Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский экономический университет имени Г.В. Плеханова»
Московский приборостроительный техникум

РАБОЧАЯ ПРОГРАММА

Учебная практика	УП.02.01 Учебная практика
Профессиональный	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Код, специальность	10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

Москва 2019

СОГЛАСОВАНА:

Цикловой методической комиссией

«Профессиональных модулей 10.02.05»

Разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация: техник по защите информации

Протокол № 14-18/19-ЗК

от «03» июля 2019 года

Председатель цикловой методической комиссии

_____

М.А. Молотков

Заместитель директора по учебной работе _____ Д.А. Клопов

подпись

РАССМОТРЕННА И ОДОБРЕНА

_____

_____ _____ С.Г. Ахмадеев

подпись

УТВЕРЖДЕНА:

Директор техникума _____ А.В. Чурилов

подпись

Составители (авторы):

Молотков Максим Алексеевич, преподаватель ФГБОУ ВО «РЭУ им. Г.В.Плеханова»,

Прищеп Михаил Сергеевич, преподаватель ФГБОУ ВО «РЭУ им. Г.В.Плеханова»,

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

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1.Область применения программы

Рабочая программа учебной практики является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО в части освоения квалификации **Техник по защите информации** и основного вида профессиональной деятельности (ВПД): Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

1.2.Цели и задачи учебной практики:

Формирование у обучающихся первоначальных практических профессиональных умений в рамках модулей ППССЗ по основным видам профессиональной деятельности для освоения методов и приемов практического применения прикладных программных продуктов для программного обеспечения компьютерных систем

1.3.Требования к результатам освоения учебной практики

В результате прохождения учебной практики по виду профессиональной деятельности обучающихся 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

1.4.Количество часов на освоение рабочей программы учебной практики:

Всего - 108 часов, в том числе:
В рамках освоения ПМ.02 – 108 часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках модуля ППССЗ (ПМ.02) по основному виду профессиональной деятельности (ВПД), Эксплуатация автоматизированных (информационных) систем в защищенном исполнении необходимых для последующего освоения ими профессиональных (ПК) компетенций по специальности.

Код	Наименование результата освоения практики
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. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Код ПК	Код и наименование профессионального модуля	Количество часов по ПМ	Виды работ	Наименования тем учебной практики	Количество часов по темам
1	**2**	**3**		**4**	**5**
ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	108	– Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах – Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности – Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности – Составление документации по учету, обработке, хранению и передаче конфиденциальной информации – Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации – Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации	72
				Раздел 2 модуля. Применение криптографических средств защиты информации	36

			– Устранение замечаний по результатам проверки – Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. – Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи		
	ВСЕГО часов	**108**			**108**

3.2.Содержание учебной практики

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень освоения
1	2	3	4
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		108	
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации	Содержание	72	
	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах		1
	Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности		2
	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности		3
	Составление документации по учету, обработке, хранению и передаче конфиденциальной информации		3
	Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации		3
	Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.		3
	Устранение замечаний по результатам проверки		3
	Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.		3
Раздел 2 модуля. Применение криптографических средств защиты информации	Содержание	36	
	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи		3

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Учебная практика проводится в учебных кабинетах и компьютерных лабораториях ФГБОУ ВО «РЭУ им. Г.В.Плеханова».

Оборудование учебного кабинета: учебная классная доска, комплект учебной мебели, жалюзи, кондиционер

Оборудование лаборатории и рабочих мест лаборатории: компьютеры, объединенные в локальную сеть с возможностью выхода в Интернет, мультимедийное оборудование (проектор «BENQ», ноутбук «Toshiba», экран), принтер лазерный, программное обеспечение общего и профессионального назначения, комплект учебно-методической документации.

4.2. Общие требования к организации образовательного процесса

Учебная практика проводится концентрированно преподавателями профессионального цикла. Каждый студент имеет индивидуальное рабочее место.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляются руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий. В результате освоения учебной практики в рамках профессиональных модулей обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Оценка «отлично» - осуществляет установку и настройку отдельных программных, программно-аппаратных средств защиты информации. Оценка «хорошо» - частично осуществляет установку и/или настройку отдельных программных, программно-аппаратных средств защиты информации. Оценка «удовлетворительно» - имеет представление об осуществлении установки и/или настройки отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Оценка «отлично» - обеспечивает защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Оценка «хорошо» - частично обеспечивает защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Оценка «удовлетворительно» - имеет представление об обеспечении защитой информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Оценка «отлично» - осуществляет тестирование функций отдельных программных и программно-аппаратных средств защиты информации Оценка «хорошо» - частично осуществляет тестирование функций отдельных программных и программно-аппаратных средств защиты информации Оценка «удовлетворительно» - имеет представление об осуществлении тестирования функций отдельных программных и программно-аппаратных средств защиты информаци
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Оценка «отлично» - осуществляет обработку, хранение и передачу информации ограниченного доступа. Оценка «хорошо» - частично осуществляет обработку, хранение и передачу информации ограниченного доступа. Оценка «удовлетворительно» - имеет представление об осуществлении обработки, хранении и передачи информации ограниченного доступа
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Оценка «отлично» - уничтожает информацию и носители информации с использованием программных и программно-аппаратных средств. Оценка «хорошо» - частично уничтожает информацию и носители информации с использованием программных и программно-аппаратных средств. Оценка «удовлетворительно» - имеет представление об уничтожении информации и носителей 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.	Оценка «отлично» - осуществляет регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. Оценка «хорошо» - частично осуществляет регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. Оценка «удовлетворительно» - имеет представление об осуществлении регистрации основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

6. ИСПОЛЬЗОВАННЫЕ МАТЕРИАЛЫ И ИНТЕРНЕТ-РЕСУРСЫ

6.1. Основные и дополнительные источники:

1. 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
2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с. https://znanium.com/bookread2.php?book=536932
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с. https://znanium.com/bookread2.php?book=536932
4. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений. https://znanium.com/bookread2.php?book=562922