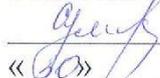


Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Колледж информатики и программирования

УТВЕРЖДАЮ

Заместитель директора по УПР и СР

 О.М. Сумлинова
«30» 06 2021 г.

РАБОЧАЯ ПРОГРАММА

производственной практики
по специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности
автоматизированных систем

ПМ.01 Эксплуатация автоматизированных (информационных) систем в
защищенном исполнении

ПМ.02 Защита информации в автоматизированных системах
программными и программно-аппаратными средствами

ПМ.03 Защита информации техническими средствами

2021 г.

Рабочая программа производственной практики разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 №15553. Зарегистрирован Министерством Юстиции Российской Федерации 26.12.2016, регистрационный № 44938

Организация-социальный партнер: ЗАО "ОКБ САПР"

Разработчики: Володин С.М.- к.т.н. преподаватель ВКК, Маринич А.Л. – преподаватель ИКК, Поколодина Е.В. – к.э.н., преподаватель ИКК, Рой А.В. – к.т.н. преподаватель ИКК, Филатов А.П.- преподаватель ИКК, Мирецкая Е.А.- методист ВКК.

Рецензент: Солдатов А.Б. - старший менеджер отдела по работе с ключевыми клиентами Департамента продаж Коммерческой дирекции Общества с ограниченной ответственностью «РусБИТех-Астра» ГК Astra Linux

Рабочая программа рассмотрена и рекомендована к утверждению на заседании предметной (цикловой комиссии) обеспечения информационной безопасности автоматизированных систем

Протокол № 10 от 19.05 2021г.

Председатель ЦК  С.М. Володин

Рабочая программа рассмотрена и одобрена Методическим советом Колледжа информатики и программирования Финансового университета при Правительстве Российской Федерации. Протокол № 3 от

24.06 2021г.

Согласована: Каннер Т.М., руководитель учебного центра ЗАО "ОКБ



М.П. от 24.06 2021г.

РЕЦЕНЗИЯ
на рабочую программу производственной практики

специальности среднего профессионального образования (СПО)
10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Рабочая программа производственной практики разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Рабочая программа производственной практики направлена на углубление первоначального практического опыта студента, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности.

Содержание представленной на рецензирование рабочей программы включает в себя следующие разделы:

1. Общая характеристика рабочей программы производственной практики
2. Структура и содержание производственной практики
3. Условия реализации производственной практики
4. Контроль и оценка результатов освоения производственной практики

В рабочей программе производственной практики определены цель и планируемые результаты освоения программы. Структура и содержание программы раскрывает последовательность этапов подготовки к выпускной квалификационной работе. Объем часов соответствует учебному плану. В разделе 3 перечислены предприятия – партнеры Финансового университета, профиль деятельности которых соответствует специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. В разделе 4 определены формы и методы контроля результатов обучения, требования к отчетной документации.

Представленная на рецензирование рабочая программа соответствует ФГОС по специальности и рекомендуется для использования в учебном процессе при подготовке обучающихся по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рецензент: Солдатов А.Б. - старший менеджер отдела по работе с ключевыми клиентами Департамента продаж Коммерческой дирекции Общества с ограниченной ответственностью «РусБИТех-Астра» ГК Astra Linux

« 24 » 06. 2021г.



СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	стр. 5
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	14
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	25
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	27

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

ПМ.03 Защита информации техническими средствами

1.1. Цель и планируемые результаты освоения программы производственной практики

- формирование у обучающихся практических умений и приобретение первичного практического опыта в рамках освоения профессиональных модулей образовательной программы СПО по основным видам деятельности в соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.1.1. Перечень общих компетенций

Код	Общие компетенции
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК09.	Использовать информационные технологии в профессиональной деятельности.
ОК10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере

1.1.2.Перечень профессиональных компетенций:

Код	Профессиональные компетенции
ПМ. 01	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении:
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
ПМ.02	Защита информации в автоматизированных системах программными и программно-аппаратными средствами:
ПК 2.1.	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.

ПМ.03	Защита информации техническими средствами
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.2.3. В результате прохождения производственной практики обучающийся должен:

Вид деятельности: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
иметь практический опыт	<ul style="list-style-type: none"> - установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; - администрирования автоматизированных систем в защищенном исполнении, <i>контроля стабильности характеристик системы защиты информации (06.033 А/01.5);</i> - эксплуатации компонентов систем защиты информации автоматизированных систем, <i>их диагностике, устранении отказов и восстановлении работоспособности, контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации (06.033 А/01.5);</i> - диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении; - <i>установки и настройки операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности*;</i> - <i>обнаружения и устранения ошибок при передаче данных в компьютерных сетях*;</i> - <i>работы с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP)*.</i>
уметь	- осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном

	<p>исполнении компонент систем защиты информации автоматизированных систем;</p> <ul style="list-style-type: none"> - организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; - осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; - производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; - настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; - обеспечивать работоспособность, обнаруживать и устранять неисправности, - обеспечивать <i>проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения (06.032 А/03.05);</i> - устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами (06.032 А/02.05); - формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;* - создавать, редактировать и обслуживать автоматизированную систему управления предприятием на базе «1С: Предприятие»;* - проверять правильность передачи данных.*
<p>знать</p>	<ul style="list-style-type: none"> - состав и принципы работы автоматизированных систем, операционных систем и сред, <i> типовые уязвимости программного обеспечения, методы их эксплуатации и порядок обеспечения безопасности информации при эксплуатации программного обеспечения (06.032 А/03.05);</i> - принципы разработки алгоритмов программ, основных приемов программирования, <i>особенности источников угроз, связанных с эксплуатацией программного обеспечения (06.032 А/03.05);</i> - модели баз данных, <i>порядок настройки систем управления базами данных и средств электронного документооборота (06.032 А/03.05);</i> - <i>эксплуатационную и проектную документацию, регламенты по уничтожению информации и машинных носителей информации автоматизированной системы (06.033 А/02.05, А/03.5);</i> - принципы построения, физические основы работы периферийных устройств,

	<ul style="list-style-type: none"> – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации (06.032 А/02.05); – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях, <i>порядок обеспечения безопасности информации при эксплуатации компьютерных сетей</i> (06.032 А/02.05); - принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; – принципы <i>построения и функционирования современных операционных систем, примеры их реализаций</i>;* – состав <i>программно-аппаратных средств обеспечения информационной безопасности в типовых операционных системах</i>;* – адресацию в сетях, организацию межсетевого взаимодействия;* – основные <i>этапы разработки простого прикладного решения в системе «1С:Предприятие»</i>*
<p>Вид деятельности: Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p>	
<p>иметь практический опыт</p>	<ul style="list-style-type: none"> – установки и настройки программных средств защиты информации (06.032 А/01.5) в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации (06.032 А/01.5); – 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, <i>информирование персонала об угрозах безопасности информации</i> (06.033 А/02.5) – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе; – <i>применения технологии фильтрации различных видов трафика,</i> – <i>осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого</i>

	<i>перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.*</i>
уметь	<ul style="list-style-type: none"> – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями (06.032 А/01.5); – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации, <i>проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах</i> (06.032 А/01.5); – 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 (06.033 А/03.5); – применять средства гарантированного уничтожения 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; – <i>оформлять эксплуатационную документацию программно-аппаратных средств защиты информации</i> (06.032 А/01.5); – <i>определять цели и задачи в изучении проекта;</i> – <i>разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;</i> – <i>осуществлять установку, развёртывание, настройку и использованием DLP-систем.*</i>

<p>знать</p>	<ul style="list-style-type: none"> - особенности и способы применения программных и программно-аппаратных средств защиты информации в автоматизированных системах (06.033 А/01.5), 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 (06.033 А/01.5); – основные понятия криптографии и типовых криптографических методов и средств защиты информации; <i>общие принципы функционирования средств защиты информации, в том числе и криптографической защиты информации</i> (06.033 А/01.5), – 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 (06.033 А/01.5); – <i>теоретические основы корпоративной защиты информации от внутренних ИТ-угроз; методiku проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; современные стандарты и средства корпоративной защиты.</i> *
<p>Вид деятельности: Защита информации техническими средствами</p>	
<p>иметь практический опыт</p>	<ul style="list-style-type: none"> – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

	<ul style="list-style-type: none"> – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – <i>технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок(06.034 А/01.5)*;</i> – <i>технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам(06.034 А/02.5)*.</i>
уметь	<ul style="list-style-type: none"> – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом, <i>технических средств защиты акустической речевой информации от утечки по техническим каналам (06.034 А/02.5);</i> – применять инженерно-технические средства физической защиты объектов информатизации, <i>производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов (06.034 А/01.5)*.</i> – <i>составлять план работы, тезисы доклада (выступления), конспекты лекций, первоисточников;</i> – <i>работать с источниками учебной информации, пользоваться ресурсами библиотеки (в том числе электронными), образовательными ресурсами сети Интернет, в том числе с учетом имеющихся ограничений здоровья;</i> – <i>выступить с докладом или презентацией перед аудиторией, вести дискуссию и аргументированно отстаивать собственную позицию*</i>

<p>знать</p>	<ul style="list-style-type: none"> – порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – <i>порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации (06.034 А/01.5)*;</i> – <i>нормативно правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации (06.034 А/01.5)*;</i> – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам* и физической защиты объектов информатизации. (06.034 А/01.5) – <i>особенности интеллектуального труда студента на различных видах аудиторных занятий;</i> – <i>основы методики самостоятельной работы*.</i>
--------------	--

1.2. Количество часов на освоение рабочей программы производственной практики:

Всего 468 часов, в том числе:

в рамках освоения ПМ.01 (ПП 01.01) – 5 нед., 180 ч.;

в рамках освоения ПМ.02 (ПП 02.01) – 4 нед., 144 ч.;

в рамках освоения ПМ.03 (ПП.03.01) – 4 нед., 144 ч.;

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

2.1. Структура производственной практики

Коды профессиональных и общих компетенций	Код и наименование профессиональных модулей	Суммарный объём нагрузки, час.	Виды работ	Наименование тем производственной практики	Количество часов по темам
ПК 1.1.-1.4. ОК.01-ОК.11	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	5 нед./180 ч	Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации Обслуживание средств защиты информации прикладного и системного программного обеспечения Настройка программного обеспечения с соблюдением требований по защите информации Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением Настройка встроенных средств защиты информации программного обеспечения Проверка функционирования встроенных средств защиты	Тема 1. Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	12
				Тема 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения	12
				Тема 3. Проведение настройки программного обеспечения с соблюдением требований по защите информации	12
				Тема 4. Проведение настройки средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	6
				Тема 5. Проведение инструктажа пользователей о соблюдении требований по защите информации при работе с программным обеспечением	12

			<p>информации программного обеспечения</p> <p>Своевременное обнаружение признаков наличия вредоносного программного обеспечения</p> <p>Составление организационной структуры управления предприятием – базы практики*</p> <p>Анализ программной и технической архитектуры ИС предприятия*</p> <p>Определение места проектируемой задачи в комплексе задач и ее описание*</p> <p>Анализ информационных потоков проектируемой задачи*</p> <p>Анализ системы обеспечения информационной безопасности и защиты информации*</p> <p>Анализ существующих разработок для автоматизации задачи*</p> <p>Выбор и обоснование стратегии автоматизации задачи*</p> <p>Выбор и обоснование способа приобретения ИС для автоматизации комплекса задач*</p> <p>Обслуживание средств защиты информации в компьютерных системах и сетях</p> <p>Обслуживание систем защиты информации в автоматизированных системах</p> <p>Участие в проведении регламентных работ по</p>	<p>Тема 6. Проведение настройки встроенных средств защиты информации программного обеспечения</p> <p>Тема 7. Проведение проверки функционирования встроенных средств защиты информации программного обеспечения</p> <p>Тема 8. Обнаружение признаков наличия вредоносного программного обеспечения</p> <p>Тема 9. Составление организационной структуры управления предприятием – базы практики</p> <p>Тема 10. Проведение анализа программной и технической архитектуры ИС предприятия.</p> <p>Тема 11. Определение места проектируемой задачи в комплексе задач и ее описание. Анализ информационных потоков проектируемой задачи.</p> <p>Тема 12. Проведение анализа системы обеспечения информационной безопасности и защиты информации. Анализ существующих разработок для автоматизации задачи.</p>	<p>12</p> <p>6</p> <p>12</p> <p>12</p> <p>6</p> <p>12</p> <p>6</p>
--	--	--	--	---	--

			<p>эксплуатации систем защиты информации автоматизированных систем</p> <p>Проверка работоспособности системы защиты информации автоматизированной системы</p> <p>Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации</p> <p>Контроль стабильности характеристик системы защиты информации автоматизированной системы</p> <p>Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем</p> <p>Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем</p>	<p>Тема 13. Выбор и обоснование стратегии автоматизации задачи. Выбор и обоснование способа приобретения ИС для автоматизации комплекса задач.</p> <p>Тема 14. Обслуживание средств защиты информации в компьютерных системах и сетях. Обслуживание систем защиты информации в автоматизированных системах</p> <p>Тема 15. Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем</p> <p>Тема 16. Проведение проверки работоспособности системы защиты информации автоматизированной системы</p> <p>Тема 17. Проведение контроля соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации. Контроль стабильности характеристик системы защиты информации автоматизированной системы</p> <p>Тема 18. Ведение технической документации, связанной с эксплуатацией систем защиты</p>	<p>12</p> <p>6</p> <p>6</p> <p>12</p> <p>6</p> <p>6</p>
--	--	--	--	--	---

				информации автоматизированных систем Тема 19. Проведение работ по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	12
ПК 2.1-2.6. ОК.01-ОК.11	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	4 нед./144 ч	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 при выполнении задач практики;	Тема 1. Анализ принципов построения систем информационной защиты производственных подразделений; Тема 2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы; Тема 3. Диагностирование, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности;	12
				Тема 4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении;	12
				Тема 5. Обеспечение учета, обработки, хранения и	12
					12
					12

			<p>Администрирование автоматизированных технических средств управления и контроля информации и информационных потоков*</p> <p>Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом*</p> <p>Выявление потоков передачи данных и возможных каналов утечки информации*</p> <p>Использование механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов*</p> <p>Проведение детектирования атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме.*</p>	<p>передачи конфиденциальной информации;</p> <p>Тема 6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики;</p> <p>Тема 7. Администрирование автоматизированных технических средств управления и контроля информации и информационных потоков.</p> <p>Тема 8. Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.</p> <p>Тема 9.Выявление потоков передачи данных и возможных каналов утечки информации.</p> <p>Тема10. Использование механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов</p> <p>Тема 11. Проведение детектирования атак (потенциальных угроз) в</p>	<p>18</p> <p>12</p> <p>18</p> <p>12</p> <p>12</p> <p>12</p>
--	--	--	--	---	---

				ручном, автоматизированном и автоматическом режиме.	
ПК 3.1-3.5. ОК.01-ОК.11	ПМ.03 Защита информации техническими средствами	4 нед./144ч	Анализ объектов информатизации предприятий, учреждений и организаций*.	Тема 1. Проведение анализа объектов информатизации предприятий, учреждений и организаций.	18
			Анализ ресурсов обеспечения инженерно-технической защиты информации*.	Тема 2. Проведение анализа ресурсов обеспечения инженерно-технической защиты информации.	18
			Изучение основных этапов проектирования системы защиты информации техническими средствами*.	Тема 3. Основные этапы проектирования системы защиты информации техническими средствами.	18
			Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации.	Тема 4. Монтаж, обслуживание и эксплуатация технических средств защиты информации.	18
			Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.	Тема 5. Монтаж, обслуживание и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.	18
			Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам.	Тема 6. Монтаж, обслуживание и эксплуатация средств защиты информации от несанкционированного съёма и утечки по техническим каналам.	18
			Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. Оценка эффективности защиты информации*.	Тема 7. Применение нормативно правовых актов, нормативных методических	18

				документов по обеспечению защиты информации техническими средствами. Тема 8. Оценка эффективности защиты информации.	18
	Всего часов	468			

2.2. Тематический план и содержание производственной практики

Профессиональные модули и междисциплинарные курсы, темы	Содержание практики	Объём часов
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении МДК.01.01 Операционные системы МДК.01.02 Базы данных МДК.01.03 Сети и системы передачи информации МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении МДК.01.05. Эксплуатация компьютерных сетей		180
Тема 1. Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации Тема 2. Обслуживание средств защиты информации прикладного и системного программного обеспечения Тема 3. Проведение настройки программного обеспечения с соблюдением требований по защите информации Тема 4. Проведение настройки средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	Установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем. Администрирование автоматизированных систем в защищенном исполнении, контроля стабильности характеристик системы защиты информации. Эксплуатация компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности, контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации. Диагностика компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных	

<p>Тема 5. Проведение инструктажа пользователей о соблюдении требований по защите информации при работе с программным обеспечением</p> <p>Тема 6. Проведение настройки встроенных средств защиты информации программного обеспечения</p> <p>Тема 7. Проведение проверки функционирования встроенных средств защиты информации программного обеспечения</p> <p>Тема 8. Обнаружение признаков наличия вредоносного программного обеспечения</p> <p>Тема 9. Составление организационной структуры управления предприятием – базы практики</p> <p>Тема 10. Проведение анализа программной и технической архитектуры ИС предприятия.</p> <p>Тема 11. Определение места проектируемой задачи в комплексе задач и ее описание. Анализ информационных потоков проектируемой задачи.</p> <p>Тема 12. Проведение анализа системы обеспечения информационной безопасности и защиты информации. Анализ существующих разработок для автоматизации задачи.</p> <p>Тема 13. Выбор и обоснование стратегии автоматизации задачи. Выбор и обоснование способа приобретения ИС для автоматизации комплекса задач.</p> <p>Тема 14. Обслуживание средств защиты информации в компьютерных системах и сетях. Обслуживание систем защиты информации в автоматизированных системах</p> <p>Тема 15. Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем</p> <p>Тема 16. Проведение проверки работоспособности системы защиты информации автоматизированной системы</p> <p>Тема 17 Проведение контроля соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации. Контроль стабильности характеристик системы защиты информации автоматизированной системы</p>	<p>(информационных) систем в защищенном исполнении. Установка и настройки операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности. Обнаружение и устранения ошибок при передаче данных в компьютерных сетях. Работа с протоколами разных уровней.</p>	
--	--	--

<p>Тема 18. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем</p> <p>Тема 19. Проведение работ по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем</p>		
<p>ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>МДК.02.01. Программные и программно-аппаратные средства защиты информации</p> <p>МДК.02.02. Криптографические средства защиты информации</p> <p>МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности</p>		144
<p>Тема 1. Анализ принципов построения систем информационной защиты производственных подразделений;</p> <p>Тема 2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы;</p> <p>Тема 3. Диагностирование, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности;</p> <p>Тема 4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении;</p> <p>Тема 5. Обеспечение учета, обработки, хранения и передачи конфиденциальной информации;</p> <p>Тема 6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики;</p> <p>Тема 7. Администрирование автоматизированных технических средств управления и контроля информации и информационных потоков.</p> <p>Тема 8. Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.</p>	<p>Установка и настройка программных средств защиты информации в автоматизированной системе. Обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами. Тестирование функций, диагностика, устранение отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации. Решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации. Применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных. Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности, информирование персонала об угрозах безопасности информации.</p> <p>Работа с подсистемами регистрации событий;</p> <p>Выявление событий и инцидентов безопасности в автоматизированной системе. Применение технологии фильтрации различных видов трафика. Осуществление фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку</p>	

<p>Тема 9.Выявление потоков передачи данных и возможных каналов утечки информации.</p> <p>Тема10. Использование механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов</p> <p>Тема 11. Проведение детектирования атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме.</p>	<p>определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности.</p>	
<p>ПМ. 03 Защита информации техническими средствами</p> <p>МДК.03.01 Техническая защита информации</p> <p>МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации</p> <p>МДК 03.03 Физические основы защиты информации</p>		144
<p>Тема 1. Проведение анализа объектов информатизации предприятий, учреждений и организаций.</p> <p>Тема 2. Проведение анализа ресурсов обеспечения инженерно-технической защиты информации.</p> <p>Тема 3. Основные этапы проектирования системы защиты информации техническими средствами.</p> <p>Тема 4. Монтаж, обслуживание и эксплуатация технических средств защиты информации.</p> <p>Тема 5. Монтаж, обслуживание и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.</p> <p>Тема 6. Монтаж, обслуживание и эксплуатация средств защиты информации от несанкционированного съёма и утечки по техническим каналам.</p> <p>Тема 7. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.</p> <p>Тема 8. Оценка эффективности защиты информации.</p>	<p>Установка, монтаж и настройка технических средств защиты информации. Техническое обслуживание технических средств защиты информации. Применение основных типов технических средств защиты информации. Выявление технических каналов утечки информации. Участие в мониторинге эффективности технических средств защиты информации. Диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации. Проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации. Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. Установка, монтажа и настройка, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. Установка, монтаж и настройка, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. Техническое обслуживание,</p>	

диагностика, устранение отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок. Техническое обслуживание, диагностика, устранение отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение

Производственная практика проходит в организациях с которыми заключены договоры о проведении практики.

- Федеральная служба государственной статистики по г. Москве (Мосгорстат), Договор № 01/2012 от 03.09.2012;
- ФГУП «НПП «Пульсар», Договор № ДИР/4740 от 01.07.2014;
- ФГБУ «Транспортный комбинат «Россия» Управления делами Президента, Договор № 01/2015 от 15.06.2015;
- ЗАО «Научно-производственный центр информационных региональных систем», Договор № 3/2015 от 25.10.2015;
- ООО Самсунг Электроникс, Договор №и 4/2015 от 28.10.2015;
- ООО «ЦЛОТ «Здоровье», Договор №6/2015 от 01.11.2015;
- ФБУ Российский федеральный центр судебной экспертизы при Министерстве юстиции РФ, Договор № 02/2015 от 08.09.2015;
- Аппарат Совета депутатов муниципального округа «Аэропорт», Договор №76-СР/2016 от 30.12.2016;
- ООО «Дело Системы», Договор № 01/КИП-18/67а-СР/2018 от 09.01.2018;
- ООО «Такском», Договор №02/2013 от 09.04.2013;
- По гарантийным письмам и договорам о проведении практики обучающимся от предприятий.

Для прохождения производственной практики организациями предоставляются автоматизированные рабочие места с программным обеспечением соответствующим профилю профессионального модуля производственной практики.

Руководство практикой осуществляется преподавателями профессионального цикла.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Контроль и оценка результатов освоения производственной практики осуществляются с использованием следующих форм и методов: наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики). В результате освоения производственной практики в рамках профессионального модуля студенты проходят промежуточную аттестацию в форме дифференцированного зачёта.

Результаты обучения (освоенные умения, практический опыт в рамках вида деятельности)	Формы и методы контроля и оценки результатов обучения
Вид деятельности: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> - установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; - администрирования автоматизированных систем в защищенном исполнении, контроля стабильности характеристик системы защиты информации (06.033 А/01.5); - эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности, контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации (06.033 А/01.5); - диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении; - установки и настройки операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности*; - обнаружения и устранения ошибок при передаче данных в компьютерных сетях*; - работы с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP)*. <p>Уметь:</p> <ul style="list-style-type: none"> - осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; - организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять 	<p>Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики)</p>

<p>неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;</p> <ul style="list-style-type: none"> - осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; - производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; - настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; - обеспечивать работоспособность, обнаруживать и устранять неисправности, - обеспечивать проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения (06.032 А/03.05); - устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами (06.032 А/02.05); - формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;* - создавать, редактировать и обслуживать автоматизированную систему управления предприятием на базе «1С: Предприятие»; - проверять правильность передачи данных.* 	
<p>Вид деятельности: Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p>	
<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> - установки и настройки программных средств защиты информации (06.032 А/01.5) в автоматизированной системе; - обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; - тестирования функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации (06.032 А/01.5); - 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, информирование персонала об угрозах безопасности информации (06.033 А/02.5) - работы с подсистемами регистрации событий; 	<p>Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики)</p>

– выявления событий и инцидентов безопасности в автоматизированной системе;

– применения технологии фильтрации различных видов трафика,

Уметь:

– осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.*

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

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями (06.032 А/01.5);

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации, проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах (06.032 А/01.5);

– 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 (06.033 А/03.5);

– применять средства гарантированного уничтожения 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;

– оформлять эксплуатационную документацию программно-аппаратных средств защиты информации (06.032 А/01.5);

– определять цели и задачи в изучении проекта;

– разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;

– осуществлять установку, развёртывание, настройку и использованием DLP-систем.*

- особенности и способы применения программных и программно-аппаратных средств защиты информации в автоматизированных системах (06.033 А/01.5), в том

<p>числе, в операционных системах, компьютерных сетях, базах данных;</p> <ul style="list-style-type: none"> – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации (06.033 А/01.5); – основные понятия криптографии и типовых криптографических методов и средств защиты информации; общие принципы функционирования средств защиты информации, в том числе и криптографической защиты информации (06.033 А/01.5), – 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 (06.033 А/01.5); – теоретические основы корпоративной защиты информации от внутренних ИТ-угроз; методику проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; современные стандарты и средства корпоративной защиты. * 	
<p>Вид деятельности: Защита информации техническими средствами</p>	
<p>Иметь практический опыт:</p> <ul style="list-style-type: none"> – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и 	<p>Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики)</p>

<p>неисправностей, восстановления работоспособности инженерно-технических средств физической защиты;</p> <ul style="list-style-type: none">– технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок(06.034 А/01.5)*;– технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам(06.034 А/02.5)*. <p>Уметь:</p> <ul style="list-style-type: none">– применять технические средства для криптографической защиты информации конфиденциального характера;– применять технические средства для уничтожения информации и носителей информации;– применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом, технических средств защиты акустической речевой информации от утечки по техническим каналам (06.034 А/02.5);– применять инженерно-технические средства физической защиты объектов информатизации, производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов (06.034 А/01.5)*.– составлять план работы, тезисы доклада (выступления), конспекты лекций, первоисточников;– работать с источниками учебной информации, пользоваться ресурсами библиотеки (в том числе электронными), образовательными ресурсами сети Интернет, в том числе с учетом имеющихся ограничений здоровья;– выступать с докладом или презентацией перед аудиторией, вести дискуссию и аргументированно отстаивать собственную позицию*	
---	--