требований к техническим, программным средствам, средствам защиты информации, используемым на предприятии.</p> | <p><i>Содержание выполняемых работ</i></p> <p>Изучение основ финансов, организации денежного обращения и кредитования предприятия, приобретение навыков использования финансово-кредитного механизма с целью повышения эффективности работы предприятия и составления финансового плана. Изучение схем защиты денежных транзакций через сеть интернет Изучение организации расчета заработной платы на предприятии, приобретение навыков проектирования трудовых процессов с учетом комплекса технических, экономических, психофизиологических и социальных факторов, оценка затрат и результатов труда.</p> | 4 | ПК 2.1-2.6 |
| <p>Тема 3.3. Выполнение производственных заданий</p> | <p><i>Содержание выполняемых работ</i></p> <p>Анализ принципов построения систем информационной защиты производственных подразделений; техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы; участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении; участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами</p> | 80 | ПК 2.1-2.6 |

| | | | |
|---|---|------------|-------------------|
| | при выполнении задач практики. | | |
| Тема 3.4. Сбор и анализ материалов для оформления отчетной документации по практике. | <i>Содержание выполняемых работ</i> | | |
| | Сбор материалов для отчета, подготовка отчетной документации по практике | 4 | ПК 2.1-2.6 |
| Итоговая аттестация | Сдача отчета в соответствии с содержанием тематического плана практики и по форме, установленной в МПТ ФГБОУ ВО «РЭУ им. Г.В. Плеханова». | | |
| Всего | | 108 | |

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

4.1 Требования к документации, необходимой для проведения практики.

Для проведения практики в учебном заведении разработана следующая документация:

- рабочая программа практики;
- календарно-тематический план;
- распоряжение о направлении студентов на производственную практику и назначении руководителей практики.
- договоры с предприятиями по проведению практики;
- графики консультаций и контроля за выполнением студентами программы практики;
- график защиты отчетов по практике.

4.2 Требования к учебно-методическому обеспечению практики.

В целях реализации требований к учебно-методическому обеспечению практики разработаны и утверждены:

- Задания на практику;
- Методические рекомендации для студентов по выполнению видов работ на практике;
- Методические рекомендации по формированию отчетов по практике;
- Методические рекомендации по оформлению дневника по практике;
- Критерии оценки прохождения практики и защиты отчетов.

4.3. Требования к материально-техническому обеспечению практики

Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

- Лаборатория программных и программно-аппаратных средств защиты информации

| № п/п | Оборудование | Технические средства обучения | Количество рабочих мест |
|-------|---|-------------------------------|-------------------------|
| 1 | 15 автоматизированных рабочих мест для обучающихся и 1 рабочее место для преподавателя с конфигурацией: Процессор Intel Core i5, оперативная память объемом 8 Гб, жесткий диск - 500 Гб, монитор 23", мышь, клавиатура; | Проектор 1 шт | 15 |
| 2 | столов 12 шт | | |
| 3 | стульев 26 шт | | |
| 4 | доска 1 шт | | |
| 5 | экран проектора 1 шт | | |
| 6 | стенды 1 шт | | |
| 7 | кабели различного типа | | |
| 8 | обжимной инструмент | | |
| 9 | коннекторы RJ-45 | | |
| 10 | тестеры для кабеля | | |
| 11 | кросс-ножи | | |
| 12 | кросспанели | | |

Программное обеспечение:

Windows 10 pro, Microsoft office2016, visio, 1С Предприятие; Visual Studio 2019; arduino, unity,php, Notepad++,1С Предприятие; Visual Studio 2019; arduino, unity,php, Notepad++,SQL

Server, My SQL, Adobe Illustrator, AutoCAD, Autodesk, ColerDraw, Mozilla Firefox, Microsoft Edge, Google Chrome, Opera

- **Лаборатория информационных технологий, программирования и баз данных**

| № п/п | Оборудование | Технические средства обучения | Количество рабочих мест |
|-------|--|-------------------------------|-------------------------|
| 1 | 10 автоматизированных рабочих мест для обучающихся и 1 рабочее место для преподавателя с конфигурацией: Процессор Intel Core i5, оперативная память объемом 8 Гб, дискретная видеокарта, жесткий диск - 1 Тб, монитор 23", мышь, клавиатура; | проектор 1 | 13 |
| 2 | 3 автоматизированных рабочих места для обучающихся с конфигурацией: Процессор Intel Core i7, оперативная память объемом 16 Гб, жесткий диск - 1 Тб, твердотельный накопитель - 256 Гб, монитор 23", мышь, клавиатура | | |
| 3 | столов 11 | | |
| 4 | стульев 28 | | |
| 5 | шкафы 1 | | |
| 6 | маркерная доска 1 | | |
| 7 | стенды 1 | | |

Программное обеспечение:

Windows 10 pro, Microsoft Office 2016, Visio 2016, Visual Studio 2019, 1С предприятие 8 (учебная версия), PascalABC.net, XAMPP, Unity, Python, notepad++, arduino, Android Studio, MySQL, T-SQL, SQL Server, Adobe Photoshop, Adobe Illustrator, AutoCAD, Autodesk, ColerDraw, Mozilla Firefox, Microsoft Edge, Google Chrome

4.4 Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

Печатные издания не используются. ПМ полностью обеспечен электронными изданиями.

4.4.1 Печатные издания

ОСНОВНЫЕ *не используются*

ДОПОЛНИТЕЛЬНЫЕ *не используются*

4.4.2 Электронные издания

ОСНОВНЫЕ

1. Платонов В.В. Программно-аппаратные средства защиты информации (2-е изд., стер.), М. Академия, 2014, <https://academia-library.ru/catalogue/4831/105545/>
2. [Душкин А.В.](#), [Барсуков О.М.](#), [Кравцов Е.В.](#), [Славнов К.В.](#) Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с. <https://znanium.com/bookread2.php?book=973806>

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2016. – 184 с. <https://znanium.com/bookread2.php?book=536932>
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с. <https://znanium.com/bookread2.php?book=536932>

ДОПОЛНИТЕЛЬНЫЕ:

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. 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.
11. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
12. 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.
13. 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.
14. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

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

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

19. 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 недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

20. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

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. 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 си-

стем 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 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

39. 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.

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

41. 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.

42. 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.

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.

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.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

4.4.3 Периодические издания:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: <http://cyberrus.com/>
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

4.4.4 Электронные ресурсы:

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. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>
10. Сайт Научной электронной библиотеки www.elibrary.ru

4.4.5 Профессиональные базы данных и справочные системы

- Федеральная служба государственной статистики - <https://rosstat.gov.ru/>
- Научометрическая и реферативная база данных SCOPUS - <https://www.scopus.com>
- Информационно-справочная система "КонсультантПлюс"

4.5 Требования к руководителю практики

Руководителем практики от техникума назначается педагогический работник, имеющий высшее образование, соответствующее профилю проводимой практики

4.5.1 Руководитель практики от образовательного учреждения:

1. разрабатывает тематику заданий для студентов;
2. проводит консультации со студентами перед направлением их на практику с разъяснением целей, задач и содержания практики;
3. принимает участие в распределении студентов по рабочим местам или перемещении их по видам работ;
4. осуществляет контроль правильного распределения студентов в период практики; формирует группы в случае применения групповых форм проведения практики;
5. проводит индивидуальные и групповые консультации в ходе практики;
6. оказывает методическую помощь студентам при выполнении ими заданий и сборе материалов к отчету по практике;

7. контролирует выполнение требований охраны труда, безопасности жизнедеятельности и пожарной безопасности;

4.5.2 Руководитель практики от организации:

1. согласовывает программу практики, планируемые результаты практики, задание на практику;
2. участвует в организации и проведении дифференцированного зачета по практике, квалификационного экзамена и экзамена по профессиональному модулю;
3. участвуют в организации и оценке результатов освоения общих и профессиональных компетенций, освоенных студентами в период прохождения практики;
4. проводит инструктаж студентов по ознакомлению с требованиями охраны труда, безопасности жизнедеятельности и пожарной безопасности

4.6 Требования к соблюдению техники безопасности и пожарной безопасности

Регламентация требований по пожарной безопасности и техники безопасности осуществляется внутренними локальными актами техникума и организации, куда был направлен обучающийся.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

По результатам усвоения программы практики студенты представляют руководителю практики от техникума: отчет, дневник и аттестационный лист на студента-практиканта от руководителя базы практики.

По окончании практики студент сдаёт дневник, отчет с дифференцированной оценкой и аттестационный лист руководителю производственной практики от образовательного учреждения. Защита дневников и отчетов проводится в организации или в техникуме (если группа размещена по разным объектам практики). На базах практики защита должна проводиться в последний день практики.

При оценке итогов работы студента на практике учитываются содержание и правильность оформления студентом дневника и отчета по практике, отзывы руководителей практики от организации, качество ответов на вопросы в ходе защиты отчета.

Зарегистрированные и защищенные дневники, отчеты хранятся в техникуме в течение трех лет в соответствии с номенклатурой дел.

Аттестация студента по итогам прохождения практики проводится только после сдачи документов по практике и фактической защиты отчета.

Защита отчета по практике, как правило, представляет собой краткий, 8-10-минутный доклад студента и его ответы на вопросы членов комиссии.

После защиты отчета руководитель практики от техникума дает свое заключение о выполнении дневника, отчета, выполнении программы практики и ставит по итогам дифференцированную оценку по пятибалльной шкале (5 «отлично», 4 «хорошо», 3 «удовлетворительно», 2 «неудовлетворительно»). Оценка одновременно проставляется в ведомость, зачетную книжку студента, дневник студента по производственной практике и аттестационный лист.

| Результаты (освоенные профессиональные компетенции) | Основные показатели оценки результата | Формы и методы контроля и оценки |
|--|---|--|
| ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты | Демонстрировать умения и практические навыки в установке и настройке отдельных программных, | оценка процесса и результатов выполнения видов работ на практике |

| | | |
|--|---|--|
| информации. | программно-аппаратных средств защиты информации | |
| ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. | Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | оценка процесса и результатов выполнения видов работ на практике |
| ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. | Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации | оценка процесса и результатов выполнения видов работ на практике |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. | Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа | оценка процесса и результатов выполнения видов работ на практике |
| ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. | Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств | оценка процесса и результатов выполнения видов работ на практике |
| ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. | Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак | оценка процесса и результатов выполнения видов работ на практике |

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 |
|--|---|----------------------------------|
| ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | <ul style="list-style-type: none"> – обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества | Интерпретация |

| | | |
|---|---|--|
| | выполнения профессиональных задач | |
| ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач | |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы; | |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных) | результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. | - грамотность устной и письменной речи, - ясность формулирования и изложения мыслей | Экспертное наблюдение и оценка при выполнении работ по производственной практикам |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. | - соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, | |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций | |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; | |
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | - эффективность использования информационно-коммуникационных | |

| | | |
|---|--|--|
| | технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; | |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках. | - эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке. | |