

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)
Институт непрерывного профессионального образования



ТВЕРЖДАЮ
Директор ИНПО

Н. С. Сивцев
Н. С. Сивцев 2017г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)
ПРАКТИКИ

ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем

Специальность СПО 10.02.03 Информационная безопасность автоматизированных систем

Цикл **профессиональный**

Форма обучения **очная**

Вид учебной работы	Объем, час.	Виды проме- жуточн ой аттеста- ции	Семестры					
			1	2	3	4	5	6
Учебная практика, час.	108	ДЗ			+			
Производственная практика (по профилю специальности), час.	144	ДЗ				+		+

Ижевск, 2017

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ ПО МОДУЛЮ

ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем

1.1. Область применения программы

Рабочая программа учебной и производственной (по профилю специальности) практики по ПМ.01 «Эксплуатация подсистем безопасности автоматизированных систем» – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО

10.02.03	Информационная безопасность автоматизированных систем
код	наименование специальности СПО

в части освоения квалификации	техник по защите информации квалификация по ФГОС
-------------------------------	---

и вида профессиональной деятельности (ВПД):

- участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
- выполнять работы по администрированию подсистем безопасности автоматизированных систем.
- производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.
- организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.
- вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.
- понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
- организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.
- осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
- использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
- работать в коллективе и команде, обеспечивать их сплочение, эффективно общаться с коллегами, руководством, потребителями.
- ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
- самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
- быть готовым к смене технологий в профессиональной деятельности.
- исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).
- формулировать задачи логического характера и применять средства математической логики для их решения.
- владеть основными методами и средствами разработки программного обеспечения.

- производить установку и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

(указать виды профессиональной деятельности в соответствии с ФГОС СПО, по данному модулю)

Рабочая программа практики может быть использована в дополнительном профессиональном образовании, в профессиональной подготовке рабочей профессии **16199 «Оператор ЭВМ»**.

(указать возможности использования программы в дополнительном профессиональном образовании (указать направленность программ повышения квалификации и переподготовки) и профессиональной подготовке (указать направленность программы профессиональной подготовки))

1.2. Место практики в структуре ОПОП

Данная практика базируется на изучении следующих дисциплин и освоении профессиональных модулей: Основы информационной безопасности, Системы и сети передачи информации, Операционные системы, Базы данных

Изучение перечисленных дисциплин и профессиональных модулей готовит студентов к освоению профессиональных компетенций, соответствующих основным видам профессиональной деятельности, а также помогает освоить общие компетенции.

1.3. Цели и задачи учебной практики

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями, обучающейся в ходе освоения учебной практики, должен:

иметь практический опыт:

- эксплуатации компонентов подсистем безопасности автоматизированных систем, их диагностики, устранения отказов и восстановления работоспособности;
- администрирования подсистем безопасности автоматизированных информационных систем;
- установки компонентов подсистем безопасности автоматизированных информационных систем;

знать:

- состав и принципы работы автоматизированных систем, операционных систем и сред;
- принципы разработки алгоритмов программ;
- основные приемы программирования;
- модели баз данных;
- классификацию, принципы построения, физические основы работы периферийных устройств;
- основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;
- правила и нормы охраны труда, техники безопасности, промышленной санитарии и противопожарной защиты;
- основные понятия компьютерных сетей и их аппаратные компоненты;
- сетевые модели, протоколы и их установку в операционных системах;
- адресацию в сетях, организацию межсетевого взаимодействия.

уметь:

- эксплуатировать компоненты подсистем безопасности автоматизированных систем;
- обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации;
- осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем

- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы;
- использовать и оформлять техническую документацию в соответствии с действующими нормативными документами;
- выполнять регламенты техники безопасности;
- организовывать и конфигурировать компьютерные сети;
- работать с протоколами разных уровней;
- устанавливать и настраивать параметры современных сетевых протоколов;
- производить монтаж компьютерных сетей;
- осуществлять диагностику компьютерных сетей;
- устранять неисправности компьютерных сетей;

1.4. Виды проведения практики

1. Учебная практика (технологическая)
2. Производственная практика (по освоению рабочей профессии)
(Указываются формы проведения практики, определяемые направлением практики)

1.5. Рекомендуемое количество часов на освоение рабочей программы практики:

всего – 252 часов, в том числе:

на учебную практику 108 часов;

на производственную (по профилю специальности) практику – 144 часов.

1.6. Базы проведения практики

Студенты специальности проходят практику в следующих организациях и предприятиях города:

- Министерстве информатизации и связи УР
- В Управление Федеральной службы Государственной регистрации кадастра и картографии УР
- ОАО «ИЭМЗ Купол»
- Страховая компания «РЕСО»
- На кафедрах и отделах ИжГТУ

Указывается место проведения практики: кафедра, лаборатория вуза, организация, предприятие, фирма и т.д.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИКИ

Процесс прохождения практики направлен на формирование элементов следующих компетенций в соответствии с ФГОС СПО и ОПОП СПО по данной специальности:

Код	Наименование результата обучения
ПК 1.1	Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
ПК 1.2	Выполнять работы по администрированию подсистем безопасности автоматизированных систем.
ПК 1.3	Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.
ПК 1.4	Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.

ПК 1.5	Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.
ОК 4	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
ОК 6	Работать в коллективе и команде, обеспечивать их сплочение, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Быть готовым к смене технологий в профессиональной деятельности.
ОК 10	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).
ОК 11	Формулировать задачи логического характера и применять средства математической логики для их решения.
ОК 12	Владеть основными методами и средствами разработки программного обеспечения.
ОК 13	Производить установку и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных умений в рамках модуля ОПОП СПО по виду профессиональной деятельности (ВПД), необходимых для последующего освоения ими профессиональных (ПК) и общих (ОК) компетенций по избранной специальности.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИКИ

3.1. Тематический план практики по профессиональному модулю

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего часов практики	Практика	
			Учебная, часов	Производственная (по профилю специальности), часов
1	2	3	4	5
ПК.1.1-1.5	Раздел 1. Настройка и эксплуатация подсистем безопасности автоматизированных систем	126	54	72
	Раздел 2. Настройка и эксплуатация компьютерных сетей	126	54	72
ПП.01	Производственная практика по профилю специальности	252	108	144
	Всего:	252	108	144

3.2. Содержание учебной практики.

Учебная практика по освоению рабочей профессии (концентрированная)

Наименование разделов и междисциплинарных курсов профессионального модуля	Виды работ	Тематика заданий по виду работ	Количество часов
Раздел 1. Настройка и эксплуатация подсистем безопасности автоматизированных систем МДК 01.01. Эксплуатация подсистем безопасности автоматизированных систем	1. Проведение анализа потенциальных каналов и методов несанкционированного доступа к информации в выделенном помещении 2. Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем 3. Проверка технического состояния подсистем безопасности автоматизированных систем 4. Проведение технического обслуживания и текущего ремонта подсистем безопасности автоматизированных систем 5. Устранение отказов и восстановление работоспособности подсистем безопасности автоматизированных	- Изучить и определить потенциальных каналов и методов несанкционированного доступа к информации. - Изучить и определить возможностей несанкцио-нированного доступа к защищаемой информации - Выявить и оценить источники утечки информации по акустическим каналам.	54

	систем. 6.Проведение анализа возможностей несанкционированного доступа к защищаемой информации в выделенном помещении.		
Раздел 2. Настройка и эксплуатация компьютерных сетей МДК 01.02. Эксплуатация компьютерных сетей	1. Принципы объединения сетей. 2. Протоколы и стандарты сетей. 3. Исследование акустических каналов утечки информации.	- Изучить принципы объединения сетей. - Построение больших сетей: протоколы, адресация.	54

3.3. Содержание производственной (по профилю специальности) практики

Вид практики: технологическая

Наименование разделов и междисциплинарных курсов профессионального модуля	Виды работ	Тематика заданий по виду работ	Количество часов
Раздел 1. Настройка и эксплуатация подсистем безопасности автоматизированных систем МДК 01.01. Эксплуатация подсистем безопасности автоматизированных систем	1. Проектирование комплексной системы защиты информации на уровне модулей. 2.Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.	-Построение комплексной системы защиты информации. - Выполнение работ по администрированию подсистем безопасности автоматизированных систем.	72
Раздел 2. Настройка и эксплуатация компьютерных сетей МДК 01.02. Эксплуатация компьютерных сетей	1. Обмен информацией в сети 2. Построение локальных сетей. 3. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них. 4.Вести контроль информации в автоматизиро-ванных системах.	- Изучить технологии обмена информацией в сети - Протоколы и стандарты локальных сетей. - Оформление технической документации, связанную с эксплуатацией средств технической защиты	72

МИНОБРАЗОВАНИЯ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)
Институт непрерывного профессионального образования



УТВЕРЖДАЮ
Директор ИНПО

Н. С. Сивцев
 2017г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)
ПРАКТИКИ

ПМ.02 Применение программно-аппаратных средств обеспечения
информационной безопасности в автоматизированных системах

Специальность СПО 10.02.03 Информационная безопасность автоматизированных систем

Цикл профессиональный

Форма обучения очная

Вид учебной работы	Объем, час.	Виды проме- жуточн ой аттеста- ции	Семестры					
			1	2	3	4	5	6
Учебная практика, час.	108	ДЗ				+		
Производственная практика (по профилю специальности), час.	144	ДЗ				+		+

Ижевск, 2017

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

1.1. Область применения программы

Программа профессионального модуля – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО **10.02.03 Информационная безопасность автоматизированных систем** в части освоения основного вида профессиональной деятельности (ВПД): **Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах** соответствующих профессиональных компетенций (ПК):

ПК.2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

ПК.2.2. Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

ПК.2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

ПК.2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ПК.2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.

ПК.2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании, при освоении профессии рабочего в рамках специальности СПО 090305 «Информационная безопасность автоматизированных систем». Опыт работы не требуется.

ОК 1 - 12

ПК 2.1 - 2.6

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- применения программно-аппаратных средств обеспечения информационной безопасности;
- диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной

безопасности;

- мониторинга эффективности программно- аппаратных средств обеспечения информационной безопасности;
- обеспечения учета, обработки, хранения и передачи конфиденциальной информации;
- решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно- аппаратными средствами;

уметь:

- применять программно-аппаратные средства обеспечения информационной безопасности;
- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
- решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно- аппаратными средствами;

знать:

- методы и формы применения программно- аппаратных средств обеспечения информационной безопасности;
- особенности применения программно- аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
- типовые модели управления доступом;
- типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- типовые средства и методы ведения аудита и обнаружения вторжений;
- типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
- основные понятия криптографии и типовые криптографические методы защиты информации

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 966 часов, в том числе:

максимальной учебной нагрузки обучающегося – 714 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 476 часов;

самостоятельной работы обучающегося – 238 часов;

учебной и производственной практики – 252 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности **«Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах»**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 2.1	Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.
ПК 2.2.	Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
ПК 2.3.	Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.
ПК 2.4.	Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.
ПК 2.5.	Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.
ПК 2.6.	Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).
ОК 11.	Формулировать задачи логического характера и применять средства математической логики для их решения.
ОК 12.	Владеть основными методами и средствами разработки программного обеспечения.
ОК 13.	Производить установку и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

3.1.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля *	Всего часов (макс. учебная нагрузка и практики)	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов <i>если предусмотрена рассредоточенная практика</i>
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК.2.1-2.6	Раздел 1. Применение и настройка программно-аппаратных средств обеспечения информационной безопасности при эксплуатации автоматизированных систем.	411	238	115	30	119		54	-
	Раздел 2. Изучение и применение крипто-графических средств и методов защиты информации	411	238	115		119		54	-
	Производственная практика (по профилю специальности), часов	144							144
	Всего:	966	476	230	30	238		108	144

3.1. 2. Тематический план профессионального модуля «Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах»

	Наименование разделов, МДК и тем	Макс. Учебная нагрузка студентов, час	Количество аудиторных часов при очной (заочной) форме обучения					Самост. Работа	Практика	
			Всего	Теорет. Занятий	Лаб. работ	Практ. занятий	Курсов. раб. (проект)		Учебная	ответствен. (по
Раздел 1	Применение и настройка программно-аппаратных средств обеспечения информационной безопасности при эксплуатации автоматизированных систем.	357	238	108	70	60		119		
МДК 02.01	Программно-аппаратные средства обеспечения информационной безопасности	357	238	108	70	60		119		
Тема 1.1	Основные программно-аппаратные средства защиты информации	60	40	20	10	10		20		
Тема 1.2	Аутентификация и идентификация с помощью программно-аппаратных средств	114	74	34	20	20		40		
Тема 1.3	Защита информации программно-аппаратными средствами	183	124	54	40	30		59		
Раздел 2	Изучение и применение криптографических средств и методов защиты информации	357	238	108	70	30	30	119		
МДК 02. 02	Криптографические средства и методы защиты информации	357	238	108	70	30	30	119		
Тема 2.1	История криптографии. Простейшие шифры замены и перестановки. Основные понятия и задачи криптографии.	40	20	10	8	2		20		
Тема 2.2	Шифры с секретными и открытыми ключами Понятие криптографической стойкости шифров	92	62	34	20	8		30		
Тема 2.3	Поточные и блочные системы шифрования Стандарты шифрования и цифровой подписи	92	62	30	20	12		30		

Тема 2.4	Простейшие криптографические протоколы (методы идентификации и аутентификации) Проблемы выработки, хранения и распределения криптографических ключей	103	64	34	22	8		39		
	Курсовой проект	30	30				30			
	ВСЕГО:	714	476	216	140	90	30	238		
УП	Учебная практика	108							108	
ПП	Производственная практика по профилю специальности	144								144
	ИТОГО:	966	476	216	140	90	30	238	108	144

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)
Институт непрерывного профессионального образования



УТВЕРЖДАЮ
Директор ИНПО

Н. С. Сивцев

Н.С. Сивцев 2017г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)
ПРАКТИКИ

ПМ.03 Применение инженерно-технических средств обеспечения
информационной безопасности

Специальность СПО 10.02.03 Информационная безопасность автоматизированных систем

Цикл профессиональный

Форма обучения очная

Вид учебной работы	Объем, час.	Виды проме- жуточн ой аттеста- ции	Семестры					
			1	2	3	4	5	6
Учебная практика, час.	72	ДЗ					+	
Производственная практика (по профилю специальности), час.	72	ДЗ						+

Ижевск, 2017

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Применение инженерно-технических средств обеспечения информационной безопасности

1.1. Область применения программы

Программа профессионального модуля – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.03 **Информационная безопасность автоматизированных систем** в части освоения основного вида профессиональной деятельности (ВПД): **Применение инженерно-технических средств обеспечения информационной безопасности** соответствующих профессиональных компетенций (ПК):

ПМ3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПМ3.2. Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

ПМ3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

ПМ3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПМ3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании, при освоении профессии рабочего в рамках специальности СПО 090305 «Информационная безопасность автоматизированных систем». Опыт работы не требуется.

ОК 1 - 12

ПК 3.1 - 3.5

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- выявления технических каналов утечки информации;
- использования основных методов и средств инженерно-технической защиты информации;
- диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;
- участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
- решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

уметь:

- применять технические средства защиты информации;
- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами;

знать:

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для съема перехвата и анализа сигналов в технических каналах утечки информации;
- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам;
- номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 477 часов, в том числе:

максимальной учебной нагрузки обучающегося – 333 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 222 часов;

самостоятельной работы обучающегося – 111 часов;

учебной и производственной практики – 144 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности **«Применение инженерно-технических средств обеспечения информационной безопасности»**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1	Применять инженерно-технические средства обеспечения информационной безопасности.
ПК 3.2.	Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности..
ПК 3.3.	Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.
ПК 3.4.	Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.
ПК 3.5.	Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).
ОК 11.	Формулировать задачи логического характера и применять средства математической логики для их решения.
ОК 12.	Владеть основными методами и средствами разработки программного обеспечения.
ОК 13.	Производить установку и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«Применение инженерно-технических средств обеспечения информационной безопасности»

3.1.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов (макс. учебная нагрузка и практики)	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов <i>если предусмотрена рассредоточенная практика</i>
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК.3.1-3.5	Раздел 1. Изучение, применение и организация инженерно-технических средств обеспечения информационной безопасности	333	222	80	30	111		72	72
	Производственная практика (по профилю специальности), часов	72							72
	Всего:	477	222	80	30	111		72	72

3.1. 2. Тематический план профессионального модуля «Применение инженерно-технических средств обеспечения информационной безопасности»

	Наименование разделов, МДК и тем	Учебная нагрузка студентов,	Количество аудиторных часов при очной (заочной) форме обучения					Самост. Работа	Практика	
			Всего	теорет. Занятия	Лабор. работ	Практ. занятия	Курсов. в. раб.		Учебная	востребован. (по
Раздел 1	Изучение, применение и организация инженерно-технических средств обеспечения информационной безопасности	333	222	112	80		30	111	72	72
МДК 03.01	Применение инженерно-технических средств обеспечения информационной безопасности	333	222	112	80		30	111	72	72
Тема 1.1	Введение. Объекты информационной защиты и обеспечения информационной безопасности	16	12	8	4			4		
Тема 1.2	Угрозы безопасности информации	70	50	30	20			20		
Тема 1.3	Методы, способы и средства инженерно-технических средств обеспечения информационной безопасности	116	76	44	32			40		
Тема 1.4	Организация инженерно-технических средств обеспечения информационной безопасности	39	12	8	4			27		
Тема 1.5	Основы методического обеспечения инженерно-технических средств обеспечения информационной безопасности	62	42	22	20			20		
	Курсовой проект	30	30				30			
	ВСЕГО:	333	222	112	80		30	111	72	72
УП	Учебная практика	72							72	
ПП	Производственная практика по профилю специальности	72								72
	ИТОГО:	477	222	112	80		30	111	72	72

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)
Институт непрерывного профессионального образования



УТВЕРЖДАЮ
Директор ИНИО

Н. С. Сивцев
[Signature] 2017г.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ И ПРОИЗВОДСТВЕННОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)
ПРАКТИКИ

ПМ.04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

Специальность СПО 10.02.03 Информационная безопасность автоматизированных систем

Цикл **профессиональный**

Форма обучения **очная**

Вид учебной работы	Объем, час.	Виды проме- жуточн ой аттеста- ции	Семестры					
			1	2	3	4	5	6
Учебная практика, час.	108	ДЗ				+		
Производственная практика (по профилю специальности), час.	144	ДЗ				+		+

Ижевск, 2017

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

1.1. Область применения программы

Программа профессионального модуля – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО **10.02.03 Информационная безопасность автоматизированных систем** в части освоения основного вида профессиональной деятельности (ВПД): **Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих** соответствующих профессиональных компетенций (ПК):

П.К.4.1 Подготавливать к работе, настраивать и обслуживать аппаратное обеспечение и операционную систему персонального компьютера

П.К.4.2 Подготавливать к работе, настраивать и обслуживать периферийные устройства персонального компьютера и компьютерную оргтехнику.

П.К.4.3 Осуществлять ввод и обмен данными между персональным компьютером и периферийными устройствами и ресурсами локальных компьютерных сетей.

П.К.4.4 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных.

П.К.4.5 Осуществлять навигацию по ресурсам, поиск, ввод и передачу данных с помощью технологий и сервисов Интернета.

П.К.4.6 Создавать и обрабатывать цифровые изображения и объекты мультимедиа.

П.К.4.7 Обеспечивать меры по информационной безопасности.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании, при освоении профессии рабочего в рамках специальности СПО 090305 «Информационная безопасность автоматизированных систем». Опыт работы не требуется.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

Цель производственной практики – закрепить в ходе практической деятельности знания, умения и навыки, полученные в процессе обучения по специальности «Оператор ЭВМ».

Целью проведения практики является:

- закрепление знаний, полученных в процессе теоретического изучения предметов: «Информационные технологии», «Теории алгоритмов», «Технические средства информатизации», «Основы программирования»
- знакомство со структурой предприятия, с технологией сбора и обработки информации на ЭВМ;
- освоение работы оператора ЭВМ, получение навыков самостоятельной работы в качестве оператора;
- привитие навыков разработки программ с использованием различных систем программирования.

Практика на получение рабочей профессии может проводиться на предприятиях и учреждениях, имеющих ЭВМ.

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- ввода и обработки информации на электронно-вычислительных машинах;
- подготовки к работе вычислительной техники и периферийных устройств;

уметь:

- вести процесс обработки информации на ЭВМ;
- выполнять ввод информации в ЭВМ с носителей данных, каналов связи и вывод ее из машины;

- подготавливать носители данных на устройствах подготовки данных, выполнять запись, считывания, копирование и перезапись информации с одного вида носителей на другой;
- обеспечить проведение и управление вычислительным процессом в соответствии с порядком обработки программ пользователя на ЭВМ;
- устанавливать причины сбоев в работе ЭВМ в процессе обработки информации;
- соблюдать требования безопасности труда и пожарной безопасности;

знать:

- состав ЭВМ, функциональные узлы ЭВМ, их назначение и принципы работы,
- операционные системы, применяемые в ЭВМ,
- правила технической эксплуатации ЭВМ,
- периферийные внешние устройства, применяемые в ЭВМ,
- функциональные узлы, их назначение,
- виды и причины отказов в работе ЭВМ,
- нормы и правила труда и пожарной безопасности.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – 492 часов, в том числе:

максимальной учебной нагрузки обучающегося – 240 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 160 часов;

самостоятельной работы обучающегося – 80 часов;

учебной и производственной практики – 252 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности **Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 4.1	Подготавливать к работе, настраивать и обслуживать аппаратное обеспечение и операционную систему персонального компьютера.
ПК 4.2.	Подготавливать к работе, настраивать и обслуживать периферийные устройства персонального компьютера и компьютерную оргтехнику.
ПК 4.3.	Осуществлять ввод и обмен данными между персональным компьютером и периферийными устройствами и ресурсами локальных компьютерных сетей.
ПК 4.4.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных.
ПК 4.5.	Осуществлять навигацию по ресурсам, поиск, ввод и передачу данных с помощью технологий и сервисов Интернета.
ПК 4.6.	Создавать и обрабатывать цифровые изображения и объекты мультимедиа.
ПК 4.7.	Обеспечивать меры по информационной безопасности.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

3.1.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов (макс. учебная нагрузка и практики)	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности), часов <i>если предусмотрена рассредоточенная практика</i>
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК.4.1-4.7	Раздел 1. Организация и реализация профессиональной деятельности оператора электронно-вычислительных и вычислительных машин	540	192	80		96		108	144
	Производственная практика (по профилю специальности), часов								144
	Всего:	540	192	80		96		108	144

3.1. 2. Тематический план профессионального модуля

Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

	Наименование разделов, МДК и тем	Учебная нагрузка студентов,	Количество аудиторных часов при очной (заочной) форме обучения					Самост. Работа	Практика	
			Всего	теорет. Занятия	Лаб. работ	Практ. занятия	Курсов. раб.		Учебная	вост. (по
Раздел 1	Организация и реализация профессиональной деятельности оператора электронно-вычислительных и вычислительных машин	288	192	112	80			96		
МДК 04.01	Компьютерные технологии в профессиональной деятельности	288	192	112	80			96		
Тема 1.1	Введение. Информационные системы и применение компьютерной техники в профессиональной деятельности	10	6	6				4		
Тема 1.2	Технические средства. Архитектура электронно-вычислительных и вычислительных машин	20	14	10	4			6		
Тема 1.3	Текстовые редакторы. Графические редакторы.	18	12	8	4			6		
Тема 1.4	Системы управления базами данных СУБД	20	14	8	6			6		
Тема 1.5	Интегрированные среды. Обучающие и учебные программы. Программы технического обслуживания.	18	12	8	4			6		
Тема 1.6	Системные программы. Операционные системы и оболочки операционных систем.	32	22	12	10			10		
Тема 1.7	Защита информации.	34	24	14	10			10		
Тема 1.8	Разработка и распространение компьютерных вирусов. Антивирусные программы. Компьютерный вирус. Программы-детекторы. Программы-ревизоры. Программы-фильтры.	40	30	16	14			10		
Тема 1.9	Подделка компьютерной информации. Хищение компьютерной информации.	36	26	16	10			10		
Тема 1.10	Internet и его службы. Протоколы передачи данных.	24	18	10	8			6		
Тема 1.11	Сканеры. Носители информации. Карты памяти.	14	12	8	4			2		
Тема 1.12	Игры. Игровые программы. Мультимедиа.	22	18	12	6			4		

	ВСЕГО:	288	192	112	80			96		
УП	Учебная практика	108							108	
ПП	Производственная практика по профилю специальности	144								144
	ИТОГО:	540	192	112	80			96	108	144

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ижевский государственный технический университет имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)
Институт непрерывного профессионального образования



УТВЕРЖДАЮ
 директор ИНПО

Н. С. Сивцев
 2017г.

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ (ПРЕДДИПЛОМНОЙ) ПРАКТИКИ

Специальность СПО 10.02.03 Информационная безопасность автоматизированных систем

Цикл **профессиональный**

Форма обучения **очная**

Вид учебной работы	Объем, час.	Виды проме- жуточн ой аттеста- ции	Семестры					
			1	2	3	4	5	6
Производственная практика (преддипломная)	144	ДЗ						+

Ижевск, 2017

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Область применения программы

Рабочая программа производственной практики (преддипломной) – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО

<u>10.02.03</u>	<u>Информационная безопасность автоматизированных систем</u>
<i>код</i>	<i>наименование специальности СПО</i>
в части освоения квалификации	<u>техник по защите информации</u>

и основных видов профессиональной деятельности (ВПД):

1. Эксплуатация подсистем безопасности автоматизированных систем.
2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.
3. Применение инженерно-технических средств обеспечения информационной безопасности.
4. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (приложение к ФГОС).
 - Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
 - Выполнять работы по администрированию подсистем безопасности автоматизированных систем.
 - Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.
 - Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.
 - Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах
 - Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.
 - Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
 - Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.
 - Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.
 - Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.
 - Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
 - Применять инженерно-технические средства обеспечения информационной безопасности.
 - Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

- Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.
- Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.
- Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами

1.2. Место практики в структуре ОПОП

Преддипломная практика является частью производственной практики, завершающей профессиональную подготовку студентов. Преддипломная практика проводится после освоения студентом программ теоретического и практического обучения и сдачи всех видов промежуточной аттестации, предусмотренных РУП СПО.

1.3. Цели и задачи производственной практики (преддипломной)

Целями производственной практики (преддипломной) являются:

- углубление первоначального профессионального опыта;
- развитие общих и профессиональных компетенций.

Задачами производственной практики (преддипломной) являются:

- проверка готовности к самостоятельной трудовой деятельности;
- сбор и проработку материалов, необходимых для написания выпускной квалификационной работы по определенной теме.

1.4. Рекомендуемое количество часов на освоение рабочей программы производственной практики (преддипломной).

Всего – 144 часа.

1.5. Базы проведения практики

Студенты специальности проходят практику в следующих организациях и предприятиях города:

- Министерстве информатизации и связи УР
- В Управление Федеральной службы Государственной регистрации кадастра и картографии УР
- ОАО «ИЭМЗ Купол»
- Страховая компания «РЕСО»
- На кафедрах и отделах ИжГТУ

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Результатом освоения рабочей программы производственной практики (преддипломной) является овладение обучающимися видами профессиональной деятельности (ВПД), в том числе профессиональными (ПК) и общими (ОК) компетенциями по избранной специальности.

Код	Наименование результата обучения
ПК 1.1	Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
ПК 1.2	Выполнять работы по администрированию подсистем безопасности автоматизированных систем.
ПК 1.3	Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.

ПК 1.4	Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.
ПК 1.5	Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.
ПК 2.1	Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.
ПК 2.2	Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.
ПК 2.3.	Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.
ПК 2.4.	Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.
ПК 2.5.	Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.
ПК 2.6.	Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
ПК 3.1	Применять инженерно-технические средства обеспечения информационной безопасности.
ПК 3.2.	Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности..
ПК 3.3.	Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.
ПК 3.4.	Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.
ПК 3.5.	Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2.	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.
ОК 4.	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, обеспечивать их сплочение, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Ставить цели, мотивировать деятельность подчиненных, организовывать и

	контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Быть готовым к смене технологий в профессиональной деятельности.
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).
ОК 11	Формулировать задачи логического характера и применять средства математической логики для их решения.
ОК 12.	Владеть основными методами и средствами разработки программного обеспечения.
ОК 13.	Производить установку и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

3.1. Тематический план производственной практики (преддипломной)

Код профессиональных и общих компетенций	Наименование разделов практики	Объем часов
1	2	3
ПК 1.1 - ПК 1.5 ОК 1 - ОК 13.	Учебная практика (технологическая)	108
	Производственная практика (по освоению рабочей профессии)	144
ПК 1.1 - ПК 1.5 ОК 1 - ОК 13.	Учебная практика (технологическая)	108
	Производственная практика (по освоению рабочей профессии)	144
ПК 1.1 - ПК 1.5 ОК 1 - ОК 13.	Учебная практика (технологическая)	72
	Производственная практика (по освоению рабочей профессии)	72
	Всего часов	648

3.2. Содержание производственной практики (преддипломной)

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов
1	2	3
Вид работы:		252

ПМ.01 Эксплуатация подсистем безопасности автоматизированных систем		
Тема 1.1. Эксплуатация компьютерных систем защиты информации, определение, задачи и организация компьютерных систем защиты информации	Содержание	72
	1. Задачи комплексной системы защиты информации	
	2. Принципы организации компьютерных систем защиты информации.	
	3. Организация компьютерных систем защиты информации	
Тема 1.2 Методы нарушения целостности, доступности и конфиденциальности информации	Содержание	90
	1. Защиты информации от несанкционированного доступа через локальную сеть программными способами.	
	2. Определение нарушений доступности информации и информационных ресурсов.	
	3. Изучение потенциальных каналов и методов несанкционированного доступа к информации.	
Тема 1.3. Разработка и эксплуатация компьютерных систем защиты информации	Содержание	90
	1. Применение специальных технических средств обеспечения информационной безопасности.	
	2. Построение компьютерных систем защиты информации.	
	3. Расчет экономической выгоды использования компьютерных систем защиты информации.	
Вид работы: ПМ.02 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах		252
Тема 2.1. Объекты информационной защиты и обеспечения информационной безопасности	Содержание	80
	1. Решение задач по проведению работ по защите и обеспечения инженерно-технической средств защиты информации.	
	2. Оценка защищенности источников и носителей конфиденциальной информации.	

Тема 2.2 Методы, способы и средства инженерно-технических средств обеспечения информационной безопасности	Содержание	82
	1. Изучение цели и задачи инженерно-технических средств обеспечения информационной безопасности.	
	2. Охрана объектов. Изучение способов и средств инженерной защиты и технической охраны.	
Тема 2.3. Разработка мер защиты инженерно-технических средств обеспечения информационной безопасности	Содержание	90
	1. Составление энергетических расчетов каналов утечки на примере организации.	
	2. Моделирование каналов утечки. Формы представления результатов моделирования.	
	3. Определение путей проникновения злоумышленника к источнику информации	
Вид работы: ПМ.03 Применение инженерно-технических средств обеспечения информационной безопасности		144
Тема 3.1. Задачи программно-аппаратной защиты информации	Содержание	30
	1. Изучение защиты данных от несанкционированного доступа.	
	2. Составление протоколов аутентификации удалённого доступа в программных средствах Microsoft.	
Тема 3.2. Защита информации программно-аппаратными средствами	Содержание	54
	1. Защищенные сетевые протоколы.	
	2. Защита программ от несанкционированного копирования. Защита от компьютерных вирусов..	
	3. Защита от несанкционированного доступа.	
Тема 3.3. Изучение криптографических протоколов. Хранение и распределение криптографических ключей	Содержание	60
	1. Изучение и применение криптографических средств и методов защиты информации	
	2. Исследование свойств генераторов псевдо-случайных чисел. Протоколы, ключи, управление ключами.	
	3. Построение моделей шифров	
Всего		648

