**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**

**РАБОЧАЯ ПРОГРАММА ПРАКТИКИ**

# Б2.Б.04(Пд) Производственная (преддипломная) практика

**Специальность: 10.05.03 - Информационная безопасность автоматизированных систем**

**Специализация: Информационная безопасность автоматизированных систем критически важных объектов**

**Квалификация выпускника**: **специалист**

**Форма обучения: очная**

## 1 АННОТАЦИЯ

1.1 Практика Преддипломная практика (далее по тексту – практика) входит в состав практики основной образовательной программы высшего профессионального образования (далее по тексту ОПОП ВПО) и учебного плана подготовки специалистов по специальности 10.05.03 – Информационная безопасность автоматизированных систем специализация – Информационная безопасность автоматизированных систем критически важных объектов

1.2 Практика проходит в __10___ семестре ___5___ курса и состоит из взаимосвязанных этапов (подготовительного, аналитического, заключительного), предполагающих выдачу индивидуального задания студенту, инструктаж по технике безопасности; консультацию научного руководителя, изучение методических и рекомендательных материалов, нормативных документов.

## 2 ВИД ПРАКТИКИ, СПОСОБЫ И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ

2.1 Вид практики: Производственная (преддипломная) практика

Основная цель проведения преддипломной практики – выполнение выпускной квалификационной работы.

2.2 Способы проведения практики: стационарная и (или) выездная

Проведение практики может осуществляться следующими способами: в качестве стационарной и (или) выездной практики.

Стационарная практика проводится в образовательной организации или ее филиале, в котором обучающиеся осваивают образовательную программу, или в иных организациях, расположенных на территории населенного пункта, в котором расположена образовательная организация или филиал. Выездная практика проводится в том случае, если место ее проведения расположено вне населенного пункта, в котором расположена образовательная организация или филиал. Выездная практика может проводится в полевой форме в случае необходимости создания специальных условий для ее проведения.

2.3 Форма проведения практики:

Дискретно по видам практик – путем выделения в календарном учебном графике непрерывного периода учебного времени для поведения каждого вида (совокупности видов) практики.

## 3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1 Взаимосвязь планируемых результатов обучения при прохождении практики (знания, умения, навыки и (или) опыт деятельности) и планируемых результатов освоения образовательной программы (компетенций обучающегося) представлена в таблице 1.

**Таблица 1. Взаимосвязь планируемых результатов обучения при прохождении практики и планируемых результатов освоения образовательной программы**

| Индекс и содержание компетенции | Знания | Умения | Навыки и (или) опыт деятельности |
|---|---|---|---|
| ПК-1 способностью осуществлять поиск, | Этап 1: основные методы поиска | Этап 1: осуществлять | Этап 1: осуществления |

| | | | |
|---|---|---|---|
| изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке | научно – технической и нормативной литературы<br>Этап 2: основные методические материалы по вопросам информационной безопасности | подбор литературы по информационной безопасности<br>Этап 2: уметь обобщать и составлять краткий обзор литературы по информационной безопасности | подбора литературы по информационной безопасности<br>Этап 2: умения обобщения и составления обзора литературы по информационной безопасности |
| ПК-2 способностью создавать и исследовать модели автоматизированных систем | Этап 1: базовые понятия основ моделирования<br>Этап 2: модели автоматизированных систем | Этап 1: использовать методы моделирования для создания моделей<br>Этап 2: использовать структурные модели | Этап 1: использования методов моделирования для создания моделей<br>Этап 2: использования структурных моделей |
| ПК-3 способностью проводить анализ защищенности автоматизированных систем | Этап 1: методику анализа защищенности автоматизированных систем<br>Этап 2: современные стандарты в области информационной безопасности | Этап 1: разрабатывать методику анализа защищенности автоматизированных систем<br>Этап 2: использовать стандарты в области информационной безопасности | Этап 1: разработки анализа защищенности автоматизированных систем<br>Этап 2: использования стандартов в области информационной безопасности |
| ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы | Этап 1основные модели угроз информационной безопасности<br>Этап 2: модели нарушителей информационной безопасности | Этап 1: разрабатывать модели угроз информационной безопасности<br>Этап 2: разрабатывать модели нарушителей информационной безопасности | Этап 1: разработки модели угроз информационной безопасности<br>Этап 2: разработки модели нарушителей информационной безопасности |
| ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы | Этап 1: основные риски информационной безопасности<br>Этап 2: основные этапы анализа рисков информационной безопасности | Этап 1: рассчитывать риски информационной безопасности<br>Этап 2: разрабатывать методику анализа рисков информационной безопасности | Этап 1: рассчета рисков информационной безопасности<br>Этап 2 разработки методики анализа рисков информационной безопасности |
| ПК-6 способностью | Этап1:- | Этап 1: выполнять | Этап 1: настройки и |

| | | | |
|---|---|---|---|
| проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | современные аппаратные средства вычислительной техники;<br>Этап 2: современные инструментальные средства и технологии программирования | работы по настройке аппаратно - программных комплексов<br>Этап 2: выполнять работы по настройке технических средств защиты информации | обслуживания аппаратно - программных комплексов<br>Этап 2: настройки технических средств защиты информации |
| ПК-7 способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ | Этап 1: основные методы поиска научно – технической и нормативной литературы<br>Этап 2: основные методические материалы по вопросам информационной безопасности | Этап 1: осуществлять подбор литературы по информационной безопасности<br>Этап 2: уметь обобщать и составлять краткий обзор литературы по информационной безопасности | Этап 1: осуществления подбора литературы по информационной безопасности<br>Этап 2: умения обобщения и составления обзора литературы по информационной безопасности |
| ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем | Этап 1: основные этапы проектирования подсистемы информационной безопасности<br>Этап 2: основные методы технико – экономического обоснования проектных решений | Этап 1: разрабатывать основные подсистемы безопасности информации<br>Этап 2: проводить технико – экономическое обоснование проектных решений | Этап 1: навыки разработки подсистем информационной безопасности<br>Этап 2: навыки технико - экономического обоснования проектных решений |
| ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности | Этап 1: основные этапы проектирования подсистемы информационной безопасности<br>Этап 2: основные методы технико – экономического обоснования проектных решений | Этап 1: разрабатывать основные подсистемы безопасности информации<br>Этап 2: проводить технико – экономическое обоснование проектных решений | Этап 1: навыки разработки подсистем информационной безопасности<br>Этап 2: навыки технико - экономического обоснования проектных решений |
| ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, | Этап 1: знать физические структуры и основные типы полупроводниковых приборов, их свойства и | Этап 1: уметь работать с современной элементной базой электронной аппаратуры; | Этап 1: владеть навыками чтения и составления принципиальных схем базовых функциональных узлов электронной |

| | | | |
|---|---|---|---|
| технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности | характеристики;<br>Этап 2: знать принципы выбора элементной базы для функциональных узлов электронной аппаратуры с учетом требований эксплуатации и экономической эффективности | Этап 2: уметь осуществлять обоснованный выбор структурных и принципиальных схем электронных устройств | аппаратуры;<br>Этап 2: владеть навыками оценки параметров электронных приборов и устройств по комплекту документации |
| ПК-11 способностью разрабатывать политику информационной безопасности автоматизированной системы | Этап 1основные составляющие политики безопасности<br>Этап 2: принципы разработки политики безопасности | Этап 1: разрабатывать политику безопасности<br>Этап 2: применять комплексный подход к обеспечению информационной безопасности | Этап 1: навыки разработки политики безопасности<br>Этап 2применения комплексного подхода к обеспечению информационной безопасности |
| ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы | Этап 1: основные этапы проектирования подсистемы информационной безопасности<br>Этап 2: основные методы технико – экономического обоснования проектных решений | Этап 1: разрабатывать основные подсистемы безопасности информации<br>Этап 2: проводить технико – экономическое обоснование проектных решений | Этап 1: навыки разработки подсистем информационной безопасности<br>Этап 2: навыки технико - экономического обоснования проектных решений |
| ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы | Этап 1: основные этапы проектирования подсистемы информационной безопасности<br>Этап 2: основные методы технико – экономического обоснования проектных решений | Этап 1: разрабатывать основные подсистемы безопасности информации<br>Этап 2: проводить технико – экономическое обоснование проектных решений | Этап 1: навыки разработки подсистем информационной безопасности<br>Этап 2: навыки технико - экономического обоснования проектных решений |
| ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и | Этап 1: основные этапы контрольных проверок технических средств защиты информации<br>Этап 2: основные принципы работы технических средств защиты информации | Этап 1: разрабатывать методику контрольных проверок технических средств защиты информации<br>Этап 2: разрабатывать | Этап 1: навыки применения контрольных проверок<br>Этап 2: навыки оценки эффективности применении аппаратно - |

| | | | |
|---|---|---|---|
| технических средств защиты информации | | способы оценки эффективности применения программных, аппаратных средств защиты информации | программных комплексов |
| ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем | Этап 1: методику проведения экспериментов<br>Этап 2: методику обработки, оценки результатов экспериментов | Этап 1: разрабатывать методику проведения экспериментов<br>Этап 2: разрабатывать методику обработки и оценки результатов эксперимента | Этап 1: разработки методики проведения экспериментов<br>Этап 2: разработки методики обработки и оценки результатов эксперимента |
| ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации | Этап 1: методику проведения экспериментов<br>Этап 2: методику обработки, оценки результатов экспериментов | Этап 1: разрабатывать методику проведения экспериментов<br>Этап 2: разрабатывать методику обработки и оценки результатов эксперимента | Этап 1: разработки методики проведения экспериментов<br>Этап 2: разработки методики обработки и оценки результатов эксперимента |
| ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации | Этап 1: методику анализа информационной безопасности<br>Этап 2: современные стандарты в области информационной безопасности | Этап 1: разрабатывать методику анализа информационной безопасности<br>Этап 2: использовать стандарты в области информационной безопасности | Этап 1: разработки анализа информационной безопасности<br>Этап 2: использования стандартов в области информационной безопасности |
| ПК-18 способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности | Этап 1: основные меры по выполнения обеспечения информационной безопасности<br>Этап 2: основные меры поддержки обеспечения информационной безопасности | Этап 1: разрабатывать меры по обеспечению информационной безопасности<br>Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности | Этап 1: разработки мер по обеспечению информационной безопасности<br>Этап 2: разработки мер поддержки обеспечения информационной безопасности |
| ПК-19 способностью разрабатывать предложения по | Этап 1: основные меры по выполнения обеспечения | Этап 1: разрабатывать меры по обеспечению | Этап 1: разработки мер по обеспечению информационной |

| | | | |
|---|---|---|---|
| совершенствованию системы управления информационной безопасностью автоматизированной системы | информационной безопасности<br>Этап 2: основные меры поддержки обеспечения информационной безопасности | информационной безопасности<br>Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности | безопасности<br>Этап 2: разработки мер поддержки обеспечения информационной безопасности |
| ПК-20 способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности | Этап 1: принципы разработки и внедрения информационных систем;<br>Этап 2: принципы эффективного применения автоматизированных информационных систем с учетом требований информационной безопасности | Этап 1: использовать методы разработки и внедрения информационных систем<br>Этап 2: реализовать разработку автоматизированной информационной системы с учетом требований информационной безопасности | Этап 1: методами разработки, внедрения, эксплуатации информационных систем<br>Этап 2: методами сопровождения информационных систем |
| ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем | Этап 1: основные этапы оформления рабочей документации<br>Этап 2: основные нормативные и методические документы | Этап 1: разрабатывать основные рабочие документы<br>Этап 2: применять нормативные документы в рабочей документации | Этап 1: навыки разработки рабочих документов<br>Этап 2: навыки применения нормативных документов |
| ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации | Этап 1основные составляющие политики безопасности<br>Этап 2: принципы разработки политики безопасности | Этап 1: разрабатывать политику безопасности<br>Этап 2: применять комплексный подход к обеспечению информационной безопасности | Этап 1: навыки разработки политики безопасности<br>Этап 2применения комплексного подхода к обеспечению информационной безопасности |
| ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа | Этап 1: основные принципы администрирования<br>Этап 2: современные инструментальные средства администрирования | Этап 1: проводить процедуру администрирования подсистемы безопасности<br>Этап 2: уметь использовать инструментальные средства | Этап 1: навыки администрирования подсистемы безопасности<br>Этап 2: навыки применения инструментальных средств администрирования |

| | | | |
|---|---|---|---|
| | | администрирования подсистемы безопасности | подсистемы безопасности |
| ПК-24 способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности | Этап 1: принципы эффективного применения информационно-технологических ресурсов;<br>Этап 2: принципы информационной безопасности | Этап 1: использовать методы эффективного применения информационно-технологических ресурсов<br>Этап 2: реализовать политику информационной безопасности | Этап 1: методами разработки, внедрения, эксплуатации информационно-технологических ресурсов<br>Этап 2: методами сопровождения информационно-технологических ресурсов |
| ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций | Этап 1: принципы эффективной реализации резервного копирования данных;<br>Этап 2: принципы информационной безопасности в процессах резервного копирования данных | Этап 1: использовать методы резервного копирования данных<br>Этап 2: реализовать политики информационной безопасности для процессов резервного копирования данных | Этап 1: методами разработки, внедрения, эксплуатации резервного копирования данных<br>Этап 2: методами сопровождения резервного копирования данных |
| ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы | Этап 1: основные принципы администрирования<br>Этап 2: современные инструментальные средства администрирования | Этап 1: проводить процедуру администрирования подсистемы безопасности<br>Этап 2: уметь использовать инструментальные средства администрирования подсистемы безопасности | Этап 1: навыки администрирования подсистемы безопасности<br>Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности |
| ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять | Этап 1: основные меры по выполнения обеспечения информационной безопасности<br>Этап 2: основные меры поддержки обеспечения информационной безопасности | Этап 1: разрабатывать меры по обеспечению информационной безопасности<br>Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности | Этап 1: разработки мер по обеспечению информационной безопасности<br>Этап 2: разработки мер поддержки обеспечения информационной безопасности |

| | | | |
|---|---|---|---|
| мониторинг и аудит безопасности автоматизированной системы | | | |
| ПК-28 способностью управлять информационной безопасностью автоматизированной системы | Этап 1: основные меры по выполнения обеспечения информационной безопасности<br>Этап 2: основные меры поддержки обеспечения информационной безопасности | Этап 1: разрабатывать меры по обеспечению информационной безопасности<br>Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности | Этап 1: разработки мер по обеспечению информационной безопасности<br>Этап 2: разработки мер поддержки обеспечения информационной безопасности |
| ПСК-3.1 способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов | Этап 1: основные информационные технологии<br>Этап 2: автоматизированные системы, применяемые при организации защиты информации | Этап 1: разрабатывать и использовать особенности информационных технологий<br>Этап 2: использовать особенности автоматизированных систем при организации системы защиты | Этап 1: использования информационных технологий при организации системы защиты<br>Этап 2: навыки использования особенностей автоматизированных систем при организации системы защиты |
| ПСК-3.2 способностью участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов | Этап 1: основные операционные системы, системы управления базами данных<br>Этап 2: комплекс задач при администрировании подсистем информационной безопасности | Этап 1: выполнять комплекс задач администрирования подсистемы безопасности<br>Этап 2: выполнять комплекс задач по безопасности операционных систем и баз данных | Этап 1:выполения комплекса задач администрирования подсистем безопасности<br>Этап 2: выполнения администрирования компьютерных сетей по безопасности |
| ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и | Этап 1: основные показатели надежности систем обеспечения информационной безопасности<br>Этап 2: комплекс мер по обеспечению надежности систем | Этап 1: планировать комплекс мер по обеспечению надежности систем безопасности<br>Этап 2:организовывать комплекс мер по обеспечению | Этап 1: планирования комплекса мер по обеспечению надежности систем безопасности<br>Этап 2: организации комплекса мер по обеспечению |

| | | | |
|---|---|---|---|
| обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов | обеспечения информационной безопасности | надежности подсистемы безопасности информации | надежности подсистемы безопасности информации |
| ПСК-3.4 способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов | Этап 1: основные этапы проектирования подсистемы информационной безопасности<br>Этап 2: основные методы технико – экономического обоснования проектных решений | Этап 1: разрабатывать основные подсистемы безопасности информации<br>Этап 2: проводить технико – экономическое обоснование проектных решений | Этап 1: навыки разработки подсистем информационной безопасности<br>Этап 2: навыки технико - экономического обоснования проектных решений |
| ПСК-3.5 способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов | Этап 1: основные меры по выполнения обеспечения информационной безопасности<br>Этап 2: основные меры поддержки обеспечения информационной безопасности | Этап 1: разрабатывать меры по обеспечению информационной безопасности<br>Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности | Этап 1: разработки мер по обеспечению информационной безопасности<br>Этап 2: разработки мер поддержки обеспечения информационной безопасности |

## 4 МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

Требования к предшествующим знаниям представлены в таблице 2. Перечень дисциплин, для которых практика «Б2.Б.04(Пд) Производственная (преддипломная) практика» является основополагающей, представлен в табл. 3.

**Таблица 2 – Требования к пререквизитам практики**

| Компетенции | Дисциплина/Практика |
|---|---|
| ПК-1 | Иностранный язык<br>Организационное и правовое обеспечение информационной безопасности<br>Информационное право и защита интеллектуальной собственности<br>Основы научных исследований<br>Английский технический<br>Учебная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)<br>Научно-исследовательская работа |
| ПК-2 | Организация ЭВМ и вычислительных систем<br>Моделирование систем<br>3D-моделирование<br>Теория графов и её приложения<br>Математические основы криптографии<br>Системы управления базами данных<br>Учебная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)<br>Научно-исследовательская работа |
| ПК-3 | Безопасность операционных систем<br>Безопасность систем баз данных<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Теория автоматов<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений<br>Научно-исследовательская работа |
| ПК-4 | Основы информационной безопасности<br>Моделирование систем<br>3D-моделирование<br>Защита информации в телекоммуникационных системах<br>Защита информации в банковских системах<br>Научно-исследовательская работа |
| ПК-5 | Основы информационной безопасности<br>Стандарты информационной безопасности<br>Безопасность веб-приложений<br>Научно-исследовательская работа |
| ПК-6 | Организация ЭВМ и вычислительных систем<br>Защита информации в телекоммуникационных |

| | |
|---|---|
| | системах<br>Защита информации в банковских системах<br>Экономика и менеджмент в информационной безопасности критически важных объектов<br>Научно-исследовательская работа |
| ПК-7 | Инженерная графика<br>Информационное право и защита интеллектуальной собственности<br>Основы научных исследований<br>Русский язык и культура речи<br>Научно-исследовательская работа |
| ПК-8 | Программно-аппаратные средства обеспечения информационной безопасности<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-9 | Разработка и эксплуатация защищенных автоматизированных систем<br>Биометрические технологии контроля доступа<br>Технология защиты информации в различных отраслях деятельности |
| ПК-10 | Теория информации<br>Антенны и устройства СВЧ<br>Надежность технических систем<br>Технологии и методы программирования<br>Электроника и схемотехника<br>Сети и системы передачи информации<br>Основы радиотехники<br>Операционные системы<br>Программирование веб-приложений<br>Операционная система FreeBSD<br>Безопасность веб-приложений |
| ПК-11 | Основы информационной безопасности<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-12 | Управление информационной безопасностью<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-13 | Разработка и эксплуатация защищенных автоматизированных систем<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-14 | Криптографические методы защиты информации<br>Метрология и электро-радиоизмерения<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений<br>Учебная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)<br>Производственная практика по получению профессиональных умений и опыта |

| | |
|---|---|
| | профессиональной деятельности |
| ПК-15 | Разработка и эксплуатация защищенных автоматизированных систем<br>Основы научных исследований<br>Учебная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)<br>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности |
| ПК-16 | Организационное и правовое обеспечение информационной безопасности<br>Основы научных исследований<br>Учебная практика (практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности)<br>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности |
| ПК-17 | Техническая защита информации<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений<br>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности |
| ПК-18 | Основы управленческой деятельности<br>Профессиональная этика<br>Психология и педагогика<br>Социология<br>Основы менеджмента |
| ПК-19 | Управление информационной безопасностью<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-20 | Программно-аппаратные средства обеспечения информационной безопасности<br>Экономика и менеджмент в информационной безопасности критически важных объектов<br>Основы менеджмента |
| ПК-21 | Организационное и правовое обеспечение информационной безопасности<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-22 | Основы информационной безопасности<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-23 | Организационное и правовое обеспечение информационной безопасности<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений |
| ПК-24 | Программно-аппаратные средства обеспечения |

| | |
|---|---|
| | информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Экономика и менеджмент в информационной безопасности критически важных объектов<br>Основы менеджмента |
| ПК-25 | Программно-аппаратные средства обеспечения информационной безопасности<br>Разработка и эксплуатация защищенных автоматизированных систем<br>Экономика и менеджмент в информационной безопасности критически важных объектов<br>Основы менеджмента |
| ПК-26 | Безопасность сетей ЭВМ<br>Защита информации в телекоммуникационных системах<br>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности |
| ПК-27 | Разработка и эксплуатация защищенных автоматизированных систем<br>Технология защиты информации в различных отраслях деятельности<br>Системы обнаружения вторжений<br>Производственная практика по получению профессиональных умений и опыта профессиональной деятельности |
| ПК-28 | Управление информационной безопасностью<br>Экономика и менеджмент в информационной безопасности критически важных объектов<br>Основы менеджмента |
| ПСК-3.1 | Основы радиотехники<br>Обеспечение информационной безопасности на критически важных объектах |
| ПСК-3.2 | Защита электронного документооборота критически важных объектов<br>Инженерно-техническая защита информации и технические средства на критически важных объектах |
| ПСК-3.2 | Основы аттестации объектов информатизации критически важных объектов |
| ПСК-3.4 | Основы аттестации объектов информатизации критически важных объектов |
| ПСК-3.5 | Метрология и электро-радиоизмерения<br>Методы и средства противодействия террористической деятельности в системах управления критически важных объектов |

**Таблица 2 – Требования к постреквизитам практики**

| Компетенции | Дисциплина/Практика |
|---|---|
| ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10; ПК-11; ПК-12; ПК-13; ПК-14; ПК-15; ПК-16; ПК-17; ПК-18; ПК-19; ПК-20; ПК-21; ПК-22; ПК-23; ПК-24; ПК-25; ПК-26; ПК-27; ПК-28; ПСК-3.1; ПСК-3.2; ПСК-3.3; ПСК-3.4; ПСК-3.5 | Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа специалиста) |

## 5 ОБЪЕМ, ПРОДОЛЖИТЕЛЬНОСТЬ И СОДЕРЖАНИЕ ПРАКТИКИ

5.1 Время проведения практики: согласно - календарного учебного графика.
5.2 Продолжительность практики составляет 12 недель.
5.3 Общая трудоёмкость преддипломной практики составляет _18_ зачетных единиц. Распределение по разделам/этапам практики, видам работ, форм текущего контроля с указанием номера осваиваемой компетенции в соответствии с ОПОП приведено в таблице 4.

**Таблица 4. Распределение по разделам/этапам практики, видам работ, форм текущего контроля**

| Разделы (этапы) практики | **Трудоёмкость** | | | | | **Результаты** | |
|---|---|---|---|---|---|---|---|
| | **Зач. Ед.** | **Часов** | | | **Кол-во дней** | форма текущего контроля | № осваиваемой компетенции по ОПОП |
| | | **всего** | контактная работа | Выполнение инд. задания | | | |
| **Общая трудоемкость по Учебному плану** | 18 | 648 | 432 | 216 | 72 | | |
| 1. *Подготовительный этап, включающий инструктаж по технике безопасности* | 1,1 | 8 | 6 | 2 | 1 | Дифференцированный зачёт | ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; |
| 2. *Производственный этап* | 9 | 424 | 282 | 142 | 40 | Дифференцированный зачёт | ПК-9; ПК-10; ПК-11; ПК-12; ПК-13; ПК-14; ПК-15; |
| 3. *Обработка и анализ полученной информации* | 4,5 | 140 | 93 | 47 | 16 | Дифференцированный зачёт | ПК-16; ПК-17;ПК-18; ПК-19; ПК-20; ПК-21; |
| 4. *Подготовка отчета по практике* | 2,4 | 72 | 48 | 24 | 14 | Дифференцированный зачёт | ПК-22; ПК-23; ПК-24; ПК-25; ПК-26; ПК-27; ПК-28; |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5. *Защита* | 1 | 4 | 3 | 1 | 1 | Дифференцированный зачёт | ПСК-3.1; ПСК-3.2; ПСК-3.3; ПСК-3.4; ПСК-3.5 |
| **Вид контроля** | Дифференцированный зачет | | | | | | |

5.3 Самостоятельная работа студентов на практике.

Самостоятельная работа студента на практике заключается в рассмотрении двух обязательных вопросов и выполнении индивидуального задания.

1. Особенности профессиональной деятельности специалиста в сфере обеспечения информационной безопасности

2. Нормативно-правовые акты в области обеспечения информативной безопасности (краткий конспект)

5.3.1 Примерный перечень вариантов индивидуальных заданий:

1. **Модернизация системы защиты информации от утечки по каналам связи.**

Обосновать актуальность защиты информации от утечки по каналам связи.

Охарактеризовать объект информатизации.

Проанализировать базовую систему защиты информации от утечки по каналам связи на объекте информатизации.

Простроить классификацию каналов связи.

Проанализировать нормативно-правовую базу по защите информации от утечки по каналам связи.

Разработать модель нарушителя и модель угроз для объекта информатизации.

Обосновать технико-экономическую эффективность модернизации системы защиты информации от утечки по каналам связи для объекта информатизации.

2. **Модернизация системы защиты информации выделенного помещения.**

Обосновать актуальность защиты информации в выделенном помещении объекта информатизации;

Охарактеризовать объект информатизации;

Проанализировать выделенное помещение на объекте информатизации;

Проанализировать организационно-технические мероприятий базовой системы защиты информации в выделенном помещении на объекте информатизации;

Построить модель угроз и модель нарушителя выделенного помещения на объекте информатизации;

Разработать технико-экономическое обоснование на модернизацию системы защиты информации выделенного помещения;

3. **Модернизация системы защиты информации при проведении совещаний по конфиденциальным вопросам.**

Обосновать актуальность защиты информации при проведении совещаний по конфиденциальным вопросам на объекте информатизации;
Охарактеризовать объект информатизации;
Провести анализ помещения для проведения совещаний по конфиденциальным вопросам на объекте информатизации;
Провести анализ организационно-технических мероприятий базовой системы защиты информации на объекте информатизации;
Построить модель угроз и модель нарушителя выделенного помещения для проведения совещаний по конфиденциальным вопросам на объекте информатизации;
Разработать технико-экономическое обоснование на модернизацию системы защиты;

4. **Модернизация системы защиты информации электронного документооборота.**

Охарактеризовать объект информатизации.
Обосновать актуальность использования системы электронного документооборота для объекта информатизации.
Проанализировать базовую систему защиты электронного документооборота объекта информатизации.
Проанализировать нормативно-правовую базу документов по защите электронного документооборота.
Разработать модель нарушителя и модель угроз безопасности электронного документооборота объекта информатизации.
Разработать технико-экономическое обоснование модернизации системы защиты электронного документооборота для объекта информатизации.

5. **Модернизация системы защиты информации в АС.**

Охарактеризовать объект информатизации.
Провести анализ защищаемой информации вАС объекта информатизации.
Провести анализ АС объекта информатизации.
Построить модель угроз и модель нарушителя дляАСобъекта информатизации.
Провести аудит базовой системы защиты АС объекта информатизации.
Определить требования к системе защиты АС объекта информатизации.
Рассчитать риски для АС объекта информатизации.

6. **Модернизация системы защиты сервера на основе технологии виртуализации.**

Обосновать актуальность внедрения технологии виртуализации сервера в информационную сеть объекта информатизации.
Составить организационную структуру и схему информационных потоков объекта информатизации.
Провести анализ информационной системы объекта информатизации.
Провести анализ базовой системы защиты сервера на объекте информатизации.
Составить модель угроз и модель нарушителя для объекта информатизации.
Разработать обобщенную структурную схему гипервизора для объекта информатизации.
Составить технико-экономическое обоснование на проект .

7. **Модернизация системы защиты информации от утечки по техническим каналам.**

Построить классификацию технических каналов утеки информации.

Охарактеризовать объект информатизации.

Проанализировать информационную систему объекта информатизации.

Проанализировать базовую систему защиты информации от утечки по техническим каналам на объекте информатизации.

Разработать модель угроз и модель нарушителя для объекта информатизации.

Разработать технико-экономическое обоснование на модернизацию системы защиты информации от утечки по техническим каналам на объекте информатизации.

8. **Модернизация системы защиты коммерческой тайны на объекте информатизации.**

Охарактеризовать объект информатизации.
Обосновать актуальность модернизации системы защиты коммерческой тайны на объекте информатизации.
Проанализировать базовую систему защиты коммерческой тайны объекта информатизации.
Составить модель угроз и модель нарушителя для системы защиты объекта информатизации.
Определить требования к системе защиты коммерческой тайны на объекте информатизации.
Разработать технико-экономического обоснования на модернизацию системы защиты коммерческой тайны на объекте информатизации.

9. **Разработка метода автоматизированной оценки эффективности средств защиты информации от утечки по каналу побочных электромагнитных излучений для объекта информатизации.**

Охарактеризовать объект информатизации.

Провести анализ особенностей технического канала утечки информации за счет ПЭМИ.
Составить топологическую схему границ контролируемой зоны и технический паспорт исследуемого объекта информатизации.
Построить модель нарушителя и модель угроз информационной безопасности объекта информатизации.
Проанализировать выполнение требований нормативных методических документов на объекте информатизации.
Определить этапы технологического процесса оценки защищенности объекта информатизации от утечки по каналу ПЭМИ.
Разработать структуру обобщенного алгоритма автоматизации процесса оценки эффективности средств защиты информации от утечки по каналу побочных электромагнитных излучений.

10. **Модернизация системы технической охраны на объекте информатизации.**

Построить классификацию технических средств охраны.
Проанализировать объект информатизации.
Дать характеристику информационной системы в объекта информатизации.
Дать характеристику базовой системы охраны объекта информатизации
Построить модель угроз и модель нарушителя для технической охраны для объекта информатизации.
Разработать модель выбора средств технической охраны для объекта информатизации.
Разработать технико-экономическое обоснование на модернизацию системы технической охраны объекта информатизации.

11. **Провести оценку системы информационной безопасности банка согласно требованиям СТО БР ИББС**

12. **Провести системный анализ бизнес-процессов ВУЗа как объекта защиты и определить требования к обеспечению информационной безопасности ВУЗа.**

Изучить нормативно-методическую базу в области построения и управления системой информационной безопасности предприятия.
Выделить ряд требований к информационной безопасности вуза.
Проанализировать организационно-информационную структуру вуза, средства защиты, используемые для защиты ресурсов информационной системы ВУЗа;
Выявить угрозы и нарушителей системе информационной безопасности ВУЗа;
Спроектировать комплекс мероприятий по управлению информационной безопасностью ВУЗа

13. **На основе СТО БР ИББС-1.2-2014 провести оценку соответствия информационной безопасности банка требованиям СТО БР ИББС-1.0 (итоговый уровень соответствия), в частности**:

оценку степени выполнения требований СТО БР ИББС-1.0 по текущему уровню ИБ банка;

оценку степени выполнения требований СТО БР ИББС-1.0 по менеджменту ИБ банка;

оценку степени выполнения требований СТО БР ИББС-1.0 по уровню осознания;

оценку степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных;

оценку степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;

оценку степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс банка;

оценку степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс банка.

14. **На основе ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018 СТО БР ИББС-1.0, ИСО/МЭК ГОСТ Р 17799-2005 определять базовый состав** организационных и технических мер по повышению уровня соответствия требованиям СТО БР ИББС-1.0 банка

15. **Разработать рекомендации по совершенствованию системы защиты электронного документооборота.**

Рассмотреть нормативно-методическую базу по проектированию системы защиты электронного документооборота судебной деятельности.

Рассмотреть концепцию защиты информационных систем судебной деятельности, обрабатывающих конфиденциальную информацию, модели безопасности, выбор механизмов защиты документооборота, и методов анализа защищенности документооборота.

Рассмотреть информационные потоки документооборота организации. Проанализировать компоненты системы электронного документооборота организации, классифицировать конфиденциальную информацию, определить место хранения, вид и срок хранения.

Построить модель угроз и нарушителей системе электронного документооборота.

Выявить недостатки в системе защиты электронного документооборота.

Разработать рекомендации по совершенствованию системы защиты электронного документооборота.

Обосновать меры защиты информации.

16. **Проанализировать систему обработки персональных данных**

**Рассмотреть нормативно-методическую базу по проектированию информационных систем зашиты персональных данных (далее – ИСПДн).**

Исследовать организационную структуру предприятия, выявить виды персональных данных, подлежащие защите.

Рассмотреть информационные активы, содержащие персональные данные субъектов и информационные взаимодействия в организации.

Проанализировать систему обработки персональных данных организации.

Исследовать программно-аппаратное и техническое обеспечение организации.

Построить модель угроз и нарушителей ИСПДн организации, определить тип угроз и уровень защищенности.

Определить требования для ИСПДн организации, проанализировать их выполнение.

Спроектировать систему защиты ИСПДн организации.

17. **Провести оценку реализации требований внутренних нормативных документов по защите коммерческой тайны предприятия**

Раскрыть теоретические аспекты защиты коммерческой тайны в коммерческих предприятиях.

Проанализировать нормативно-методическую базу в области построения защиты коммерческой тайны.

Исследовать организационную структуру предприятия, выявить виды конфиденциальной информации и ресурсы, подлежащие защите.

Выделить документы и информационные потоки предприятия, содержащие коммерческую тайну.

Провести оценку реализации требований внутренних нормативных документов по защите коммерческой тайны

18. **Провести анализ особенностей реализации информационных процессов в системе информационно-аналитического обеспечения деятельности УМВД России.**

Анализ нормативно-правовой базы в области построения обеспечения безопасности систем управления внутренних дел

Исследование материалов, собранных в УМВД России

Провести: определение конфиденциальной информации, обрабатываемой различными отделами, в частности данные, передаваемые в другие структуры;
анализ обработки информационных ресурсов в каждой БД информационно-аналитической системы УМВД России;
анализ угроз безопасности системе информационно-аналитического обеспечения деятельности;
анализ контрмер ИБ, применяемые в УМВД России.
Обосновать актуальные угрозы и определить нарушителей информационных процессов в системе информационно-аналитического обеспечения деятельности УМВД России.
Исследовать способы защиты информационных процессов в системе информационно-аналитического обеспечения деятельности УМВД России в условиях противодействия угрозам информационной безопасности.
Спроектировать защищенную систему информационно-аналитического обеспечения деятельности УМВД.

19. **Проектирование комплексной системы защиты информации предприятия**

**Описать этапы создания КСЗИ, рассмотреть нормативно-правовую базу;**
**Проанализировать характеристику объекта защиты, описать документооборот предприятия;**
Провести аудит информационной безопасности предприятия;
Проанализировать информацию, циркулирующую на защищаемом объекте, определить её виды, гриф и степень секретности;
Выделить актуальные угрозы предприятия;
Провести подбор инженерно технических средств защиты системы предприятия, программно аппаратных средств защиты;

## 6. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

6.1 По окончании практики обучающийся должен предоставить на кафедру следующие документы не позднее 7 календарных дней с даты начала занятий или окончания практики:

- заполненный рабочий дневник с отзывом (оценкой работы практиканта администрацией и старшим специалистом предприятия). Дневник должен быть заверен подписью ответственного лица и круглой печатью организации;

- отчет по практике. Отчет по практике подписывается обучающимся, проверяется и визируется руководителем практики. Защита отчетов производится в соответствии с установленным графиком защиты отчетов, но не позднее трех месяцев с начала учебного процесса. Нарушение сроков прохождения практики и сроков защиты считается невыполнением учебного плана. По результатам защиты отчетов, а также отзыва с места прохождения практики обучающимся выставляется оценка по практике;

- индивидуальное задание.

## 7 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

7.1 Форма аттестации практики дифференцированный зачет.

7.2 Время проведения аттестации согласно графику Календарного учебного плана

7.3 Зачет получает обучающийся, прошедший практику, представивший соответствующую документацию рабочий дневник с отзывом с места прохождения практики, отчет по практике в виде расчетно-пояснительной записки, и успешно защитивший отчет по практике.

7.4 Описание системы оценок. По итогам защиты отчета студенту выставляется дифференцированный зачет с учетом указанных ниже критериев:

Общая оценка выставляется на титульном листе работы, в экзаменационной ведомости и зачетной книжке студента. Для студентов очного отделения критерием успешности освоения учебного материала является экспертная оценка преподавателя, учитывающая регулярность посещения учебных занятий, знаний теоретического раздела программы и выполнение установленных на данный семестр требований технической подготовки.

Итоговый контроль – дифференцированный зачет получает студент прошедший практику, имеющий отчет со всеми отметками о выполнении.

Студенты, не выполнившие программу практики по уважительной причине, направляются на практику вторично, в свободное от учебы время, либо практика переносится на следующий год с оформлением соответствующего приказа.

Студенты, не выполнившие программу практики без уважительной причины, или получившие отрицательный результат отчисляются из Университета, как имеющие академическую задолженность в порядке, предусмотренном Уставом ВУЗа.

7.4.1 По результатам прохождения практики начисляется максимум 100 балов.

7.4.2 Критерии бально-рейтинговой оценки результатов прохождения обучающимися практики формируются на кафедре, за которой закреплена дисциплина. Перечень критериев зависит от специфики практики.

Основные критерии:

- полнота представленного материала, выполнение индивидуального задания, соответствующие программе практики – до 50 баллов;
- своевременное представление отчета, качество оформления – до 20 баллов;
- защита отчета, качество ответов на вопросы – до 30 баллов.

Форма фиксации с возможным вариантом критериев представлена в таблице 5.

**Таблица 5. Структура формирования балльно-рейтинговой оценки результатов прохождения обучающимися практики.**

| № | Критерии оценок | Баллы |
|---|---|---|
| 1 | полнота представленного материала, выполнение индивидуального задания | 25 |
| 2 | соответствие представленных результатов программе практики | 25 |
| 3 | своевременное представление отчета | 10 |
| 4 | качество оформления отчета | 10 |
| 5 | доклад по отчету | 20 |
| 6 | качество ответов на дополнительные вопросы | 10 |
| | ИТОГО | 100 |

7.4.3 Структура формирования балльно-рейтинговой оценки прохождения обучающимися практики определяется ведущим преподавателем, рассматривается и одобряется на заседании кафедры, утверждается в установленном порядке в составе программы практики.

7.4.4 Система оценок представлена в таблице 6.

**Таблица 6. Система оценок**

| **Диапазон оценки в баллах** | европейская шкала (ECTS) | традиционная шкала | **Зачет** |
|---|---|---|---|
| [95; 100] | **A** - (5+) | **отлично** – (5) | зачтено |
| [85; 95) | **B** - (5) | | |
| [70; 85) | **C** – (4) | **хорошо** – (4) | |
| [60; 70) | **D** – (3+) | **удовлетворительно** – (3) | |
| [50; 60) | **E** – (3) | | незачтено |
| [33,3; 50) | **FX** – (2+) | **неудовлетворительно** – (2) | |
| [0; 33,3) | **F** – (2) | | |

7.4.5 Прохождение всех этапов практики (выполнение всех видов работ) является обязательным. Набрав высокий балл за один из этапов практики, обучающийся не освобождается от прохождения других этапов.

7.4.6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике. (Представлен в отдельном документе.)

Представлен в отдельном документе.

## 8 ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

8.1.1 Основная литература

1. Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации. Научно-практическое пособие. Орел: 2008.-300с.

2. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. - М.: Радио и связь, 2007. - 192 с.: ил..

3. Малюк А.А., Пазизин С.В.,Погожин Н.С. Введение в защиту информации в автоматизированных системах. –М, Горячая линия –Телеком. Учебное пособие. 2009.

8.1.2 Дополнительная литература и Интернет-ресурсы.

1. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: "Инкомбук", 2007. - 540с.

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. М,: Энергоатомиздат -2012

8.1.3 Методические указания и материалы по практике, в т. ч. методические материалы, в которых содержится форма отчетности по практике (указывать собственные кафедральные разработки).

1.Урбан В.А. Методические указания по подготовке и оформлению отчета по Производственной (преддипломной) практике для студентов по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Информационная безопасность автоматизированных систем критически важных объектов».

## 9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

9.1. Программное обеспечение и информационные справочные системы.

Программное обеспечение преддипломной практики определяется местом, где она проходит и соответственно информационными технологиями, которые применяются в организации, где проходит практику студент. MS Windows

MS Office
Open Office
Базы данных, информационно-справочные и поисковые системы:
1. Консультант плюс;
2. Гарант

## 10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Материально – техническое обеспечение преддипломной практики определяется местом, где она проходит и соответственно материально – технической обеспеченностью организации, где проходит практику студент.

Программа разработана в соответствии с федеральным государственным образовательным стандартом высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденным приказом Министерства образования и науки РФ от 1 декабря 2016 г. №1509.

Разработал: Урбан В.А.