

**МИНОБРНАУКИ РОССИИ**  
**Федеральное государственное автономное образовательное**  
**учреждение высшего образования "Пермский**  
**государственный национальный исследовательский**  
**университет"**

Авторы-составители: **Лунегов Игорь Владимирович**

Программа производственной практики  
**ПРЕДДИПЛОМНАЯ ПРАКТИКА**  
Код УМК 94397

Утверждено  
Протокол №4  
от «24» июня 2021 г.

Пермь, 2021

## **1. Вид практики, способ и форма проведения практики**

Вид практики **производственная**

Тип практики **преддипломная практика**

Способ проведения практики **стационарная, выездная**

Форма (формы) проведения практики **дискретная**

## **2. Место практики в структуре образовательной программы**

Производственная практика « Преддипломная практика » входит в обязательную часть Блока « С.2 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем  
направленность Безопасность открытых информационных систем

### **Цель практики :**

Целями преддипломной практики являются:

- закрепление и конкретизация результатов теоретического обучения;
- приобретение студентами умений и навыков самостоятельной практической работы по специальности "Информационная безопасность автоматизированных систем";
- получение студентами практических навыков выполнения мероприятий по организационной, правовой и технической защите информации, овладение методами работы с техническими и программно-аппаратными средствами защиты информации;
- развитие у студентов навыков проведения анализа деятельности предприятий и организаций по усовершенствованию их работы;
- подготовка выпускной квалификационной работы.

### **Задачи практики :**

Задачами преддипломной практики являются:

- использование нормативных правовых документов по обеспечению защиты информации;
- изучение принципов формирования комплекса мер по обеспечению информационной безопасности с учетом их правовой обоснованности, административно-управленческой и технической реализуемости, а также экономической целесообразности;
- изучение видов и форм информации, подверженной угрозам, видов и возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;
- участие в эксплуатации и администрировании подсистем управления информационной безопасностью предприятия;
- участие в работах по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;
- проведение предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности с учетом экономической эффективности разработок;
- оформление рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности;
- применение программных средств системного, прикладного и специального назначения;
- использование инструментальных средств и систем программирования для решения профессиональных задач;

- проведение анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

### **3. Перечень планируемых результатов обучения**

В результате прохождения практики **Преддипломная практика** у обучающегося должны быть сформированы следующие компетенции:

**10.05.03** Информационная безопасность автоматизированных систем (направленность : Безопасность открытых информационных систем)

**ОПК.10** Способен разрабатывать компоненты систем защиты информации автоматизированных систем

#### **Индикаторы**

**ОПК.10.2** Проектирует защищенные автоматизированные системы с учетом действующих нормативных и методических документов

**ОПК.11** Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем

#### **Индикаторы**

**ОПК.11.1** Оценивает эффективность и надежность защиты операционных систем

**ОПК.12** Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем

#### **Индикаторы**

**ОПК.12.1** Организует диагностику и тестирование систем защиты информации автоматизированных систем

**ОПК.12.2** Проводит анализ уязвимостей систем защиты информации автоматизированных систем

**ОПК.13** Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений

#### **Индикаторы**

**ОПК.13.2** Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем

**ОПК.14** Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

#### **Индикаторы**

**ОПК.14.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

**ОПК.14.2** Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

**ОПК.15** Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности

#### **Индикаторы**

**ОПК.15.1** Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области

**ОПК.15.2** Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач

**ОПК.16** Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности

## **Индикаторы**

**ОПК.16.1** Осуществляет обоснованный выбор технологий, инструментария, языка программирования и способов оптимизации программ

**ОПК.17** Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

## **Индикаторы**

**ОПК.17.2** Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности

**ОПК.4** Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

## **Индикаторы**

**ОПК.4.3** Организует защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

**ОПК.6** Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

## **Индикаторы**

**ОПК.6.3** Применяет методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

**ОПСК.1** Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

## **Индикаторы**

**ОПСК.1.2** Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации

**ОПСК.2** Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем

## **Индикаторы**

**ОПСК.2.1** Осуществляет планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации

**ОПСК.2.2** Формирует политики безопасности и профили защиты, оценивает их эффективность, обоснованно выбирает методы и средства защиты информации

**ОПСК.3** Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

## **Индикаторы**

**ОПСК.3.1** Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах

**ОПСК.3.2** Определяет источники и причины возникновения инцидентов безопасности в автоматизированных системах

**ПК.1** Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты

## **Индикаторы**

**ПК.1.1** Проводит моделирование безопасности информационных систем

**ПК.1.3** Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем

**ПК.3** Способен управлять функционированием и защищенностью автоматизированных систем

**Индикаторы**

**ПК.3.1** Контролирует соответствие параметров подсистем защиты автоматизированной системы установленным требованиям

**ПК.3.2** Устанавливает и настраивает программное обеспечение, необходимое для защиты автоматизированной системы от НСД

**ПК.3.3** Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД

**УК.1** Способен осуществлять анализ проблемных ситуаций и вырабатывать решение на основе системного подхода

**Индикаторы**

**УК.1.2** Работает с противоречивой информацией из разных источников, находит пробелы в необходимой для разрешения проблемы информации, определяет варианты устранения пробелов

**УК.11** Способен формировать нетерпимое отношение к коррупционному поведению

**Индикаторы**

**УК.11.3** Осуществляет взаимодействие на основе нетерпимого отношения к коррупционному поведению в социальной и профессиональной сферах

**УК.2** Способен управлять проектом, организовывать и руководить работой команды

**Индикаторы**

**УК.2.3** Разрабатывает мероприятия по реализации проекта на разных этапах его жизненного цикла, вносит корректировки в ходе реализации проекта

**УК.3** Способен осуществлять коммуникации в рамках академического и профессионального взаимодействия на русском и иностранном языках

**Индикаторы**

**УК.3.1** Осуществляет коммуникацию, грамотно и аргументированно строит устную и письменную речь на русском и иностранном языках

**УК.3.3** Представляет результаты деятельности на публичных мероприятиях в устной и письменной формах

**УК.3.4** Устанавливает и поддерживает контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий

**УК.5** Способен управлять своими ресурсами, определять приоритеты собственной деятельности, выстраивать и реализовывать траекторию саморазвития

**Индикаторы**

**УК.5.3** Осуществляет выбор направленности профессиональной деятельности в зависимости от собственных интересов, ресурсов и накопленного опыта

**УК.9** Способен использовать базовые дефектологические знания в социальной и профессиональной сферах

**Индикаторы**

**УК.9.3** Выстраивает профессиональное взаимодействие с лицами, имеющими психофизиологические особенности, с учетом нозологии

#### 4. Содержание и объем практики, формы отчетности

Преддипломная практика проводится для выполнения выпускной квалификационной работы (ВКР) и, являясь обязательной, включена в учебный план в соответствии с требованиями СУОС. Преддипломная практика проводится после завершения курса теоретического обучения и обеспечивает возможность применения студентами знаний и практических навыков в области информационной безопасности для определения практической и теоретической подготовленности выпускника. Эта практика относится к производственной практике и является стационарной. Выбор темы выпускной квалификационной работы предопределяет цели и задачи преддипломной практики. Тема выпускной квалификационной работы окончательно утверждается на заседании кафедры радиоэлектроники и защиты информации, после чего никакие ее корректировки не допускаются.

<b>Специальность</b>	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для прохождения практики</b>	16
<b>Объем практики (з.е.)</b>	6
<b>Объем практики (ак.час.)</b>	216
<b>Форма отчетности</b>	Экзамен (16 триместр)

#### Примерный график прохождения практики

Количество часов	Содержание работ	Место проведения
<b>Преддипломная практика. Подготовительный этап</b>		
108	Преддипломная практика студентов является составной частью основной образовательной программы высшего образования и представляет собой форму организации учебного процесса, непосредственно ориентированную на профессионально-практическую подготовку обучающихся. Преддипломная практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм (далее организациях), основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по специальности "Информационная безопасность автоматизированных систем" или на кафедре радиоэлектроники и защиты информации,, обладающей необходимым кадровым и научно-техническим потенциалом. Преддипломная практика является завершающим этапом учебного процесса, предназначенным для подготовки выпускной квалификационной работы.	Организации, область деятельности которых связана с защитой информации или кафедра радиоэлектроники и защиты информации
<b>Введение</b>		

Количество часов	Содержание работ	Место проведения
10	Введение. Производственный инструктаж, в том числе инструктаж по технике безопасности. Постановка задач практики. Получение заданий от руководителя. Согласование плана прохождения практики и плана будущей выпускной работы.	Кафедра радиоэлектроники и защиты информации
Основная часть 1-й период		
90	<p>Знакомство с организацией (темой выпускной работы) и анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности:</p> <ul style="list-style-type: none"> <li>- автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите;</li> <li>- информационных технологий, формирующих информационную инфраструктуру предприятия (организации) в условиях существования угроз в информационной сфере и задействующих информационно-технологические ресурсы, подлежащие защите;</li> <li>- технологий обеспечения информационной безопасности автоматизированных систем;</li> <li>- систем управления информационной безопасностью автоматизированных систем.</li> </ul> <p>Выбор объекта проектирования. Сбор, обработка и систематизация фактического материала по выбранному объекту проектирования.</p> <p>Знакомство с нормативными правовыми актами в области обеспечения информационной безопасности и нормативными методическими документами ФСБ России и ФСТЭК России в области защиты информации, необходимыми для обеспечения информационной безопасности выбранного объекта проектирования</p> <p>Разработка комплекса организационно-технических мероприятий, необходимых для обеспечения информационной безопасности выбранного объекта проектирования</p> <p>Выбор программно-аппаратных и технических средств защиты информации, необходимых для обеспечения информационной безопасности выбранного объекта проектирования</p> <p>Разработка документационного обеспечения защиты информации выбранного объекта проектирования. Проведение технико-экономического обоснования разработанных проектных решений для обеспечения защиты информации выбранного объекта проектирования. Вопросы ТБ, ОТ и БЖД Проведение заключительных работ по оформлению ВКР.</p>	Организации, область деятельности которых связана с защитой информации или кафедра радиоэлектроники и защиты информации
Предварительный отчет		



Количество часов	Содержание работ	Место проведения
8	Подготовка эскиза будущей выпускной квалификационной работы	Кафедра радиоэлектроники и защиты информации
Преддипломная практика. Завершающий этап		
108		
Основная часть 2-й период		
90	<p>Выбор объекта проектирования. Сбор, обработка и систематизация фактического материала по выбранному объекту проектирования.</p> <p>Знакомство с нормативными правовыми актами в области обеспечения информационной безопасности и нормативными методическими документами ФСБ России и ФСТЭК России в области защиты информации, необходимыми для обеспечения информационной безопасности выбранного объекта проектирования</p> <p>Разработка комплекса организационно-технических мероприятий, необходимых для обеспечения информационной безопасности выбранного объекта проектирования</p> <p>Выбор программно-аппаратных и технических средств защиты информации, необходимых для обеспечения информационной безопасности выбранного объекта проектирования</p> <p>Разработка документационного обеспечения защиты информации выбранного объекта проектирования. Проведение технико-экономического обоснования разработанных проектных решений для обеспечения защиты информации выбранного объекта проектирования. Вопросы ТБ, ОТ и БЖД</p> <p>Проведение заключительных работ по оформлению ВКР.</p>	Организации, область деятельности которых связана с защитой информации или кафедра радиоэлектроники и защиты информации
Заключительный этап		
18	Оформление отчета по преддипломной практике. Подготовка готового варианта выпускной квалификационной работы.	Организации, область деятельности которых связана с защитой информации или кафедра радиоэлектроники и защиты информации

## **5. Перечень учебной литературы, необходимой для проведения практики**

### **Основная**

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/87995.html>
2. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 с. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/77317.html>

### **Дополнительная**

1. Информационная безопасность и защита информации : учебно-методический комплекс / составители С. А. Омарова, К. А. Искакова, Н. А. Тойганбаева. — Алматы : Нур-Принт, 2012. — 98 с. — ISBN 9965-756-05-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/67055.html>
2. Гаибова, Т. В. Преддипломная практика : учебное пособие / Т. В. Гаибова, В. В. Тугов, Н. А. Шумилина. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2016. — 131 с. — ISBN 978-5-7410-1554-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/69932.html>

## 6. Перечень ресурсов сети «Интернет», требуемых для проведения практики

При прохождении практики требуется использование следующих ресурсов сети «Интернет» :

<https://www.securitycode.ru/> сайт компании "Код безопасности"

<https://nelk.ru/> сайт компании "Нелк"

<http://www.silicontaiga.ru> Альянс разработчиков программного обеспечения

## 7. Перечень информационных технологий, используемых при проведении практики

Образовательный процесс по практике **Преддипломная практика** предполагает использование следующего программного обеспечения и информационных справочных систем:

В учебном процессе для освоения дисциплины могут использоваться различные информационные технологии:

- презентационные материалы (слайды по темам лекционных и практических занятий);
  - доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
  - доступ в электронную информационно-образовательную среду университета;
  - интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).
- Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:

1. Приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC».
2. Программы для демонстрации видео материалов (проигрыватель) «WindowsMediaPlayer».
3. Программа просмотра интернет контента (браузер) «Google Chrome».
4. Операционная система AltLinux
5. Офисный пакет приложений «LibreOffice».

## 8. Описание материально-технической базы, необходимой для проведения практики

Аудитория для проведения занятий лекционного и семинарского типа, оснащенная презентационной техникой. При освоении материала и выполнении заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ ([student.psu.ru](http://student.psu.ru)).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел).

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

Аудитория для проведения занятий семинарского типа (семинары, практические занятия);

система LMS Moodle (<http://e-learning.psu.ru>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а также тесты, проверяемые задания, задания для совместной работы.

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел).

система тестирования Moodle (<https://moodle.psu.ru>).

Аудитория для проведения групповых (индивидуальных) консультаций:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел).

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ ([student.psu.ru](http://student.psu.ru)).

Аудитория для проведения мероприятий текущего контроля:

- 1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
- 2) мультимедийное оборудование (проектор, экран);
- 3) маркерная доска и маркеры (или меловая доска и мел).

Аудитория для самостоятельной работы:

- 1) компьютерная техника с возможностью подключения к сети «Интернет», с доступом в электронную информационно-образовательную среду ПГНИУ;
- 2) помещения Научной библиотеки ПГНИУ.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

- Операционная система ALT Linux;
- Офисный пакет Libreoffice.
- Справочно-правовая система «КонсультантПлюс»

## **9. Методические указания для обучающихся по прохождению практики**

Преддипломная практика предназначена для подготовки выпускной квалификационной работы, представляющая собой законченную разработку, в которой содержится реферативная часть, отражающая общую профессиональную эрудицию автора, а также самостоятельная исследовательская часть, выполненная индивидуально или в составе творческого коллектива по материалам, собранным или полученным самостоятельно студентом в период прохождения производственной практики. В их основе могут быть материалы научно-исследовательских или научно-производственных работ кафедры, научных или производственных организаций. Самостоятельная часть должна быть законченным исследованием, свидетельствующим об уровне профессиональной подготовки автора. Студенты обязаны ежедневно находиться в местах прохождения практики, полноценно использовать запланированное рабочее время. По окончании практики студент представляет своему научному руководителю за-конченную рукопись выпускной квалификационной работы.

Для успешного прохождения практики необходимо:

- обсуждение индивидуального плана прохождения практики с научным руководителем;
- перед началом практики участвовать в организационно-инструктивных собраниях с группой студентов-практикантов;
- выразить свое желание по выбору предприятия, учреждения и конкретного руководителя, сообщив об этом ответственному за прохождение практики;
- изучать и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии;
- прислушаться советам руководителя от кафедры радиоэлектроники и защиты информации;
- подчиняться действующим на предприятии, в учреждении правилам внутреннего трудового распорядка;

- стараться полностью выполнять задания, предусмотренные индивидуальным планом;
- наравне со штатными работниками нести ответственность за выполненную работу и ее результаты;
- своевременно сообщать научному руководителю о непредвиденных препятствиях, трудностях при выполнении индивидуального плана работы;
- вести дневник, где записывать необходимые цифровые материалы, содержание лекций и бесед, делать эскизы, зарисовки, схемы и т.д.;
- отзыв индивидуального руководителя (в соответствующем месте дневника или в виде отдельного документа) должен быть передан на кафедру радиоэлектроники и защиты информации.

Примерный перечень тематик выпускных квалификационных работ.

1. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия)
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия).
3. Автоматизация учета конфиденциальных документов на предприятии (название предприятия).
4. Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия).
5. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (название предприятия).
6. Разработка комплексной системы защиты информации (СЗИ) предприятия (название предприятия).
7. Организация системы планирования и контроля функционирования СЗИ на предприятии (название предприятия).
8. Разработка основных направлений совершенствования СЗИ предприятия (наименование предприятия).
9. Организация подсистемы, обеспечивающей управление СЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
10. Разработка методологии проектирования СЗИ.
11. Разработка моделей процессов защиты информации при проектировании СЗИ.
12. Анализ методов оценки качества функционирования СЗИ.
13. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).
14. Разработка проекта программно-аппаратной защиты информации предприятия (наименование предприятия).
15. Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия (наименование предприятия).
16. Криптографические средства защиты информации на основе дискретных носителей.
17. Разработка игровой (дискретной) модели программно-аппаратной защиты информации предприятия (наименование предприятия).
18. Разработка изолированной программно-аппаратной среды в Windows NT (WINDOWS 2000, LINUX и т.д.) (наименование предприятия).
19. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
20. Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).
21. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
22. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).

23. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
24. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (название предприятия).
25. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).
26. Организация защиты персональных данных на основе использования правовых мер (название предприятия).
27. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия).
28. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно (название предприятия).
29. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).
30. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).

Для обучающихся с ОВЗ научно-исследовательская работа проводится с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее – индивидуальные особенности). При выполнении НИР обеспечивается соблюдение следующих общих требований:

- проведение групповых и индивидуальных консультаций обучающихся с ОВЗ в одной аудитории совместно с остальными обучающимися, если это не создает трудностей для обучающихся с ОВЗ и иных обучающихся;
- присутствие при защите НИР в аудитории ассистента (ассистентов), оказывающего обучающимся с ОВЗ необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться);
- пользование необходимыми обучающимся с ОВЗ техническими средствами.

## Фонды оценочных средств для проведения промежуточной аттестации

### Планируемые результаты обучения по практике для формирования компетенции. Индикаторы и критерии их оценивания

#### ОПК.14

**Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<b>ОПК.14.2</b> Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	знать программные и программно-аппаратные средства используемые для защиты информационной системы, уметь настраивать программные и аппаратные средства защиты, владеть навыками администрирования подсистемы информационной безопасности автоматизированной системы	<p style="text-align: center;"><b>Неудовлетворительно</b></p> не знает программные и программно-аппаратные средства используемые для защиты информационной системы, не умеет настраивать программные и аппаратные средства защиты, не владеет навыками администрирования подсистемы информационной безопасности автоматизированной системы <p style="text-align: center;"><b>Удовлетворительно</b></p> частично сформированные знания программных и программно-аппаратных средств используемых для защиты информационной системы, частично сформированные умения настраивать программные и аппаратные средства защиты, частично сформированные навыки администрирования подсистемы информационной безопасности автоматизированной системы <p style="text-align: center;"><b>Хорошо</b></p> сформированные, но содержащие пробелы знания программных и программно-аппаратных средств используемых для защиты информационной системы, сформированные, но содержащие пробелы умения настраивать программные и аппаратные средства защиты, сформированные, но содержащие пробелы навыки администрирования подсистемы информационной безопасности автоматизированной системы <p style="text-align: center;"><b>Отлично</b></p> сформированные знания программных и программно-аппаратных средств используемых для защиты информационной

		<p><b>Отлично</b></p> <p>системы, сформированные умения настраивать программные и аппаратные средства защиты, сформированные навыки администрирования подсистемы информационной безопасности автоматизированной системы</p>
<p><b>ОПК.14.1</b></p> <p>Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем</p>	<p>сформированные знания требований безопасности автоматизированных систем, сформированные умения разрабатывать политики информационной безопасности автоматизированных систем, сформированные навыки реализации политики информационной безопасности автоматизированных систем</p>	<p><b>Неудовлетворительно</b></p> <p>не знает требований безопасности автоматизированных систем, не умеет разрабатывать политики информационной безопасности автоматизированных систем, не владеет навыками их реализации</p> <p><b>Удовлетворительно</b></p> <p>частично сформированные знания требований безопасности автоматизированных систем, частично сформированные умения разрабатывать политики информационной безопасности автоматизированных систем, частично сформированные навыки реализации политики информационной безопасности автоматизированных систем</p> <p><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы знания требований безопасности автоматизированных систем, сформированные, но содержащие пробелы умения разрабатывать политики информационной безопасности автоматизированных систем, сформированные, но содержащие пробелы навыки реализации политики информационной безопасности автоматизированных систем</p> <p><b>Отлично</b></p> <p>сформированные знания требований безопасности автоматизированных систем, сформированные умения разрабатывать политики информационной безопасности автоматизированных систем, сформированные навыки реализации политики информационной безопасности автоматизированных систем</p>

#### ОПК.15

Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы



## и модели для решения задач профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ОПК.15.1</b> Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области</p>	<p>знать виды оборудования, используемого при проведении экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем, уметь выбирать необходимое оборудование при проведении экспериментально-исследовательских работ, владеть навыками использования специализированных средств при анализе технических каналов утечки информации</p>	<p><b>Неудовлетворительно</b> знать виды оборудования, используемого при проведении экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем, уметь выбирать необходимое оборудование при проведении экспериментально-исследовательских работ, владеть навыками использования специализированных средств при анализе технических каналов утечки информации</p> <p><b>Удовлетворительно</b> частично сформированные знания видов оборудования, используемого при проведении экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем, частично сформированные умения выбирать необходимое оборудование при проведении экспериментально-исследовательских работ, частично сформированные навыки использования специализированных средств при анализе технических каналов утечки информации</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания видов оборудования, используемого при проведении экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем, сформированные, но содержащие пробелы умения выбирать необходимое оборудование при проведении экспериментально-исследовательских работ, сформированные, но содержащие пробелы навыки использования специализированных средств при анализе технических каналов утечки информации</p> <p><b>Отлично</b> сформированные знания видов оборудования, используемого при проведении экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем,</p>

		<p><b>Отлично</b></p> <p>сформированные умения выбирать необходимое оборудование при проведении экспериментально-исследовательских работ, сформированные навыки использования специализированных средств при анализе технических каналов утечки информации</p>
<p><b>ОПК.15.2</b></p> <p>Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач</p>	<p>владеть навыками анализа защищенности информационной системы с использованием специализированного оборудования</p>	<p><b>Неудовлетворительно</b></p> <p>не владеет навыками анализа защищенности информационной системы с использованием специализированного оборудования</p> <p><b>Удовлетворительно</b></p> <p>частично сформированные навыки анализа защищенности информационной системы с использованием специализированного оборудования</p> <p><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы навыки анализа защищенности информационной системы с использованием специализированного оборудования</p> <p><b>Отлично</b></p> <p>сформированные навыки анализа защищенности информационной системы с использованием специализированного оборудования</p>

## ОПК.12

**Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ОПК.12.1</b></p> <p>Организует диагностику и тестирование систем защиты информации автоматизированных систем</p>	<p>Знать возможные пути вторжений в АС, владеть навыками защиты информационной системы от внешних вторжений</p>	<p><b>Неудовлетворительно</b></p> <p>не знает возможные пути вторжений в АС, не владеет навыками защиты информационной системы от внешних вторжений</p> <p><b>Удовлетворительно</b></p> <p>частично сформированные знания возможных путей вторжений в АС, частично сформированные навыки защиты АС от внешних вторжений</p> <p><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы знания возможных путей вторжений в АС, сформированные, но содержащие пробелы навыки защиты АС от внешних вторжений</p>

		<p><b>Отлично</b> сформированные знания возможных путей вторжений в АС, сформированные навыки защиты АС от внешних вторжений</p>
<p><b>ОПК.12.2</b> Проводит анализ уязвимостей систем защиты информации автоматизированных систем</p>	<p>уметь корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий</p>	<p><b>Неудовлетворительно</b> не умеет корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий</p> <p><b>Удовлетворительно</b> частично сформированные умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий</p> <p><b>Отлично</b> сформированные умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий</p>

## ОПК.11

**Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ОПК.11.1</b> Оценивает эффективность и надежность защиты операционных систем</p>	<p>Знать возможные пути вторжений в АС, владеть навыками защиты информационной системы от внешних вторжений</p>	<p><b>Неудовлетворительно</b> не знает возможные пути вторжений в АС, не владеет навыками защиты информационной системы от внешних вторжений</p> <p><b>Удовлетворительно</b> частично сформированные знания возможных путей вторжений в АС, частично сформированные навыки защиты АС от внешних вторжений</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания возможных путей вторжений в АС, сформированные, но содержащие пробелы навыки защиты АС от внешних вторжений</p> <p><b>Отлично</b> сформированные знания возможных путей</p>

		<b>Отлично</b> вторжений в АС, сформированные навыки защиты АС от внешних вторжений
--	--	--

#### ОПК.4

**Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ОПК.4.3</b> Организует защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	знать нормативно-правовую базу в области защиты информации, уметь разрабатывать методические материалы по обслуживанию систем безопасности информационной системы, владеть навыками оценки и контроля полноты содержания нормативных и методических материалов	<p><b>Неудовлетворительно</b> не знает нормативно-правовую базу в области защиты информации, не умеет разрабатывать методические материалы по обслуживанию систем безопасности информационной системы, не владеет навыками оценки и контроля полноты содержания нормативных и методических материалов</p> <p><b>Удовлетворительно</b> частично сформированные знания нормативно-правовой базы в области защиты информации, частично сформированные умения разрабатывать методические материалы по обслуживанию систем безопасности информационной системы, частично сформированные навыки оценки и контроля полноты содержания нормативных и методических материалов</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания нормативно-правовой базы в области защиты информации, сформированные, но содержащие пробелы умения разрабатывать методические материалы по обслуживанию систем безопасности информационной системы, сформированные, но содержащие пробелы навыки оценки и контроля полноты содержания нормативных и методических материалов</p> <p><b>Отлично</b> сформированные знания нормативно-правовой базы в области защиты информации, сформированные умения разрабатывать методические материалы по</p>

		<p style="text-align: center;"><b>Отлично</b></p> <p>обслуживанию систем безопасности информационной системы, сформированные навыки оценки и контроля полноты содержания нормативных и методических материалов</p>
--	--	--

## ОПК.16

**Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ОПК.16.1</b> Осуществляет обоснованный выбор технологий, инструментария, языка программирования и способов оптимизации программ</p>	<p>знать методологии и методы проектирования программного обеспечения, уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками тестирования программ в интегрированной среде разработки.</p>	<p style="text-align: center;"><b>Неудовлетворительно</b></p> <p>отсутствие знаний методологии и методов проектирования программного обеспечения, отсутствие умения работать с интегрированной средой разработки программного обеспечения, отсутствие навыков тестирования программ в интегрированной среде разработки.</p> <p style="text-align: center;"><b>Удовлетворительно</b></p> <p>частично сформированное знание методологии и методов проектирования программного обеспечения, частично сформированное умение работать с интегрированной средой разработки программного обеспечения, частично сформированные навыки тестирования программ в интегрированной среде разработки.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>сформированное, но содержащее пробелы знание методологии и методов проектирования программного обеспечения, сформированное, но содержащее пробелы умение работать с интегрированной средой разработки программного обеспечения, сформированные, но содержащее пробелы навыки тестирования программ в интегрированной среде разработки.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>сформированное знание методологии и методов проектирования программного обеспечения, сформированное умение работать с интегрированной средой разработки программного обеспечения, сформированные навыки тестирования</p>

		<b>Отлично</b> программ в интегрированной среде разработки.
--	--	--

### ОПК.17

**Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ОПК.17.2</b> Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Знать современные коммуникативные технологии, умеет устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, владеет навыками делового общения	<p><b>Неудовлетворительно</b> не знает современные коммуникативные технологии, не умеет устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, не владеет навыками делового общения</p> <p><b>Удовлетворительно</b> частично сформированные знания современных коммуникативных технологий, частично сформированные умения устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, частично сформированные навыки делового общения</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания современных коммуникативных технологий, сформированные, но содержащие пробелы умения устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, сформированные, но содержащие пробелы навыки делового общения</p> <p><b>Отлично</b> сформированные знания современных коммуникативных технологий, сформированные умения устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий,</p>

		<b>Отлично</b> сформированные навыки делового общения
--	--	--

### ОПК.13

**Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ОПК.13.2</b> Оценивает эффективность и надежность средств защиты информации программного обеспечения автоматизированных систем	знать основные требования информационной безопасности, предъявляемые к АС, уметь организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности, владеть навыками администрирования компьютерной сети предприятия	<b>Неудовлетворительно</b> не знает основные требования информационной безопасности, предъявляемые к АС, не умеет организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности, не владеет навыками администрирования компьютерной сети предприятия
		<b>Удовлетворительно</b> частично сформированные знания основных требований информационной безопасности, предъявляемые к АС, частично сформированные умения организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности, частично сформированные навыки администрирования компьютерной сети предприятия
		<b>Хорошо</b> сформированные, но содержащие пробелы знания основных требований информационной безопасности, предъявляемые к АС, сформированные, но содержащие пробелы умения организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности, сформированные, но содержащие пробелы навыки администрирования компьютерной сети предприятия
		<b>Отлично</b> сформированные знания основных требований информационной безопасности,

		<p><b>Отлично</b></p> <p>предъявляемые к АС, сформированные умения организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности, сформированные навыки администрирования компьютерной сети предприятия</p>
--	--	---

### ОПК.6

**Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ОПК.6.3</b></p> <p>Применяет методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p>	<p>Знать основные принципы проведения научных исследований, уметь ставить и решать задачи, владеть навыками исследовательской деятельности</p>	<p><b>Неудовлетворительно</b></p> <p>не знает основные принципы проведения научных исследований, не умеет ставить и решать задачи, не владеет навыками исследовательской деятельности</p> <p><b>Удовлетворительно</b></p> <p>частично сформированные знания основных принципов проведения научных исследований, частично сформированные умения ставить и решать задачи, частично сформированные навыки исследовательской деятельности</p> <p><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы знания основных принципов проведения научных исследований, сформированные, но содержащие пробелы умения ставить и решать задачи, сформированные, но содержащие пробелы навыки исследовательской деятельности</p> <p><b>Отлично</b></p> <p>сформированные знания основных принципов проведения научных исследований, сформированные умения ставить и решать задачи, сформированные навыки исследовательской деятельности</p>

### ОПК.10

**Способен разрабатывать компоненты систем защиты информации автоматизированных систем**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
----------------------------	------------------------------------	---



<p><b>ОПК.10.2</b>  Проектирует защищенные автоматизированные системы с учетом действующих нормативных и методических документов</p>	<p>Знать средства поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке, уметь искать, анализировать научно-техническую информацию, в сфере информационной безопасности, владеть навыками обобщения научно-технической информации в сфере информационной безопасности</p>	<p><b>Неудовлетворительно</b>  отсутствие знаний средств поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке, отсутствие умений поиска и анализа научно-технической информации в сфере информационной безопасности, отсутствие навыков обобщения научно-технической информации в сфере информационной безопасности</p> <p><b>Удовлетворительно</b>  частично сформированные знания средств поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке, частично сформированные умения поиска и анализа научно-технической информации в сфере информационной безопасности, частично сформированные навыки обобщения научно-технической информации в сфере информационной безопасности</p> <p><b>Хорошо</b>  сформированные, но содержащие пробелы знания средств поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке, сформированные, но содержащие пробелы умения поиска и анализа научно-технической информации в сфере информационной безопасности, сформированные, но содержащие пробелы навыки обобщения научно-технической информации в сфере информационной безопасности</p> <p><b>Отлично</b>  сформированные знания средств поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке, сформированные умения поиска и анализа научно-технической информации в сфере информационной безопасности, сформированные навыки обобщения научно-технической информации в сфере</p>
--	---	---

		<b>Отлично</b> информационной безопасности
--	--	---

### ОПСК.3

**Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>ОПСК.3.1</b> Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных системах	знать правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности АС, уметь формировать и эффективно применять комплекс мер для обеспечения информационной безопасности АС	<p><b>Неудовлетворительно</b> не знает правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности автоматизированной системы, не умеет формировать и эффективно применять комплекс мер для обеспечения информационной безопасности автоматизированной системы</p> <p><b>Удовлетворительно</b> частично сформированные знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности автоматизированной системы, частично сформированные умения формировать и эффективно применять комплекс мер для обеспечения информационной безопасности автоматизированной системы</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности автоматизированной системы, сформированные, но содержащие пробелы умения формировать и эффективно применять комплекс мер для обеспечения информационной безопасности автоматизированной системы</p> <p><b>Отлично</b> сформированные знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности ОИС, сформированные умения формировать и эффективно применять комплекс мер для обеспечения информационной безопасности</p>

		<b>Отлично</b> автоматизированной системы
<b>ОПСК.3.2</b> Определяет источники и причины возникновения инцидентов безопасности в автоматизированных системах	знать виды угроз и модели нарушителя информационной безопасности автоматизированной системы, уметь разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы, владеть навыками формирования перечня и вероятности угроз информационной безопасности	<p><b>Неудовлетворительно</b></p> <p>отсутствие знания видов угроз и моделей нарушителя информационной безопасности автоматизированной системы, отсутствие умения разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы, отсутствие навыков формирования перечня и вероятности угроз информационной безопасности</p> <p><b>Удовлетворительно</b></p> <p>частично сформированные знания видов угроз и моделей нарушителя информационной безопасности автоматизированной системы, частично сформированные умения разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы, частично сформированные навыки формирования перечня и вероятности угроз информационной безопасности</p> <p><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы знания видов угроз и моделей нарушителя информационной безопасности автоматизированной системы, сформированные, но содержащие пробелы умения разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы, сформированные, но содержащие пробелы навыки формирования перечня и вероятности угроз информационной безопасности</p> <p><b>Отлично</b></p> <p>сформированные знания видов угроз и моделей нарушителя информационной безопасности автоматизированной системы, сформированные умения разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы, сформированные навыки формирования перечня и вероятности угроз информационной безопасности</p>

## ОПСК.2

### Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<b>ОПСК.2.1</b> Осуществляет планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации	уметь планировать работы по регламентному обслуживанию информационных систем и систем защиты информации	<b>Неудовлетворительно</b> не умеет планировать работы по регламентному обслуживанию информационных систем и систем защиты информации <b>Удовлетворительно</b> частично сформированные умения планировать работы по регламентному обслуживанию информационных систем и систем защиты информации <b>Хорошо</b> сформированные, но содержащие пробелы умения планировать работы по регламентному обслуживанию информационных систем и систем защиты информации <b>Отлично</b> сформированные умения планировать работы по регламентному обслуживанию информационных систем и систем защиты информации
<b>ОПСК.2.2</b> Формирует политики безопасности и профили защиты, оценивает их эффективность, обоснованно выбирает методы и средства защиты информации	знать требования безопасности открытых информационных систем, уметь разрабатывать политики информационной безопасности открытых информационных систем, владеть навыками их реализации	<b>Неудовлетворительно</b> не знает требований безопасности открытых информационных систем, не умеет разрабатывать политики информационной безопасности открытых информационных систем, не владеет навыками их реализации <b>Удовлетворительно</b> частично сформированные знания требований безопасности открытых информационных систем, частично сформированные умения разрабатывать политики информационной безопасности открытых информационных систем, частично сформированные навыки реализации политики информационной безопасности открытых информационных систем <b>Хорошо</b> сформированные, но содержащие пробелы знания требований безопасности открытых информационных систем, сформированные,

		<p><b>Хорошо</b> но содержащие пробелы умения разрабатывать политики информационной безопасности открытых информационных систем, сформированные, но содержащие пробелы навыки реализации политики информационной безопасности открытых информационных систем</p> <p><b>Отлично</b> сформированные знания требований безопасности открытых информационных систем, сформированные умения разрабатывать политики информационной безопасности открытых информационных систем, сформированные навыки реализации политики информационной безопасности открытых информационных систем</p>
--	--	--

#### **ОПСК.1**

**Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<p><b>ОПСК.1.2</b> Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации</p>	<p>знать требования к информационной безопасности открытой информационной системы, владеть навыками проведения контроля обеспечения информационной безопасности открытой информационной системы</p>	<p><b>Неудовлетворительно</b> не знает требований к информационной безопасности открытой информационной системы, не владеет навыками проведения контроля обеспечения информационной безопасности открытой информационной системы</p> <p><b>Удовлетворительно</b> частично сформированные знания требований к информационной безопасности открытой информационной системы, частично сформированные навыки проведения контроля обеспечения информационной безопасности открытой информационной системы</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания требований к информационной безопасности открытой информационной системы, сформированные, но содержащие пробелы навыки проведения контроля обеспечения информационной безопасности открытой информационной системы</p> <p><b>Отлично</b></p>

		<p><b>Отлично</b></p> <p>сформированные знания требований к информационной безопасности открытой информационной системы, сформированные навыки проведения контроля обеспечения информационной безопасности открытой информационной системы</p>
--	--	--

### ПК.1

**Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.1.3</b></p> <p>Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем</p>	<p>знать правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности ОИС, уметь формировать и эффективно применять комплекс мер для обеспечения информационной безопасности ОИС</p>	<p><b>Неудовлетворительно</b></p> <p>не знает правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности ОИС, не умеет формировать и эффективно применять комплекс мер для обеспечения информационной безопасности ОИС</p> <p><b>Удовлетворительно</b></p> <p>частично сформированные знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности ОИС, частично сформированные умения формировать и эффективно применять комплекс мер для обеспечения информационной безопасности ОИС</p> <p><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности ОИС, сформированные, но содержащие пробелы умения формировать и эффективно применять комплекс мер для обеспечения информационной безопасности ОИС</p> <p><b>Отлично</b></p> <p>сформированные знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности ОИС, сформированные умения формировать</p>

		<p><b>Отлично</b></p> <p>и эффективно применять комплекс мер для обеспечения информационной безопасности ОИС</p>
<p><b>ПК.1.1</b></p> <p>Проводит моделирование безопасности информационных систем</p>	<p>Знать особенности построения автоматизированных систем, уметь строить модели автоматизированных систем, владеть навыками разработки моделей автоматизированных систем</p>	<p><b>Неудовлетворительно</b></p> <p>отсутствие знания особенностей построения автоматизированных систем, отсутствие умения строить модели автоматизированных систем, отсутствие навыка разработки моделей автоматизированных систем</p> <p><b>Удовлетворительно</b></p> <p>частично сформированные знания особенностей построения автоматизированных систем, частично сформированные умения строить модели автоматизированных систем, частично сформированные навыки разработки моделей автоматизированных систем</p> <p><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы знания особенностей построения автоматизированных систем, сформированные, но содержащие пробелы умения строить модели автоматизированных систем, сформированные, но содержащие пробелы навыки разработки моделей автоматизированных систем</p> <p><b>Отлично</b></p> <p>сформированные знания особенностей построения автоматизированных систем, сформированные умения строить модели автоматизированных систем, сформированные навыки разработки моделей автоматизированных систем</p>

### ПК.3

#### Способен управлять функционированием и защищенностью автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.3.1</b></p> <p>Контролирует соответствие параметров подсистем защиты автоматизированной системы установленным требованиям</p>	<p>знать средства защиты информации и средств контроля защищенности автоматизированной системы, уметь проектировать средства защиты информации и средства контроля защищенности автоматизированной системы, владеть навыками настройки и</p>	<p><b>Неудовлетворительно</b></p> <p>не знает средства защиты информации и средств контроля защищенности автоматизированной системы, не умеет проектировать средства защиты информации и средства контроля защищенности автоматизированной системы, не владеет навыками настройки и оптимизации действующих средств защиты информации</p>

	оптимизации действующих средств защиты информации	<p><b>Удовлетворительно</b> частично сформированные знания средств защиты информации и средств контроля защищенности автоматизированной системы, частично сформированные умения проектировать средства защиты информации и средства контроля защищенности автоматизированной системы, частично сформированные навыки настройки и оптимизации действующих средств защиты информации</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания средств защиты информации и средств контроля защищенности автоматизированной системы, сформированные, но содержащие пробелы умения проектировать средства защиты информации и средства контроля защищенности автоматизированной системы, сформированные, но содержащие пробелы навыки настройки и оптимизации действующих средств защиты информации</p> <p><b>Отлично</b> сформированные знания средств защиты информации и средств контроля защищенности автоматизированной системы, сформированные умения проектировать средства защиты информации и средства контроля защищенности автоматизированной системы, сформированные навыки настройки и оптимизации действующих средств защиты информации</p>
<p><b>ПК.3.3</b> Проводит мероприятия по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p>	<p>владеть навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p>	<p><b>Неудовлетворительно</b> не владеет навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p> <p><b>Удовлетворительно</b> частично сформированные навыки контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы навыки контроля защищенности автоматизированной системы с помощью</p>



		<p><b>Хорошо</b> технических, программно-аппаратных и криптографических средств</p> <p><b>Отлично</b> сформированные навыки контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p>
<p><b>ПК.3.2</b> Устанавливает и настраивает программное обеспечение, необходимое для защиты автоматизированной системы от НСД</p>	<p>знать требования предъявляемые к информационной безопасности предприятия, уметь устанавливать, настраивать и обслуживать средства информационной безопасности предприятия, владеть навыками совершенствования существующих систем информационной безопасности предприятия</p>	<p><b>Неудовлетворительно</b> не знает требования предъявляемые к информационной безопасности предприятия, не умеет устанавливать, настраивать и обслуживать средства информационной безопасности предприятия, не владеет навыками совершенствования существующих систем информационной безопасности предприятия</p> <p><b>Удовлетворительно</b> частично сформированные знания требований предъявляемых к информационной безопасности предприятия, частично сформированные умения устанавливать, настраивать и обслуживать средства информационной безопасности предприятия, частично сформированные навыки совершенствования существующих систем информационной безопасности предприятия</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания требований предъявляемых к информационной безопасности предприятия, сформированные, но содержащие пробелы умения устанавливать, настраивать и обслуживать средства информационной безопасности предприятия, сформированные, но содержащие пробелы навыки совершенствования существующих систем информационной безопасности предприятия</p> <p><b>Отлично</b> сформированные знания требований предъявляемых к информационной безопасности предприятия, сформированные умения устанавливать, настраивать и обслуживать средства информационной безопасности предприятия, сформированные навыки совершенствования существующих систем информационной безопасности предприятия</p>

		<b>Отлично</b> систем информационной безопасности предприятия
--	--	---

### УК.3

**Способен осуществлять коммуникации в рамках академического и профессионального взаимодействия на русском и иностранном языках**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<b>УК.3.1</b> Осуществляет коммуникацию, грамотно и аргументированно строит устную и письменную речь на русском и иностранном языках	знать грамматику одного из иностранных языков, уметь поддерживать диалог на иностранном языке, владеть навыками представления информации на иностранном языке	<p><b>Неудовлетворительно</b> не знает грамматику одного из иностранных языков, не умеет поддерживать диалог на иностранном языке, не владеет навыками технического перевода</p> <p><b>Удовлетворительно</b> частично сформированные знания грамматики одного из иностранных языков, частично сформированные умения поддерживать диалог на иностранном языке, частично сформированные навыки технического перевода</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания грамматики одного из иностранных языков, сформированные, но содержащие пробелы умения поддерживать диалог на иностранном языке, сформированные, но содержащие пробелы навыки технического перевода</p> <p><b>Отлично</b> сформированные знания грамматики одного из иностранных языков, сформированные умения поддерживать диалог на иностранном языке, сформированные навыки технического перевода</p>
<b>УК.3.3</b> Представляет результаты деятельности на публичных мероприятиях в устной и письменной формах	знать основные требования к подготовке презентации на публичных мероприятиях, уметь пользоваться презентационной техникой, владеть навыками использования приложений для подготовки презентаций	<p><b>Неудовлетворительно</b> не знает основные требования к подготовке презентации на публичных мероприятиях, не умеет пользоваться презентационной техникой, не владеет навыками использования приложений для подготовки презентаций</p> <p><b>Удовлетворительно</b> частично сформированные знания основных требований к подготовке презентации на публичных мероприятиях, частично сформированные умения пользоваться</p>

		<p><b>Удовлетворительно</b> презентационной техникой, частично сформированные навыки использования приложений для подготовки презентаций</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания основных требований к подготовке презентации на публичных мероприятиях, сформированные, но содержащие пробелы умения пользоваться презентационной техникой, сформированные, но содержащие пробелы навыки использования приложений для подготовки презентаций</p> <p><b>Отлично</b> сформированные знания основных требований к подготовке презентации на публичных мероприятиях, сформированные умения пользоваться презентационной техникой, сформированные навыки использования приложений для подготовки презентаций</p>
<p><b>УК.3.4</b> Устанавливает и поддерживает контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий</p>	<p>Знать современные коммуникативные технологии, умеет устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, владеет навыками делового общения</p>	<p><b>Неудовлетворительно</b> не знает современные коммуникативные технологии, не умеет устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, не владеет навыками делового общения</p> <p><b>Удовлетворительно</b> частично сформированные знания современных коммуникативных технологий, частично сформированные умения устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, частично сформированные навыки делового общения</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания современных коммуникативных технологий, сформированные, но содержащие пробелы умения устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий,</p>

		<p><b>Хорошо</b> сформированные, но содержащие пробелы навыки делового общения</p> <p><b>Отлично</b> сформированные знания современных коммуникативных технологий, сформированные умения устанавливать и поддерживать контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий, сформированные навыки делового общения</p>
--	--	--

### УК.1

**Способен осуществлять анализ проблемных ситуаций и вырабатывать решение на основе системного подхода**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>УК.1.2</b> Работает с противоречивой информацией из разных источников, находит пробелы в необходимой для разрешения проблемы информации, определяет варианты устранения пробелов</p>	<p>Знать инструменты для поиска информации, уметь находить пробелы в необходимой для разрешения проблемы информации</p>	<p><b>Неудовлетворительно</b> не знает инструментов для поиска информации, не умеет находить пробелы в необходимой для разрешения проблемы информации</p> <p><b>Удовлетворительно</b> частично сформированные знания инструментов для поиска информации, частично сформированные умения находить пробелы в необходимой для разрешения проблемы информации</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания инструментов для поиска информации, сформированные, но содержащие пробелы умения находить пробелы в необходимой для разрешения проблемы информации</p> <p><b>Отлично</b> сформированные знания инструментов для поиска информации, сформированные умения находить пробелы в необходимой для разрешения проблемы информации</p>

### УК.5

**Способен управлять своими ресурсами, определять приоритеты собственной деятельности, выстраивать и реализовывать траекторию саморазвития**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
----------------------------	------------------------------------	---

<p><b>УК.5.3</b> Осуществляет выбор направленности профессиональной деятельности в зависимости от собственных интересов, ресурсов и накопленного опыта</p>	<p>уметь выбирать направленности профессиональной деятельности в зависимости от собственных интересов, ресурсов и накопленного опыта</p>	<p><b>Неудовлетворительно</b> не умеет выбирать направленности профессиональной деятельности в зависимости от собственных интересов, ресурсов и накопленного опыта</p> <p><b>Удовлетворительно</b> частично сформированные умения выбирать направленности профессиональной деятельности в зависимости от собственных интересов, ресурсов и накопленного опыта</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы умения выбирать направленности профессиональной деятельности в зависимости от собственных интересов, ресурсов и накопленного опыта</p> <p><b>Отлично</b> сформированные умения выбирать направленности профессиональной деятельности в зависимости от собственных интересов, ресурсов и накопленного опыта</p>
--	--	---

## УК.9

**Способен использовать базовые дефектологические знания в социальной и профессиональной сферах**

<b>Компетенция (индикатор)</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
<p><b>УК.9.3</b> Выстраивает профессиональное взаимодействие с лицами, имеющими психофизиологические особенности, с учетом нозологии</p>	<p>Уметь работать с лицами, имеющими психофизиологические особенности, с учетом нозологии</p>	<p><b>Неудовлетворительно</b> не умеет работать с лицами, имеющими психофизиологические особенности, с учетом нозологии</p> <p><b>Удовлетворительно</b> Частично сформированное умение работать с лицами, имеющими психофизиологические особенности, с учетом нозологии</p> <p><b>Хорошо</b> Сформированное, но содержащие пробелы умение работать с лицами, имеющими психофизиологические особенности, с учетом нозологии</p> <p><b>Отлично</b> Сформированное умение работать с лицами, имеющими психофизиологические особенности, с учетом нозологии</p>

## УК.11

**Способен формировать нетерпимое отношение к коррупционному поведению**

<b>УК.11.3</b> <b>Компетенция</b> Осуществляет взаимодействие на <b>(индикатор)</b>	<b>Планируемые результаты</b> <b>обучения</b> Знает способы противодействия различным проявлениям коррупционного поведения.	<b>Критерии оценивания результатов</b> <b>обучения</b> <b>Неудовлетворительно</b> Не знает способы противодействия различным проявлениям коррупционного поведения. Не знает признаки проявления коррупционного поведения. Не демонстрирует умение противодействовать различным проявлениям коррупционного поведения.
основе нетерпимого отношения к коррупционному поведению в социальной и профессиональной сферах	Знает признаки проявления коррупционного поведения. Демонстрирует умение противодействовать различным проявлениям коррупционного поведения.	<b>Удовлетворительно</b> Частично знает способы противодействия различным проявлениям коррупционного поведения. Частично знает признаки проявления коррупционного поведения. Частично демонстрирует умение противодействовать различным проявлениям коррупционного поведения. <b>Хорошо</b> Знает способы противодействия различным проявлениям коррупционного поведения. Знает признаки проявления коррупционного поведения. Не всегда демонстрирует умение противодействовать различным проявлениям коррупционного поведения. <b>Отлично</b> Знает способы противодействия различным проявлениям коррупционного поведения. Знает признаки проявления коррупционного поведения. Демонстрирует умение противодействовать различным проявлениям коррупционного поведения.

## УК.2

### Способен управлять проектом, организовывать и руководить работой команды

<b>Компетенция</b> <b>(индикатор)</b>	<b>Планируемые результаты</b> <b>обучения</b>	<b>Критерии оценивания результатов</b> <b>обучения</b>
<b>УК.2.3</b> Разрабатывает мероприятия по реализации проекта на разных этапах его жизненного цикла, вносит корректировки в ходе реализации проекта	знать жизненный цикл реализации проектов, уметь разрабатывать мероприятия по реализации проектов	<b>Неудовлетворительно</b> не знает жизненных циклов реализации проектов, не умеет разрабатывать мероприятия по реализации проектов <b>Удовлетворительно</b> частично сформированные знания жизненных циклов реализации проектов, частично сформированные умения разрабатывать мероприятия по реализации проектов <b>Хорошо</b> сформированные, но содержащие пробелы знания жизненных циклов реализации

		<p><b>Хорошо</b> проектов, сформированные, но содержащие пробелы умения разрабатывать мероприятия по реализации проектов</p> <p><b>Отлично</b> сформированные знания жизненных циклов реализации проектов, сформированные умения разрабатывать мероприятия по реализации проектов</p>
--	--	---

### Оценочные средства

**Вид мероприятия промежуточной аттестации :** Экзамен

**Способ проведения мероприятия промежуточной аттестации :** Защищаемое контрольное мероприятие

**Продолжительность проведения мероприятия промежуточной аттестации :**  
время отводимое на доклад 1

### Показатели оценивания

Оценивается работа студента, не выполнившего программу практики, или представившего отчет о практике, выполненный на крайне низком уровне, не предоставивший документы по практике.	<b>Неудовлетворительно</b>
Оценивается работа студента, который выполнил программу практики, но при этом не проявил самостоятельности, допустил небрежность в формулировании выводов в отчете практики, не показал интереса к выполнению заданий практики, небрежно оформил документы практики, несвоевременно представил необходимые документы.	<b>Удовлетворительно</b>
Оценивается работа студента, который полностью выполнил программу практики, проявил самостоятельность, интерес к профессиональной деятельности, однако, при оформлении документов практики допустил недочеты и(или) его защита вызвала нарекания со стороны комиссии.	<b>Хорошо</b>
Оценивается работа студента, выполнившего весь объем работы, определенной программой практики, проявившего теоретическую подготовку и умелое применение полученных знаний в ходе практики, оформившего документы практики, отчет в соответствии со всеми требованиями и защитивший его.	<b>Отлично</b>